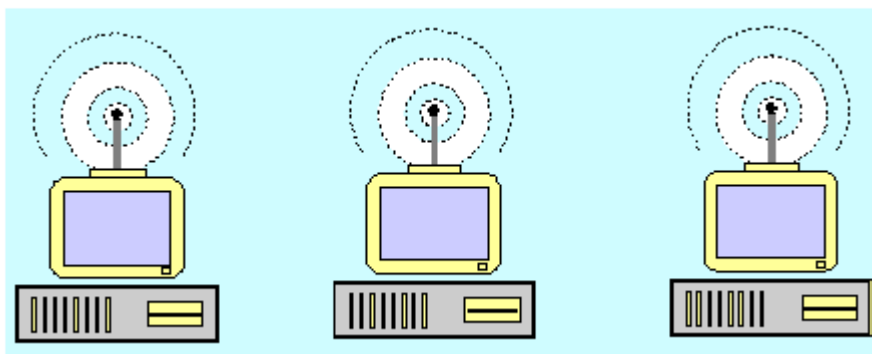


ПРИЛОЖЕНИЕ Г (информационное)

Стандарт IEEE 802.11a, b, g, n.

Беспроводные сети передачи данных Wi-Fi.



Повсеместное распространение беспроводных сетей в последние годы побуждает разработчиков задумываться о новых стандартах связи, предусматривающих всё более высокие скорости соединения. Так, если первоначально беспроводные устройства поддерживали скорость соединения только 1 и 2 Мбит/с, чего было явно недостаточно, то сейчас максимальная скорость соединения составляет уже 54 Мбит/с, и это уже может составить конкуренцию традиционным кабельным сетям. Существуют различные типы беспроводных сетей, отличающиеся друг от друга и радиусом действия, и поддерживаемыми скоростями соединения, и технологией кодирования данных. Наибольшее распространение получили беспроводные сети стандарта IEEE 802.11a/b/g, на очереди IEEE 802.11n.

Оглавление

[Что такое Wi-Fi?](#)

[Развитие технологии беспроводных сетей: стандарт IEEE 802.11](#)

[Стандарт IEEE 802.11b](#)

[Стандарт IEEE 802.11a](#)

[Стандарт IEEE 802.11g](#)

[Стандарт IEEE 802.11n](#)

[Спецификации IEEE 802.11](#)

[Опасны ли для здоровья человека беспроводные сети?](#)

[Список предметных сокращений](#)

[Список использованных источников](#)

Что такое Wi-Fi?

Что такое беспроводная локальная сеть (WLAN)?

Сеть WLAN - вид локальной вычислительной сети (LAN), использующий для связи и передачи данных между узлами высокочастотные радиоволны, а не кабельные соединения. Это гибкая система передачи данных, которая применяется как расширение - или альтернатива - кабельной локальной сети внутри одного здания или в пределах определенной территории.

Каковы преимущества использования WLAN вместо проводной локальной сети?

Повышение производительности. Сеть WLAN обеспечивает не привязанную к отдельным помещениям сеть и доступ в Интернет. Сеть WLAN дает пользователям возможность перемещаться по территории предприятия или организации, оставаясь подключенными к сети.

Простое и быстрое построение локальной сети. Не нужно тянуть и укреплять кабели.

Гибкость установки. Беспроводную сеть можно построить там, где нельзя протянуть кабели;

технология WLAN облегчает временную установку сети и ее перемещение.

Снижение стоимости эксплуатации. Беспроводные сети снижают стоимость установки, поскольку не требуются кабельные соединения. В результате достигается экономия, тем более значительная, чем чаще меняется окружение.

Масштабируемость. Расширение и реконфигурация сети для WLAN не является сложной задачей: пользовательские устройства можно интегрировать в сеть, установив на них беспроводные сетевые адаптеры.

Совместимость. Различные марки совместимых клиентских и сетевых устройств будут взаимодействовать между собой.

Трудна ли установка и администрирование сети WLAN?

Нет. Беспроводную локальную сеть строить проще, чем кабельную, администрирование же обоих типов сетей почти не отличается друг от друга. Клиентское решение сети WLAN построено на принципе Plug-and-Play, который предполагает, что компьютеры просто подключаются к одноранговой сети (peer-to-peer).

Какова дальность связи устройств WLAN?

Дальность действия радиочастот, особенно в помещениях, зависит от характеристик изделия (в том числе от мощности передатчика), конструкции приемника, помехозащищенности и пути прохождения сигнала. Взаимодействие радиоволн с обычными объектами здания, например со стенами, металлическими конструкциями и даже людьми, может повлиять на дальность распространения сигнала, и таким образом, изменить зону действия конкретной системы. Беспроводные сети используют радиочастоты, поскольку радиоволны внутри помещения проникают через стены и перекрытия. Область охвата систем WLAN с простейшими антеннами достигает 300м, имея антенны с большим усилением – до 7 км в зависимости от количества и вида препятствий. С помощью дополнительных точек доступа можно расширить зону действия, и тем самым обеспечить свободу передвижения.

Надежны ли сети WLAN?

Да, сети WLAN исключительно надежны. Поскольку беспроводная технология уходит корнями в оборонную промышленность, обеспечение безопасности беспроводных устройств предусматривалось с самого начала. Вот почему беспроводные сети обычно более надежны, чем кабельные. В сетях WLAN используется технология Direct Sequence Spread Spectrum (DSSS), которая отличается высокой устойчивостью к искажению данных, помехам, в том числе преднамеренным, и обнаружению. Кроме того, все пользователи беспроводной сети проходят аутентификацию по системному идентификатору, что предотвращает несанкционированный доступ к данным.

Для передачи особо уязвимых данных пользователи могут использовать режим Wired Equivalent Privacy (WEP), при котором сигнал шифруется дополнительным алгоритмом, а данные контролируются с помощью электронного ключа. Вообще говоря, в отдельных узлах перед включением в сетевой трафик должны приниматься свои меры безопасности. В сетях WLAN, работающих по спецификации 802.11b, для обеспечения более высокой надежности сети вместе с аутентификацией пользователя могут применяться 40-битные и 128-битные алгоритмы шифрования. Перехват трафика, как умышленный, так и неумышленный, практически невозможен.

Что такое точка доступа?

Точка доступа соединяет кабельную и беспроводную сеть и позволяет клиентам последней получить доступ к ресурсам кабельной сети. Каждая точка доступа расширяет общую вычислительную мощность системы. Пользователи могут перемещаться между точками доступа, не теряя соединения с сетью, - как и при подключении к сети с помощью сотового телефона. Другими словами, точка доступа - это программно-аппаратное устройство, которое выполняет роль концентратора для клиента беспроводной сети и обеспечивает подключение к кабельной сети.

Сколько пользователей может поддерживать одна система WLAN?

Количество пользователей практически неограниченно. Его можно увеличивать, просто устанавливая новые точки доступа. С помощью перекрывающихся точек доступа, настроенных на разные частоты (каналы), беспроводную сеть можно расширить за счет увеличения числа пользователей в одной зоне. Перекрывающихся каналов, которые не будут создавать взаимные помехи, одновременно может быть установлено не более трех; эти каналы втрое увеличат количество пользователей сети. Подобным образом можно расширять беспроводную сеть, устанавливая точки доступа в различных частях здания. Это увеличивает общее число пользователей и дает им возможность перемещаться по зданию или территории организации.

Сколько пользователей одновременно поддерживает одна точка доступа?

Количество пользователей в этом случае зависит, в первую очередь, от загруженности трафика. В сети WLAN полоса пропускания делится между пользователями так же, как в кабельной сети. Исходя из числа пользователей производительность сети зависит также от рода выполняемых пользователями задач.

Развитие технологии беспроводных сетей: стандарт IEEE 802.11

Комитет по стандартам IEEE 802 сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11 в 1990 году. Эта группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2,4 ГГц, со скоростями доступа 1 и 2 Mbps (Megabits-per-second). Работы по созданию стандарта были завершены через 7 лет, и в июне 1997 года была ратифицирована первая спецификация 802.11. Стандарт IEEE 802.11 являлся первым стандартом для продуктов WLAN от независимой международной организации, разрабатывающей большинство стандартов для проводных сетей. Однако к тому времени заложенная первоначально скорость передачи данных в беспроводной сети уже не удовлетворяла потребностям пользователей. Для того, чтобы сделать технологию Wireless LAN популярной, дешёвой, а главное, удовлетворяющей современным жёстким требованиям бизнес-приложений, разработчики были вынуждены создать новый стандарт.

В сентябре 1999 года IEEE ратифицировал расширение предыдущего стандарта. Названное IEEE 802.11b (также известное, как 802.11 High rate), оно определяет стандарт для продуктов беспроводных сетей, которые работают на скорости 11 Mbps (подобно Ethernet), что позволяет успешно применять эти устройства в крупных организациях. Совместимость продуктов различных производителей гарантируется независимой организацией, которая называется Wireless Ethernet Compatibility Alliance (WECA). Эта организация была создана лидерами индустрии беспроводной связи в 1999 году. В настоящее время членами WECA являются более 80 компаний, в том числе такие известные производители, как [Cisco](#) , [Lucent](#) , [3Com](#) , [IBM](#) , [Intel](#), [Apple](#), [Compaq](#), [Dell](#), [Fujitsu](#), [Siemens](#), [Sony](#), [AMD](#) и пр. С продуктами, удовлетворяющими требованиям Wi-Fi (термин WECA для IEEE 802.11b), можно ознакомиться на сайте [WECA](#) .

Потребность в беспроводном доступе к локальным сетям растёт по мере увеличения числа мобильных устройств, таких как ноутбуки и PDA, а также с ростом желания пользователей быть подключенными к сети без необходимости "втыкать" сетевой провод в свой компьютер. По прогнозам, к 2003 году в мире будет насчитываться более миллиарда мобильных устройств, а стоимость рынка продукции WLAN к 2002 году прогнозируется более чем в 2 миллиарда долларов.

Стандарт IEEE 802.11 и его расширение 802.11a/b/g

Как и все стандарты IEEE 802, 802.11 работает на нижних двух уровнях модели ISO/OSI, физическом уровне и канальном уровне (рис. 1). Любое сетевое приложение, сетевая операционная система, или протокол (например, TCP/IP), будут так же хорошо работать в сети 802.11, как и в сети Ethernet.

Основная архитектура, особенности и службы 802.11a/b/g определяются в первоначальном стандарте 802.11. Спецификация 802.11a/b/g затрагивает только физический уровень, добавляя лишь более высокие скорости доступа.

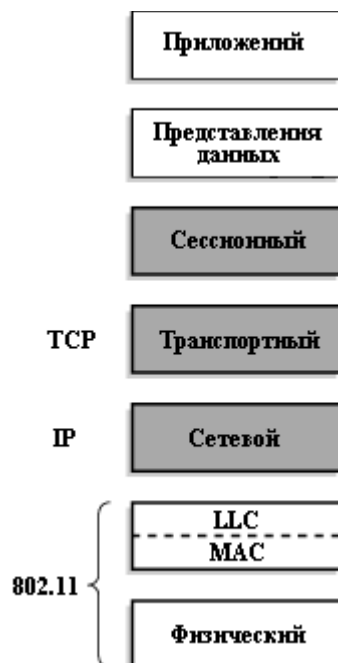


Рис. 1. Уровни модели ISO/OSI и их соответствие стандарту 802.11.

Режимы работы 802.11

802.11 определяет два типа оборудования – клиент, который обычно представляет собой компьютер, укомплектованный беспроводной сетевой интерфейсной картой (Network Interface Card, NIC), и точку доступа (Access point, AP), которая выполняет роль моста между беспроводной и проводной сетями. Точка доступа обычно содержит в себе приёмопередатчик, интерфейс проводной сети (802.3), а также программное обеспечение, занимающееся обработкой данных. В качестве беспроводной станции может выступать ISA, PCI, PC Card или ARD2,4 (ARD5) в стандарте 802.11, либо встроенные решения, например, телефонная гарнитура 802.11.

Стандарт IEEE 802.11 определяет два режима работы сети – режим "Ad-hoc" и клиент/сервер (или режим инфраструктуры – infrastructure mode).

Физический уровень 802.11

На физическом уровне определены два широкополосных радиочастотных метода передачи и один – в инфракрасном диапазоне. Радиочастотные методы работают в ISM-диапазоне 2,4 ГГц и обычно используют полосу 83 МГц от 2,400 ГГц до 2,483 ГГц. Технологии широкополосного сигнала, используемые в радиочастотных методах, увеличивают надёжность, пропускную способность, позволяют многим несвязанным друг с другом устройствам разделять одну полосу частот с минимальными помехами друг для друга.

Стандарт 802.11 использует метод прямой последовательности (Direct Sequence Spread Spectrum, DSSS) и метод частотных скачков (Frequency Hopping Spread Spectrum, FHSS). Эти методы кардинально отличаются, и несовместимы друг с другом.

Метод передачи в инфракрасном диапазоне (IR)

Реализация этого метода в стандарте 802.11 основана на излучении ИК передатчиком ненаправленного (diffuse IR) сигнала. Вместо направленной передачи, требующей соответствующей ориентации излучателя и приёмника, передаваемый ИК сигнал излучается в потолок. Затем происходит отражение сигнала и его приём. Такой метод имеет очевидные преимущества по сравнению с использованием направленных излучателей, однако есть и существенные недостатки – требуется потолок, отражающий ИК излучение в заданном диапазоне длин волн (850 – 950 нм); радиус действия всей системы ограничен 10 метрами. Кроме того, ИК лучи чувствительны к погодным условиям, поэтому метод рекомендуется применять только внутри помещений.

Поддерживаются две скорости передачи данных – 1 и 2 Mbps. На скорости 1 Mbps поток

данных разбивается на квартеты, каждый из которых затем во время модуляции кодируется в один из 16-ти импульсов. На скорости 2 Mbps метод модуляции немного отличается – поток данных делится на битовые пары, каждая из которых модулируется в один из четырёх импульсов. Пиковая мощность передаваемого сигнала составляет 2 Вт.

Канальный (Data Link) уровень 802.11

Канальный уровень 802.11 состоит из двух подуровней: управления логической связью (Logical Link Control, LLC) и управления доступом к носителю (Media Access Control, MAC). 802.11 использует тот же LLC и 48-битовую адресацию, что и другие сети 802, что позволяет легко объединять беспроводные и проводные сети, однако MAC уровень имеет кардинальные отличия.

MAC уровень 802.11 очень похож на реализованный в 802.3, где он поддерживает множество пользователей на общем носителе, когда пользователь проверяет носитель перед доступом к нему. Для Ethernet сетей 802.3 используется протокол Carrier Sense Multiple Access with Collision Detection (CSMA/CD), который определяет, как станции Ethernet получают доступ к проводной линии, и как они обнаруживают и обрабатывают столкновения, возникающие в том случае, если несколько устройств пытаются одновременно установить связь по сети. Чтобы обнаружить столкновения, станция должна обладать способностью и принимать, и передавать одновременно. Стандарт 802.11 предусматривает использование полудуплексных приёмопередатчиков, поэтому в беспроводных сетях 802.11 станция не может обнаружить столкновения во время передачи.

Чтобы учесть это отличие, 802.11 использует модифицированный протокол, известный как Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), или Distributed Coordination Function (DCF). CSMA/CA пытается избежать столкновений путём использования явного подтверждения пакета (ACK), что означает, что принимающая станция посылает ACK пакет для подтверждения того, что пакет получен неповреждённым.

CSMA/CA работает следующим образом. Станция, желающая передавать, тестирует канал, и если не обнаружено активности, станция ожидает в течение некоторого случайного промежутка времени, а затем передаёт, если среда передачи данных всё ещё свободна. Если пакет приходит целым, принимающая станция посылает пакет ACK, по приёме которого отправителем завершается процесс передачи. Если передающая станция не получила пакет ACK, в силу того, что не был получен пакет данных, или пришёл повреждённый ACK, делается предположение, что произошло столкновение, и пакет данных передаётся снова через случайный промежуток времени.

Для определения того, является ли канал свободным, используется алгоритм оценки чистоты канала (Channel Clearance Algorithm, CCA). Его суть заключается в измерении энергии сигнала на антенне и определения мощности принятого сигнала (RSSI). Если мощность принятого сигнала ниже определённого порога, то канал объявляется свободным, и MAC уровень получает статус CTS. Если мощность выше порогового значения, передача данных задерживается в соответствии с правилами протокола. Стандарт предоставляет ещё одну возможность определения занятости канала, которая может использоваться либо отдельно, либо вместе с измерением RSSI – метод проверки несущей. Этот метод является более выборочным, так как с его помощью производится проверка на тот же тип несущей, что и по спецификации 802.11. Наилучший метод для использования зависит от того, каков уровень помех в рабочей области.

Таким образом, CSMA/CA предоставляет способ разделения доступа по радиоканалу. Механизм явного подтверждения эффективно решает проблемы помех. Однако он добавляет некоторые дополнительные накладные расходы, которых нет в 802.3, поэтому сети 802.11 будут всегда работать медленнее, чем эквивалентные им Ethernet локальные сети.

Другая специфичная проблема MAC-уровня – это проблема "скрытой точки", когда две станции могут обе "слышать" точку доступа, но не могут "слышать" друг друга, в силу большого расстояния или преград (рис. 2). Для решения этой проблемы в 802.11 на MAC уровне добавлен необязательный протокол Request to Send/Clear to Send (RTS/CTS). Когда используется этот протокол, посылающая станция передаёт RTS и ждёт ответа точки доступа с CTS. Так как все станции в сети могут "слышать" точку доступа, сигнал CTS заставляет их отложить свои

передачи, что позволяет передающей станции передать данные и получить АСК пакет без возможности столкновений. Так как RTS/CTS добавляет дополнительные накладные расходы на сеть, временно резервируя носитель, он обычно используется только для пакетов очень большого объёма, для которых повторная передача была бы слишком дорогостоящей.

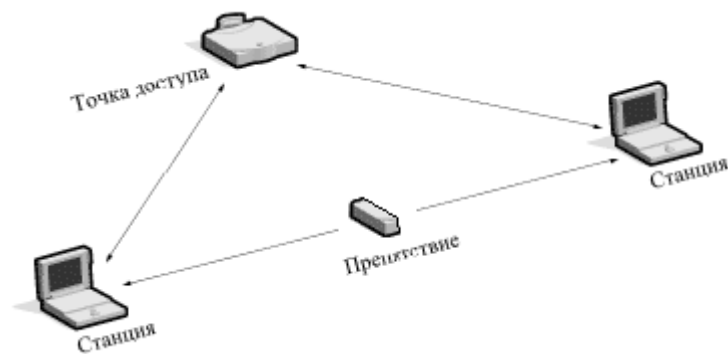


Рис. 2. Иллюстрация проблемы "скрытой точки".

Наконец, MAC уровень 802.11 предоставляет возможность расчёта CRC и фрагментации пакетов. Каждый пакет имеет свою контрольную сумму CRC, которая рассчитывается и прикрепляется к пакету. Здесь наблюдается отличие от сетей Ethernet, в которых обработкой ошибок занимаются протоколы более высокого уровня (например, TCP). Фрагментация пакетов позволяет разбивать большие пакеты на более маленькие при передаче по радиоканалу, что полезно в очень "заселённых" средах или в тех случаях, когда существуют значительные помехи, так как у меньших пакетов меньше шансов быть повреждёнными. Этот метод в большинстве случаев уменьшает необходимость повторной передачи и, таким образом, увеличивает производительность всей беспроводной сети. MAC уровень ответственен за сборку полученных фрагментов, делая этот процесс "прозрачным" для протоколов более высокого уровня.

Подключение к сети

MAC уровень 802.11 несёт ответственность за то, каким образом клиент подключается к точке доступа. Когда клиент 802.11 попадает в зону действия одной или нескольких точек доступа, он на основе мощности сигнала и наблюдаемого значения количества ошибок выбирает одну из них и подключается к ней. Как только клиент получает подтверждение того, что он принят точкой доступа, он настраивается на радиоканал, в котором она работает. Время от времени он проверяет все каналы 802.11, чтобы посмотреть, не предоставляет ли другая точка доступа службы более высокого качества. Если такая точка доступа находится, то станция подключается к ней, перенастраиваясь на её частоту (рис. 3).

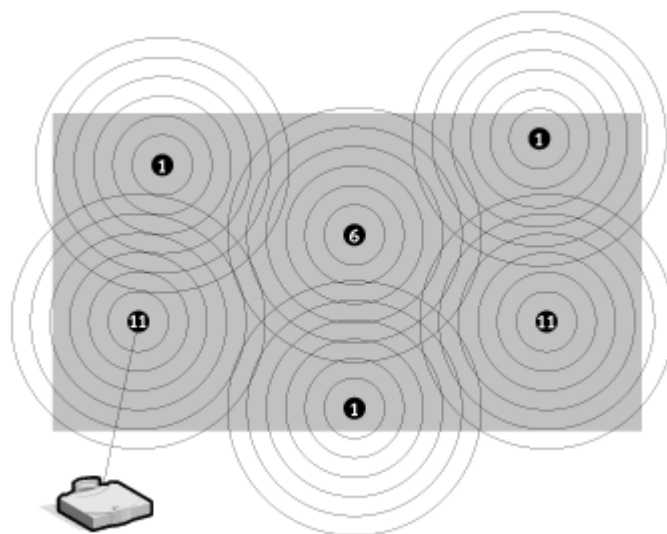


Рис. 3. Подключение к сети и иллюстрация правильного назначения каналов для точек доступа.

Переподключение обычно происходит в том случае, если станция была

физически перемещена вдаль от точки доступа, что вызвало ослабление сигнала. В других случаях повторное подключение происходит из-за изменения радиочастотных характеристик здания, или просто из-за большого сетевого трафика через первоначальную точку доступа. В последнем случае эта функция протокола известна как "балансировка нагрузки", так как её главное назначение – распределение общей нагрузки на беспроводную сеть наиболее эффективно по всей доступной инфраструктуре сети.

Процесс динамического подключения и переподключения позволяет сетевым администраторам устанавливать беспроводные сети с очень широким покрытием, создавая частично перекрывающиеся "соты". Идеальным вариантом является такой, при котором соседние перекрывающиеся точки доступа будут использовать разные DSSS каналы, чтобы не создавать помех в работе друг другу (Рис. 3).

Поддержка потоковых данных

Потоковые данные, такие как видео или голос, поддерживаются в спецификации 802.11 на MAC уровне посредством Point Coordination Function (PCF). В противоположность Distributed Coordination Function (DCF), где управление распределено между всеми станциями, в режиме PCF только точка доступа управляет доступом к каналу. В том случае, если установлен BSS с включенной PCF, время равномерно распределяется промежутками для работы в режиме PCF и в режиме CSMA/CA. Во время периодов, когда система находится в режиме PCF, точка доступа опрашивает все станции на предмет получения данных. На каждую станцию выделяется фиксированный промежуток времени, по истечении которого производится опрос следующей станции. Ни одна из станций не может передавать в это время, за исключением той, которая опрашивается. Так как PCF даёт возможность каждой станции передавать в определённое время, то гарантируется минимальное время ожидания. Недостатком такой схемы является то, что точка доступа должна производить опрос всех станций, что становится чрезвычайно неэффективным в больших сетях.

Управление питанием

Дополнительно по отношению к управлению доступом к носителю, MAC уровень 802.11 поддерживает энергосберегающие режимы для продления срока службы батарей мобильных устройств. Стандарт поддерживает два режима потребления энергии, называемые "режим продолжительной работы" и "сберегающий режим". В первом случае радио всегда находится во включенном состоянии, в то время как во втором случае радио периодически включается через определённые промежутки времени для приёма "маячковых" сигналов, которые постоянно посылает точка доступа. Эти сигналы включают в себя информацию относительно того, какая станция должна принять данные. Таким образом, клиент может принять маячковый сигнал, принять данные, а затем вновь перейти в "спящий" режим.

Безопасность

802.11b обеспечивает контроль доступа на MAC уровне (второй уровень в модели ISO/OSI), и механизмы шифрования, известные как Wired Equivalent Privacy (WEP), целью которых является обеспечение беспроводной сети средствами безопасности, эквивалентными средствам безопасности проводных сетей. Когда включен WEP, он защищает только пакет данных, но не защищает заголовки физического уровня, так что другие станции в сети могут просматривать данные, необходимые для управления сетью. **Для контроля доступа в каждую точку доступа помещается так называемый ESSID (или WLAN Service Area ID), без знания которого мобильная станция не сможет подключиться к точке доступа.**

Дополнительно **точка доступа может хранить список разрешённых MAC адресов, называемый списком контроля доступа (Access Control List, ACL), разрешая доступ только тем клиентам, чьи MAC адреса находятся в списке.**

Для шифрования данных стандарт предоставляет возможности шифрования с использованием алгоритма RC4 с 40-битным разделяемым ключом. После того, как станция подключается к точке доступа, все передаваемые данные могут быть зашифрованы с использованием этого ключа. Когда используется шифрование, точка доступа будет посылать зашифрованный пакет

любой станции, пытающейся подключиться к ней. Клиент должен использовать свой ключ для шифрования корректного ответа для того, чтобы аутентифицировать себя и получить доступ в сеть. Выше второго уровня сети 802.11b поддерживают те же стандарты для контроля доступа и шифрования (например, IPSec), что и другие сети 802.

Стандарт IEEE 802.11b

Между кабельными сетями Ethernet и беспроводными сетями Radio Ethernet есть много общего, но много и различий. Это и понятно — разные среды передачи данных требуют принципиально различного подхода к способам передачи и кодирования данных, то есть к непосредственной подготовке данных для передачи. Поэтому основные различия между кабельными и беспроводными сетями сконцентрированы на так называемом физическом подуровне (Physical Layer, PHY) и подуровне доступа к среде передачи данных (Medium Access Control, MAC). В соответствии с эталонной моделью сетевых взаимодействий OSI (Open System Interconnection), именно на этих подуровнях данные формируются и кодируются нужным образом для дальнейшей передачи по сети.

Теоретические аспекты функционирования сетей Radio Ethernet регламентированы стандартами IEEE 802.11 и IEEE 802.11b. Именно в этих стандартах определяется порядок организации беспроводных сетей на уровне доступа к среде передачи данных (MAC-уровень) и на физическом уровне (PHY-уровень).

Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости 1 Мбит/с и опционально на скорости 2 Мбит/с. В более поздней версии — IEEE 802.11b, фактически являющейся дополнением к основному стандарту, определяется скорость передачи 1, 2, 5,5 и 11 Мбит/с.

Физический уровень

Начнем с рассмотрения физического уровня. Стандартом IEEE 802.11b предусмотрено использование частотного диапазона **от 2,4 до 2,4835 ГГц, который предназначен для безлицензионного использования в промышленности, науке и медицине.** Разрешение выдается изготовителю и передается заказчику после приобретения продукта в виде сертификата. Здесь следует заметить, что в России использование этого частотного диапазона, кроме сертификатов, требует получения разрешения от Государственного комитета по радиочастотам (ГКРЧ) и Главгоссвязьнадзора РФ.

На физическом уровне стандартом IEEE 802.11 предусмотрено два типа радиоканалов (DSSS и FHSS), которые различаются способом модуляции, но используют одну и ту же технологию расширения спектра.

Технология расширения спектра методом прямой последовательности (DSSS)

Основная идея технологии расширения спектра (Spread Spectrum, SS) заключается в том, чтобы от узкополосного спектра сигнала, возникающего при обычном потенциальном кодировании, перейти к широкополосному спектру. Именно это позволяет значительно повысить помехоустойчивость передаваемых данных. Рассмотрим более детально, как это происходит.

При потенциальном кодировании информационные биты 0 и 1 передаются прямоугольными импульсами напряжений. Из курса математики и физики хорошо известно, что любую функцию и соответственно любой сигнал (ограничения, налагаемые на функцию, мы для простоты опускаем) можно представить в виде дискретного или непрерывного набора гармоник - синусоидальных сигналов с определенным образом подобранными весовыми коэффициентами и частотами. Такое представление называют преобразованием Фурье, а сами частоты гармонических сигналов образуют спектральное разложение функции.

При передаче прямоугольного импульса длительностью T спектр сигнала описывается функцией:

$$T * \left| \frac{\sin(\pi * f * T)}{\pi * f * T} \right|$$

, где

f — частота спектральной составляющей.

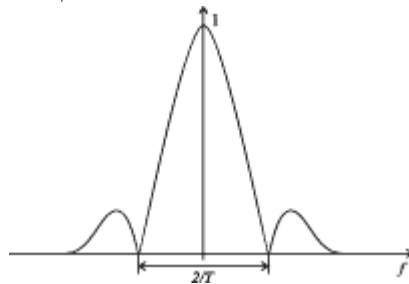


Рис. 4. Спектр прямоугольного импульса длительностью T

Несмотря на бесконечный спектр сигнала, наиболее весомые гармоники, то есть вносящие значительный вклад в результирующий сигнал, сосредоточены в небольшой частотной области, ширина которой обратно пропорциональна длительности импульса. Таким образом, с хорошей степенью точности исходный сигнал можно представить как совмещение гармоник в спектральной полосе, ширина которой равна длительности импульса T . Соответственно, чем меньше длительность импульса, тем больший спектральный диапазон занимает такой сигнал. Для того чтобы повысить помехоустойчивость передаваемого сигнала, то есть увеличить вероятность безошибочного распознавания сигнала на приемной стороне в условиях шума, можно воспользоваться методом перехода к широкополосному сигналу, добавляя избыточность в исходный сигнал. Для этого в каждый передаваемый информационный бит «встраивают» определенный код, состоящий из последовательности так называемых чипов

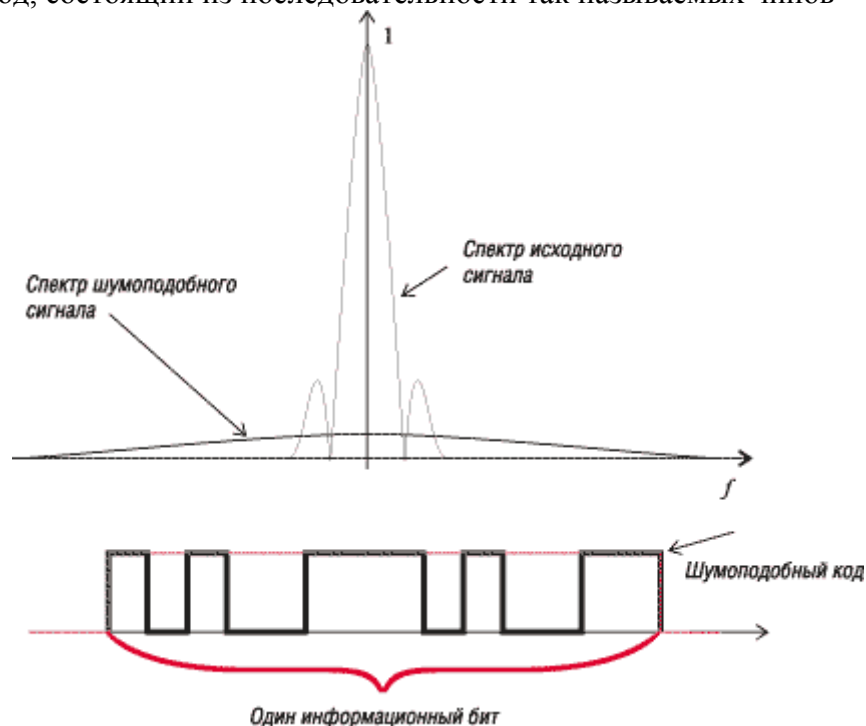


Рис. 5. Изменение спектра сигнала при добавлении шумоподобного кода

Фактически информационный бит, представляемый прямоугольным импульсом, разбивается на последовательность более мелких импульсов-чипов. В результате спектр сигнала значительно расширяется, так как ширину спектра можно с хорошей степенью точности считать обратно пропорциональной длительности одного чипа. Такие кодовые последовательности часто называют шумоподобными кодами. Дело в том, что наряду с расширением спектра сигнала уменьшается и спектральная плотность энергии. То есть энергия сигнала как бы «размазывается» по всему спектру. Результирующий сигнал становится шумоподобным в том смысле, что его теперь трудно отличить от естественного шума. Возникает вопрос— для чего усложнять первоначальный сигнал, если в результате он становится неотличимым от шума? Дело в том, что кодовые последовательности чипов обладают уникальным свойством автокорреляции. Попробуем на интуитивном уровне пояснить, в чем смысл корреляции. Под корреляцией в математике понимают степень взаимоподобия двух функций, то есть насколько

две различные функции похожи друг на друга. Соответственно под автокорреляцией понимается степень подобия функции самой себе в различные моменты времени. Например, если некоторая функция зависит (меняется) от времени и эта зависимость выражается в виде

$$f(t)$$

, то можно рассмотреть функцию в некоторый момент времени

$$t_0$$

и в момент времени

$$t_0 + \tau$$

. Степень соответствия этих двух функций друг другу в различные моменты времени и называется автокорреляцией. Оказывается, что можно подобрать такую последовательность чипов, для которой функция автокорреляции, отражающая степень подобия функции самой себе через определенный временной интервал, будет иметь резко выраженный пик лишь для одного момента времени. То есть функция будет подобна самой себе только для одного момента времени и совсем не похожа на себя для всех остальных моментов времени. Одна из наиболее известных (но не единственная) таких последовательностей— код Баркера длиной в 11 чипов: 11100010010. Коды Баркера обладают наилучшими среди известных псевдослучайных последовательностей свойствами шумоподобности, что и обусловило их широкое применение. Для передачи единичного и нулевого символов сообщения используются соответственно прямая и инверсная последовательности.

Для упрощенного вычисления автокорреляционной функции последовательности Баркера можно рассчитать разницу между числом совпадений и несовпадений между отдельными чипами последовательности при их циклическом почиповом сдвиге относительно друг друга.

Таблица 1. Вычисление автокорреляционной функции последовательности Баркера

Сдвиг	Последовательность										Результат корреляции	
0	1	1	1	0	0	0	1	0	0	1	0	
1	0	1	1	1	0	0	0	1	0	0	1	-1
2	1	0	1	1	1	0	0	0	1	0	0	-1
3	0	1	0	1	1	1	0	0	0	1	0	-1
4	0	0	1	0	1	1	1	0	0	0	1	-1
5	1	0	0	1	0	1	1	1	0	0	0	-1
6	0	1	0	0	1	0	1	1	1	0	0	-1
7	0	0	1	0	0	1	0	1	1	1	0	-1
8	0	0	0	1	0	0	1	0	1	1	1	-1
9	1	0	0	0	1	0	0	1	0	1	1	-1
10	1	1	0	0	0	1	0	0	1	0	1	-1
11	1	1	1	0	0	0	1	0	0	1	0	11

Как видно из Таблицы 1 последовательность Баркера обладает ярко выраженным автокорреляционным пиком, соответствующим наложению функции самой на себя. Проведя аналогичные расчеты, нетрудно убедиться, что другие последовательности не обладают подобным свойством, то есть имеют несколько пиков корреляции, которые значительно снижают помехоустойчивость передаваемого сигнала.

В приемнике полученный сигнал умножается на код Баркера (вычисляется корреляционная функция сигнала), в результате он становится узкополосным, поэтому его фильтруют в узкой полосе частот, равной удвоенной скорости передачи. Любая помеха, попадающая в полосу исходного широкополосного сигнала, после умножения на код Баркера, наоборот, становится широкополосной, поэтому в узкую информационную полосу попадает лишь часть помехи, по мощности примерно в 11 раз меньшая чем помеха, действующая на входе приемника.

Итак, основной смысл использования кодов Баркера заключается в том, чтобы, имея возможность передавать сигнал практически на уровне помех, гарантировать высокую степень достоверности принимаемой информации. Как известно, радиоволны приобретают способность переносить информацию в том случае, если они определенным образом модулируются. При этом необходимо, чтобы модуляция синусоидального несущего сигнала соответствовала требуемой последовательности информационных бит. Существует три основных типа модуляции: амплитудная, частотная и фазовая. В стандарте IEEE 802.11 для передачи сигналов используют фазовую модуляцию, поэтому остановимся на ней более подробно.

Фазовая модуляция

Различают два типа фазовой модуляции: собственно фазовую и относительную фазовую модуляцию. При фазовой модуляции (Phase Shift Key, PSK) для передачи логических нулей и единиц используют сигналы одной и той же частоты и амплитуды, но смещенные относительно друг друга по фазе. Например, логический нуль передается синфазным сигналом, а логическая единица — сигналом, сдвинутым по фазе на 180°

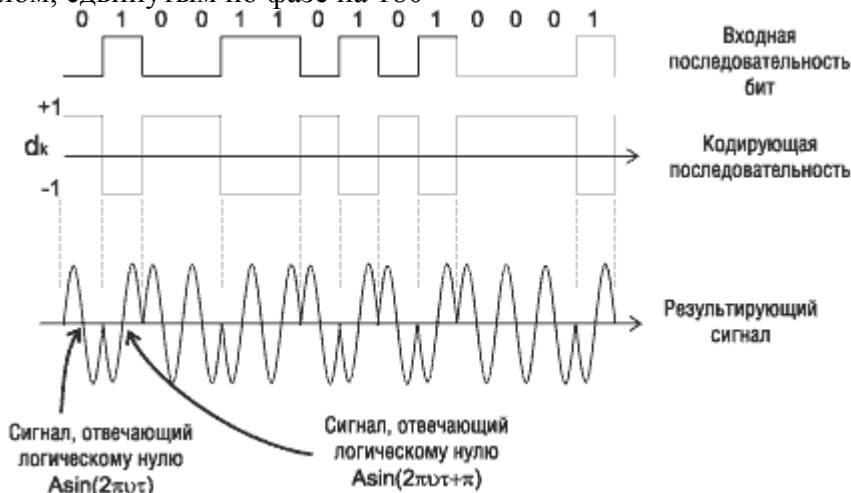


Рис. 6. Двоичная фазовая модуляция BPSK

Если изменение фазы может принимать всего два значения, то говорят о двоичной фазовой модуляции (Binary Phase Shift Key, BPSK). Математически сигнал, соответствующий логическому нулю, можно представить как

$$S_0(t) = A \sin(2\pi ft)$$

а сигнал, соответствующий логической единице, — как

$$S_1(t) = A \sin(2\pi ft + \pi) = -A \sin(2\pi ft)$$

Тогда модулированный сигнал можно записать в виде:

$$S_{BPSK}(t) = AV(t) \sin(2\pi ft)$$

где $V(t)$ — управляющий сигнал, принимающий значения $+1$ и -1 . Причем значение сигнала $+1$ соответствует логическому нулю, а значение сигнала -1 — логической единице.

Изменение фазы может иметь и более двух значений, например четыре ($0, 90, 180$ и 270°). В этом случае говорят о так называемой квадратурной фазовой модуляции (Quadrature Phase Shift Key, QPSK).

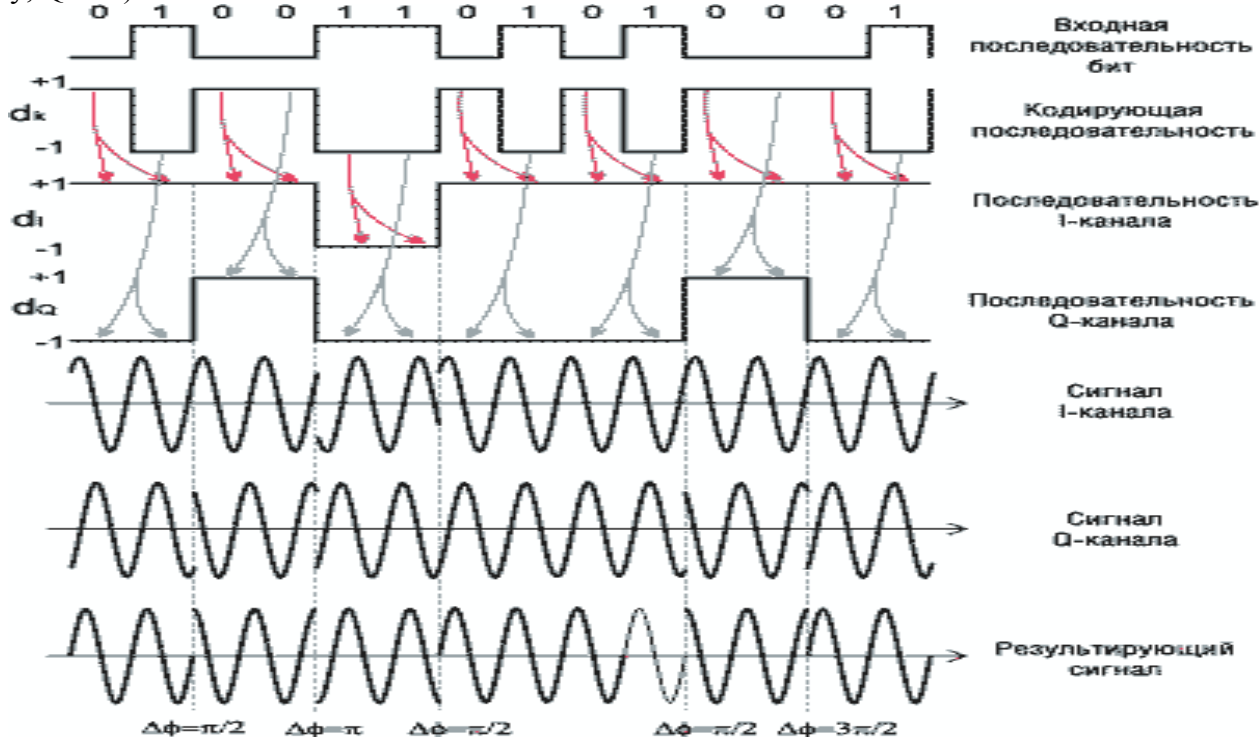


Рис. 7. Квадратурная фазовая модуляция QPSK

Чтобы понять происхождение этого термина, рассмотрим общий вид сигнала, модулированного по фазе:

$$S(t) = A \sin(2\pi ft + \varphi(t))$$

С учетом простейших тригонометрических соотношений данную формулу несложно привести к виду:

$$S(t) = A \sin(2\pi ft) \cos \varphi(t) + A \cos(2\pi ft) \sin \varphi(t)$$

Из полученного выражения видно, что исходный сигнал можно представить в виде суммы двух гармонических составляющих, смещенных друг относительно друга по фазе на 90° , так как

$$\cos(2\pi ft) = \sin(2\pi ft + \frac{\pi}{2})$$

В передатчике, производящем модуляцию, одна из этих составляющих синфазна сигналу генератора, а вторая находится в квадратуре по отношению к этому сигналу (отсюда — квадратурная модуляция). Синфазная составляющая обозначается как I (In Phase), а квадратурная — как Q (Quadrature).

Исходный сигнал несложно преобразовать:

$$\begin{aligned} S(t) &= A \sin(2\pi ft + \varphi) = \\ &= \frac{A}{\sqrt{2}} \sin(2\pi ft + \frac{\pi}{4})(\cos \varphi + \sin \varphi) - \\ &- \frac{A}{\sqrt{2}} \cos(2\pi ft + \frac{\pi}{4})(\cos \varphi - \sin \varphi) \end{aligned}$$

Если ввести обозначения

$$d_i = \cos \varphi + \sin \varphi$$

то получим следующий вид сигнала:

$$\begin{aligned} S_{QPSK}(t) &= \frac{A}{\sqrt{2}} d_i \sin(2\pi ft + \frac{\pi}{4}) - \\ &- \frac{A}{\sqrt{2}} d_q \cos(2\pi ft + \frac{\pi}{4}) \\ I &= \frac{A}{\sqrt{2}} d_i \sin(2\pi ft + \frac{\pi}{4}) \\ Q &= \frac{A}{\sqrt{2}} d_q \cos(2\pi ft + \frac{\pi}{4}) \end{aligned}$$

Кодирующие сигналы d_i и d_q могут принимать значения +1 и -1; учитывая, что

$$d_i = \cos \varphi + \sin \varphi; \quad d_q = \cos \varphi - \sin \varphi$$

получим соотношение между сдвигом фазы и кодирующими сигналами (см. Таблицу 2)

Таблица 2. соотношение между сдвигом фазы и кодирующими сигналами

Фаза сигнала	d_i	d_q
0°	+1	+1
90°	+1	-1
180°	-1	-1
270°	-1	+1

При реализации квадратурной фазовой модуляции входной поток бит преобразуется в кодирующую последовательность $\{d_k\}$ так, что логическому нулю соответствует кодирующий бит +1, а логической единице — кодирующий бит -1. После этого кодирующий поток разделяется на четные и нечетные биты. Четные биты поступают в I-канал, а нечетные — в Q-канал. Причем длительность каждого управляющего импульса d_i и d_q в два раза больше длительности исходного импульса d_k .

Управляющие биты d_i модулируют по фазе сигнал

$$\sin(2\pi ft + \pi / 4)$$

а биты d_q модулируют ортогональный сигнал (смещенный по фазе на 90°), то есть

$$\cos(2\pi ft + \pi / 4)$$

После этого оба сигнала складываются и образуется модулированный сигнал

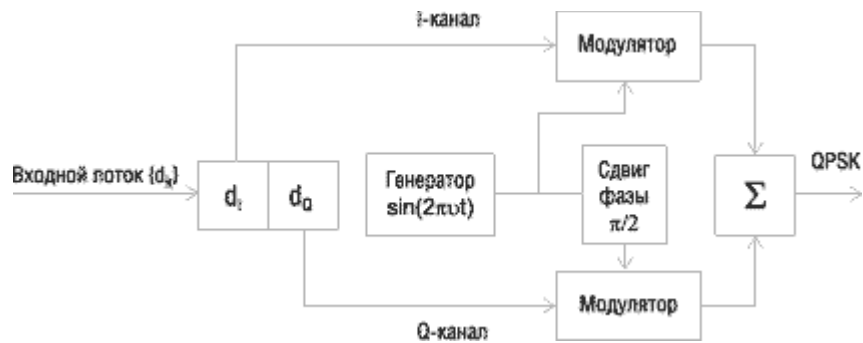


Рис. 8. Реализация квадратурной фазовой модуляции

В приведенной выше схеме квадратурной фазовой модуляции фаза результирующего сигнала может изменяться только каждые $2T$ секунд.

Отличительной особенностью квадратурной фазовой модуляции является наличие четырех дискретных состояний сигнала, отвечающих различным фазам. Это позволяет закодировать в одном дискретном состоянии последовательность двух информационных бит (так называемый дибит). Действительно, последовательность двух бит может иметь всего четыре различные комбинации: 00, 01, 10 и 11. Следовательно, ровно в два раза повышается и скорость передачи данных, то есть бодовая скорость в два раза больше битовой (1 Бод = 2 бит/с).

Учитывая, что кодирующему биту +1 отвечает логический нуль, а кодирующему биту -1 — логическая единица, и, принимая во внимание соответствие между фазой сигнала и значениями d_i и d_q , получим таблицу соответствия между входными дибитами и фазами модулированного сигнала

Таблица 3. Соответствия между входными дибитами и фазами модулированного сигнала

Фаза сигнала	d_i	d_q	Входной дибит
0°	+1	+1	00
90°	+1	-1	01
180°	-1	-1	11
270°	-1	+1	10

Возможные дискретные состояния сигнала принято изображать на векторной диаграмме состояния или на плоскости сигнального созвездия.

При использовании векторной диаграммы состоянию каждому значению сигнала ставится в соответствие вектор, длина которого — это условная амплитуда сигнала, а угол поворота вектора относительно горизонтальной оси — это фаза сигнала. То есть векторная диаграмма — это не что иное, как изображение векторов состояния в полярной системе координат. Примеры диаграмм состояния для двоичной и квадратурной фазовой модуляций показаны на

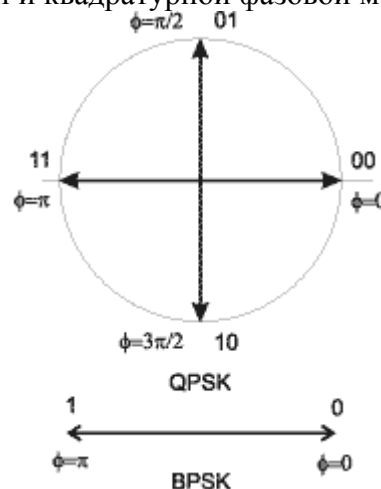


Рис. 9. Векторная диаграмма состояния

Более широкое распространение получил способ отображения различных состояний сигнала на сигнальном созвездии. Сигнальное созвездие — это декартова система координат, по оси абсцисс которой откладываются значения кодирующего сигнала d_i (ось I), а по оси ординат — значения кодирующего сигнала d_q (ось Q). В случае двоичной фазовой модуляции плоскость

вырождается в прямую, вдоль которой откладываются значения кодирующего сигнала d_k . В этом случае на сигнальном созвездии располагаются всего две точки, отвечающие значениям кодирующих битов +1 и -1. Эти две точки соответствуют всем возможным состояниям сигнала.

В случае QPSK-модуляции сигнальное созвездие состоит уже из четырех точек с координатами (+1, +1), (+1, -1), (-1, +1), (-1, -1). Эти четыре точки соответствуют четырем возможным дибитам и образуют совокупность всех возможных состояний сигнала

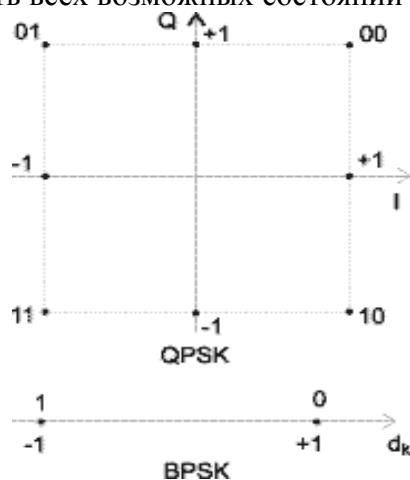


Рис. 10. Сигнальное созвездие для BPSK-и QPSK-модуляций

Несмотря на кажущуюся простоту метода фазовой модуляции ему присущи некоторые недостатки, связанные с трудностями технической реализации.

Один из недостатков связан с тем, что в случае квадратурной фазовой модуляции при одновременной смене символов в обоих каналах модулятора (с +1, -1 на -1, +1 или с +1, +1 на -1, -1) в сигнале QPSK происходит скачок фазы на 180°. Такие скачки фазы, имеющие место и при обыкновенной двухфазной модуляции, вызывают паразитную амплитудную модуляцию огибающей сигнала. В результате этого при прохождении сигнала через узкополосный фильтр возникают провалы огибающей до нуля. Такие изменения сигнала нежелательны, поскольку приводят к увеличению энергии боковых полос и помех в канале связи.

Для того чтобы избежать этого нежелательного явления, прибегают к так называемой квадратурной фазовой модуляции со сдвигом (Offset QPSK, OQPSK). При таком типе модуляции формирование сигнала в квадратурной схеме происходит так же, как и в модуляторе QPSK, за исключением того, что кодирующие биты в Q-канале имеют временную задержку на длительность одного элемента T . Изменение фазы при таком смещении кодирующих потоков определяется лишь одним элементом последовательности, а не двумя. В результате скачки фазы на 180° отсутствуют, поскольку каждый элемент последовательности, поступающий на вход модулятора синфазного или квадратурного канала, может вызвать изменение фазы на 0, 90 или 270° (-90°).

Другим, более серьезным недостатком фазовой модуляции является то обстоятельство, что при декодировании сигнала приемник должен определять абсолютное значение фазы сигнала, так как в фазовой модуляции информация кодируется именно абсолютным значением фазы сигнала. Для этого необходимо, чтобы приемник имел информацию об «эталонном» синфазном сигнале передатчика. Тогда путем сравнения принимаемого сигнала с эталонным можно определять абсолютный сдвиг фазы. Следовательно, необходимо каким-то способом синхронизировать сигнал передатчика с эталонным сигналом приемника (по этой причине фазовая модуляция получила название синхронной). Реализация синхронной передачи достаточно сложна, поэтому более широкое распространение получила разновидность фазовой модуляции, называемая относительной фазовой модуляцией (Differential Phase Shift Keying, DPSK). При относительной фазовой модуляции (также называемой относительной фазовой манипуляцией) кодирование информации происходит за счет сдвига фазы по отношению к предыдущему состоянию сигнала. Фактически приемник должен улавливать не абсолютное значение фазы принимаемого сигнала, а лишь изменение этой фазы. То есть информация кодируется изменением фазы. Естественно, такая модуляция уже не является синхронной и проще реализуется. Во всем остальном DPSK-модуляция не отличается от PSK-модуляции.

Для технической реализации DPSK-модуляции входной поток информационных бит

первоначально преобразуется, а затем подвергается обычной фазовой модуляции. Если необходимо, чтобы скачки по фазе происходили при появлении логического нуля, то преобразование исходной последовательности сводится к следующему: при появлении нуля происходит преобразование сигнала на инверсный, а при появлении единицы сигнал не меняется. Для примера рассмотрим преобразование 11-чиповой последовательности Баркера по описанному правилу

Таблица 4

Исходная последовательность	1	1	1	0	0	0	1	0	0	1	0	
Преобразованная последовательность	1	1	1	1	0	1	0	0	1	0	0	1

Данный алгоритм можно записать как логическую операцию неравнозначности над исходной последовательностью и преобразованной последовательностью, задержанной на один бит (смещенной по времени)

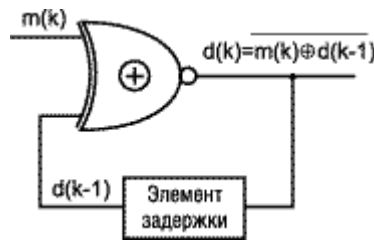


Рис. 11. Преобразование входящей последовательности для получения относительной фазовой модуляции

Математически это записывается в виде формулы

$$d_k = m_k \oplus d_{k-1}$$

где m_k — исходная последовательность, d_k — преобразованная последовательность (при расчетах предполагается, что первый бит преобразованной последовательности равен 1).

Аналогично производится преобразование входящей последовательности для получения относительной фазовой модуляции и во втором случае, то есть когда требуется, чтобы фаза сигнала менялась каждый раз при появлении на входе логической единицы. Однако в этом случае формула преобразования будет выглядеть так:

$$d_k = m_k \oplus d_{k-1}$$

Пример получения двоичной относительной фазовой модуляции DBPSK показан на

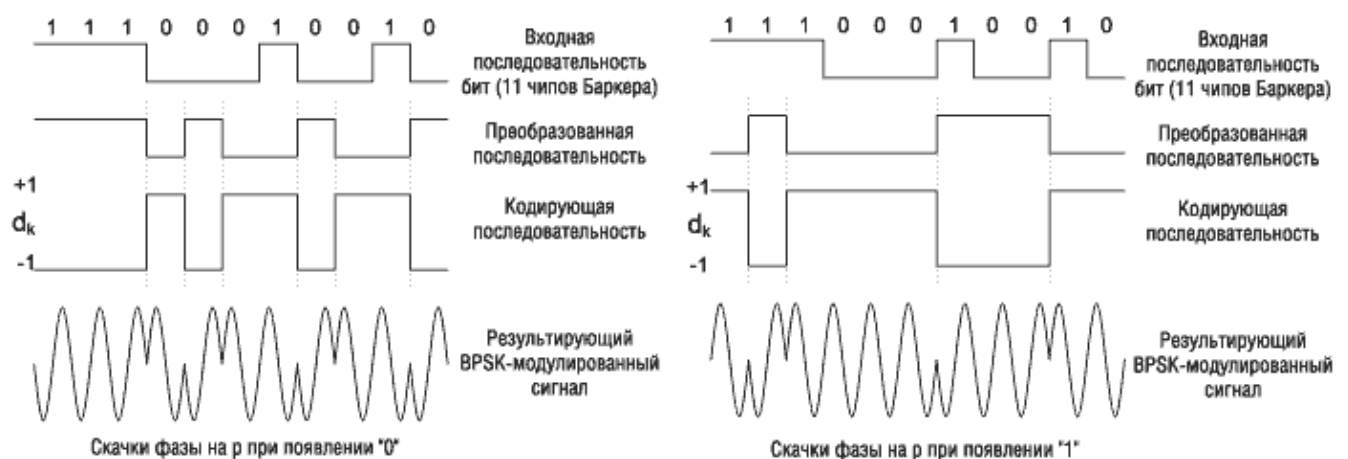


Рис. 12. Получение двоичной относительной фазовой модуляции DBPSK

Скорости передачи протокола IEEE 802.11

Кодирование DSSS/DPSK

Столь пристальное внимание фазовой модуляции мы уделили потому, что именно она используется в протоколе IEEE 802.11 для кодирования данных. При передаче данных на скорости 1Мбит/с используется двоичная относительная фазовая модуляция (DBPSK). При этом сам информационный единичный бит передается 11-чиповой последовательностью Баркера, а нулевой бит — инверсной последовательностью Баркера. Поэтому, сама относительная фазовая модуляция применяется именно к отдельным чипам последовательности.

Учитывая, что ширина спектра прямоугольного импульса обратно пропорциональна его длительности, а точнее, $2/T$ (см. рис 4) нетрудно посчитать, что при информационной скорости 1 Мбит/с скорость следования отдельных чипов последовательности Баркера составит 11 Мчип/с, а ширина спектра такого сигнала — 22 МГц, так как длительность одного чипа составляет 1/11 мкс.

Информационная скорость 1 Мбит/с является обязательной в стандарте IEEE 802.11 (basic access rate), но опционально возможна передача и на скорости 2 Мбит/с (enhanced access rate). Для передачи данных на такой скорости также используется относительная фазовая модуляция, но уже квадратурная (DQPSK). Это позволяет в два раза повысить информационную скорость передачи. При этом ширина самого спектра остается прежней, то есть 22 МГц.

В стандарте 802.11b, кроме 1 и 2 Мбит/с обязательными являются также скорости 5,5 и 11 Мбит/с, на таких скоростях используется уже несколько иной способ расширения спектра.

Кодирование ССК

В настоящей версии стандарта IEEE 802.11b используется несколько способов кодирования с использованием комплементарных кодов (Complementary Code Keying, ССК).

Использование ССК-кодов позволяет кодировать 8 бит на один символ при скорости 11 Мбит/с и 4 бита на символ при скорости 5,5 Мбит/с. При этом сами кодовые последовательности являются 8-чиповыми и при скорости передачи 11 Мбит/с кодирование 8 бит на символ соответствует символьной скорости 1,385 мегасимволов в секунду ($11/8 = 1,385$). Аналогичная символьная скорость используется и при скорости передачи 5,5 Мбит/с, так как при такой скорости в одном символе кодируется только 4 бита.

Особый интерес представляют сами ССК-последовательности. Прежде всего определим, что следует называть ССК-последовательностью. Для двух ССК-последовательностей равной длины сумма их автокорреляционных функций для любого циклического сдвига, отличного от нуля, всегда равна нулю.

Исходя из того, что автокорреляционная функция определяется как сумма попарных произведений последовательности при ее циклическом сдвиге, обозначим через a_i элементы первой последовательности, а через b_i — элементы второй. Тогда автокорреляционная функция для первой последовательности длиной n для циклического сдвига на j элементов запишется как:

$$c_j = \sum_{i=1}^{n-j} a_i a_{i+j}$$

Аналогично, для второй последовательности автокорреляционная функция примет вид:

$$d_j = \sum_{i=1}^{n-j} b_i b_{i+j}$$

При этом две последовательности будут называться комплементарными, если

$$\begin{cases} c_j + d_j = 0, & j \neq 0; \\ c_0 + d_0 = 2n. \end{cases}$$

Аналогично тому, как были рассмотрены комплементарные двоичные последовательности, элементы которых принимали только значения +1 и -1 можно определить комплементарные последовательности на множестве комплексных чисел или многофазовые последовательности Polyphase Codes.

Таблица 5

Сдвиг	Первая последовательность								c(j)	Вторая последовательность								d(j)	c(j)+d(j)
0	-1	-1	-1	1	1	1	-1	1	8	-1	-1	-1	1	-1	-1	1	-1	8	16
1	1	-1	-1	-1	1	1	1	-1	0	-1	-1	-1	-1	1	-1	-1	1	0	0
2	-1	1	-1	-1	-1	1	1	1	0	1	-1	-1	-1	-1	1	-1	-1	0	0
3	1	-1	1	-1	-1	-1	1	1	-4	-1	1	-1	-1	-1	-1	1	-1	4	0
4	1	1	-1	1	-1	-1	-1	1	0	-1	-1	1	-1	-1	-1	-1	1	0	0
5	1	1	1	-1	1	-1	-1	-1	-4	1	-1	-1	1	-1	-1	-1	-1	4	0
6	-1	1	1	1	-1	1	-1	-1	0	-1	1	-1	-1	1	-1	-1	-1	0	0
7	-1	-1	1	1	1	-1	1	-1	0	-1	-1	1	-1	-1	1	-1	-1	0	0

В стандарте IEEE 802.11b речь идет как раз о таких комплексных комплементарных последовательностях, содержащих элементы с четырьмя различными фазами, то есть о комплементарных последовательностях, определенных на множестве комплексных элементов $\{1, -1, j, -j\}$. Сами комплементарные последовательности, как и прежде, используются для уширения спектра сигнала (DSSS) и являются 8-чиповыми. Скорость передачи при этом составляет 11 Мчип/с, что дает скорость 1,375 мегасимволов в секунду. При этом ширина спектра сигнала, как и при использовании последовательностей Баркера, составляет 22 МГц, что позволяет использовать в частотном диапазоне от 2,4 до 2,4835 ГГц три неперекрывающиеся частотные полосы.

Сами комплементарные 8-чиповые комплексные последовательности образуются по следующей формуле:

$$\left\{ \begin{array}{l} e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, \\ e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, \\ e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, \\ -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1} \end{array} \right\}$$

Значения фаз

$$\varphi_1, \varphi_2, \varphi_3, \varphi_4$$

определяются последовательностью входных битов, причем значение

$$\varphi_1$$

выбирается по первому дибиту,

$$\varphi_2$$

— по второму,

$$\varphi_3$$

— по третьему и

$$\varphi_4$$

— по четвертому. Таким образом, для однозначного определения ССК-последовательности требуется 8 бит входных данных. Обратим внимание, что фаза

$$\varphi_1$$

а соответственно и член

$$e^{j\varphi_1}$$

присутствуют во всех членах последовательности. Фактически это означает сдвиг по фазе всех членов последовательности на один и тот же угол, то есть поворот вектора, задающего последовательность, или символа, определяемого последовательностью. По этой причине первый дибит данных — как для скорости передачи 5,5 Мбит/с, так и для скорости 11 Мбит/с — задает сдвиг целого символа по фазе по отношению к фазе предыдущего переданного символа.

Скорость 5,5 Мбит/с

Для скорости 5,5 Мбит/с в одном символе кодируется 4 бита, то есть два дибита ($d_0 - d_3$). Первый дибит определяет фазовый сдвиг четных и нечетных символов (см.Таблицу 6)

Таблица 6.

d_0, d_1	Фазовый сдвиг четных символов	Фазовый сдвиг нечетных символов
00	0	π
01	$\pi/2$	$-\pi/2$
11	π	0
10	$-\pi/2$	$\pi/2$

.Следующий дибит, то есть биты d_2, d_3 , определяет остальные фазы ССК-последовательности по формулам:

$$\begin{cases} \varphi_2 = (d_2 * \pi) + \frac{\pi}{2}, \\ \varphi_3 = 0, \\ \varphi_4 = d_3 * \pi. \end{cases}$$

Рассмотрим, к примеру, последовательность данных 11011000. Разбивая ее на пару четырехбитовых символов 1101 и 1000, первый из которых нечетный, а второй — четный, получим, что для нечетного символа

$$\varphi_1 = 0 \quad \varphi_2 = \pi / 2 \quad \varphi_3 = 0$$

и

$$\varphi_4 = \pi$$

Тогда комплексная ССК-последовательность примет вид: $\{-j, -1, -j, 1, j, 1, -j, 1\}$.

Аналогично для второго символа

$$\varphi_1 = -\pi/2 \quad \varphi_2 = \pi/2 \quad \varphi_3 = 0 \quad \varphi_4 = 0$$

а ССК-последовательность имеет вид: $\{1, -j, 1, j, 1, -j, -1, -j\}$. Как нетрудно заметить, обе последовательности сдвинуты друг относительно друга на 90° , точнее, вторая последовательность, соответствующая четному символу, сдвинута относительно первой последовательности на

$$\varphi_1 = -\frac{\pi}{2} (e^{-j\frac{\pi}{2}} = -j)$$

Скорость 11 Мбит/с

При скорости 11 Мбит/с в одном символе кодируется одновременно 8 бит данных. При этом первый дибит последовательности данных, как и прежде, задает сдвиг фазы при относительной фазовой модуляции целого символа в зависимости от того, четный он или нечетный, точно так же, как и для скорости 5,5 Мбит/с. Остальные три дибита 8-битовой последовательности данных определяют фазы

$\varphi_2, \varphi_3, \varphi_4$

причем значение

φ_2

выбирается по второму дибиту,

φ_3

по третьему и

φ_4

— по четвертому. Значение сдвига фаз определяется по Таблице 7

Таблица 7. Значение сдвига фаз

d_i, d_{i+1}	Фазовый сдвиг символа
00	0
01	$\pi/2$
10	π
11	$-\pi/2$

.Если, к примеру, на вход поступает последовательность 8 бит данных 00111011 и символ является четным, то, пользуясь таблицами, найдем:

$$\begin{cases} \varphi_1 = 0, \\ \varphi_2 = 0, \\ \varphi_3 = \pi, \\ \varphi_4 = -\frac{\pi}{2}. \end{cases}$$

Тогда сама ССК-последовательность примет вид: $\{j, j, -j, j, -1, -1, -1, 1\}$.

Как уже отмечалось, для задания ССК-последовательности используются только 6 бит данных (второй, третий и четвертый дибиты). Первый дибит определяет сдвиг по фазе всего символа и используется в относительной фазовой модуляции. Шесть бит данных могут иметь 64 различные комбинации ($2^6 = 64$). Поэтому говорят, что в протоколе IEEE 802.11b при кодировании каждого символа используется одна из 64 возможных восьмиразрядных ССК-последовательностей. Последовательности, формируемые в ССК-модуляторе, в дальнейшем поступают на I- и Q-каналы QPSK-модулятора.

С помощью описанных выше алгоритмов кодирования можно представить схему ССК-модулятора



Рис. 13. Блок-схема ССК-модулятора.

В заключение обзора различных методов модуляции на физическом уровне, принятых в стандарте IEEE 802.11b, можно составить итоговую таблицу

Таблица 8

Скорость передачи, Мбит/с	Кодовая последовательность	Тип модуляции	Символьная скорость, мегасимволов в секунду	Количество бит на символ
1	11-чиповая (Баркера)	DBPSK	1	1
2	11-чиповая (Баркера)	DQPSK	1	2
5,5	8-чиповая (ССК)	DQPSK	1,375	4
11	8-чиповая (ССК)	DQPSK	1,375	8

MAC-уровень

На MAC-уровне определяются базовые структуры архитектуры сети и перечень услуг, предоставляемых этим уровнем. Стандартом определяются два основных типа архитектуры сетей: Ad Hoc и Infrastructure Mode.

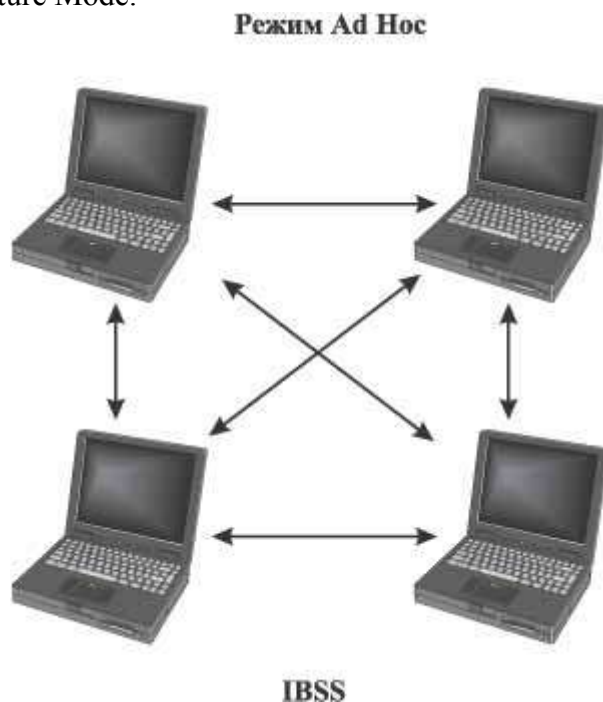


Рис. 14. Режим взаимодействия Ad Hoc.

В режиме Ad Hoc, который называют также IBSS (Independent Basic Service Set) или режим Peer to Peer (точка-точка), станции непосредственно взаимодействуют друг с другом. Для этого режима требуется минимум оборудования — каждая станция должна быть оснащена беспроводным адаптером. При такой конфигурации не требуется создания какой-либо сетевой инфраструктуры. Основным недостатком режима Ad Hoc является ограниченный диапазон

действия, или радиус, возможной сети, а также возможность подключения к внешней сети (например, к Интернету).

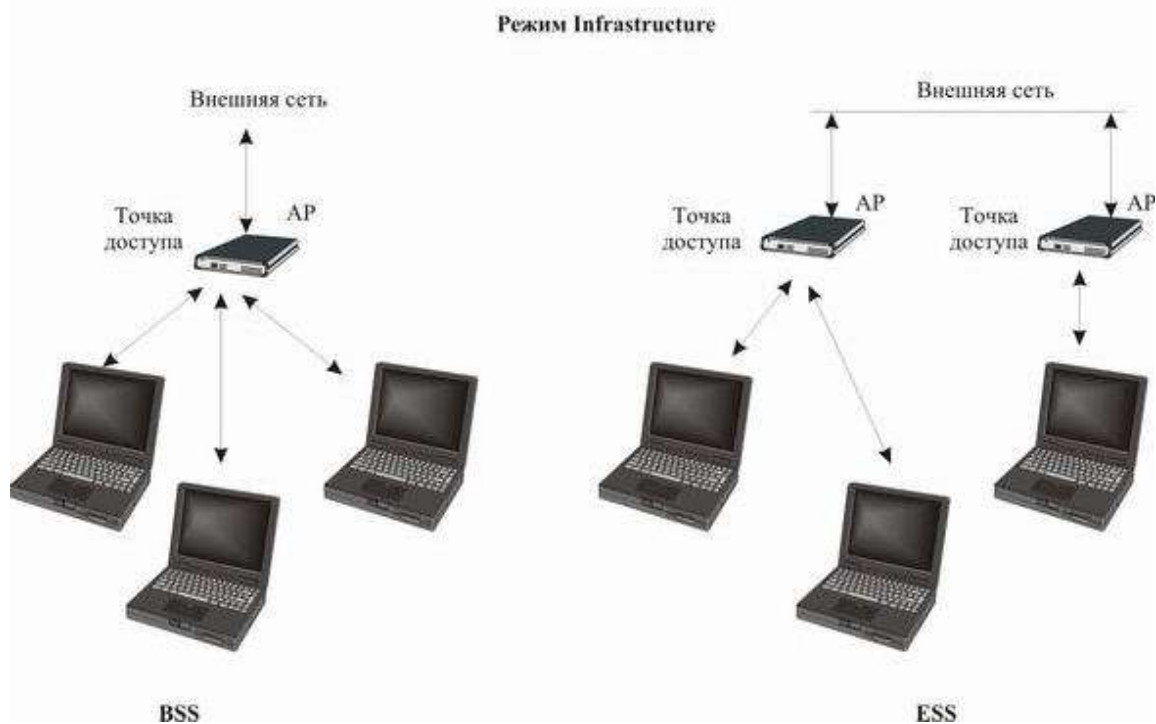


Рис. 15. Режим взаимодействия Infrastructure Mode.

В режиме Infrastructure Mode станции взаимодействуют друг с другом не напрямую, а через точку доступа (Access Point), которая выполняет в беспроводной сети роль своеобразного концентратора (аналогично тому, как это происходит в традиционных кабельных сетях). Рассматривают два режима взаимодействия с точками доступа: BSS (Basic Service Set) и ESS (Extended Service Set). В режиме BSS все станции связываются между собой только через точку доступа, которая может выполнять также функцию моста с внешней сетью. В расширенном режиме — ESS существует инфраструктура нескольких сетей BSS, причем сами точки доступа взаимодействуют друг с другом, что позволяет передавать трафик от одной BSS к другой. Сами точки доступа соединяются между собой либо с помощью сегментов кабельной сети, либо с помощью радиомостов.

Для доступа к среде передачи данных в беспроводных сетях стандарта IEEE 802.11b используется метод коллективного доступа с обнаружением несущей и избеганием коллизий (Carrier Sense Multiple Access / Collision Avoidance, CSMA/CA). Собственно, метод даже по названию напоминает технологию коллективного доступа, используемую в сетях Ethernet. Действительно, в сетях Ethernet используется метод коллективного доступа с опознанием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD). Единственное отличие заключено во второй части метода — вместо обнаружения коллизий используется технология избегания коллизий.

Перед тем как послать данные в «эфир», станция сначала посылает специальное сообщение, называемое RTS (Ready To Send), которое трактуется как готовность данного узла к отправке данных. Данное RTS-сообщение содержит информацию о продолжительности предстоящей передачи и адресате и доступно всем узлам в сети. Это позволяет другим узлам задержать передачу на время, равное объявленной длительности сообщения. Приемная станция, получив сигнал RTS, отвечает посылкой сигнала CTS (Clear To Send), соответствующего готовности станции к приему информации. После этого передающая станция посылает пакет данных, а приемная станция должна передать кадр ACK, подтверждающий безошибочный прием. Если ACK не получен, попытка передачи пакета данных будет повторена. Таким образом, с использованием такого четырехэтапного протокола передачи данных (4-Way Handshake) реализуется регламентирование коллективного доступа с минимизацией вероятности возникновения столкновений



Рис. 16. Реализация метода коллективного доступа

IEEE 802.11b MAC Frame Format

Заголовок MAC-уровня (30 байт)	Данные (0-2312 байт)	CRC (4 байт)
-----------------------------------	-------------------------	-----------------

Рис. 17. Структура пакета данных

Каждый пакет данных снабжается контрольной суммой CRC, что гарантирует обнаружение битых кадров при приеме. Пакетная фрагментация, определяемая в стандарте, предусматривает разбивку большого пакета данных на малые порции. Такой подход позволяет снизить вероятность повторной передачи кадра данных, поскольку с увеличением размера кадра возрастает и вероятность ошибки при его передаче. Если же переданный кадр оказался битым, то в случае малого размера кадра передающей станции придется повторить только малый фрагмент сообщения.

Спецификация пакетирования данных, предусмотренная стандартом, предписывает разбивку данных на пакеты, снабженные контрольной и адресной информацией длиной в 30 байт, блока данных длиной до 2048 байт и 4-байтного CRC-блока. Стандарт рекомендует использовать пакеты длиной 1500 или 2048 байт.

Стандарт IEEE 802.11a

Рассмотренный ранее стандарт 802.11b обеспечивает максимальную скорость передачи данных до 11 Мбит/с в частотном диапазоне 2,4 ГГц (от 2,4 до 2,4835 ГГц). Этот диапазон не требует лицензирования и зарезервирован для использования в промышленности, науке и медицине (ISM), однако при использовании технологии расширения спектра DSSS на частотах около 2,4 ГГц могут возникать проблемы из-за помех, порождаемых другими бытовыми беспроводными устройствами, в частности микроволновыми печами и радиотелефонами. Кроме того, современные приложения и объемы передаваемых по сети данных нередко требуют большей пропускной способности, чем может предложить стандарт 802.11b. Выход из создавшегося положения предлагает стандарт 802.11a (табл. 9), рекомендуемый передачу данных со скоростью до 54 Мбит/сек в частотном диапазоне 5 ГГц (от 5,15 до 5,350 ГГц и от 5,725 до 5,825 ГГц). В США данный диапазон именуют диапазоном нелицензионной национальной информационной инфраструктуры (Unlicensed National Information Infrastructure, UNII).

Таблица 9. Частотный диапазон стандарта IEEE 802.11a

Диапазон	Частота, ГГц	Ограничение по мощности, мВт
UNII	5,150 - 5,250	50
UNII	5,250 - 5,350	250
UNII	5,725 - 5,825	1000
ISM	2,400 - 2,4835	1000

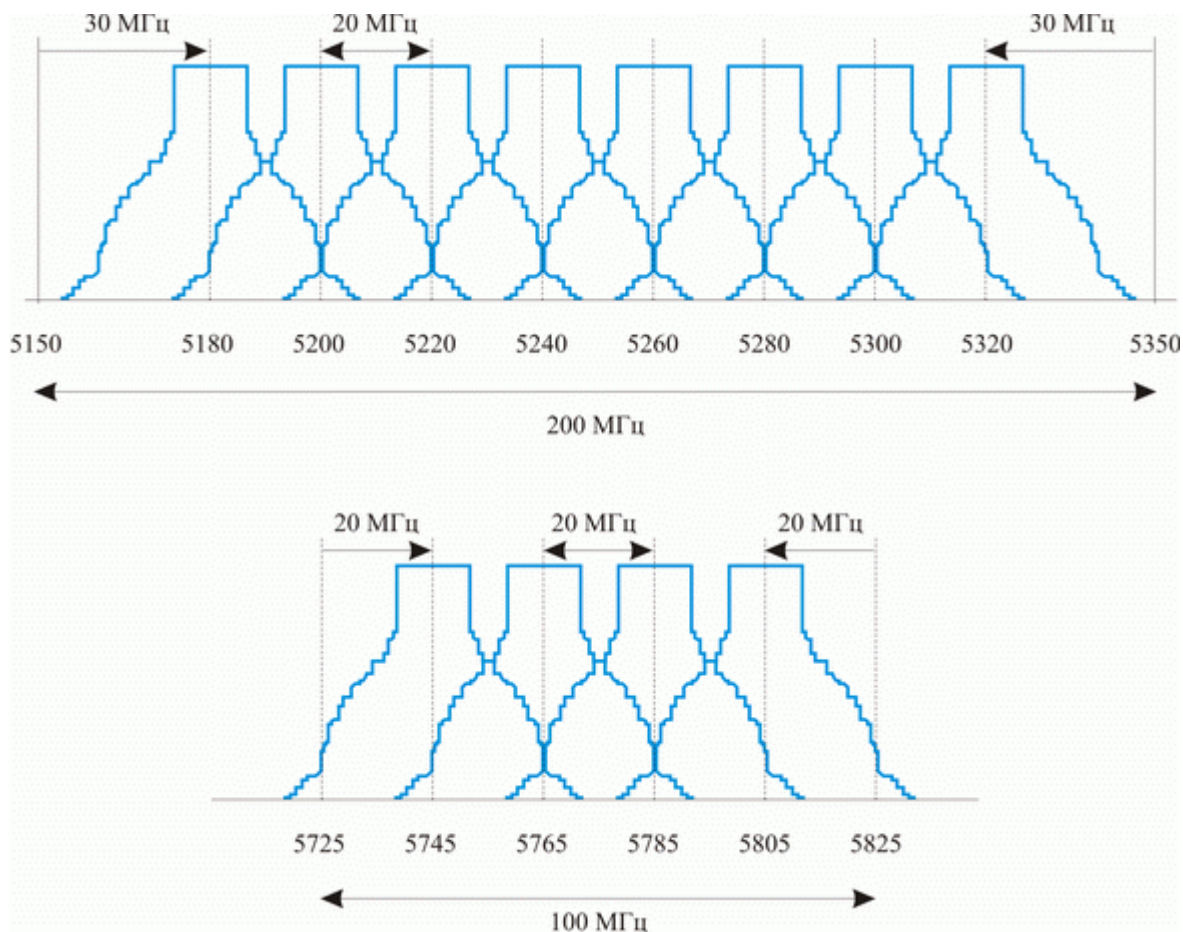


Рис. 18. Разделение диапазона UNII на 12 частотных поддиапазонов.

В соответствии с правилами FCC частотный диапазон UNII разбит на три 100-мегагерцевых поддиапазона, различающихся ограничениями по максимальной мощности излучения. Нижний диапазон (от 5,15 до 5,25 ГГц) предусматривает мощность всего 50 мВт, средний диапазон (от 5,25 до 5,35 ГГц) - 250 мВт, а верхний диапазон (от 5,725 до 5,825 ГГц) - 1 Вт. Использование трёх частотных поддиапазонов с общей шириной 300 МГц делает стандарт 802.11a самым, так сказать, широкополосным из семейства стандартов 802.11 и позволяет разбить весь частотный диапазон на 12 каналов, каждый из которых имеет ширину 20 МГц, восемь из которых лежат в 200-мегагерцевом диапазоне от 5,15 до 5,35 ГГц, а остальные четыре канала - в 100-мегагерцевом диапазоне от 5,725 до 5,825 ГГц (рис. 18). При этом четыре верхних частотных канала, предусматривающие наибольшую мощность передачи, используются преимущественно для передачи сигналов вне помещений.

Предусмотренная протоколом 802.11a ширина канала 20 МГц вполне достаточна для организации высокоскоростной передачи. Использование же частот свыше 5 ГГц и ограничение мощности передачи приводят к возникновению ряда проблем при попытке организовать высокоскоростную передачу данных, и это необходимо учитывать при выборе метода кодирования данных. Напомним, что распространение любого сигнала неизбежно сопровождается его затуханием, причём величина затухания сигнала зависит как от расстояния от точки передачи, так и от частоты сигнала. При измерении в децибелах величины затухания сигнала (ослабление при распространении) пользуются формулой:

$$L_p = X \lg\left(\frac{4\pi df}{c}\right)$$

где: X - коэффициент ослабления, равный 20 для открытого пространства, d - расстояние от точки передачи, f - частота сигнала, c - скорость света.

Из данной формулы непосредственно вытекает, что с увеличением частоты передаваемого сигнала увеличивается и его затухание. Так, при распространении сигнала в открытом пространстве с частотой 2,4 ГГц он ослабевает на 60 дБ при удалении от источника на 10 м. Если же частота равна 5 ГГц, ослабление сигнала при удалении на 10 м составит уже 66 дБ. Учитывая, что правила FCC диктуют использование существенно меньшей мощности излучения в нижних поддиапазонах UNII, чем в диапазоне ISM 2,4 ГГц, становится понятно, что использование более высоких частот в протоколе 802.11a приводит к несколько меньшему

радиусу действия сети, чем в протоколе 802.11b.

Второй важный момент, который необходимо учитывать при использовании высокочастотных сигналов с большой частотной шириной канала, связан с возникновением эффекта многолучевой интерференции: в результате многократных отражений один и тот же сигнал может попадать в приёмник различными путями. Но различные пути распространения имеют и разные длины, а потому для различных путей распространения ослабление сигнала будет неодинаковым. Следовательно, в точке приёма результирующий сигнал представляет собой суперпозицию (интерференцию) многих сигналов с различными амплитудами и смещёнными относительно друг друга по времени, что эквивалентно сложению сигналов с разными фазами. Если предположить, что передатчик распространяет гармонический сигнал $y_{in} = A \sin 2\pi \nu t$ с частотой несущей ν и амплитудой A , то в приёмнике будет получен сигнал

$$y_{out} = \sum_{i=1}^N A_i \sin 2\pi \nu (t - t_i)$$

, где t_i - задержка распространения сигнала по i -му пути (рис. 19).

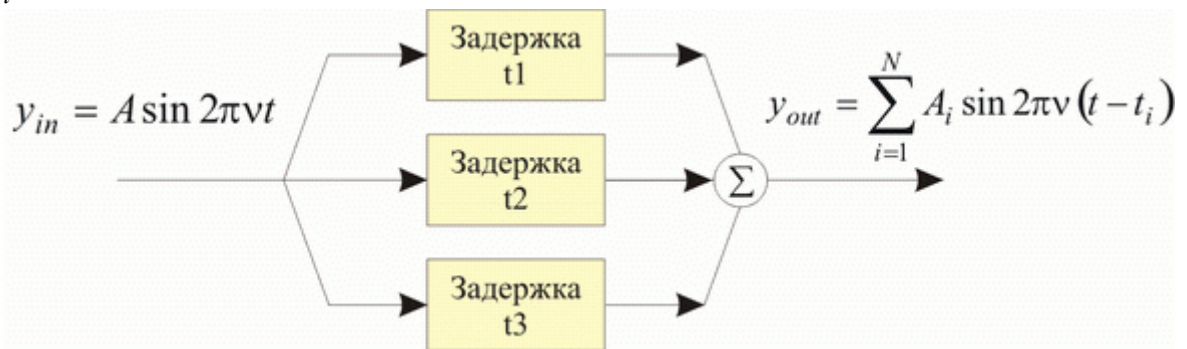


Рис. 19. Модель многолучевого распространения сигнала.

Следствием многолучевой интерференции является искажение принимаемого сигнала. Многолучевая интерференция присуща любому типу сигналов, но особенно негативно она сказывается на широкополосных сигналах. Дело в том, что при использовании широкополосного сигнала в результате интерференции определённые частоты складываются синфазно, что приводит к увеличению сигнала, а некоторые, наоборот, - противофазно, вызывая ослабление сигнала на данной частоте (рис. 20).

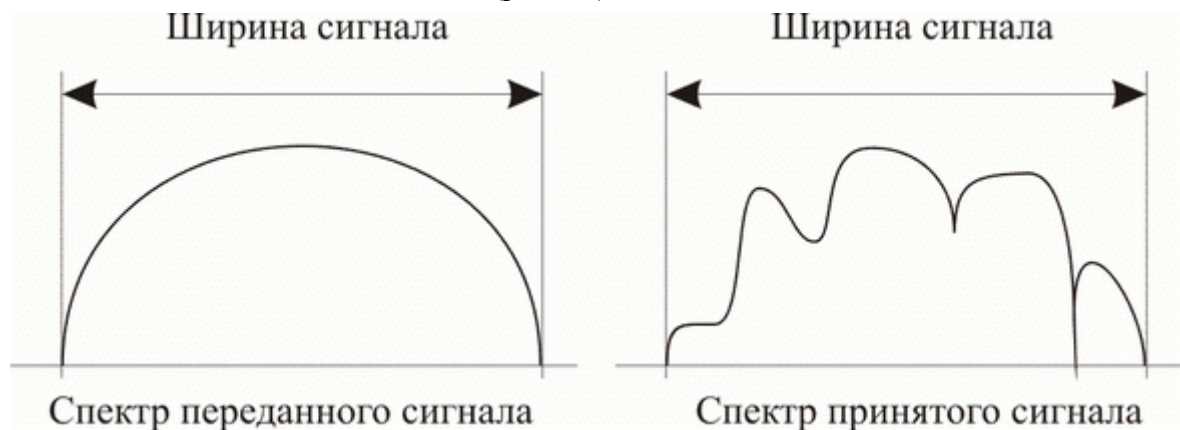


Рис. 20. Искажение сигнала за счёт присутствия многолучевой интерференции.

Говоря о многолучевой интерференции, возникающей при передаче сигналов, различают два крайних случая. В первом случае максимальная задержка между различными сигналами не превосходит времени длительности одного символа, и интерференция возникает в пределах одного передаваемого символа. Во втором случае максимальная задержка между различными сигналами больше длительности одного символа, а в результате интерференции складываются сигналы, представляющие разные символы, и возникает так называемая межсимвольная интерференция (Inter Symbol Interference, ISI - рис. 21).

Наиболее отрицательно на искажении сигнала сказывается межсимвольная интерференция. Поскольку символ - это дискретное состояние сигнала, характеризующееся значениями частоты несущей, амплитуды и фазы, то для различных символов меняются амплитуда и фаза сигнала, поэтому восстановить исходный сигнал крайне сложно.

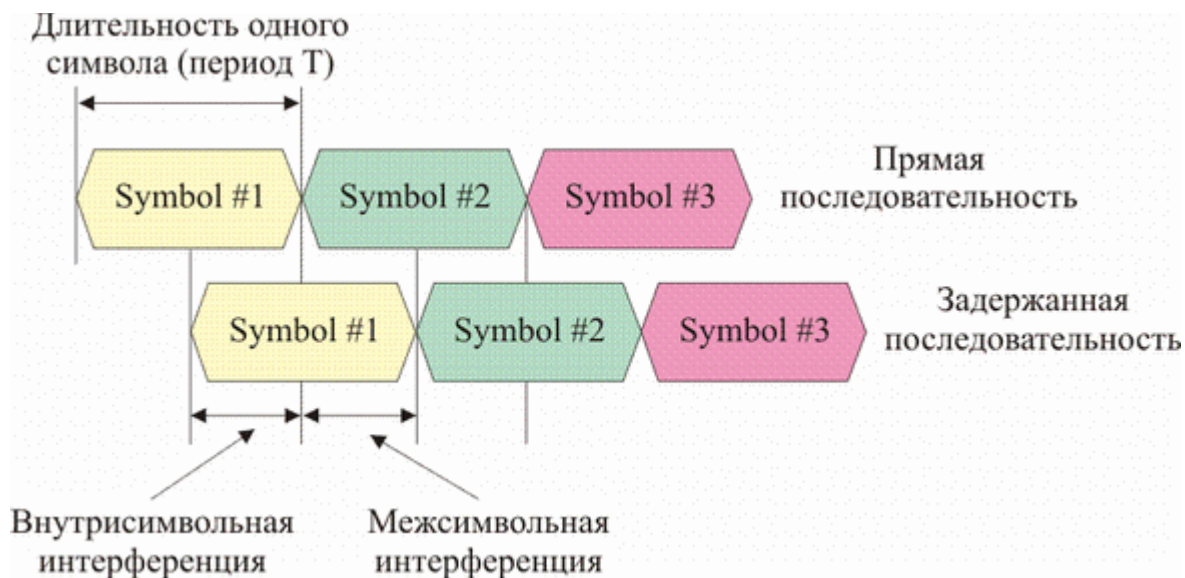


Рис. 21. Возникновение межсимвольной и внутрисимвольной интерференции.

Чтобы избежать, а точнее, частично компенсировать эффект многолучевого распространения, используются частотные эквалайзеры, однако, по мере роста скорости передачи данных либо за счёт увеличения символьной скорости, либо за счёт усложнения схемы кодирования, эффективность использования эквалайзеров падает.

В стандарте 802.11b с максимальной скоростью передачи 11 Мбит/с при использовании ССК-кодов и QDPSK-кодирования применение схем компенсации межсимвольной интерференции вполне успешно справляется с возложенной на них задачей, но при более высоких скоростях, как в протоколе 802.11a, такой подход становится неприемлем. Поэтому в стандарте 802.11a используется принципиально иной метод кодирования данных, который состоит в том, что поток передаваемых данных распределяется по множеству частотных подканалов и передача ведётся параллельно на всех этих подканалах. При этом высокая скорость передачи достигается именно за счёт одновременной передачи данных по всем каналам, а скорость передачи в отдельном подканале может быть и не высокой. Если скорость передачи обозначить S_i в i -ом частотном канале, то общая скорость передачи посредством N каналов будет равной

$$S = \sum_{i=1}^N S_i$$

Поскольку в каждом из частотных подканалов скорость передачи данных можно сделать не слишком высокой, это создает предпосылки для эффективного подавления межсимвольной интерференции.

При частотном разделении каналов необходимо, чтобы ширина отдельного канала была, с одной стороны, достаточно узкой для минимизации искажения сигнала в пределах отдельного канала, а с другой - достаточно широкой для обеспечения требуемой скорости передачи. Кроме того, для экономного использования всей полосы канала, разделяемого на подканалы, желательно как можно более плотно расположить частотные подканалы, но при этом избежать межканальной интерференции, чтобы обеспечить полную независимость каналов друг от друга. Частотные каналы, удовлетворяющие перечисленным требованиям, называются ортогональными. Несущие сигналы всех частотных подканалов (а точнее, функции, описывающие эти сигналы) ортогональны друг другу. С точки зрения математики ортогональность функций означает, что их произведение, усреднённое на некотором интервале, должно быть равно нулю. В нашем случае это выражается простым соотношением:

$$\int_0^T \sin 2\pi f_l t \sin 2\pi f_k t dt = 0, k \neq l$$

где T - период символа, f_k, f_l - несущие частоты каналов k и l .

Ортогональность несущих сигналов можно обеспечить в том случае, если за время длительности одного символа несущий сигнал будет совершать целое число колебаний. Примеры нескольких несущих ортогональных колебаний представлены на рис. 22.

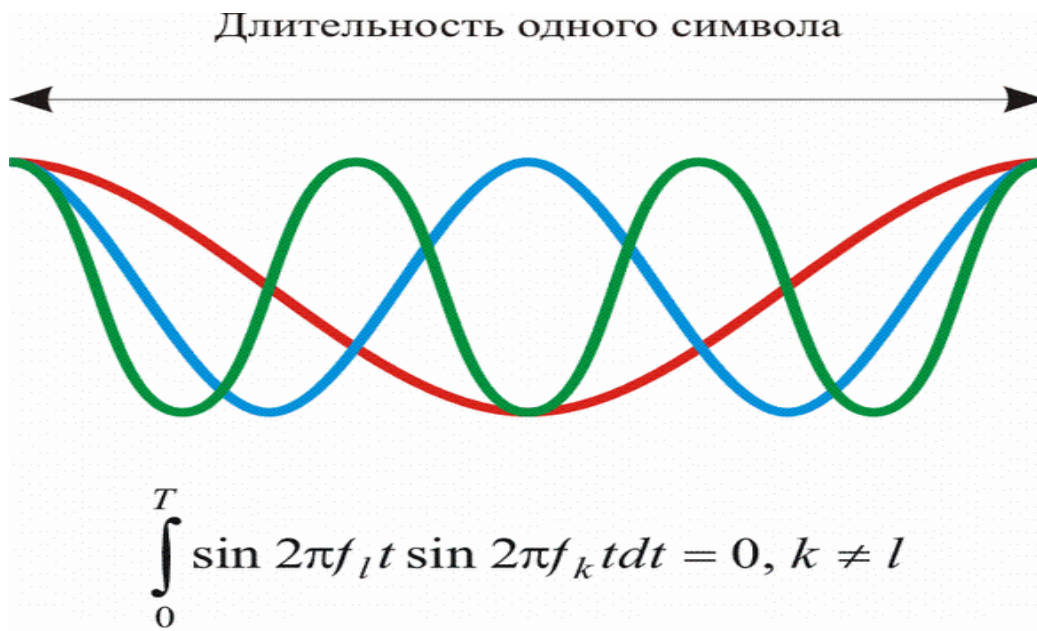


Рис. 22. Ортогональные частоты.

Учитывая, что каждый передаваемый символ длительности T передается ограниченной по времени синусоидальной функцией, нетрудно найти и спектр такой функции (рис 23), который будет описываться функцией

$$\frac{\sin 2\pi(f - f_i)}{2\pi(f - f_i)}$$

, где f_i - центральная (несущая) частота i -го канала.

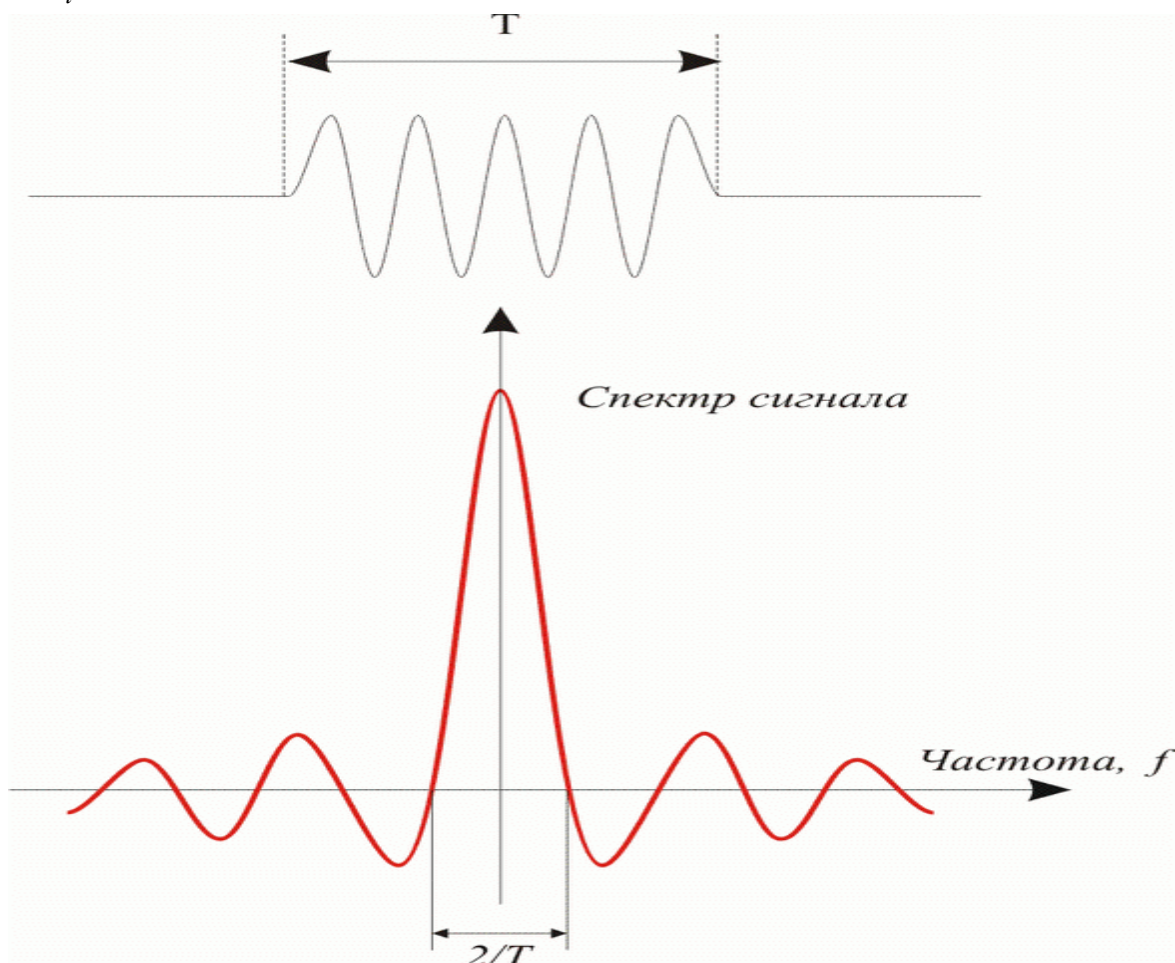


Рис. 23. Символ длительностью T и его спектр.

Такой же функцией описывается и форма частотного подканала. При этом важно, что хотя сами частотные подканалы могут и перекрывать друг друга, однако ортогональность несущих сигналов гарантирует частотную независимость каналов друг от друга, а следовательно, отсутствие межканальной интерференции (рис. 24).

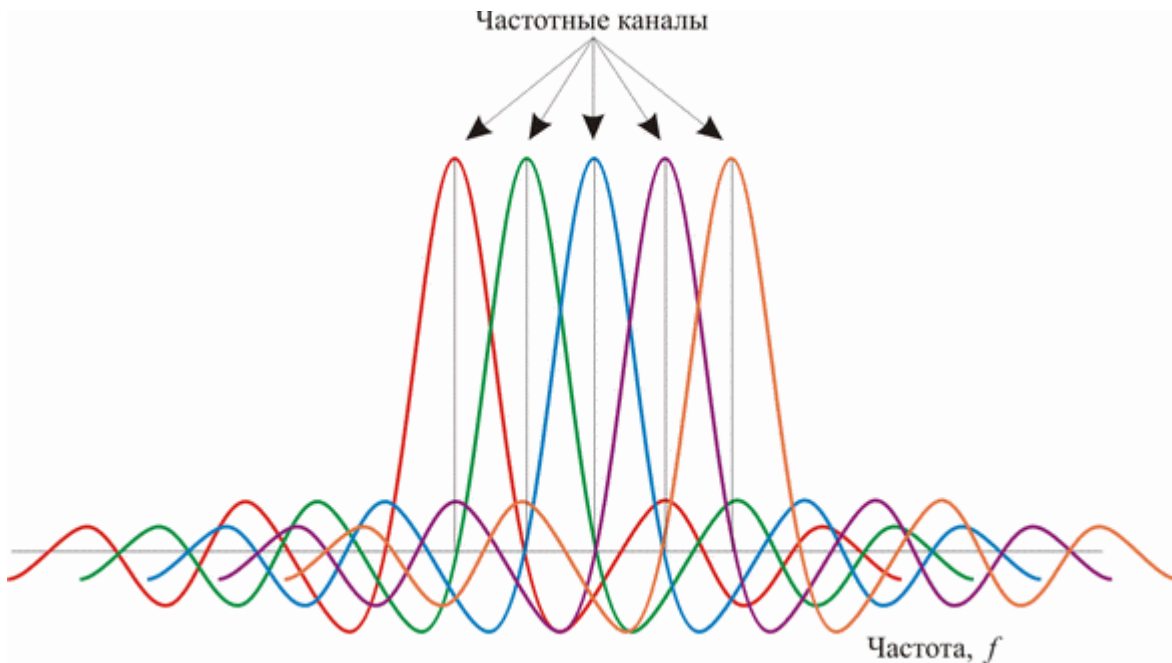


Рис. 24. Частотное разделение каналов с ортогональными несущими сигналами.

Рассмотренный способ деления широкополосного канала на ортогональные частотные подканалы называется ортогональным частотным разделением с мультиплексированием (Orthogonal Frequency Division Multiplexing, OFDM). Для его реализации в передающих устройствах используется обратное быстрое преобразование Фурье (IFFT), переводящее предварительно мультиплексированный на N -каналов сигнал из временного представления в частотное.

$$f(t) \rightarrow F(\omega)$$

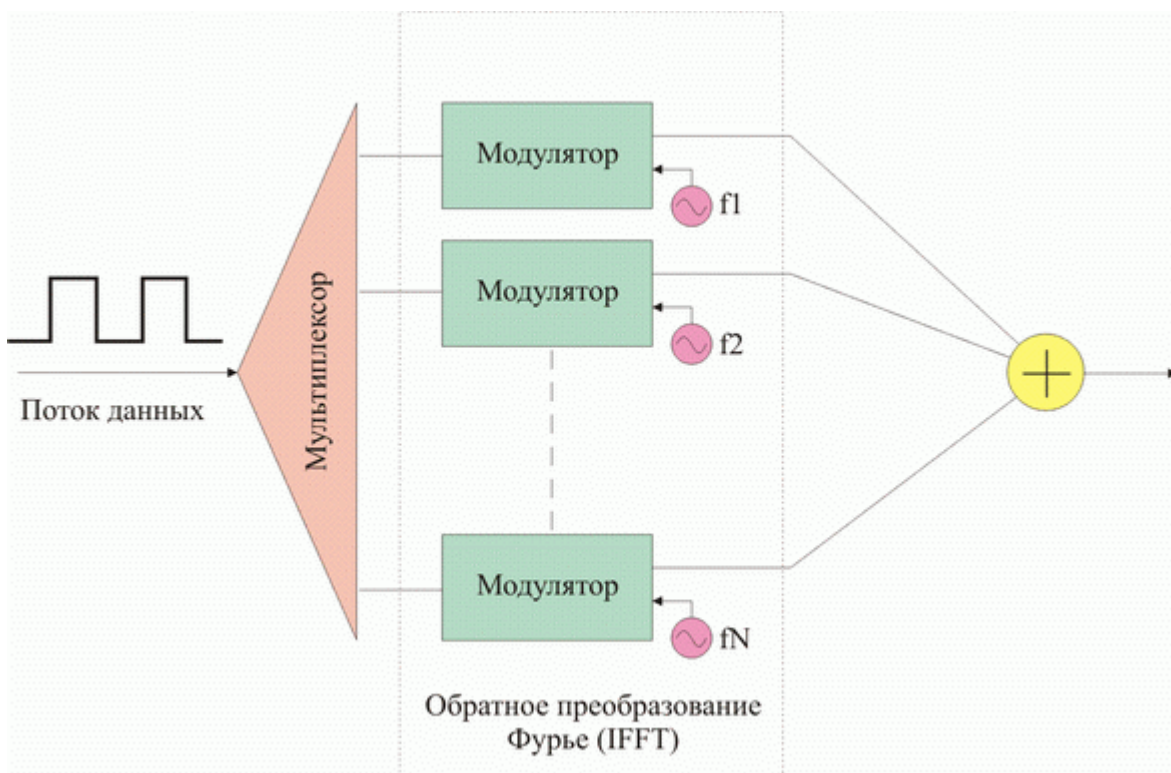


Рис. 25. Осуществление обратного быстрого преобразования Фурье для получения N ортогональных частотных подканалов

В протоколе 802.11a используется обратное преобразование Фурье с окном в 64 частотных подканала. Поскольку ширина каждого из 12 каналов, определяемых в стандарте 802.11a, имеет ширину 20 МГц, получаем, что каждый ортогональный частотный подканал имеет ширину 20 МГц: $64=312,5$ кГц. Однако из 64 ортогональных подканалов используются только 52, причем 48 подканалов используются для передачи данных (Data Tones), а остальные - для передачи служебной информации (Pilot Tones).

Как уже отмечалось, одним из ключевых преимуществ метода OFDM является сочетание

высокой скорости передачи с эффективным противостоянием многолучевому распространению. Если говорить точнее, то сама по себе технология OFDM не устраняет многолучевого распространения, но создаёт предпосылки для устранения эффекта межсимвольной интерференции. Дело в том, что неотъемлемой частью технологии OFDM является понятие охранного интервала (Guard Interval, GI) - это циклическое повторение окончания символа, пристраиваемое в начале символа (рис. 26). Охранный интервал является избыточной информацией и в этом смысле снижает полезную (информационную) скорость передачи. Эта избыточная информация добавляется к передаваемому символу в передатчике и отбрасывается при приёме символа в приёмнике, но именно она служит защитой от возникновения межсимвольной интерференции.

Циклическое копирование

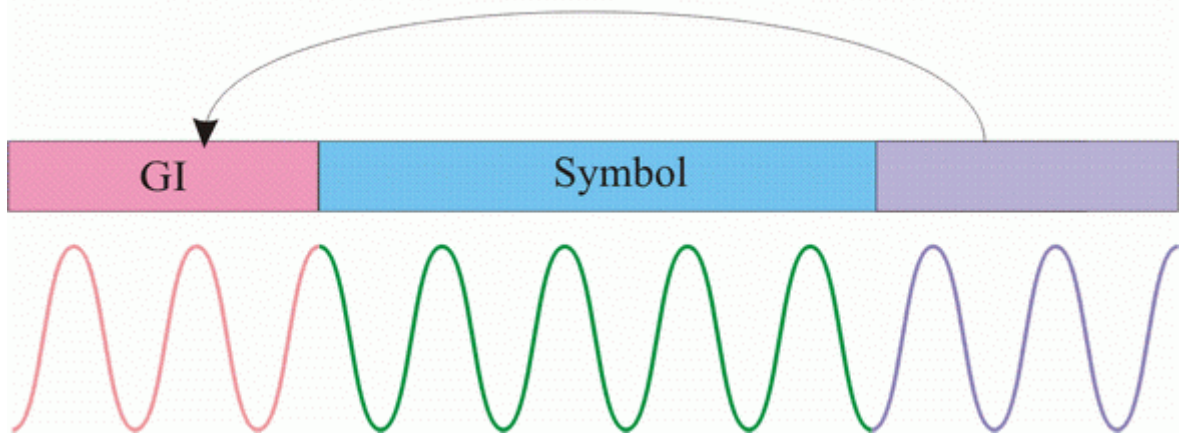


Рис. 26. Охранный интервал, пристраиваемый в начало символа.

Наличие охранного интервала создаёт временные паузы между отдельными символами, и если длительность охранного интервала превышает максимальное время задержки сигнала в результате многолучевого распространения, то межсимвольной интерференции не возникает.

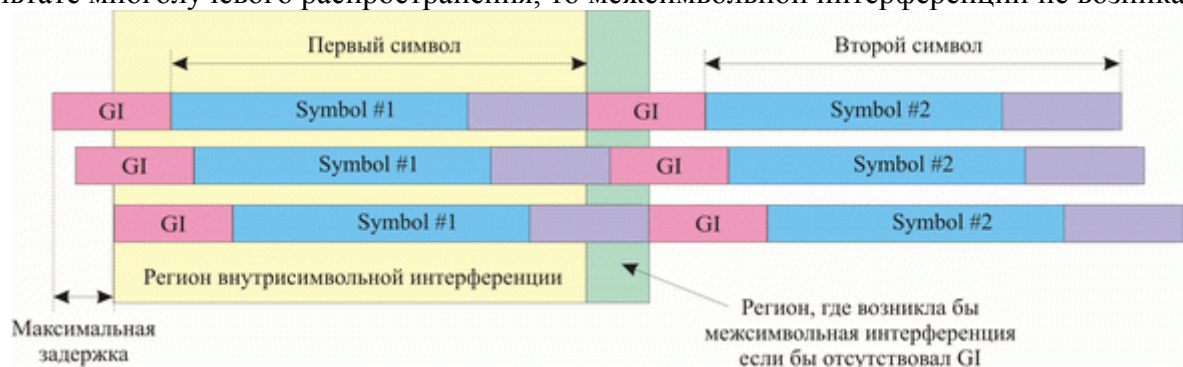


Рис. 27. Охранный интервал препятствует возникновению межсимвольной интерференции.

В протоколе 802.11a длительность охранного интервала составляет одну четвертую длительности самого символа. При этом сам символ имеет длительность 3,2 мкс, а охранный интервал - 0,8 мкс. Таким образом, длительность символа вместе с охранным интервалом составляет 4 мкс.

Говоря о передаче данных в протоколе 802.11a, мы до сих пор не касались вопроса о методе кодирования, позволяющем в одном дискретном состоянии символа закодировать несколько информационных битов. Напомним, что в протоколе 802.11b для кодирования использовалась либо двоичная (BPSK), либо квадратурная (QPSK) относительная фазовая модуляция. В протоколе 802.11a используются те же методы фазовой модуляции (только не дифференциальные), то есть двоичная и квадратурная фазовые модуляции BPSK и QPSK. При использовании BPSK-модуляции в одном символе кодируется только один информационный бит. Соответственно при использовании QPSK-модуляции, то есть когда фаза сигнала может принимать четыре различных значения, в одном символе кодируется два информационных бита.

Модуляция BPSK используется для передачи данных на скоростях 6 и 9 Мбит/с, а модуляция QPSK - на скоростях 12 и 18 Мбит/с.

Для передачи на более высоких скоростях используется квадратурная амплитудная модуляция QAM (Called Quadrature Amplitude Modulation). Данный тип модуляции подразумевает, что информация кодируется не только за счёт изменения фазы сигнала, но и за счёт его амплитуды. В протоколе 802.11a используется модуляция 16-QAM и 64-QAM. В первом случае имеется 16

различных состояний сигнала, что позволяет закодировать 4 бита в одном символе. Во втором случае имеется уже 64 возможных состояния сигнала, что позволяет закодировать последовательность 6 битов в одном символе. Модуляция 16-QAM применяется на скоростях 24 и 36 Мбит/с, а модуляция 64-QAM - на скоростях 48 и 54 Мбит/с.

Естественно возникает вопрос: почему при одном и том же типе модуляции возможны различные скорости передачи? Рассмотрим, к примеру, модуляцию BPSK, при которой скорость передачи данных составляет 6 или 9 Мбит/с. Время длительности одного символа вместе с охранным интервалом составляет 4 мкс. Следовательно, частота следования импульсов составит 250 кГц. Учитывая, что в каждом подканале кодируется по одному биту, а всего таких подканалов 48, получим, что общая скорость передачи составит 250 кГц x 48 каналов = 12 МГц. Однако далеко не все биты, кодируемые в символе, являются информационными. Для того чтобы обеспечить достоверность принимаемых данных, то есть иметь возможность обнаруживать и исправлять ошибки, используют избыточную информацию и так называемое свёрточное кодирование. Суть свёрточного кодирования заключается в том, что к последовательности передаваемых битов добавляются служебные биты, значения которых зависят от нескольких предыдущих переданных битов. Использование свёрточного кодирования в сочетании с алгоритмом Витерби позволяет не только обнаруживать, но и в подавляющем большинстве случаев исправлять ошибки передачи на приёмной стороне.

Не вдаваясь в подробности свёрточного кодирования, скажем лишь, что при скорости свёрточного кодирования 1/2, на каждый информационный бит добавляется один служебный (избыточность равна 2). Именно по этой причине при скорости свёрточного кодирования 1/2 информационная скорость вдвое меньше полной скорости. При скорости свёрточного кодирования 3/4 на каждые три информационных бита добавляется один служебный, поэтому в данном случае полезная (информационная) скорость составляет 3/4 от полной скорости.

Из этого следует, что при использовании одного и того же типа модуляции могут получаться разные значения информационной скорости (табл. 10) - всё зависит от скорости свёрточного кодирования. Так, при использовании BPSK-модуляции со скоростью свёрточного кодирования 1/2 получаем информационную скорость 6 Мбит/с, а при использовании свёрточного кодирования со скоростью 3/4 - 9 Мбит/с. Аналогичным образом каждому типу модуляции соответствуют две различные скорости передачи. При этом подчеркнём, что в самом протоколе 802.11a обязательными являются только скорости 6, 12 и 24 Мбит/с, а все остальные - опциональными.

Таблица 10. Различные скорости в протоколе 802.11a.

Скорость данных, Мбит/с	Тип модуляции	Скорость свёрточного кодирования	Количество битов на символ в одном подканале	Общее количество битов в OFDM-символе (48 подканалов)	Количество битов данных в OFDM-символе
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Стандарт IEEE 802.11g

Если на канальном уровне все беспроводные сети семейства 802.11 имеют одну и ту же архитектуру, то физический уровень для сетей разных стандартов различен. Именно на физическом уровне определяются возможные скорости соединения и методы модуляции и физического кодирования при передаче данных.

Стандарт IEEE 802.11g предусматривает различные скорости соединения: 1; 2; 5,5; 6; 9; 11; 12; 18; 22; 24; 33; 36; 48 и 54 Мбит/с. Одни из них являются обязательными для стандарта, а другие — опциональными. Кроме того, для различных скоростей соединения применяются разные методы модуляции сигнала.

При разработке стандарта 802.11g рассматривались две конкурирующие технологии: метод ортогонального частотного разделения OFDM, заимствованный из стандарта 802.11a и предложенный к рассмотрению компанией Intersil, и метод двоичного пакетного свёрточного кодирования PBCC, опционально реализованный в стандарте 802.11b и предложенный компанией Texas Instruments. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии OFDM и ССК, а опционально предусмотрено использование технологии PBCC.

Прежде чем переходить к рассмотрению методов модуляции, используемых в 802.11g, отметим, что данным стандартом, как и стандартами 802.11b/b+, **предусмотрено применение частотного диапазона от 2,4 до 2,4835 ГГц, который предназначен для безлицензионного использования в промышленности, науке и медицине (Industry, Science and Medicine, ISM)**. Однако, несмотря на возможность безлицензионного применения данного частотного диапазона, **существует жесткое ограничение максимальной мощности передатчика**. Поэтому при выборе способов кодирования и модуляции сигнала необходимо решить две основные проблемы.

С одной стороны, скорость передачи в беспроводной сети должна быть как можно более высокой, чтобы конкурировать с проводными сетями и удовлетворять современным потребностям пользователей. Рост скорости передачи приводит к увеличению ширины спектра, что крайне нежелательно, поскольку частотный диапазон передачи ограничен.

С другой стороны, уровень полезного сигнала должен быть достаточно низким, чтобы не создавать помех другим устройствам в ISM-диапазоне. Таким образом, передаваемый сигнал должен быть едва различим на уровне шума, но в этом случае необходимо разработать алгоритм безошибочного выделения сигнала на уровне шума. Уменьшение мощности передаваемого сигнала достигается за счет использования технологии расширения спектра и «размазывания» сигнала по всему спектру.

Еще одна проблема — это обеспечение должного уровня помехоустойчивости протокола.

К сожалению, одновременное выполнение всех перечисленных условий невозможно, поскольку они противоречат друг другу. Таким образом, выбор конкретного метода кодирования и модуляции сигнала — это поиск золотой середины между требованиями высокой скорости, помехоустойчивости и ограничения по мощности передачи.

Последовательности Баркера. Скорости передачи 1 и 2 Мбит/с

Скорости передачи 1 и 2 Мбит/с, предусмотренные стандартом 802.11g в качестве обязательных скоростей соединения, применяются также и в стандартах 802.11b/b+. Для реализации этих скоростей соединения используются одни и те же технологии модуляции сигнала и расширения спектра DSSS методом прямой последовательности (Direct Sequence Spread Spectrum, DSSS).

Основной принцип технологии расширения спектра (Spread Spectrum, SS) заключается в том, чтобы от узкополосного спектра сигнала, возникающего при обычном потенциальном кодировании, перейти к широкополосному спектру, что позволит значительно повысить помехоустойчивость передаваемых данных.

При потенциальном кодировании информационные биты передаются прямоугольными импульсами напряжений длительности T . При этом ширина спектра сигнала обратно

пропорциональна длительности импульса. Поэтому чем меньше длительность импульса, тем больший спектральный диапазон занимает такой сигнал.

Чтобы повысить помехоустойчивость передаваемого сигнала (то есть увеличить вероятность безошибочного распознавания сигнала на приемной стороне в условиях шума), можно воспользоваться методом перехода к широкополосному сигналу, добавляя избыточность в исходный сигнал. Для этого в каждый передаваемый информационный бит встраивают определенный код, состоящий из последовательности так называемых чипов.

Информационный бит, представляемый прямоугольным импульсом, разбивается на последовательность более мелких импульсов-чипов. В результате спектр сигнала значительно расширяется, поскольку ширину спектра можно с достаточной степенью точности считать обратно пропорциональной длительности одного чипа. Такие кодовые последовательности часто называют шумоподобными кодами. Наряду с расширением спектра сигнала уменьшается и спектральная плотность энергии, так что энергия сигнала как бы размазывается по всему спектру, а результирующий сигнал становится шумоподобным, то есть его трудно отличить от естественного шума.

Возникает вопрос: для чего усложнять первоначальный сигнал, если в результате он становится неотличимым от шума? Дело в том, что кодовые последовательности чипов обладают уникальным свойством автокорреляции. При этом можно подобрать такую последовательность чипов, для которой функция автокорреляции, отражающая степень подобия функции самой себе через определенный временной интервал, будет иметь резко выраженный пик лишь для одного момента времени. Таким образом, функция будет подобна самой себе только для одного момента времени и совсем не похожа на самое себя для всех остальных моментов времени. Одна из наиболее известных таких последовательностей — код Баркера длиной в 11 чипов. Код Баркера обладает наилучшими среди известных псевдослучайных последовательностей свойствами шумоподобности, что и обусловило его широкое применение. Для передачи единичного и нулевого символов сообщения используются соответственно прямая и инверсная последовательности Баркера.

В приемнике полученный сигнал умножается на код Баркера (вычисляется корреляционная функция сигнала), в результате чего он становится узкополосным, поэтому его фильтруют в узкой полосе частот, равной удвоенной скорости передачи. Наоборот: любая помеха, попадающая в полосу исходного широкополосного сигнала, после умножения на код Баркера становится широкополосной, а в узкую информационную полосу попадает лишь часть помехи — по мощности примерно в 11 раз меньшая, чем помеха на входе приемника. Основным смыслом применения кода Баркера заключается в том, чтобы гарантировать высокую степень достоверности принимаемой информации и при этом передавать сигнал практически на уровне помех.

Технология расширения спектра кодами Баркера используется для скорости передачи как 1, так и 2 Мбит/с. Различие этих двух режимов передачи заключается в методах модуляции сигнала.

При передаче данных на **скорости 1 Мбит/с** применяется двоичная относительная фазовая модуляция (Differential Binary Phase Shift Keying, DBPSK).

Напомним, что при фазовой модуляции для передачи логических нулей и единиц используют сигналы одной и той же частоты и амплитуды, но смещенные относительно друг друга по фазе. При относительной фазовой модуляции (также именуемой относительной фазовой манипуляцией) кодирование информации происходит за счет сдвига фазы относительно предыдущего состояния сигнала. При относительной двоичной фазовой модуляции изменение фазы сигнала может принимать всего два значения: 0 и 180°. Например, при передаче логического нуля фаза может не меняться (сдвиг равен 0), а при передаче логической единицы сдвиг фазы составляет 180°.

Учитывая, что ширина спектра прямоугольного импульса обратно пропорциональна его длительности (а точнее, $2/T$), нетрудно посчитать, что при информационной скорости 1 Мбит/с скорость следования отдельных чипов последовательности Баркера составит 11S106 чип/с, а ширина спектра — 22 МГц, так как длительность одного чипа составляет 1/11 мкс.

При передаче данных на **скорости 2 Мбит/с** вместо двоичной относительной фазовой модуляции используется квадратурная относительная фазовая модуляция (Differential

Quadrature Phase Shift Keying, DQPSK). Ее отличие от двоичной относительной фазовой модуляции заключается в том, что изменение фазы может принимать четыре различных значения: 0, 90, 180 и 270°.

Применение четырех возможных значений изменения фазы позволяет закодировать в одном дискретном символе последовательность двух информационных битов (так называемый дибит), поскольку последовательность двух битов может иметь всего четыре различные комбинации: 00, 01, 10 и 11. Но это означает, что ровно в два раза повышается и скорость передачи данных, то есть битовая скорость в два раза выше символьной. Таким образом, при информационной скорости 2 Мбит/с символьная скорость составляет 1С106 символов в секунду. Важно, что скорость следования отдельных чипов последовательности Баркера будет равна, как и прежде, 11С106 чип/с, а ширина спектра сигнала — 22 МГц, то есть столько же, как и при скорости 1 Мбит/с.

Комплементарные ССК-последовательности. Скорости передачи 5,5 и 11 Мбит/с

В стандарте 802.11b/b+, кроме скоростей 1 и 2 Мбит/с, обязательными являются также скорости 5,5 и 11 Мбит/с. Поэтому для обеспечения совместимости эти скорости обязательны и в стандарте 802.11g.

Для работы на таких скоростях используется иной способ расширения спектра. В данном случае вместо шумоподобных последовательностей Баркера применяются комплементарные коды (Complementary Code Keying, ССК). Однако, кроме функции расширения спектра, ССК-последовательности имеют и другое предназначение. В отличие от 11-чиповых последовательностей Баркера, которых существует всего два варианта (прямая и инверсная) для кодирования логического нуля и единицы, вариантов ССК-последовательностей значительно больше (о том, каким образом они образуются, мы расскажем далее). Использование различных ССК-последовательностей позволяет кодировать в одном символе не один бит, а больше, то есть увеличивать информационную скорость передачи. В частности, в стандарте 802.11g применяются 64 различные комплементарные последовательности, что позволяет кодировать 8 бит на один символ при скорости 11 Мбит/с и 4 бит на символ при скорости 5,5 Мбит/с. При этом символьная скорость составляет 1385С106 символов в секунду при информационной скорости как 11Мбит/с, так и 5,5 Мбит/с.

Комплементарными принято называть такие последовательности, для которых сумма их автокорреляционных функций для любого циклического сдвига, отличного от нуля, всегда равна нулю. Последнее обстоятельство позволяет легко выделять эти последовательности на уровне шума, что в значительной степени увеличивает помехоустойчивость при передаче данных.

В стандарте IEEE 802.11b речь идет о 8-чиповых комплексных комплементарных последовательностях, содержащих элементы с четырьмя различными фазами, значения которых определяются последовательностью входных битов.

Элементы 8-чиповой ССК-последовательности образуются по формулам:

$$\begin{cases} c_0 = e^{j(\varphi_1 + \varphi_2 + \varphi_3 + \varphi_4)}, \\ c_1 = e^{j(\varphi_1 + \varphi_3 + \varphi_4)}, \\ c_2 = e^{j(\varphi_1 + \varphi_2 + \varphi_4)}, \\ c_3 = -e^{j(\varphi_1 + \varphi_4)}, \\ c_4 = e^{j(\varphi_1 + \varphi_2 + \varphi_3)}, \\ c_5 = e^{j(\varphi_1 + \varphi_3)}, \\ c_6 = -e^{j(\varphi_1 + \varphi_2)}, \\ c_7 = e^{j\varphi_1}. \end{cases}$$

Значение фазы φ_1 выбирается по первому дибиту, φ_2 — по второму, φ_3 — по третьему и φ_4 — по четвертому. Таким образом, для однозначного определения ССК-последовательности φ требуется 8 бит входных данных. Обратите внимание, что фаза j_1 присутствует во всех членах последовательности. Практически это означает сдвиг по фазе всех членов последовательности на одно и то же значение. По этой причине первый дибит данных задает сдвиг целого символа по фазе по отношению к фазе предыдущего переданного символа.

Для скорости 5,5 Мбит/с в одном символе кодируется 4 бита (два дибита): $\{d_0, d_1, d_2, d_3\}$. Для того чтобы закодировать 4 бита в одном символе, необходимо иметь 16 различных дискретных состояний сигнала, каждое из которых определяется той или иной комплементарной ССК-последовательностью. Поэтому для реализации скорости 5,5 Мбит/с требуется иметь набор из 16 различных комплементарных последовательностей. Такой набор сформировать нетрудно, поскольку сами последовательности являются 8-чиповыми и определяются на множестве комплексных элементов $\{+1, -1, +j, -j\}$, то есть всего можно сформировать 65 536 различных последовательностей. Выбор требуемой последовательности для кодирования символа происходит следующим образом. Поступающий поток битов группируется по два дибита, то есть каждая группа формирует один символ. При этом символы делятся на четные и нечетные, а первый дибит $\{d_0, d_1\}$ задает фазовый сдвиг четных и нечетных символов. Поскольку каждый дибит может принимать четыре различных значения, то и для четных и нечетных символов существуют по четыре возможных сдвига фаз

$\{d_0, d_1\}$	Фазовый сдвиг четных символов	Фазовый сдвиг нечетных символов
00	0	π
01	$\frac{\pi}{2}$	$-\frac{\pi}{2}$
11	π	0
10	$-\frac{\pi}{2}$	$\frac{\pi}{2}$

Таблица 11. Фазовые сдвиги символов, определяемые первым дибитом $\{d_0, d_1\}$.

Следующий дибит $\{d_2, d_3\}$ определяет остальные фазы ССК-последовательности по формулам:

$$\begin{cases} \varphi_2 = d_2\pi + \frac{\pi}{2}, \\ \varphi_3 = 0, \\ \varphi_4 = d_3\pi. \end{cases}$$

Таким образом, для задания ССК-последовательности при кодировании 4 бит/символ используют только 2 бита данных (второй дибит). Этот дибит, принимающий одно из четырех возможных значений, позволяет задать одну из четырех комплементарных ССК-последовательностей. Первый дибит определяет сдвиг по фазе всего символа (причем возможен сдвиг на четыре различных значения) и применяется в относительной фазовой модуляции. Следовательно, набор из четырех возможных комплементарных последовательностей с последующей относительной квадратурной фазовой модуляцией позволяет сформировать 16 дискретных состояний сигнала и закодировать 4 бита в одном символе. Как нетрудно рассчитать, при информационной скорости 5,5 Мбит/с символьная скорость составит $5,5/4 = 1,375$ мегасимволов в секунду. Учитывая, что сами по себе ССК-последовательности являются 8-чиповыми, частота следования отдельных чипов составляет 11 МГц, а ширина спектра сигнала — соответственно 22 МГц.

При скорости 11 Мбит/с в одном символе кодируется одновременно 8 бит данных. При этом первый дибит последовательности данных, как и прежде, задает сдвиг фазы при относительной фазовой модуляции целого символа в зависимости от того, четный он или нечетный, а остальные три дибита 8-битовой последовательности данных определяют оставшиеся фазы, причем значение φ_2 выбирается по второму дибиту, φ_3 — по третьему и φ_4 — по четвертому.

Итак, для задания ССК-последовательности используют только 6 бит данных (второй, третий и четвертый дибиты). А поскольку 6 бит данных могут иметь 64 различные комбинации, то при кодировании каждого символа применяется одна из 64 возможных восьмиразрядных ССК-последовательностей.

$\{d_j, d_{j+1}\}$	Фазовый сдвиг символа
00	0
01	$\frac{\pi}{2}$
10	π
11	$-\frac{\pi}{2}$

Таблица 12. Фазовые сдвиги символа, определяемые вторым, третьим и четвертым дибитами.

Набор из 64 возможных комплементарных последовательностей с последующей относительной квадратурной фазовой модуляцией позволяет сформировать 256 дискретных состояний сигнала и закодировать 8 бит в одном символе. При информационной скорости 11 Мбит/с символьная скорость составит $11/8 = 1.375 \cdot 10^6$ символов в секунду. Учитывая, что сами по себе ССК-последовательности являются 8-чиповыми, частота следования отдельных чипов составляет 11 МГц ($1.375 \text{ МГц} \cdot 8$), а ширина спектр сигнала — 22 МГц.

Двоичное пакетное сверточное кодирование РВСС. Скорости передачи 5,5 и 11 Мбит/с

Кроме комплементарных ССК-последовательностей, в стандарте IEEE 802.11g для скоростей 5,5 и 11 Мбит/с опционально предусмотрено использование технологии двоичного пакетного сверточного кодирования РВСС.

В основе метода РВСС лежит так называемое сверточное кодирование со скоростью 1/2. Сверточное кодирование подразумевает, что входной последовательности битов $\{X_i\}$ ставится в соответствие по определенному алгоритму выходная последовательность битов $\{Y_i\}$, причем значение каждого бита выходной последовательности зависит от значения нескольких битов входной последовательности, то есть для расчета одного бита выходной последовательности учитывается некоторая предыстория входной последовательности.

Для того чтобы значение выходного бита зависело от значений нескольких битов входной последовательности, в сверточном кодере применяются запоминающие ячейки и логические элементы XOR. Кроме того, любой сверточный кодер подразумевает определенную степень избыточности, что повышает помехоустойчивость закодированной информации.

В протоколе 802.11g используются сверточные кодеры, состоящие из шести запоминающих ячеек

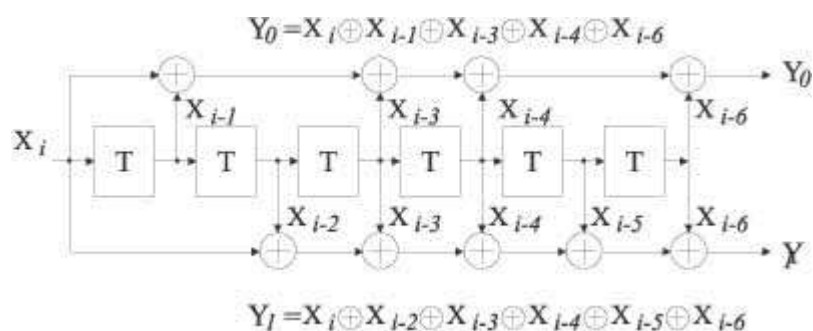


Рис. 28. Схема сверточного кодера ($K=7$); скорость кодирования равна 1/2.

Поэтому всего существует семь различных состояний входного сигнала: текущее и шесть значений, хранящихся в запоминающих ячейках. Такие кодеры называются сверточными кодерами на семь состояний ($K = 7$). Кроме того, каждому входному биту X_0 ставятся в соответствие два выходных бита — Y_0 и Y_1 . Если скорость входной последовательности составляет k бит/с, то скорость выходной последовательности — k дибит/с или $2k$ бит/с. При этом говорят, что скорость кодирования равна 1/2.

Значение каждого формируемого дибита $\{Y_0, Y_1\}$ зависит не только от входящего информационного бита X_0 , но и от шести предыдущих битов, значения которых хранятся в двух запоминающих ячейках.

Главным достоинством сверточных кодеров является помехоустойчивость формируемой ими последовательности. Дело в том, что при избыточности кодирования (вспомним, что каждому информационному биту ставится в соответствие дибит) даже в случае возникновения ошибок приема (к примеру, вместо дибита 11 ошибочно принят дибит 10) исходная последовательность битов может быть безошибочно восстановлена. Для этого на стороне приемника применяется декодер Витерби.

Дибит $\{Y_0, Y_1\}$, формируемый в сверточном кодере, используется в дальнейшем в качестве передаваемого символа, но предварительно он подвергается фазовой модуляции



Рис. 29. Схема PBCC-модулятора.

Если скорость передачи составляет 11 Мбит/с, то применяется квадратичная фазовая модуляция QPSK. В данном случае каждому из четырех возможных состояний дибита соответствует одна из четырех возможных фаз. При этом в каждом символе кодируется по одному входному биту, а скорость передачи битов соответствует скорости передачи символов. Если же скорость передачи составляет 5,5 Мбит/с, то используется двоичная фазовая модуляция BPSK. Каждый бит Y_0 или Y_1 , формируемый сверточным кодером, последовательно подвергается фазовой модуляции. Поскольку каждому входному биту в данном случае соответствуют два выходных символа, скорость передачи битов равна половине скорости передачи символов. Поэтому для скорости и 5,5 и 11 Мбит/с символьная скорость составляет 115106 символов в секунду.

При применении технологии двоичного пакетного сверточного кодирования PBCC необходимо, чтобы ширина спектра передаваемого сигнала оставалась такой же, как и в случае ССК-последовательностей или кодов Баркера, то есть была бы равна 22 МГц. В отличие от технологии DSSS, в этом случае используется не технология расширения спектра, а шумоподобные последовательности, однако и здесь предусмотрено расширение спектра до стандартных 22 МГц. Для этого применяют вариации возможных сигнальных созвездий QPSK и BPSK. Напомним, что сигнальные созвездия представляют собой геометрическое отображение возможных выходных состояний сигнала. Для QPSK-модуляции имеются четыре дискретных состояния сигнала: 00, 01, 10 и 11. Каждому из этих дибитов соответствует одна из четырех возможных фаз несущего сигнала. Понятно, что расположение точек на сигнальном созвездии может быть различным. Именно этот принцип реализован в методе PBCC. Для расширения спектра выходного сигнала используются по два сигнальных созвездия QPSK и BPSK

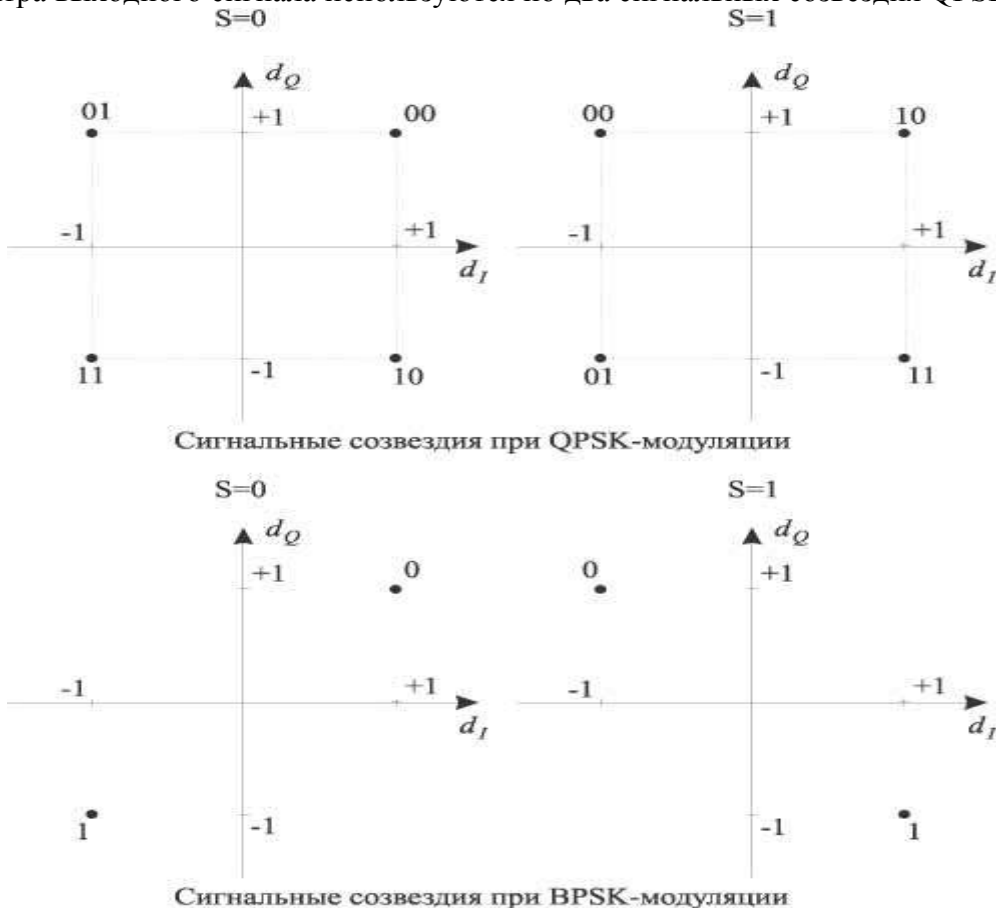


Рис. 30. Возможные типы сигнальных созвездий.

Выбор между конкретным типом применяемого созвездия задается управляющим сигналом S, принимающим значение 0 или 1. Этот сигнал задается псевдослучайной последовательностью с периодом повторения 256 бит, которая формируется из 16-битной базовой последовательности 0011001110001011. Для того чтобы из данной базовой 16-битной последовательности получить 256-битную, используют циклический сдвиг трех первых символов одновременно. Так получают еще пятнадцать 16-битовых последовательностей, что в сумме дает одну 256-битную.

Как уже отмечалось, рассмотренный метод РВСС-кодирования опционально используется как в протоколе 802.11g, так и в протоколе 802.11b/b+ на скоростях 5,5 и 11 Мбит/с.

Пунктурное кодирование. Скорости передачи 22 и 33 Мбит/с

Опционально в протоколе 802.11g технология двоичного пакетного сверточного кодирования РВСС может применяться при скоростях передачи 22 и 33 Мбит/с. Отметим, что скорость 22 Мбит/с при использовании технологии РВСС предусмотрена и в стандарте 802.11b+. При скорости 22 Мбит/с, по сравнению с уже рассмотренной нами схемой РВСС, имеются два отличия. Прежде всего, применяется не квадратичная, а 8-позиционная фазовая модуляция 8-PSK, то есть фаза сигнала может принимать восемь различных значений. Это позволяет в одном символе кодировать уже не два, а три бита и, следовательно, увеличить информационную скорость передачи.

Кроме сверточного кодера в схему добавлен пунктурный кодер (Puncture). Смысл такого решения достаточно прост: избыточность сверточного кодера равная 2 (на каждый входной бит приходится два выходных) достаточно высока и при определенных условиях помеховой обстановки является излишней, поэтому можно уменьшить избыточность, чтобы, к примеру, каждым двум входным битам соответствовали три выходных.

Для этого можно, конечно, разработать соответствующий сверточный кодер, но лучше добавить в схему блок, который будет просто уничтожать лишние биты.

Допустим, что пунктурный кодер удаляет один бит из каждых четырех входных битов. Тогда каждым четверем входящим битам будут соответствовать три выходящих. Скорость такого кодера составляет 4:3.

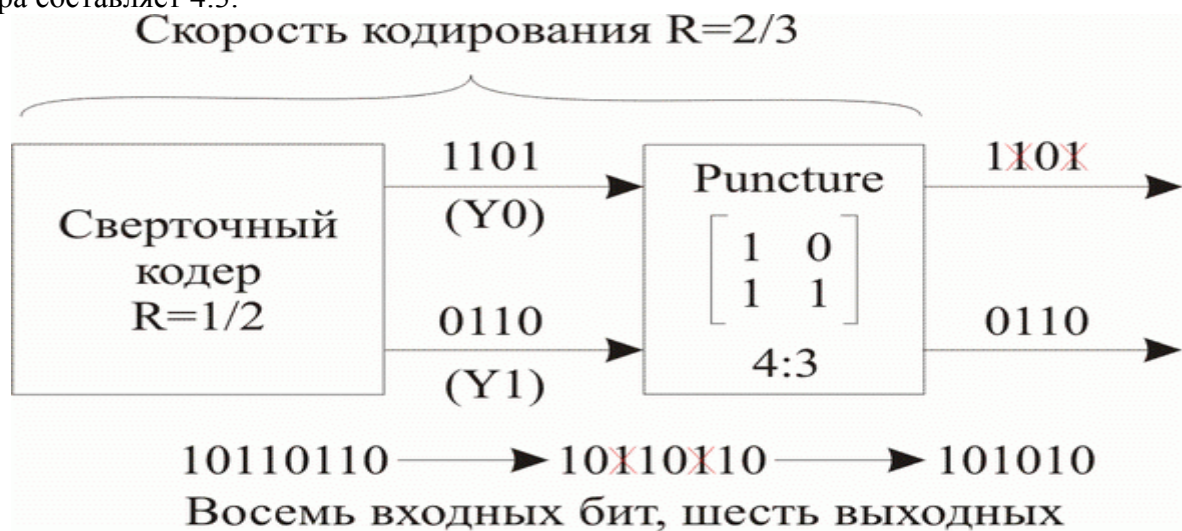


Рис. 31. Принцип работы пунктурного кодера.

Если же такой кодер используется в паре со сверточным кодером со скоростью 1/2, то общая скорость кодирования составляет уже 2/3, то есть каждым двум входным битам будут соответствовать три выходных.

Поняв принцип работы пунктурного кодера, вернемся к рассмотрению кодирования РВСС на скорости 22 Мбит/с в протоколе 802.11g. В сверточный кодер ($K = 7, R = 1/2$) данные поступают со скоростью 22 Мбит/с. После добавления избыточности в сверточном кодере биты со скоростью потока 44 Мбит/с поступают в пунктурный кодер 4:3, в котором избыточность уменьшается так, чтобы на каждые четыре входных бита приходилось три выходных. Следовательно, после пунктурного кодера скорость потока составит уже 33 Мбит/с (не информационная скорость, а общая скорость с учетом добавленных избыточных битов). Полученная в результате последовательность направляется в фазовый модулятор 8-PSK, где

каждые три бита упаковываются в один символ. При этом скорость передачи составит 11S106 символов в секунду, а информационная скорость — 22 Мбит/с

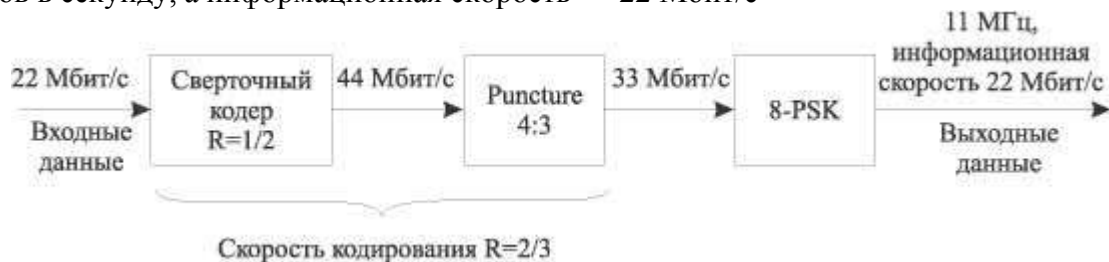


Рис. 32. Схема кодирования при скорости передачи 22 Мбит/с.

Аналогичная технология кодирования предусматривается протоколом 802.11g и на скорости 33 Мбит/с, но для повышения скорости используются увеличение входной скорости данных (до 33 Мбит/с) и еще большее уменьшение избыточности (пунктурный кодер 2:1). В результате при символьной скорости 11S106 символов в секунду информационная скорость составляет 33 Мбит/с.

Ортогональное частотное разделение каналов

При передаче радиосигналов в открытом пространстве неизбежно сталкиваешься с таким паразитным явлением, как многолучевая интерференция. Эффект многолучевой интерференции заключается в том, что в результате многократных отражений один и тот же сигнал может попадать в приемник разными путями. Но различные пути распространения имеют и разные длины, а потому ослабление сигнала для них будет неодинаковым. Следовательно, в точке приема результирующий сигнал представляет собой сумму многих сигналов с различными амплитудами и начальными фазами, что эквивалентно сложению сигналов с разными фазами.

Следствием многолучевой интерференции является искажение принимаемого сигнала. Многолучевая интерференция присуща любому типу сигналов, но особенно негативно она сказывается на широкополосных сигналах. Дело в том, что при использовании широкополосного сигнала в результате интерференции одни частоты складываются синфазно, что приводит к увеличению сигнала, а другие, наоборот, противофазно, вызывая ослабление сигнала на данной частоте.

Говоря о многолучевой интерференции, возникающей при передаче сигналов, различают два крайних случая. В первом случае максимальная задержка между различными сигналами не превышает длительности одного символа и интерференция возникает в пределах одного передаваемого символа. Во втором случае максимальная задержка между различными сигналами больше длительности одного символа, а в результате интерференции складываются сигналы, представляющие разные символы, — так возникает межсимвольная интерференция (Inter Symbol Interference, ISI).

Наиболее сильно на искажении сигнала сказывается межсимвольная интерференция. Поскольку символ — это дискретное состояние сигнала, характеризующееся значениями частоты несущей, амплитуды и фазы, то для различных символов меняются амплитуда и фаза сигнала, поэтому восстановить исходный сигнал крайне сложно.

Чтобы избежать, а точнее, частично компенсировать эффект многолучевого распространения, используются частотные эквалайзеры, однако по мере роста скорости передачи данных либо за счет увеличения символьной скорости, либо за счет усложнения схемы кодирования эффективность их применения падает.

При скорости передачи 11 или 22 Мбит/с в случае использования ССК-кодов или пакетного сверточного кодирования схемы компенсации межсимвольной интерференции вполне успешно справляются с возложенной на них задачей, но при более высоких скоростях такой подход становится неприемлемым. Поэтому для реализации более высоких скоростей передачи в стандарте 802.11g применяется принципиально иной метод кодирования данных, который состоит в том, что поток передаваемых данных распределяется по множеству частотных подканалов и передача ведется параллельно на всех этих подканалах. При этом высокая скорость передачи достигается именно за счет одновременной передачи данных по всем каналам, причем скорость передачи в отдельном подканале может быть и невысокой.

Поскольку в каждом из частотных подканалов скорость передачи данных можно сделать не

слишком высокой, это создает предпосылки для эффективного подавления межсимвольной интерференции.

При частотном разделении каналов необходимо, чтобы ширина каждого канала была, с одной стороны, достаточно узкой для минимизации искажения сигнала в его пределах, а с другой — достаточно широкой для обеспечения требуемой скорости передачи. Кроме того, для экономного использования всей полосы канала, разделяемого на подканалы, желательно как можно плотнее расположить частотные подканалы, но при этом избежать межканальной интерференции, чтобы обеспечить полную независимость каналов друг от друга. Частотные каналы, удовлетворяющие перечисленным требованиям, называются ортогональными. Несущие сигналы всех частотных подканалов (а точнее, функции, описывающие эти сигналы) ортогональны друг другу. Ортогональность несущих сигналов гарантирует частотную независимость каналов друг от друга, а следовательно, отсутствие межканальной интерференции. Рассмотренный способ деления широкополосного канала на ортогональные частотные подканалы называется ортогональным частотным разделением с мультиплексированием (Orthogonal Frequency Division Multiplexing, OFDM). Эта технология была заимствована из стандарта 802.11a. Для ее реализации в передающих устройствах используется обратное быстрое преобразование Фурье (IFFT), переводящее предварительно мультиплексированный на N -каналов сигнал из временного представления в частотное.

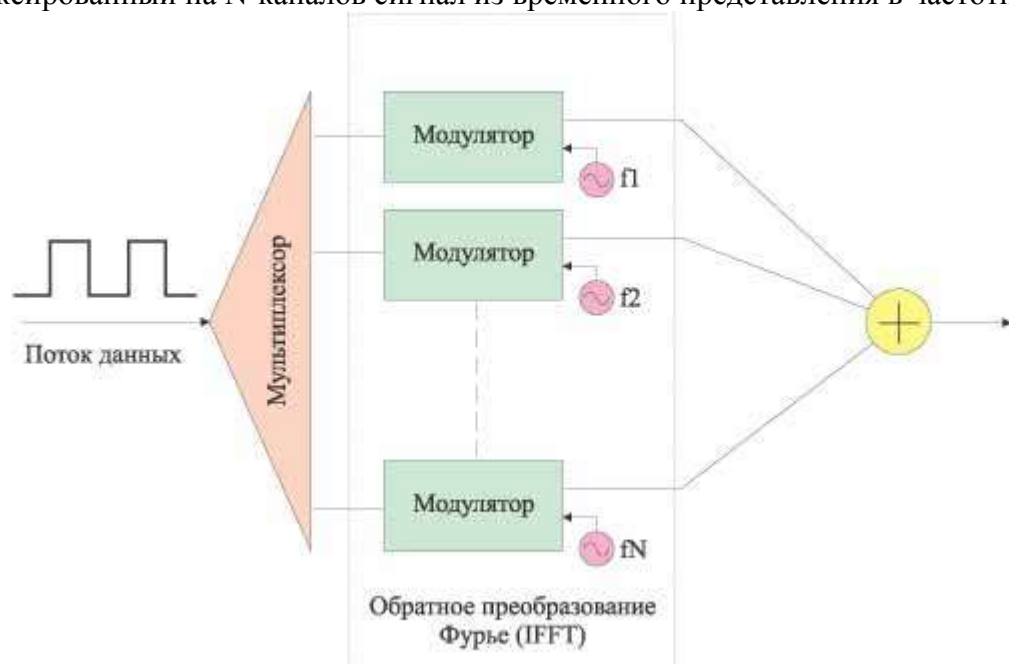


Рис. 33. Реализация ортогонального частотного разделения каналов

Как уже отмечалось, одним из ключевых преимуществ метода OFDM является сочетание высокой скорости передачи с эффективным противостоянием многолучевому распространению. Если точнее, то сама по себе технология OFDM не предотвращает многолучевого распространения, но создает предпосылки для устранения эффекта межсимвольной интерференции. Дело в том, что неотъемлемой частью технологии OFDM является понятие «охранный интервал» (Guard Interval, GI) — это циклическое повторение окончания символа, пристраиваемое в начале символа. Охранный интервал является избыточной информацией и в этом смысле снижает полезную (информационную) скорость передачи. GI добавляется к отсылаемому символу в передатчике и отбрасывается при приеме символа в приемнике, но именно он защищает от возникновения межсимвольной интерференции.

Охранный интервал задает паузы между отдельными символами, и если его длительность превышает максимальное время задержки сигнала в результате многолучевого распространения, то межсимвольной интерференции не возникает.

В стандарте IEEE 802.11g технология ортогонального частотного разделения каналов OFDM является обязательной при скоростях передачи 6, 12 и 24 Мбит/с и опциональной при скоростях передачи 9, 18, 36, 48 и 54 Мбит/с .

Отметим, что в самом стандарте обязательными являются скорости передачи 1; 2; 5,5; 6; 11; 12 и 24 Мбит/с, а более высокие скорости передачи (33, 36, 48 и 54 Мбит/с) - опциональными. Кроме того, одна и та же скорость передачи может реализовываться при различной технике

модуляции. Например, скорость передачи 24 Мбит/с может быть достигнута как при многочастотном кодировании OFDM, так и при гибридной технике кодирования CCK-OFDM (табл. 13).

Таблица 13. Скорости передачи, предусмотренные протоколом 802.11g.

Скорость, Мбит/с	Метод кодирования	
	Обязательно	Опционально
1	Последовательность Баркера	
2	Последовательность Баркера	
5,5	CCK	PBCC
6	OFDM	CCK-OFDM
9		OFDM, CCK-OFDM
11	CCK	PBCC
12	OFDM	CCK-OFDM
18		OFDM, CCK-OFDM
22		PBCC
24	OFDM	CCK-OFDM
33		PBCC
36		OFDM, CCK-OFDM
48		OFDM, CCK-OFDM
54		OFDM, CCK-OFDM

Технология гибридного кодирования CCK-OFDM

Кроме технологии ортогонального частотного разделения каналов OFDM, для опциональных скоростей (6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с) может использоваться также технология гибридного кодирования CCK-OFDM.

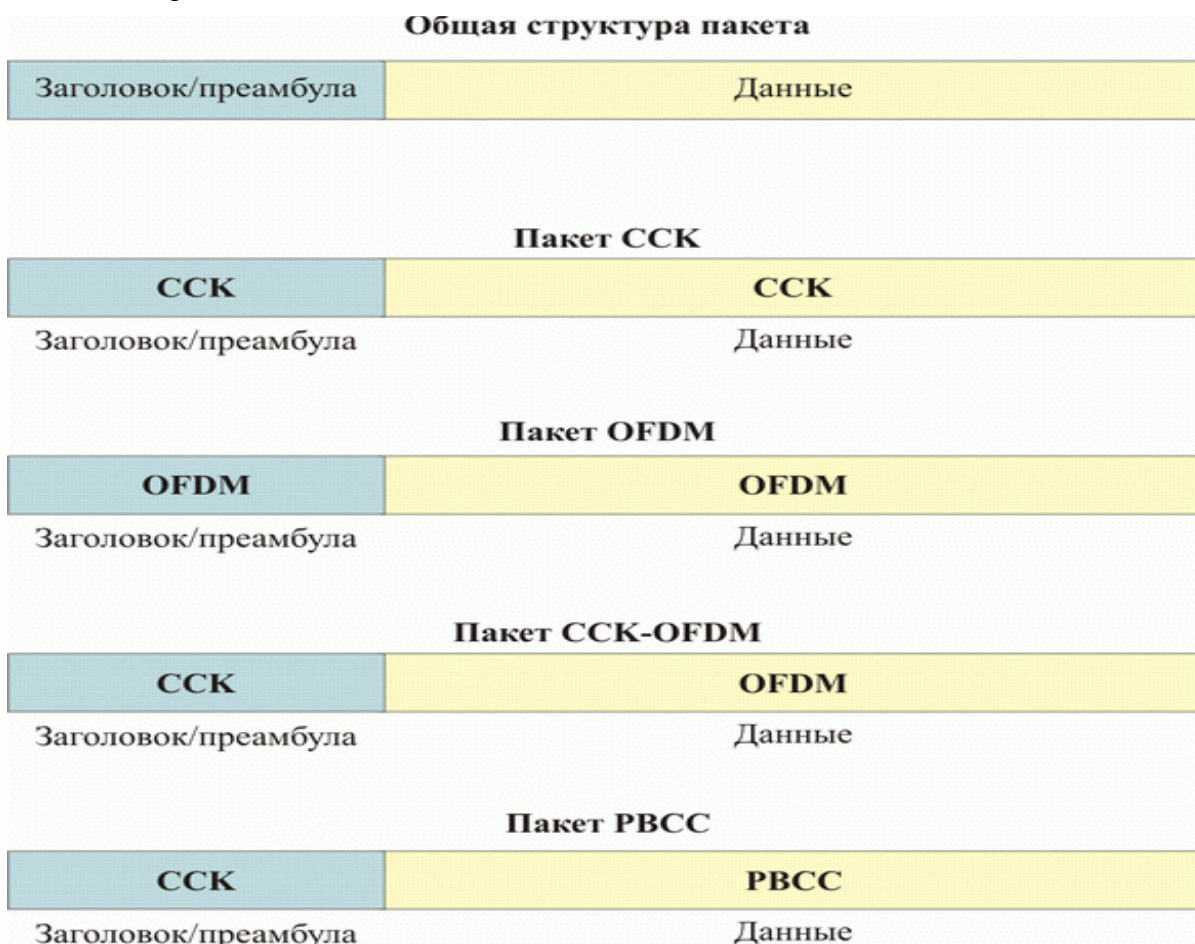


Рис. 34. Форматы кадров при использовании различного кодирования.

Для того чтобы понять сущность этого термина, вспомним, что любой передаваемый пакет данных содержит заголовок/преамбулу со служебной информацией и поле данных. Когда речь идет о пакете в формате ССК, имеется в виду, что заголовок и данные кадра передаются в формате ССК. Аналогично при использовании технологии OFDM заголовок кадра и данные передаются посредством OFDM-кодирования. При применении технологии ССК-OFDM заголовок кадра кодируется с помощью ССК-кодов, но сами данные кадра передаются с использованием многочастотного OFDM-кодирования. Таким образом, технология ССК-OFDM является своеобразным гибридом ССК и OFDM. Технология ССК-OFDM не единственная гибридная технология - при использовании пакетного кодирования РВСС заголовок кадра передаётся с использованием ССК-кодов, только данные кадра кодируются с использованием РВСС (рис 34).

Зона покрытия

Рассматривая особенности стандарта 802.11g, мы до сих пор не касались такой важной характеристики, как радиус действия (зона покрытия) беспроводной сети. Кроме того, было бы логично сравнить IEEE 802.11g с другими популярными стандартами беспроводной связи — IEEE 802.11a и 802.11b/b+.

Говоря о зоне покрытия беспроводной сети, следует учитывать несколько обстоятельств. Во-первых, максимальное расстояние между двумя беспроводными адаптерами в значительной степени зависит от того, есть ли между ними преграды или эти адаптеры находятся в зоне прямой видимости. Радиус действия беспроводной сети зависит также от того, имеется ли в этой сети точка доступа (режим Infrastructure BSS) или же сеть функционирует в режиме Ad Hoc. Далеко не последнюю роль играет и мощность передатчика точки доступа. Поэтому понятие радиуса действия беспроводной сети довольно условно. К тому же, используя несколько точек доступа в режиме Infrastructure ESS, зону покрытия можно неограниченно увеличивать.

Если же говорить о зоне покрытия с одной точкой доступа в идеальных условиях (отсутствие преград и радиочастотных помех), то при сравнении возможностей различных беспроводных стандартов сети стандарта IEEE 802.11g оказываются и более скоростными, и более «дальнобойными», чем сети стандартов IEEE 802.11a и 802.11b/b+. Так, не уступая по своим скоростным характеристикам стандарту IEEE 802.11a, стандарт IEEE 802.11g обеспечивает такую же зону покрытия, как и стандарт IEEE 802.11b.

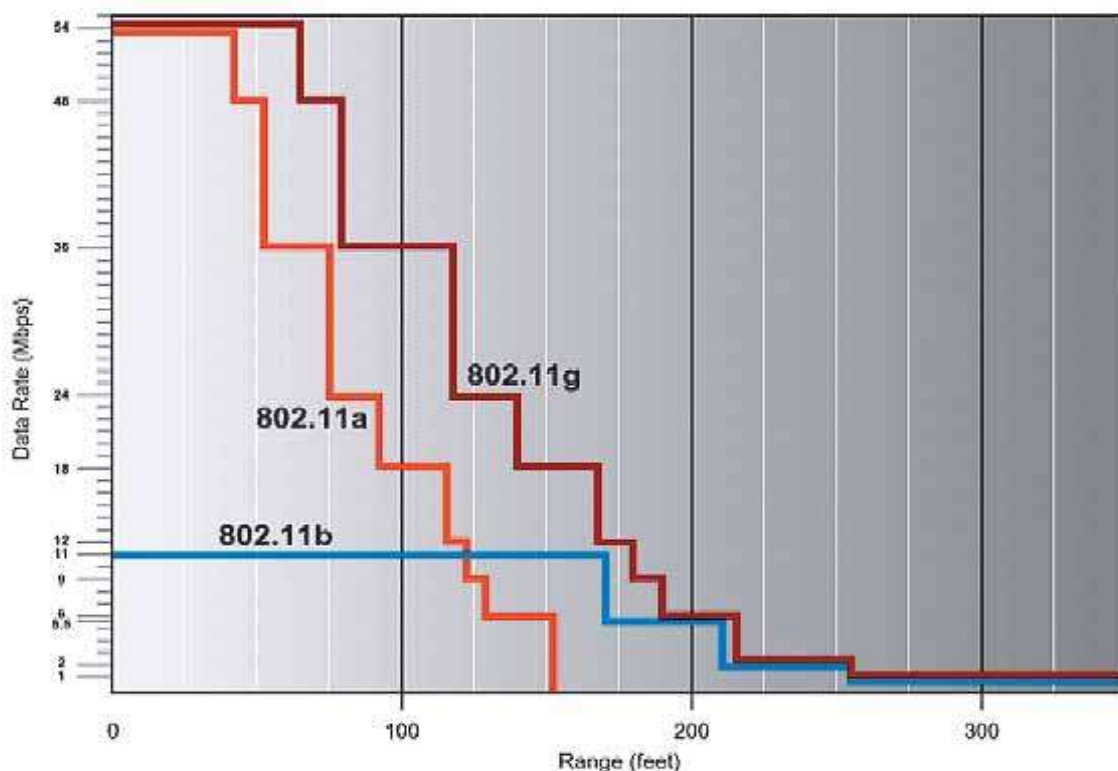


Рис. 35. Сравнение стандартов беспроводной связи по скорости и зоне покрытия.

Если средний радиус сети стандарта IEEE 802.11a составляет 50 м, то радиус действия сетей 802.11b и 802.11g — порядка 100 м.

Стандарт 802.11n: первый взгляд

Институт инженеров по электротехнике и электронике ([IEEE](#)) одобрил создание рабочей группы 802.11n. Целью группы стала разработка нового физического уровня (PHY) и уровня доступа к среде передачи (MAC), которые бы позволили достичь реальной скорости передачи данных, как минимум, 100 Мбит/с. То есть увеличить её в сравнении с существующими сегодня решениями примерно в четыре раза (мы имеем в виду реальную пропускную способность). Всё это, вместе с обратной совместимостью с существующими стандартами, должно будет не только сделать работу в беспроводных сетях более комфортной, но и обеспечить достаточный запас скорости на ближайшее будущее.

Сравнение скорости различных стандартов

Стандарт беспроводной связи	Скорость работы	Реальная скорость передачи данных
802.11b	11 Мбит/с	5 Мбит/с
802.11g	54 Мбит/с	25 Мбит/с
802.11a	54 Мбит/с	25 Мбит/с
802.11n	200+ Мбит/с	100 Мбит/с

Таблица 14. Сравнение скорости различных стандартов

Самое непосредственное участие в разработке и процессе развития стандарта принимает компания [Intel](#), которая возглавила комитет, разрабатывающий основу для реализации стандарта, также в сферу деятельности компании входит разработка уровней MAC и PHY и другие аспекты. Безусловно, Intel сегодня является технологическим лидером в этой области, однако для разработки окончательных спецификаций стандарта необходимы усилия многих компаний.

В разработке стандарта 802.11n Intel предлагает пойти эволюционным путём, используя уже проверенные технологии, добавив к ним новые разработки, позволяющие достичь высоких скоростей передачи данных. Например, в 802.11n предлагается использовать такие "наследственные" технологии, как OFDM (ортогональное частотное мультиплексирование) и QAM (квадратурная амплитудная модуляция). Подобный подход не только обеспечит обратную совместимость, но и снизит стоимость разработки. Перед инженерами стоит нелёгкая задача, ведь новый стандарт не должен мешать работе старых устройств 11a/g, и в то же время он должен поддерживать высокую скорость работы. Многие читатели знакомы со снижением скорости работы сетей 802.11g при одновременном использовании устройств 11b. Надеемся, что в новом стандарте такого не будет.

Увеличение физической скорости передачи

Первый способ увеличения скорости беспроводной передачи данных использует несколько антенн для передатчика и приёмника. Технология называется множественным вводом/выводом MIMO (multiple input multiple output). В случае её использования параллельно передаётся множество сигналов, увеличивая тем самым суммарную пропускную способность. Вообще, у MIMO достаточно много преимуществ из-за одновременной передачи данных по разным каналам. Технология использует мультиплексирование Spatial Division Multiplexing (SDM), то есть сигнал передаётся по нескольким различным частотам, после приёма превращаясь в скоростной поток данных. Однако для реализации MIMO на практике необходимо, чтобы для каждого потока данных использовались свои антенны приёма/передачи, цепи RF и АЦП. В то же время использование более двух антенных цепей RF может привести к значительному повышению стоимости устройства, так что разработчикам придётся искать определённый баланс между скоростью и ценой.

Кроме того, Intel предлагает повысить скорость беспроводной связи, расширив частотные диапазоны каналов. В принципе, идея эта отнюдь не нова. Из теоремы Шеннона следует, что теоретический предел пропускной способности "C" повышается при увеличении частотного диапазона "B" ($C=B \log_2(1+SNR)$).

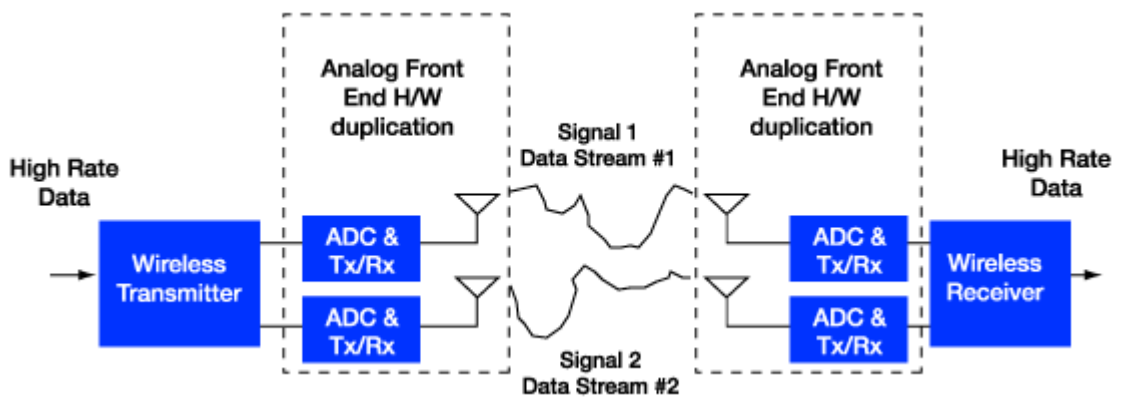


Рис.36 Простейшая система MIMO с двумя антенными цепями. Источник: Intel.

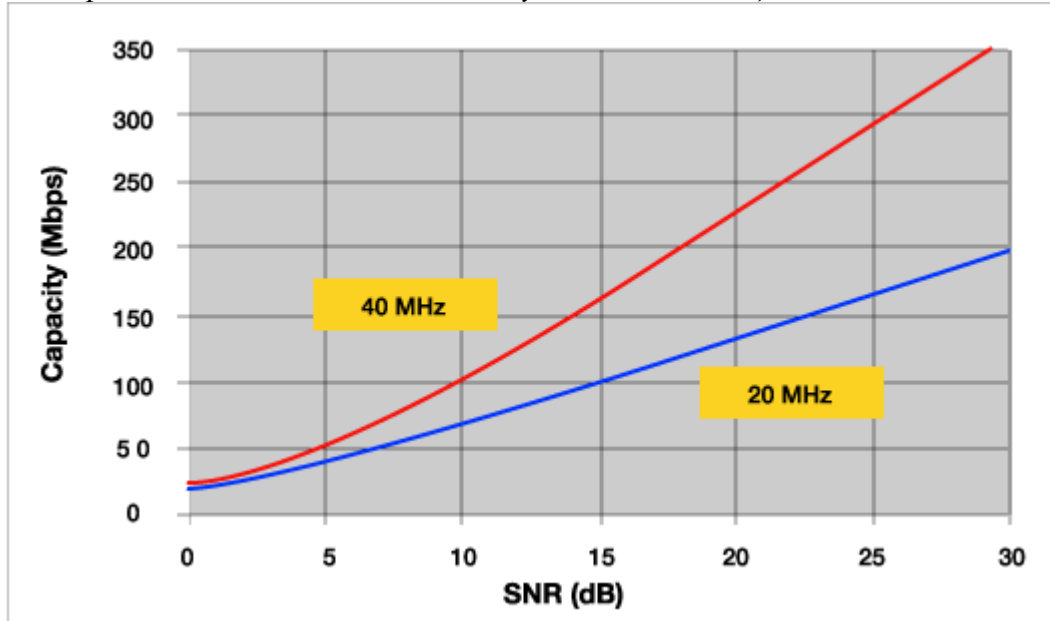


Рис.37 Расширение частотного диапазона приводит к увеличению пропускной способности канала. Источник: Intel.

Расширив частотный диапазон, можно сравнительно недорого и легко увеличить скорость работы сети. При этом нагрузка на ЦСП вырастет незначительно. При хорошей реализации каналы по 40 МГц могут дать более, чем в два раза полезную пропускную способность, чем два канала старых стандартов 802.11 (см. ниже). Добавив к этому MIMO можно создать мощные и недорогие системы с высокой скоростью передачи.

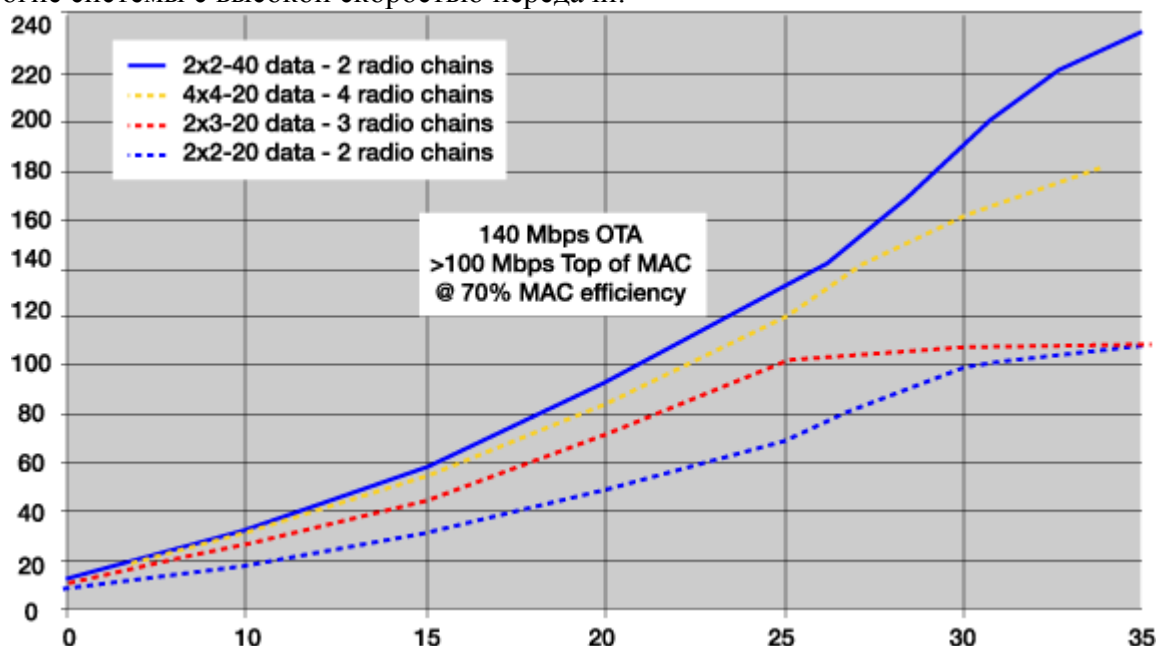


Рис.38 Зависимость теоретической пропускной способности от SNR, числа каналов и диапазонов. Источник: Intel.

Если же использовать MIMO с каналами по 20 МГц, то стоимость такой системы возрастает.

Дело в том, что нужные нам 100 Мбит/с на физическом уровне здесь можно получить только при трёх антенных цепях на передатчике и приёмнике.

На рис.38 приведена зависимость теоретической пропускной способности ОТА от значения SNR, которое измерялось после спаривания каналов. Эффективность уровня MAC составляет 70%, то есть реальные 100 Мбит/с превращаются в теоретические 140 Мбит/с. График позволяет сравнить эффективность работы сетей на 20-МГц и 40-МГц каналах. Расшифровка легенды следующая: "2x2-40 MHz" означает два потока данных, две антенные цепи на приёмнике и передатчике и каналы по 40 МГц.

Как видим, реализация 2x3-20 имеет лучший показатель SNR, чем 2x2-20. Это приведёт к увеличению радиуса действия сети при равной скорости. В то же время график наглядно показывает, что использование двух потоков MIMO 20 МГц не позволяет достичь цели в 100 Мбит/с реальной скорости. Для этого необходимо использовать три потока MIMO, как мы уже говорили выше. Преимущество подхода 2x2-40 здесь очевидно. Обратите внимание, что удвоение числа RF-цепей с каналами по 20 МГц и передача четырёх потоков MIMO даёт меньшую производительность, чем два канала по 40 МГц. Так что переход на 40-МГц каналы позволит не только снизить сложность и стоимость систем, но и повысить производительность.

Intel считает, что совместное использование технологий позволит выполнить требования будущего стандарта 802.11n. Сделав ставку на увеличение используемой полосы частот совместно с технологией MIMO, удастся не только достичь требуемых 100 Мбит/с, но и сохранить при этом низкую стоимость оборудования. Например, использование 40-мегагерцовых каналов и технологии MIMO в будущем позволит даже превзойти требования стандарта по мере развития возможностей ЦСП (вспомним закон Мура). Устройства 802.11n будут поддерживать как 20-, так и 40-МГц каналы, при этом 40-МГц каналы будут образовываться из двух смежных 20-МГц. Таким образом, если частотный спектр будет перегружен или необходимо связаться по старому стандарту, устройство может перейти на узкие 20-МГц каналы. Надеемся, что в момент выхода стандарта законодательные органы примут соответствующие поправки, разрешающие использование 40-мегагерцовых каналов там, где это пока запрещено.

Чтобы получить физическую скорость 100 Мбит/с 802.11n должен поддерживать технологию MIMO не меньше, чем для двух потоков. Для этого потребуется минимум две антенные цепи на каждом устройстве стандарта 802.11n. Опционально устройства смогут поддерживать и большее число потоков MIMO, но не больше четырёх.

Кроме того, в 802.11n могут быть внесены различные опциональные решения, увеличивающие пропускную способность. Сюда относятся увеличение числа антенных цепей, адаптивные каналы и технология кодирования FEC и т.д.

Конечно же, высокую скорость нельзя получить без эффективных механизмов управлением физическим уровнем. Хотя уровень MAC и не влияет напрямую на физическую скорость передачи, он играет важную роль при выборе режимов оптимизации передачи PHY. Первоначально связь будет устанавливаться средствами физического уровня, а уже затем, со временем, подключится MAC-уровень, который определит долговременные параметры связи типа модуляции, кодирования, конфигурации антенн, частотных диапазонов каналов и т.д.

Повышаем эффективность передачи на MAC-уровне

Конечно же, изменения коснутся и MAC-уровня, который получит новые функции. Важно понимать, что скорость передачи существенно ограничивается заголовками PHY и задержками. К сожалению, они плохо поддаются улучшению. Более того, заголовки PHY приходится делать даже больше, чтобы поддержать новые режимы.

В 802.11n будут введён режим передачи нескольких кадров MAC в блок данных физического уровня (агрегация). Также появляются и блочные подтверждения (Block ACK) на запросы нескольких кадров (BAR). Таким образом, теперь не нужно начинать процедуру передачи отдельно для каждого кадра. Если не использовать блочную передачу, то для скорости 100 Мбит/с потребовались бы 500 Мбит/с на уровне PHY.

Блочная передача данных будет работать в обоих направлениях. Что интересно, Intel

предусматривает MAC-кадры нового формата, которые позволят создавать пакеты PHY с информацией сразу для нескольких клиентов.

Совместимость со старыми стандартами 802.11

Рабочая группа IEEE гарантирует обратную совместимость новых устройств 802.11n с оборудованием 802.11a/b/g при условии использования одного и того же частотного диапазона и канала. Другими словами, как мы уже говорили, поддержка 20-мегагерцовых каналов пригодится для обратной совместимости.

Совместимость с существующим оборудованием 802.11a/b/g будет обеспечиваться средствами MAC-уровня. То есть все существующие устройства стандартов 802.11a/b/g смогут подключаться к точкам доступа 802.11n. На уровне MAC также будет обеспечена совместимость схем модуляции для соответствующих частотных диапазонов. Естественно, придётся решить проблемы, возникающие при взаимодействии оборудования различных стандартов.

Спецификации IEEE 802.11

802.11a, 802.11b и 802.11g относятся к физическому уровню среды передачи;

802.11d, 802.11e, 802.11i, 802.11j, 802.11h и 802.11r - к вышележащему MAC-уровню,

802.11f и 802.11c - к более высоким уровням (модель OSI).

Спецификация 802.11d

Стремясь расширить географию распространения сетей стандарта 802.11, IEEE разрабатывает универсальные требования к физическому уровню 802.11 (процедуры формирования каналов, псевдослучайные последовательности частот, дополнительные параметры для MIB и т.д.). Стандарт определял требования к физическим параметрам каналов (мощность излучения и диапазоны частот) и устройств беспроводных сетей с целью обеспечения их соответствия законодательным нормам различных стран.

Спецификация 802.11e

Спецификации разрабатываемого стандарта 802.11e позволяют создавать мультисервисные беспроводные ЛС, ориентированные на различные категории пользователей, как корпоративных так и индивидуальных. При сохранении полной совместимости с уже принятыми стандартами 802.11a и b, он позволит расширить их функциональность за счет поддержки потоковых мультимедиа-данных и гарантированного качества услуг (QoS).

Спецификация 802.11h

Рабочая группа IEEE 802.11h рассматривает возможность дополнения существующих спецификаций 802.11 MAC (уровень доступа к среде передачи) и 802.11a PHY (физический уровень в сетях 802.11a) алгоритмами эффективного выбора частот для офисных и уличных беспроводных сетей, а также средствами управления использованием спектра, контроля за излучаемой мощностью и генерации соответствующих отчетов.

Предполагается, что решение этих задач будет базироваться на использовании протоколов Dynamic Frequency Selection (DFS) и Transmit Power Control (TPC), предложенных Европейским институтом стандартов по телекоммуникациям (ETSI). Указанные протоколы предусматривают динамическое реагирование клиентов беспроводной сети на интерференцию радиосигналов путем перехода на другой канал, снижения мощности либо обоими способами.

Разработка данного стандарта связана с проблемами при использовании 802.11a в Европе, где в диапазоне 5 ГГц работают некоторые системы спутниковой связи. Для предотвращения взаимных помех стандарт 802.11h имеет механизм "квазиинтеллектуального" управления мощностью излучения и выбором несущей частоты передачи.

Спецификация 802.11i

Целью создания данной спецификации является повышение уровня безопасности беспроводных сетей. В ней реализован набор защитных функций при обмене информацией через беспроводные сети - в частности, технология AES (Advanced Encryption Standard) - алгоритм шифрования, поддерживающий ключи длиной 128, 192 и 256 бит. Предусматривается совместимость всех используемых в данное время устройств - в частности, Intel Centrino - с 802.11i-сетями.

Спецификация 802.11j

Спецификация предназначена для Японии и расширяет стандарт 802.11a добавочным каналом 4,9 ГГц.

Спецификация 802.11r

Данный стандарт предусматривает создание универсальной и совместимой системы роуминга для возможности перехода пользователя из зоны действия одной сети в зону действия другой.

Спецификация 802.11f

Спецификация описывает протокол обмена служебной информацией между точками доступа (Inter-Access Point Protocol, IAPP), что необходимо для построения распределенных беспроводных сетей передачи данных.

Спецификация 802.11с

Стандарт, регламентирующий работу беспроводных мостов. Данная спецификация используется производителями беспроводных устройств при разработке точек доступа

Опасны ли для здоровья человека беспроводные сети?

Излучение радиоволн аппаратурой и его влияние на здоровье человека занимает центральное место в обсуждениях, посвященных беспроводным сетям. Авторы этой статьи постарались объяснить, насколько безопасно использование беспроводного оборудования. Здесь вы найдете ответы на часто задаваемые вопросы, касающиеся безопасности беспроводных сетей.

Безопасное маломощное радио

Оборудование беспроводных сетей излучает электромагнитную энергию в радиочастотном диапазоне и функционируют в соответствии с установленными нормами и стандартами безопасности при радиоизлучении, и потому исключается любая возможность причинения вреда здоровью потребителей. Эти стандарты и рекомендации являются результатом обсуждения проблемы научным сообществом и различными научными комиссиями и комитетами.

Стандарты безопасности на радиочастоты

Следующие независимые организации опубликовали рекомендации касательно электромагнитного излучения радиочастотного диапазона.

Комитет координации стандартов № 28 при Институте инженеров электротехники и электроники (IEEE - Institute of Electrical and Electronics Engineers).

Комитет по Национальной Радиологической защите Великобритании - NRPB (National Radiological Protection Boards in the United Kingdom).

Комитет Неионизирующего Излучения при Ассоциации Международной Защиты от Радиации - IRPA/INIRC International Radiation Protection Association's International Non-Ionizing Radiation

Стандарты IEEE/ANSI (ANSI/IEEE C95.1-1992)

В сентябре 1992 года Комитет по Стандартам при IEEE одобрил стандарты IEEE для Уровней Безопасности с учетом воздействия на здоровье человека электромагнитных полей радиочастотного диапазона, 3 кГц до 300 ГГц, IEEE C95.1-1991. Настоящее издание - это переработанные результаты издания Американских Национальных Стандартов для Уровней Безопасности с учетом воздействия на здоровье человека электромагнитных полей радиочастотного диапазона, 3 кГц - 100 ГГц, ANSI C95.1-1982. Настоящие Стандарты IEEE появились в результате обсуждения проблем беспроводных сетей с участием 120 биологов, биофизиков, физиологов, физиков, медиков, инженеров - представителей академий, федеральных агентств, отраслей промышленности и прочих заинтересованных организаций. В ноябре 1992 Институт Американских Национальных Стандартов одобрил Стандарты IEEE C95.1-1991. В документе зафиксировано следующее положение: "предположения об опасности воздействия электромагнитного излучения в пределах частот и коэффициента поглощения, указанных в предыдущих стандартах ANSI включая ANSI C95.1-1982 не подтвердились" - Положение IEEE USAB.

"Измерения показали, что обычное электромагнитное излучение маломощных компактных и мобильных передатчиков и сотовых телефонов не превышает максимально допустимые нормы поглощения энергии, указанные в этом руководстве" [IEEE, ANSI]. Таким образом, основываясь на настоящих данных, излучения маломощных передатчиков считаются безопасными для пользователей (по материалам IEEE USAB о влиянии на человека радиочастотных полей от компактных и мобильных телефонов и прочих коммуникационных устройств, 2 декабря, 1992).

Результатом исследований в этой области стало единое мнение в отношении вопросов безопасности электромагнитного излучения. Результаты исследований нашли отражение в рекомендациях и стандартах, разработанных комиссиями экспертов, такими как научный комитет №53 при NCRP, Комитет координации стандартов № 28 при IEEE, IRPA/INIRC и NRPB. Оборудование изготовлено с учетом этих стандартов и рекомендаций и, соответственно, считается безопасным для здоровья.

Список предметных сокращений

ACK - Acknowledgement Packet – Явно Подтвержденный Пакет

ACL - Access Control List – Список Контроля Доступа

AES - Advanced Encryption Standard – Продвинутый Шифрованный Стандарт

ANSI - American National Standards Institute - Национальный Институт Стандартов США

AP - Access Point – Точка Доступа

BDPSK - Binary Differential Phase Shift Key – Бифазная Дифференциальная Манипуляция

BPSK - Binary Phase Shift Key – Бифазная Манипуляция

BSS - Basic Service Set – Базовая Станция

CCA - Channel Clearance Algorithm – Алгоритм Оценки Чистоты Канала

CCK - Complementary Code Keying

CRC - Cyclic Redundancy Check

CSMA/CD - Carrier Sence Multiple Access with Collision Detection

CSMA/CA - Carrier Sence Multiple Access with Collision Aviodance

DBPSK - Differential Binary Phase Shift Key

DCF - Distributed Coordination Function

DFS - Dynamic Frequency Selection

DPSK - Differential Phase Shift Key

DQPSK – Differential Quadrature Phase Shift Key

DSSS - Direct Sequence Spread Spectrum

ESS - Extended Service Set – Расширенная Станция

ETSI - European Telecommunication Standards Institute – Европейский Институт Телекоммуникационных Стандартов

FCC - Federal Communication Commission – Федеральная Комиссия Связи США

FEC - Forward Error Correction – Прямая Коррекция Ошибок

FHSS - Frequency Hopping Spread Spectrum – Скачкообразное Изменение Частоты сигналов с Полным Спектром

GI - Guard Interval – Охранный Интервал

IAPP - Intel Access Point Protocol – Протокол Доступа к Точке компании ИНТЕЛ

IBSS - Independent Basic Service Set – Автономная Базовая Станция

IEEE - Institute of Electrical and Electronics Engineers – Институт Инженеров Энергетики и Электроники

IFFT - Inverse Fast Fourier Transform - Обратное Быстрое Преобразование Фурье

IRPA/INIR - International Radiation Protection Association's International Non-Ionizing Radiation Committee

ISI - Inter Symbol Interference – Межсимвольный Интерфейс

ISM - Industry, Science and Medicine – Промышленность, Наука и Медицина

LLC - Logical Link Control - Управление логической связью

MAC - Media Access Control – Уровень Доступа к Среде Передачи Данных

Mbps – Megabits-per-second – Мегабит в секунду

MIB - Management Information Base

MIMO - Multiple Input Multiple Output

NIC - Network Interface Card – Карточка(Код) сетевого Интерфейса

NRPB - National Radiological Protection Boards in United Kingdom

OFDM - Orthogonal Frequency Division Multiplexing – Ортогональное Частотное Разделение с Мультиплексированием

OSI/ISO - Reference Model Open System Interconnection- Эталонная Модель Сетевых Взаимодействий

PBCC - Packet Binary Convolutional Coding

PCF - Point Coordination Function

PDA - Personal Digital Assistant – Персональный Цифровой Секретарь

PHY - Physical Layer – Физический Уровень

PSK - Phase Shift Key – Фазовая Манипуляция

QAM - Quadrature Amplitude Modulation Квадратурная Амплитудная Модуляция

QDPSK - Quadrature Differential Phase Shift Key – Квадратурная Дифференциальная Манипуляция

QoS – Quality of Services - Гарантированное Качество Услуг

QPSK - Quadrature Phase Shift Key – Квадратурная Манипуляция

RF Radio Frequency – Высокая Частота

RSSI - Received Signal Strength Indication – Индикация Мощности Принимаемого Сигнала

RTS/CTS - Ready to Send/Clear to Send – сигналы подтверждения Приема/Передачи

SNR - Signal-to-Noise Ration – Отношение Сигнал к Шуму

SS - Spread Spectrum – Полный Спектр

TCP/IP - Transmission Control Protocol/Internet Protocol – ИНТЕРНЕТ Протокол

TPC - Transmit Power Control – Контроль Мощности Передачи

UNIL - Unlicensed National Information Infrastructure – Безлицензионная Инфраструктура

WEP - Wired Equivalent Privacy

WECA - Wireless Ethernet Compatibility Alliance – Альянс Совместимости Беспроводного Ethernet

Wi-Fi - Wireless-Fidelity – Точное Радио

WLAN - Wireless Local Area Network - Беспроводная Сеть

Вт - Ватт

Список использованных источников

<http://www.kunegin.narod.ru/ref7/wifi/index.htm>

<http://www.comptek.ru/wireless/info/health.html>

<http://www.wi-fi.ru/s.php/66.htm>

<http://www.thg.ru/network/20030828/print.html>

<http://www.thg.ru/network/20040902/index.html>

<http://www.astron.com.ua/article/radio/802-11vb/>

<http://www.astron.com.ua/article/radio/802-11va/>

<http://www.ixbt.com/comm/wlan.shtml>

<http://www.compress.ru/Article.asp?id=4483>

<http://www.compress.ru/Article.asp?id=5004>

<http://www.wireless.ru/wireless/108924>

<http://www.wireless.ru/wireless/108921>

http://www.wireless.ru/wireless/wrl_80211e

Сергей Пахомов. Анатомия беспроводных сетей//КомпьютерПресс. 2002.№7. С.167-175