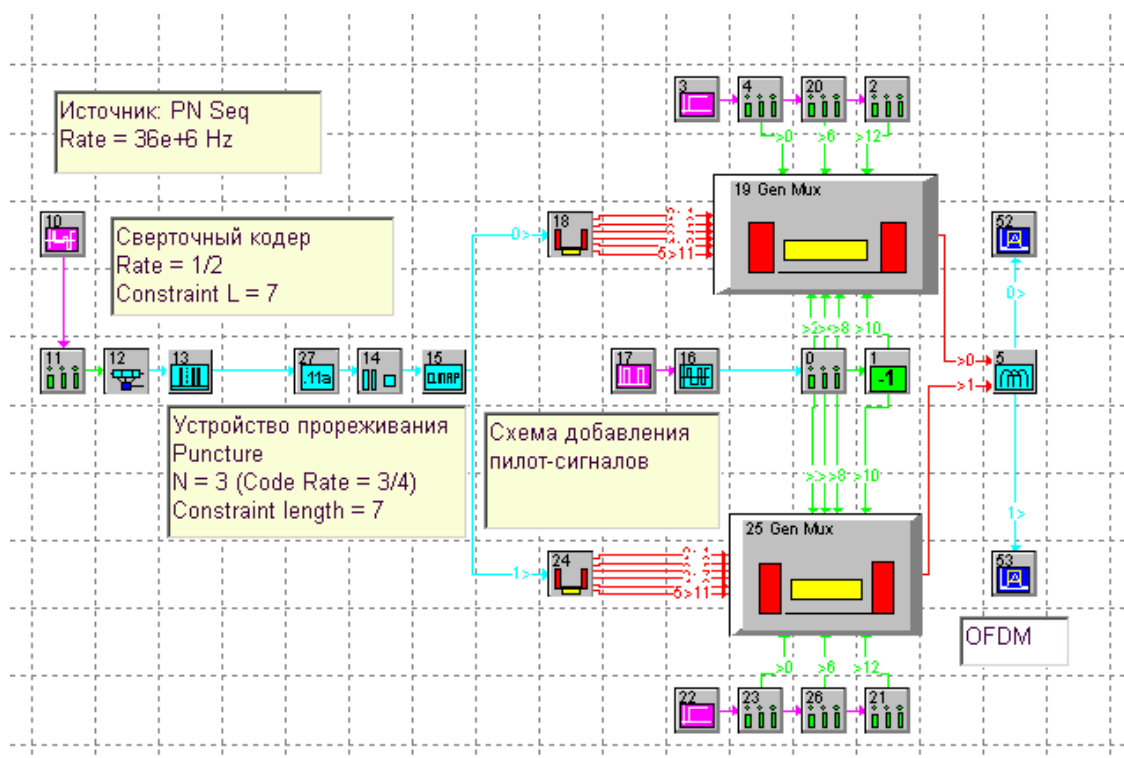


ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ОСНОВЫ ПОСТРОЕНИЯ БЕСПРОВОДНЫХ СЕТЕЙ СТАНДАРТА 802.11

Методические указания к лабораторной работе



УДК 681.3.07

Основы построения беспроводных сетей стандарта 802.11: методические указания к лабораторной работе / Рязан. гос. радиотехн. ун-т; сост.: А.В. Бакке. -Рязань, 2008. -44 с.

Приведены принципы построения и основы функционирования беспроводных сетей стандарта 802.11, рассматриваются вопросы доступа станций 802.11 к каналу связи и способ организации физического уровня спецификации 802.11a. Включены указания по выполнению лабораторной работы «Изучение сигналов физического уровня стандарта 802.11a» курса «Системы и сети связи с подвижными объектами». Описание лабораторной работы содержит сведения о модели физического уровня стандарта 802.11a, разработанной в среде SystemView, рекомендации по подготовке и выполнению лабораторного задания по изучению физического уровня стандарта 802.11a.

Предназначены для студентов дневного отделения специальности 201200 «Средства связи с подвижными объектами».

Табл. 5. Ил. 28. Библиогр.: 5 назв.

Физический уровень, стандарт 802.11, Radio Ethernet, сеть ad hoc, System View, сетевая платформа, MAC-уровень, точка доступа, терминал WiFi

Печатается по решению редакционно-издательского совета Рязанского государственного радиотехнического университета.

Рецензент: кафедра ТОР Рязанского государственного радиотехнического университета (зав. кафедрой проф. В.В. Витязев)

Основы построения беспроводных сетей стандарта 802.11

Составитель Б а к к е Андрей Васильевич

Редактор М.Е. Цветкова

Корректор С.В. Макушина

Подписано в печать .10.11.08. Формат бумаги 60x84 1/16.

Бумага газетная. Печать трафаретная. Усл. печ. л. 2,75.

Уч.-изд. л. 2,75. Тираж 50 экз. Заказ

Рязанский государственный радиотехнический университет.

390005, Рязань, ул. Гагарина, 59/1.

Редакционно-издательский центр РГРТУ.

І. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ О ПОСТРОЕНИИ И ПРИНЦИПАХ ФУНКЦИОНИРОВАНИЯ СЕТИ СТАНДАРТА 802.11

1. Введение

Технологии беспроводных локальных вычислительных сетей (*Wireless Local Area Network, WLAN*) открывают новые возможности перед пользователями локально-вычислительных сетей (ЛВС) - прежде всего, мобильность терминалов и простоту изменения конфигурации сети. В общих чертах сети WLAN обладают следующими преимуществами [1]:

- *гибкость* - узлы сети WLAN могут соединяться друг с другом в области покрытия сети без существенных ограничений, связанных с их расположением;
- *простота планирования* - планирование сети связано с обеспечением заданной зоны уверенного приема и электромагнитной совместимости;
- *возможность создания временных конфигураций сети* - беспроводная связь дает возможность создавать локальные сети, требующиеся на короткий период времени.

Сети WLAN также обладают некоторыми недостатками, большая часть которых обусловлена свойствами распространения сигналов по радиоканалам. К ним относятся [1]:

- *худшее качество передачи данных* по сравнению с обычными проводными ЛВС - вероятность появления ошибок при передаче сигнала по радиоканалу составляет 10^{-3} или даже больше. Для достижения лучшего качества необходимо использовать помехоустойчивое кодирование (FEC) или процедуры повторной передачи ARQ;
- *региональное регулирование использования радиоспектра* - различные страны накладывают ограничения на выделение частотных ресурсов. Это, в свою очередь, накладывает ограничения на всемирные стандарты сетей WLAN;
- *стоимость беспроводного оборудования* существенно выше стоимости аналогичного оборудования для проводных сетей;
- *меньшая конфиденциальность и безопасность*.

2. Конфигурации сетей WLAN

Сеть WLAN может быть сконфигурирована по одной из трех возможных топологий [2,3]:

- независимые базовые зоны обслуживания - как сеть «*ad hoc*» (сеть с отсутствующим централизованным управлением, каждая АС является сетевым узлом) – *independent basic service sets, IBBS* (рис.1, б);
- базовые зоны обслуживания – как основной элемент **структурированной сети** - *basic service set, BSS*;

- расширенные зоны обслуживания - или как **структурированная сеть** - *extended service set, ESS* (рис.1, а).

Под зоной обслуживания (*service set*) подразумевается совокупность логически сгруппированных устройств, имеющих одинаковый идентификатор зоны обслуживания (*service set identifier, SSID*). Каждая передающая станция начинает цикл передачи с идентификатора SSID, а станции-приемники используют это значение для фильтрации получаемых сообщений.

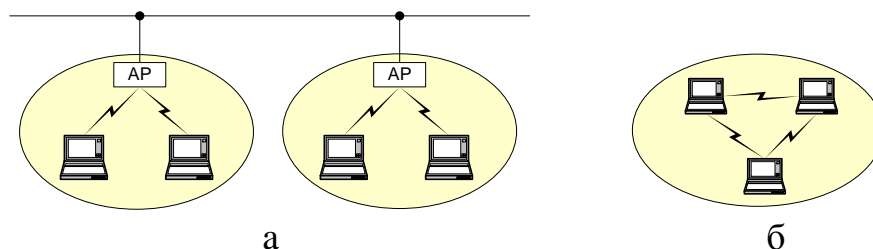


Рис. 1. Конфигурации сетей WLAN:

а - структурированная сеть; б - сеть «ad hoc»

Топология базовой зоны обслуживания **BSS** подразумевает наличие в сети дополнительного стационарного устройства - точки доступа (*Access Point - AP*). В большинстве случаев передача сообщений осуществляется только между точкой доступа и *абонентскими станциями (AC)*, т.е. две AC могут передавать сообщения друг другу только через соответствующую точку доступа. Таким образом, точки доступа выполняют те же функции, что и базовые станции в системах сотовой связи. Точка доступа реализует большинство процедур, связанных с управлением передачей данных и доступом AC к радиоканалу. Такой способ организации сети позволяет упростить управление доступом к сети и избежать коллизий.

Структурированная сеть **ESS** WLAN (рис.1, а) обладает проводной инфраструктурой, соединяющей ее с другими проводными сетями. В этом случае точки доступа обеспечивают взаимодействие мобильных терминалов (AC) друг с другом по радиоканалу через радиointерфейс стандарта 802.11, а также с сетью передачи данных общего пользования по одному из протоколов проводных сетей. Точка доступа в общем случае может быть представлена как беспроводный мост, который подключается через коммутатор к общей сети. Каждая точка доступа обеспечивает радиопокрытие в *базовой зоне обслуживания BSS*, включающей определенный набор станций, объединенных идентификатором зоны обслуживания **SSID**. Радиус зоны обслуживания *BSS* зависит от параметров физического уровня (PHY) точки доступа.

На рис. 2 показано место BSS в архитектуре структурированной сети. Точки доступа AP соединены *распределительной системой (Distribution System - DS)*, в качестве которой, к примеру, может выступать проводная сеть Ethernet. Различные BSS, объединенные одной системой, получают возможность взаимодействовать друг с другом и таким образом формируют *расширенную зону обслуживания ESS*. Распределительная система выступает в роли

магистральной сети и может быть построена на основе любой проводной или беспроводной сети, городской оптоволоконной сети с *распределенным интерфейсом передачи данных по волоконно-оптическим каналам (Fiber Distributed Data Interface - FDD)* или другой сети стандарта IEEE 802.11.

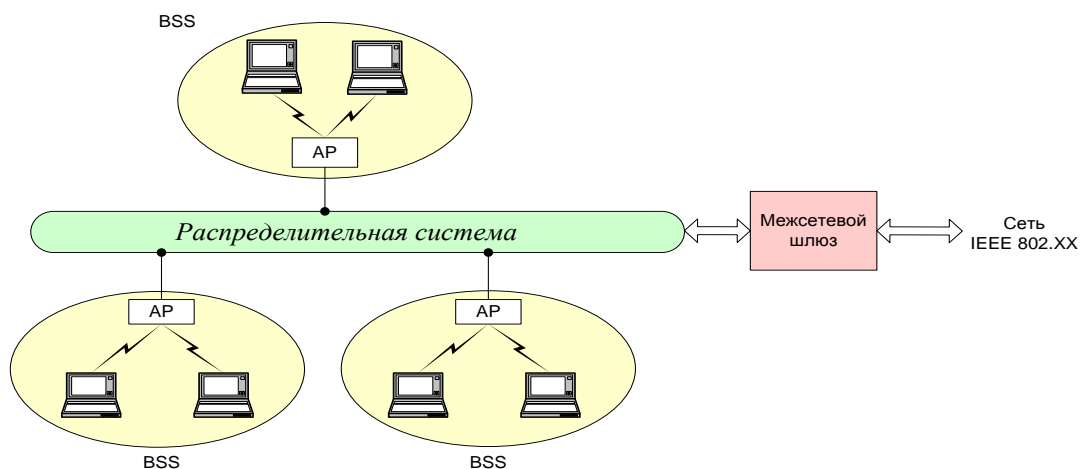


Рис. 2. Архитектура структурированной сети 802.11

Фактически такая сеть (рис. 2) представляет собой набор базовых станций с перекрывающимися зонами охвата. Стандарт IEEE 802.11 допускает перемещения устройств из зоны одной AP в зону другой (роуминг), тем самым обеспечивая мобильность абонентов в пределах расширенной зоны обслуживания ESS.

Однако структурированные сети ESS не обладают гибкостью по причине наличия проводной части. Этот недостаток отсутствует в сетях типа «*ad hoc*» (рис. 1, б).

Беспроводные сети типа **IBBS** «*ad hoc*» не имеют опорной проводной инфраструктуры. Беспроводные терминалы не только соединяют пользователей с сетью, но и выступают в роли сетевых узлов AP. Они могут взаимодействовать между собой все время, пока находятся в зоне взаимной радиодоступности. Концепция сети типа «*ad hoc*» подразумевает наличие технически более сложных терминалов. Здесь АС принимает и отправляет сообщения, а также обеспечивает при этом доступ к сетевым ресурсам с помощью процедур многостанционного доступа, маршрутизацию передаваемых пакетов и назначение их приоритетов.

Поскольку в сети **IBBS** отсутствует AP, координация работы терминалов осуществляется децентрализованно. Терминал, первый начавший передачу в сети, задает сигнальный (маячковый) тактовый интервал (beacon interval), относительно которого строится цикл синхронизации, передачи и получения подтверждения приема. Время действия маячкового интервала ограничено некоторым временем TBTT (*target beacon transmission time*). Когда завершается TBTT, каждый терминал выполняет следующее:

- приостанавливает все активные таймеры задержки из предыдущего интервала ТВТТ (подробнее о таймерах задержки будет сказано далее, п.5.2);
- определяет случайную задержку;
- если маячковый сигнал поступает до окончания случайной задержки, то осуществляет настройку на принятый опорный сигнал и возобновляет работу приостановленных таймеров задержки;
- если никакой маячковый сигнал не поступил до окончания случайной задержки, то терминал начинает передавать маячковый сигнал в соответствии со своей временной шкалой и возобновляет работу приостановленных таймеров задержки.

Маячковые сигналы выполняют важную функцию синхронизации опорного тактового генератора терминала. Каждая АС сравнивает принятый синхросигнал с собственным опорным и, если обнаруживается факт запаздывания «собственных часов» тактового генератора, то осуществляется его подстройка под принятую последовательность. Такой механизм подстройки собственной шкалы времени имеет долговременный эффект синхронизации работы всей сети по терминалу с самым «быстрым» тактовым генератором (таймером) [2-4].

3. Проблема скрытой станции

Беспроводная передача данных в сетях WLAN может быть связана с некоторыми проблемами, если зоны радиопокрытия различных частей сети WLAN частично перекрываются (рис. 3).

Станция *B* находится в зоне досягаемости станций *A* и *C* (рис. 3, а), однако расстояние между станциями *A* и *C* настолько велико, что ни одна из них не попадает в зону покрытия другой и не в состоянии определить, производит ли передачу другая.

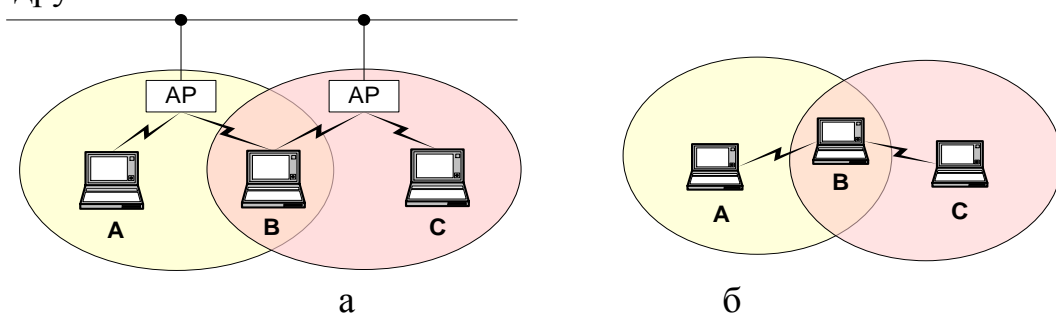


Рис. 3. Иллюстрация проблемы скрытой станции:
а – в сетях «ad hoc»; б – в структурированных сетях

Станция *A* выполняет передачу данных станции *B*, станция *C*, используя метод многостанционного доступа с контролем несущей и обнаружением коллизий *CSMA/CD* (*Carrier Sense Multiple Access with Collision Detection, CSMA/CD*), определяет, что радиоканал свободен, после чего также начинает

передавать данные станции *B*. Таким образом, возникает коллизия. Обе станции передают пакеты данных на станцию *B* до их завершения, не зная, что эти пакеты не могут быть корректно приняты. Как следствие коллизии - потеря времени передачи всего пакета обеими станциями. В таких случаях считают, что станция *C* *скрыта* для станции *A*. Аналогичная ситуация возможна и для структурированных сетей WLAN (рис. 3, б). Если две точки доступа попытаются одновременно передать данные станции, расположенной в зонах радиодоступности обеих, и при этом их действия не будут скоординированы проводной частью сети, то возникнет такая же конфликтная ситуация, что и в первом случае.

Проблема скрытой станции может быть частично решена, если обеспечить радиус обнаружения сигнала, существенно превышающий размеры зоны радиодоступа, в которой на данном канале гарантируется уверенная радиосвязь (рис. 4, а). Такой метод используется в Hiper LAN 1 [2]. Другой способ заключается в использовании метода многостанционного доступа с предотвращением коллизий (*Multiple Access with Collision Avoidance, MACA*). Схема реализации *MACA* приведена на рис. 4,б. Прежде чем начать передачу данных станции *B*, станция *A* передает пакет **RTS** (*Request To Send* - *запрос на передачу*). Пакет **RTS** содержит адреса передающей и принимающей станций, а также сведения о длительности предполагаемой передачи данных. Станция *B* в ответ посылает станции *A* пакет **CTS** (*Clear To Send* - «*готов к твоей передаче*»), который получает и станция *C*. Пакет **CTS** содержит адреса отправителя, получателя и длительность передачи, поэтому получившая извещение станция *C* не будет пытаться получить доступ к занятому каналу до истечения указанного времени. Конфликт может произойти только в случае, если станции *C* и *B* одновременно отправят пакеты **RTS**; однако эти пакеты намного короче, и время коллизии будет существенно меньше. Такой способ решения проблемы скрытой станции может опционально использоваться в беспроводных сетях на основе стандарта IEEE 802.11 (п. 5.2.4).

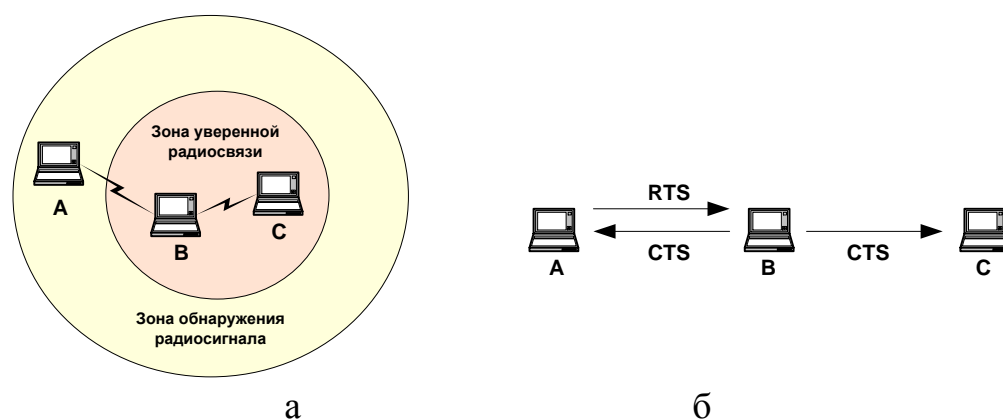


Рис. 4. Решения проблемы скрытой станции

Проблема скрытой станции намного проще решается в случае применения на физическом уровне технологий расширения спектра. Достаточно того, что передающие станции будут использовать свои псевдослучайные сигналы (используя методы прямой последовательности **DSSS** или скачкообразной перестройки частоты **FHSS**). Поскольку подобные сигналы будут взаимно практически ортогональны, это позволит принимающей станции выделить любой из них с помощью согласованной фильтрации.

4. Стандарты IEEE 802.11 для сетей WLAN

Концепция сети **Ethernet** (*Ether net* – эфирная сеть) была впервые введена фирмой Xerox в 1973 г. и отражала основные принципы работы новой локальной компьютерной сети, позднее воплощенной в стандарте 802.3 (**Ethernet**).

Работы над единым стандартом беспроводных локальных вычислительных сетей **WLAN** (*Wireless Local Area Network*) начались значительно позднее – в 1989 г. по инициативе IEEE (Институт инженеров электротехники и радиоэлектроники США) с целью создания беспроводного расширения существующих стандартов ЛВС 802 серии. С этой целью была образована рабочая группа 11-го комитета IEEE 802, основной задачей которой являлась разработка архитектуры беспроводных сетей WLAN и спецификаций канального и физического уровней, обеспечивающих скорости передачи данных в канале 1 Мбит/с и выше.

В июле 1997 г. в результате работы этой группы был опубликован стандарт IEEE 802.11 «Спецификация физического уровня и уровня контроля доступа к каналу передачи беспроводных локальных сетей» (*Wireless LAN Medium Access Control and Physical Layer Specifications*). Он определял архитектуру сети и требования к функциям устройств, принципы доступа устройств к каналам связи, формат пакетов передачи, способы аутентификации и защиты данных. На физическом уровне в стандарте определялись три способа работы: два радиочастотных и оптический. В инфракрасном диапазоне предусматривалась импульсно-позиционная модуляция, в диапазоне 2,400-2,4835 ГГц - режимы модуляции с расширением спектра методом частотных скачков (*Frequency Hopping Spread Spectrum*, FHSS) и методом прямой последовательности (*Direct Sequence Spread Spectrum* - DSSS). Скорости обмена устанавливались на уровне 1 и 2 Мбит/с [3]. В окончательном виде стандарт стал известен под названием **Radio Ethernet**.

В связи с резким увеличением пропускной способности проводных сетей Ethernet к моменту опубликования стандарта максимальная скорость передачи 2 Мбит/с, предусмотренная в IEEE 802.11 (**Radio Ethernet**), не удовлетворяла требованиям пользователей. Проблема была решена разработкой стандартов (дополнений) IEEE 802.11b, 802.11a и 802.11g.

Первым стал утвержденный 16 сентября 1999 г. стандарт **IEEE 802.11b**. Он описывал физический уровень и уровень контроля доступа к каналу передачи данных (*Medium Access Control, MAC*) беспроводных сетей для работы в диапазоне 2,4 ГГц. Стандарт определял работу на скоростях 1 и 2 Мбит/с с модуляцией только методом DSSS и предусматривал скорости обмена до 11 Мбит/с (опционально 33 Мбит/с). Передача данных на скоростях 5,5 и 11 Мбит/с реализовывалась посредством модуляции комплементарных кодовых последовательностей (*Complementary Code Keying, CCK*), а работа на скоростях 22 и 33 Мбит/с осуществлялась посредством пакетного бинарного сверточного кодирования (*Packet Binary Convolutional Coding, PBCC*).

Стандарт 802.11a, регламентирующий работу WLAN в диапазоне 5 ГГц, был принят одновременно с 802.11b. В нем использован принципиально иной, чем в 802.11b, способ организации физического уровня, основанный на использовании частотного мультиплексирования посредством ортогональных несущих (OFDM). В конце 1999 г. были закончены основные работы по созданию европейского 5-ГГц стандарта беспроводных сетей **HiperLan2** (*HiperLan type 2*), который так и не получил массового развития. В июне 2003 г. был утвержден высокоскоростной (до 54 Мбит/с) стандарт в диапазоне 2,4 ГГц - IEEE 802.11g.

В настоящее время завершена работа по созданию стандарта IEEE 802.11n, определяющего способ организации сети со скоростью обмена свыше 100 Мбит/с на основе технологии антенных систем (*Multiple Output Multiple Input, MIMO*), а также разработано дополнение **802.11e**, предназначенное для предоставления гарантированного качества связи (QoS).

5. Стандарт IEEE 802.11

Оборудование **Radio Ethernet**, несмотря на ряд недостатков (относительно невысокая скорость передачи информации - до 2 Мбит/с, малая емкость частотного диапазона, значительные потери пропускной способности из-за несовершенства протоколов множественного доступа), оказалось очень удачным и получило широкое распространение.

В стандарте IEEE 802.11 [4, 5] как базовом для всех последующих спецификаций рассматриваются два нижних уровня модели взаимодействия открытых систем (*Open System Interconnection - OSI*): физический (PHY) и канальный (*Data Link Control - DLC*). Канальный уровень **DLC** (рис. 5) подразделяется на два подуровня: верхний - Logical Link Control (**LLC**) и нижний подуровень - Medium Access Control (**MAC**) - управление доступом к каналу связи. На уровне PHY определяются способы работы со средой передачи, скорость и методы модуляции; на MAC-уровне - принцип, по которому устройства используют общий для всех канал, способы подключения устройств к точкам доступа и их аутентификации, механизмы защиты данных. Поскольку стандарт 802.11 разрабатывался как «беспроводной Ethernet», он

предусматривает пакетную передачу с 48-битными адресами пакетов, как и любая сеть Ethernet.

В соответствии со спецификацией IEEE 802.11 на физическом уровне РНУ стандартизованы три различных метода передачи данных. В двух из них используется диапазон ISM (*Industrial, Scientific and Medical* - промышленный, научный и медицинский) - **2,4...2,4835 ГГц**. С некоторыми ограничениями он доступен во всем мире. В третьем - реализуется технология передачи данных в инфракрасном (*Infrared* - *IR*) диапазоне. Все эти методы работают с одним и тем же MAC-уровнем, так как высокие уровни модели одинаковы для всех сетей 802 серии (рис. 5).

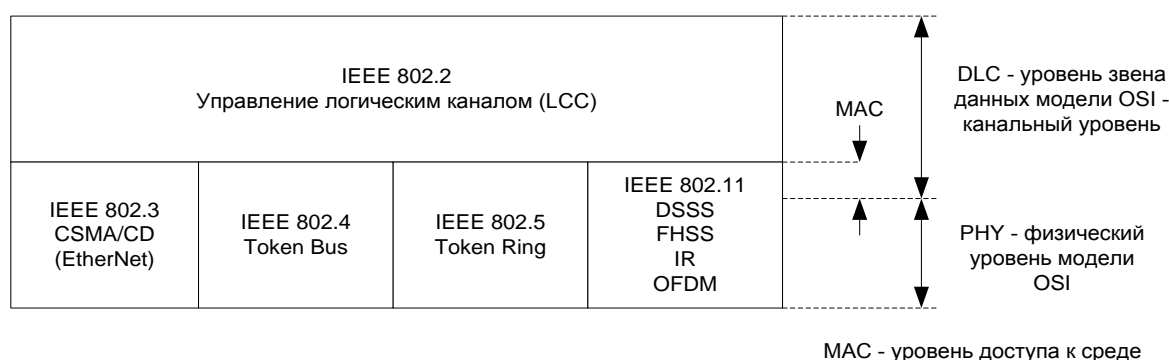


Рис. 5. Семейство стандартов IEEE 802

Физический уровень стандарта 802.11 разделен на два подуровня (рис.6). Нижний называется подуровнем, *зависимым от физической среды* (*Physical Medium Dependent* - **PMD**). Он определяет правила организации физического канала и включает в себя все стадии передачи сигнала, включая кодирование и модуляцию. Второй - *подуровень обеспечения сходимости физического уровня* (*Physical Layer Convergence Procedure* - **PLCP**). Его первая задача - отображение блоков данных подуровня MAC (**MPDU**) в пакеты, используемые на подуровне PMD. Вторая задача подуровня - контроль состояния физического канала с передачей информации о нем на MAC-уровень.

На уровне MAC реализован механизм предоставления доступа на основе метода CSMA (п.5.2), а также фрагментация и шифрование пакетов данных.

Уровень звена данных	Подуровень управления доступом к среде (MAC)	Управление MAC-подуровнем	Управление станцией
Физический уровень	Подуровень обеспечения сходимости физического уровня (PLCP)	Управление физическим подуровнем	
	Подуровень, зависимый от физической среды (PMD)		

Рис. 6. Эталонная модель взаимодействия IEEE 802.11

Физические подуровни контролируются блоком управления физическим уровнем. Этот блок использует базу данных с информацией о физическом уровне и управляет адаптацией физического уровня к различным условиям соединений. Подуровень MAC также имеет свой блок управления, который отвечает за синхронизацию, регулировку мощности и управления процедурами присоединения к сети и разъединения.

С целью обеспечения безопасности передачи данных на MAC-уровне предусмотрен механизм защиты данных, включающий аутентификацию станций и собственно шифрование передаваемых данных. Этот механизм должен обеспечивать такой же уровень защиты, как и в обычных сетях Ethernet (*Wired Equivalent Privacy* - **WEP**). Алгоритм WEP основан на использовании четырех общих для одной сети секретных ключей длиной 40 бит. Само шифрование происходит по алгоритму *RC4* компании RSA Security. Алгоритм использует умножение блоков исходных данных на псевдослучайную последовательность такой же длины, что и блок шифруемых данных. Генератор псевдослучайной последовательности инициализируется 64-разрядным числом, состоящим из 24-разрядного вектора инициализации (*initialization vector* - **Iv**) и 40-разрядного секретного ключа. Секретный ключ известен устройствам сети и неизменен, а вектор **Iv** может изменяться от пакета к пакету. Для защиты от несанкционированного изменения передаваемой информации каждый зашифрованный пакет защищается 32-разрядной контрольной суммой (*integrity check value* - **ICV**). Таким образом, при шифровании к передаваемым данным добавляется 8 байт: 4 для **ICV**, 3 для **Iv**, и еще 1 байт содержит информацию о номере используемого секретного ключа (одного из четырех). Дополнительные методы защиты информации и аутентификации в сетях 802.11 описаны в стандарте IEEE 802.11i.

5.1. Физический уровень IEEE 802.11

В базовой версии стандарта IEEE 802.11 предусмотрено три различных варианта реализации физического уровня **PLCP** [5]. В каждом из трех вариантов пересылаемый по каналу пакет состоит из трех частей - преамбулы **PLCP**, заголовка **PLCP** и данных **MPDU**; при этом в каждом радиointерфейсе используются свои преамбула и заголовки. Базовая скорость передачи данных во всех радиointерфейсах составляет 1 Мбит/с. Допускается передача данных со скоростью до 2 Мбит/с.

5.1.1. Физический уровень DSSS

На физическом уровне этого типа используется технология DSSS (*расширение спектра методом прямой последовательности, Direct Sequence Spread Spectrum*). В технологии DSSS каждый закодированный информационный бит

представляется в виде некоторой расширяющей последовательности. В DSSS-интерфейсе сетей стандарта IEEE 802.11 в качестве расширяющей последовательности используется 11-элементный код Баркера. Таким образом, исходный поток битов, следующих со скоростью 1 Мбит/с, преобразуется в поток символов, имеющих скорость 11 Мбит/с. После модуляции DBPSK или DQPSK ширина спектра сигнала будет составлять приблизительно 22 МГц. Для того чтобы разместить частично перекрывающиеся зоны BSS, их центральные частоты таким образом должны быть разнесены на 30 МГц. Максимальная мощность на передачу ограничена значениями 1 Вт в США и 100 мВт в Европе.

В 1998 г. рабочая группа IEEE 802.11 представила расширение физического уровня, которое позволяет передавать пакеты данных со скоростью 11 Мбит/с или резервной скоростью 5,5 Мбит/с, причем изменения не затронули символьную скорость расширяющей последовательности и ширину спектра стандартизированного ранее канала DSSS. Вместо 11-элементного кода Баркера, используемого совместно с DBPSK или DQPSK модуляцией, в пакетах данных **MPDU** используется *ССК-модуляция* (комплементарная кодовая манипуляция, *Complementary Code Keying, CCK*).

В DSSS-версии физического уровня радиointерфейс 802.11 обеспечивает высокую скорость передачи данных и большую дальность связи системы, однако оборудование DSSS характеризуется большей стоимостью и энергоемкостью, чем оборудование FSSS.

5.1.2. Физический уровень FHSS

Физический интерфейс FHSS (*расширение спектра со скачкообразной перестройкой частоты, Frequency Hopping Spread Spectrum*) характеризуется хорошей устойчивостью к искажениям, высокой емкостью системы, низким энергопотреблением, средней дальностью связи и небольшой стоимостью радиочастотного оборудования [2]. Система FHSS функционирует в ISM-диапазоне. В США и Европе для нее было выделено 79 частот с шагом 1 МГц. В Японии было выделено 23 частоты. Как и в случае DSSS, максимальная мощность на передачу ограничена значениями 1 Вт в США и 100 мВт в Европе. Передача данных производится с применением GFSK-модуляции на несущих из выделенного набора частот в соответствии со схемой скачкообразной перестройки частоты. Для базовой скорости 1 Мбит/с используется двухуровневая GFSK-модуляция, для 2 Мбит/с - четырехуровневая. Ширина спектра радиосигнала составляет 1 МГц. Скачки по частоте должны происходить с определенной скоростью: как правило, минимальная скорость перестройки частоты составляет 2,5 скачка в секунду. Скорость перестройки частоты задается точкой доступа AP. Подвижный терминал определяет скорость перестройки частоты в процессе установления соединения с конкретной точкой доступа. Схемы перестройки частоты выбираются таким образом, чтобы минимизировать использование одинаковых частотных каналов в смежных зонах BSS.

5.1.3. Физический уровень инфракрасного диапазона

В третьем типе физического уровня стандартизована передача данных в инфракрасном диапазоне. Данные передаются с помощью инфракрасных лучей с длиной волны в диапазоне 850...950 нм с использованием *импульсно-позиционной модуляции* (*Pulse-Position Modulation - PPM*). Стандартизованы две скорости передачи данных - 1 и 2 Мбит/с. При передаче данных с меньшей скоростью биты группируются в 4-битовые блоки. Содержимое блока определяет, в каком из 16 слотов будет передан инфракрасный импульс, т.е. применяется 16-уровневая модуляция PPM (16-PPM). При передаче данных со скоростью 2 Мбит/с поток разбивается на 2-битовые блоки, каждый из которых определяет, в каком из четырех временных слотов будет передан инфракрасный импульс. В обоих случаях длительность импульса составляет 250 нс. Поскольку пиковая мощность сигнала достигает 2 Вт, то средняя мощность равна 125 мВт при скорости 1 Мбит/с и 250 мВт при скорости 2 Мбит/с.

Инфракрасный интерфейс - самый дешевый из всех физических интерфейсов стандарта 802.11 и не требует частотного регулирования и достаточно защищен от перехвата. Однако системы, использующие этот интерфейс, характеризуются самой маленькой дальностью связи среди всех систем стандарта 802.11. Этот интерфейс может функционировать внутри помещений, поскольку стены и перекрытия отражают инфракрасные лучи.

5.2. Подуровень MAC системы IEEE 802.11

В эталонной модели IEEE 802.11 подуровень MAC расположен над физическим уровнем. Он решает следующие задачи: выделение каналов путем предоставления доступа на основе метода CSMA, адресация блоков данных PDU (*Protocol Data Unit*), форматирование кадров, обнаружение ошибок, а также фрагментация и сборка блоков данных.

5.2.1. Принцип доступа к среде стандарта 802.11

Работа сети стандарта 802.11 основана на концепции «общая шина», аналогичной Ethernet. В соответствии с этой концепцией в сети существует единственный широкополосный симплексный канал связи, который может быть занят только одним передающим устройством (AC или AP). Все остальные участники сети находятся в режиме ожидания освобождения канала связи. Если в сети начинается одновременная передача двух и более сетевых устройств, то неизбежно возникает коллизия. Для предотвращения коллизий необходим тщательный контроль уровня сигнала в канале связи (КС).

С этой целью в сетях Ethernet используется многостанционный доступ с контролем несущей и обнаружением коллизий *CSMA/CD*, в беспроводных сетях стандарта 802.11 применяется подобный протокол *CSMA/CA* (*Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA*). Протокол *CSMA/CA*

накладывает более строгие правила на право доступа к каналу связи и схематично состоит в следующем [4, 5].

1. Прежде чем участник сети начнет передачу сообщения, он должен уведомить о том, насколько длительной будет передача. Это, к примеру, дает возможность всем остальным терминалам перейти в режим энергосбережения на указанный интервал времени.

2. Терминалы и АР не могут начать передавать, пока не истечет время, зарезервированное участником сети, занявшим канал связи.

3. Терминал, передающий сообщение, не располагает информацией о том, что его сообщение принимается. Это становится известным только после получения подтверждения приема по окончании передачи.

4. Если два и более терминала начали передачу одновременно, то возникает коллизия. Факт коллизии будет обнаружен терминалами только в том случае, если они не получают подтверждения приема по окончании передачи.

5. Если по окончании передачи подтверждение не было получено, то терминал выжидает некоторое случайное время и по его истечении снова пытается получить доступ к каналу связи и повторить передачу.

Таким образом, при использовании протокола **CSMA/CA** в сетях стандарта 802.11 коллизия обнаруживается только при неполучении передающей станцией ожидаемого подтверждения.

Важнейшие компоненты протокола **CSMA/CA**:

- контроль несущей;
- распределенная функция координации DCF;
- пакеты подтверждения;
- резервирование канала связи по технологии RTS/CTS.

Кроме **CSMA/CA**, доступ к среде может быть организован на основе других механизмов, не имеющих отношения к **CSMA/CA**:

- фрагментация пакетов;
- точечная функция фрагментации PCF.

5.2.2. Принцип **CSMA/CA**: контроль несущей

Станция, которая намеревается осуществить передачу, должна вначале проверить, используется ли канал связи. Если это так, то передача должна быть отложена до момента освобождения среды.

В стандарте 802.11 предусматривается два механизма контроля за активностью в канале (обнаружения несущей): физический и виртуальный.

Первый механизм (*physical carrier sensing*) реализован на физическом уровне - на уровне физического интерфейса и сводится к определению уровня сигнала в приемном тракте и сравнению его с пороговой величиной. Таким образом, контроль на физическом уровне позволяет обнаруживать другие активные WLAN-терминалы путем измерения мощности радиосигнала.

Виртуальный (*virtual carrier sensing*) механизм обнаружения несущей осуществляется на MAC-уровне и основан на том, что в передаваемых кадрах

данных, а также в управляющих кадрах ACK и RTS/CTS, содержится информация о времени, необходимом для передачи пакета (или группы пакетов), и последующем получении подтверждения. Все устройства сети принимают информацию о текущей передаче и фиксируют время занятия канала связи. Для контроля активности в канале на MAC-подуровне используется поле ID – поле идентификации длительности MAC-кадра, который, в свою очередь, может включать запрос на передачу (RTS), сообщение о готовности к приему (CTS) или данные. Терминалы, относящиеся к тому же самому BSS, считывают значение поля ID и помещают это значение в свои *векторы резервирования сети (Network Allocation Vector — NAV)*. Вектор NAV – это своего рода таймер, задающий время, в течение которого канал будет занят. Прослушивание канала возобновляется по истечении периода NAV и следующего за ним *межкадрового промежутка (Interframe Space - IFS)*. Этот промежуток служит для установления приоритетов WLAN-терминалов по соблюдению очередности занятия канала связи. Существует четыре типа промежутков IFS, различающихся по длине: короткий IFS (*Short IFS-SIFS*), увеличенный межкадровый интервал (EIFS), *интервал IFS централизованной координации (Point coordination function IFS - PIFS)* и интервал DCF-IFS (**DIFS**).

5.2.3. Принцип CSMA/CA: распределенная функция координации DCF

С точки зрения подуровня MAC существуют два режима работы беспроводной сети передачи данных стандарта 802.11:

- *режим конкуренции CP (Contention Period - CP)*, в котором все терминалы WLAN, желающие передать пакет, конкурируют за доступ к совместно используемому каналу связи с широковещанием – все функции управления сетью распределены между всеми устройствами (*Distributed coordination function - DCF*);
- *смешанный режим*, в котором *периоды конкуренции CP* сменяются *периодами отсутствия конкуренции (Contention-Free Period - CFP)* за доступ к каналу (*Point coordination function - PCF*). В этом случае все функции управления сосредоточены в одной точке.

Распределенная функция координации DCF является утвержденным IEEE механизмом доступа для сетей стандарта 802.11, основанным на методе CSMA/CA.

При работе с использованием DCF станция, намеревающаяся передать блок данных, должна выждать определенное время после того, как освободилась среда и истек вектор резервирования сети NAV. Этот интервал времени называется межкадровым интервалом DCF (**DIFS**). По истечении интервала времени DIFS станция-терминал может принять участие в состязании за право доступа к среде.

Предположим, что в инфраструктуре BSS имеются три мобильные станции (рис. 7) и Терминал 1 передает данные Терминалу 3. Поскольку для всех

участников сети канал связи общий (широковещательный), то Терминал 2 также принимает пакет. Передаваемый в пакете вектор продолжительности передачи NAV достаточно велик для того, чтобы осуществить передачу пакета и получить его подтверждение. Терминалы 2 и 3 обновляют свои векторы резервирования сети полученным значением и не пытаются начать передачу, пока NAV не уменьшится до нуля.

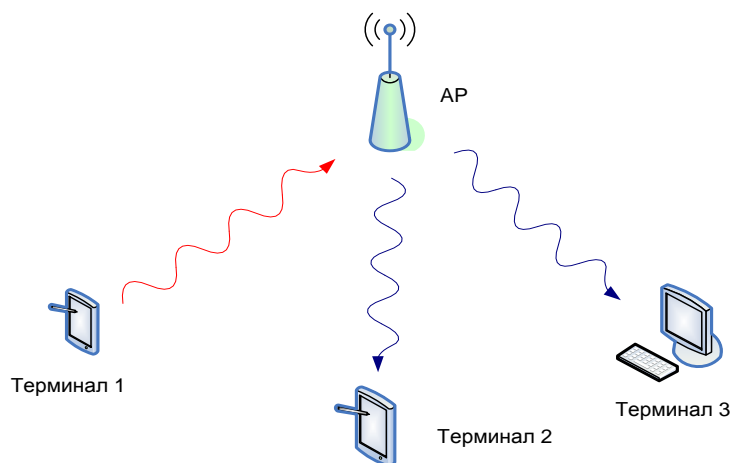


Рис.7. Передача сообщений через точку доступа

Поскольку обе станции используют одно и то же значение вектора NAV и одновременно зафиксируют отсутствие несущей в КС по окончании передачи, то существует большая вероятность того, что обе станции одновременно попытаются начать передачу сразу после истечения DIFS (рис. 8)

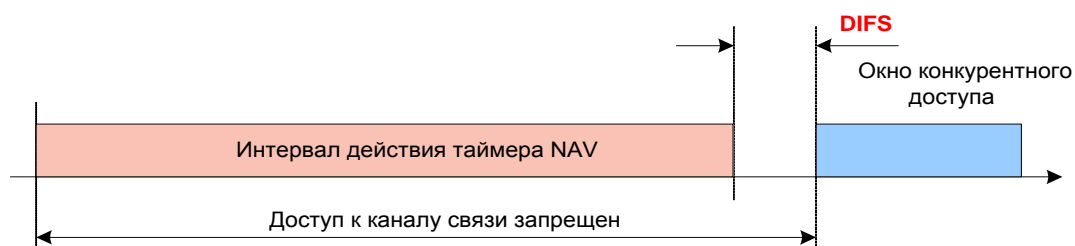


Рис. 8. Интервал ожидания DIFS

Для того чтобы избежать этого, DCF использует таймер случайной задержки (*random backoff timer*). Суть алгоритма случайной задержки состоит в следующем [4].

По истечении интервала DIFS терминалами случайным образом выбирается значение в диапазоне от 0 до значения, соответствующего длительности окна конкурентного доступа (*contention window, CW*). Выбранное значение представляет собой количество канальных интервалов (*slot times*), в течение которых станция, уже после освобождения КС (интервал DIFS), должна воздерживаться от передачи.

Возвращаясь к примеру, Терминал 2 (рис. 8) готов начать передачу. Значение таймера NAV терминала уменьшено до 0, а служба физического уровня РНУ подтверждает незанятость широковещательного канала. Служба канального уровня выбирает случайное время задержки в диапазоне от 0 до CW (например, 3) и воздерживается от передачи в течение выбранного количества канальных интервалов, при этом постоянно опрашивая службу физического уровня РНУ на предмет занятости канала (рис. 9).

По окончании трех канальных интервалов Терминал 2 может начать передачу. Если какая-либо станция начнет передачу раньше (например, по истечении 2 канальных интервалов), то Терминал 2 приостанавливает работу таймера задержки, извлекает из переданного сообщения значение вектора NAV. Терминал 2 должен подождать, уменьшая значение NAV до 0. После этого Терминал 2 запрашивает службу физического уровня РНУ о незанятости среды и, если ответ положительный, возобновляется отсчет полученной ранее случайной задержки (оставшееся значение – 1 канальный интервал). При завершении последнего такта задержки станция немедленно начинает передачу пакета данных.

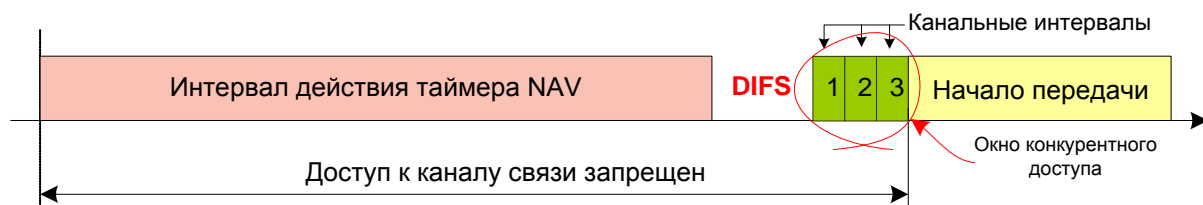


Рис. 9. Канальные интервалы окна конкурентного доступа

Спецификация 802.11 требует, чтобы принимающая станция передала станции-отправителю пакет подтверждения. Этот пакет позволяет станции-отправителю непосредственно определить, произошла ли в канале коллизия. Если передающая станция не получает пакет подтверждения, то делается вывод о том, что произошла коллизия, и принимаются следующие действия.

1. Передающий терминал обновляет счетчик числа попыток передачи.
2. Удваивается длительность окна конкуренции CW .
3. Начинается заново процесс доступа к каналу связи.

5.2.4. Принцип CSMA/CA: пакет подтверждения

Станция, получившая пакет, подтверждает факт его безошибочного приема путем отправки передающей станции пакета подтверждения ACK (ACKnowledge) (рис. 10).

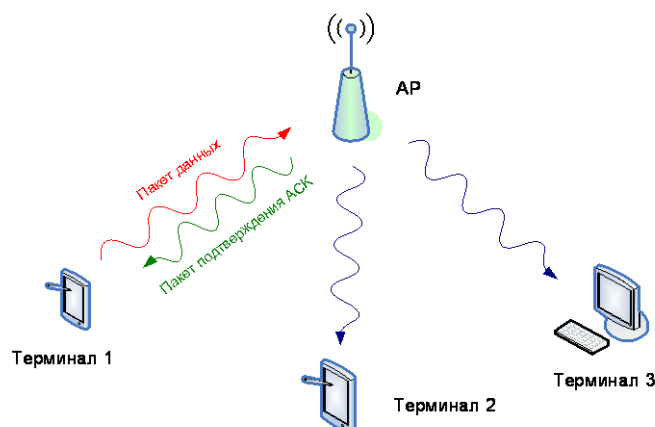


Рис. 10. Отправка пакета подтверждения

Передача пакета ACK – особый случай спецификации 802.11. Терминал-получатель сообщения для передачи подтверждения не принимает участия в процессе случайной задержки. Короткий промежуток времени, который приемная станция проводит в ожидании передачи подтверждения, называется коротким межкадровым интервалом **SIFS** (*Short IFS*). Интервал **SIFS** **короче интервала DIFS** на два канальных интервала. Это гарантирует принимающей станции наибольший шанс получения доступа к КС по сравнению с другими станциями (рис.11).

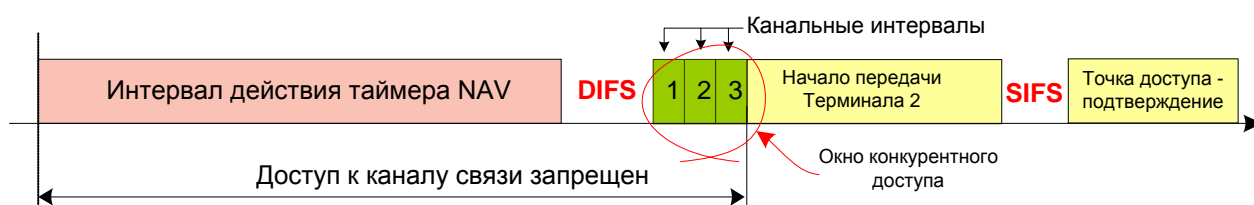


Рис. 11. Диаграмма получения подтверждения ACK

Таким образом, процедура передачи сообщения в сети 802.11 без использования кадров RTS/CTS может быть представлена в виде, показанном на рис.12.

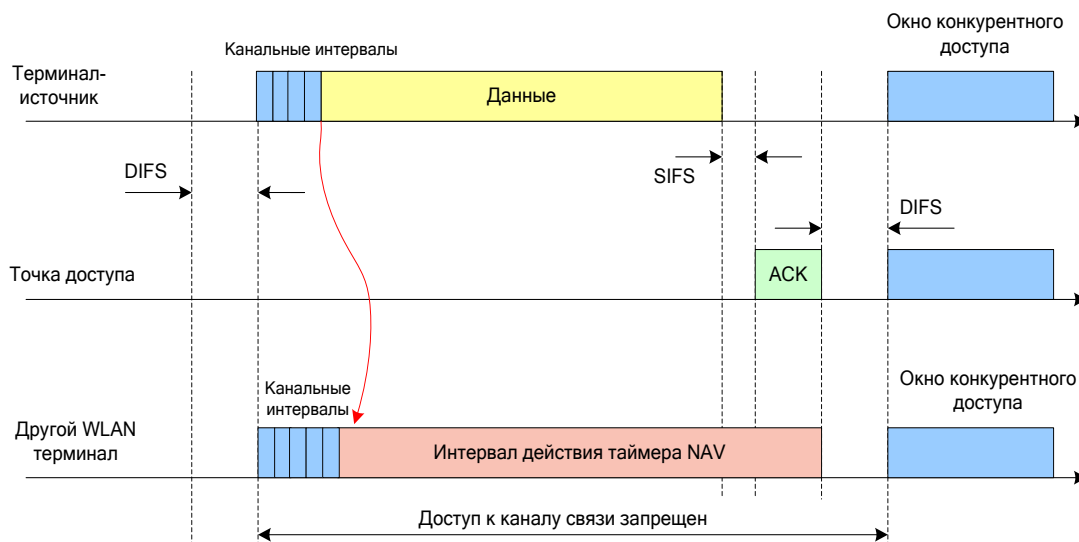


Рис. 12. Конкурентный доступ без использования кадров RTS/CTS

В этом случае станция, получившая право на передачу данных, отправляет свой пакет. Остальные станции считывают это сообщение и из поля ID определяют, как долго будет занят канал. На основании этого они устанавливают свои NAV-таймеры на соответствующий период времени. Окно конкурентного доступа начинается по истечении периода DIFS, следующего за

пакетом подтверждения АСК станции-получателя данных. Квитанция (пакет) АСК служит подтверждением терминалу-источнику о правильности приема блока данных терминалом-получателем. Конкурирующие за доступ к каналу станции случайным образом выбирают время обратного отсчета, по истечении которого вновь начинают прослушивать канал. Станция, которая установила наименьшее число канальных интервалов, обнаруживает, что канал свободен, и начинает немедленно передавать свои данные.

5.2.5. Принцип CSMA/CA: проблема скрытого узла и RTS/CTS

Сущность проблемы скрытого узла подробно изложена в п. 3 и дополнительно иллюстрируется на рис. 13.

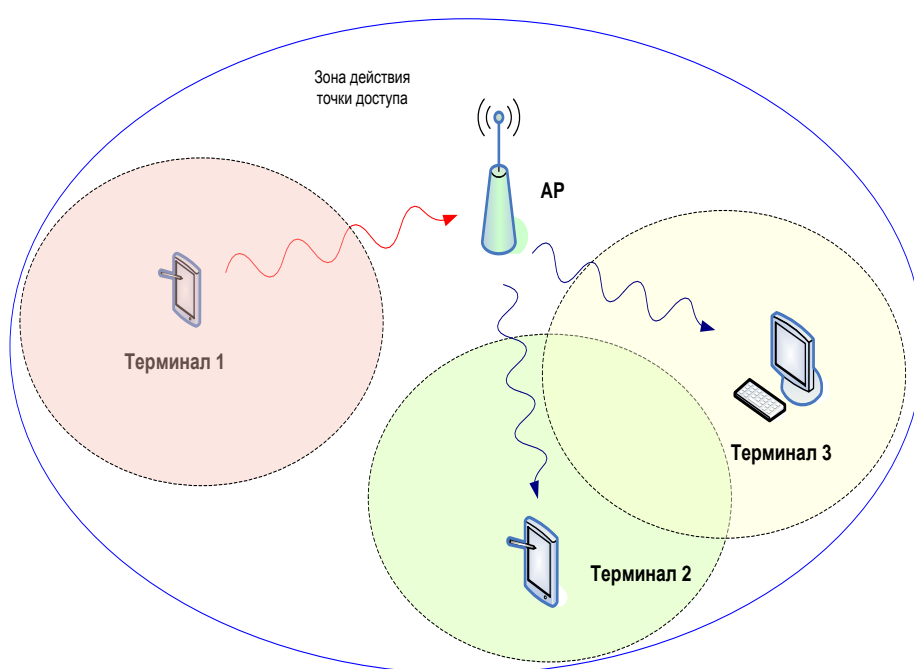


Рис. 13. Проблема скрытой станции

Рассмотрим решение проблемы скрытого узла на примере (рис. 13). Терминал 1 находится в зоне радиопокрытия AP, но вне досягаемости станций 2 и 3. При попытке занятия канала связи Терминал 1 будет «невидим» для станций 2 и 3, следовательно, Терминал 1 для них – скрытый узел. Проблема скрытого узла в стандарте 802.11 решается с использованием специальных кадров RTS/CTS.

Терминал 1, имея сообщение для передачи, к примеру, для Терминала 2, пытается зарезервировать КС с помощью кадра **RTS** (*Request To Send* - *запрос на передачу*). Посредством процедуры DCF кадр RTS посылается точке доступа. Все станции, которые находятся в зоне действия Терминала 1, извлекают из переданного пакета значение вектора NAV и ожидают в течение времени, необходимого Терминалу 1 для получения подтверждения CTS и передачи собственно сообщения. Другие станции, не находящиеся в зоне

действия Терминала 1, не в состоянии принять этот сигнал, поэтому могут начать передачу своих сообщений в любой момент. Пока точка доступа не ответит на запрос RTS кадром CTS, вероятность коллизии высока.

Точка доступа получает кадр RTS от Терминала 1 и отвечает управляющим кадром CTS (*Clear To Send* - «готов к твоей передаче»). Последний содержит поле продолжительности, значение которого достаточно для того, чтобы Терминал 1 мог завершить передачу сообщения и получить подтверждение приема данных. Все станции в зоне действия AP получают кадр CTS и обновляют свои NAV-таймеры (рис. 14).

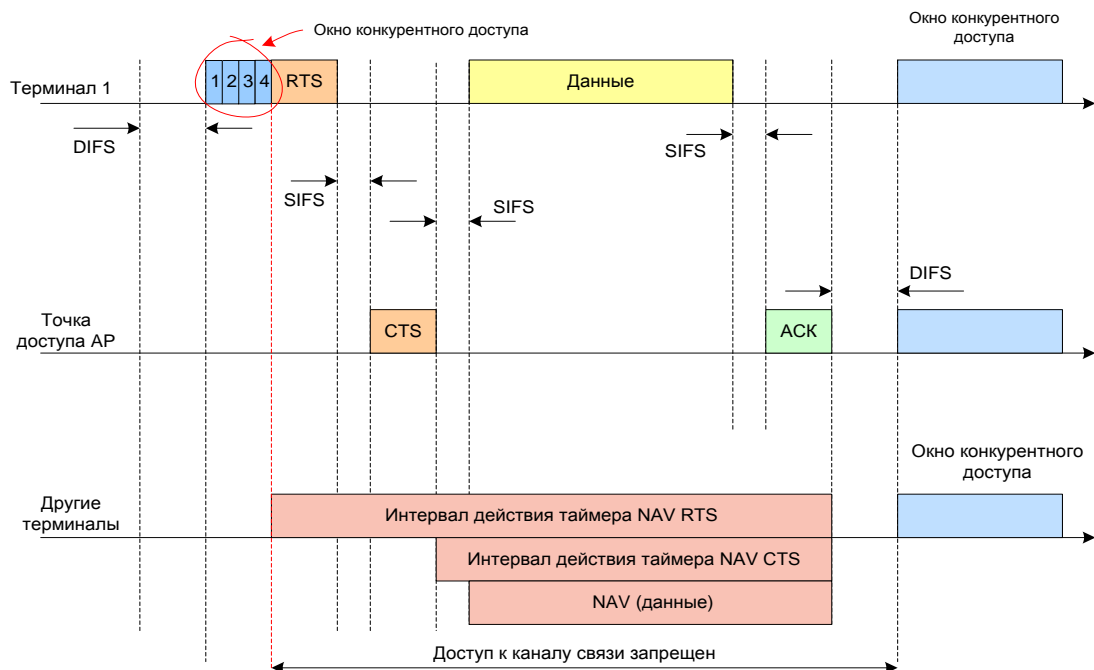


Рис. 14. Конкурентный доступ с использованием кадров RTS/CTS

Таким образом, кадр RTS, посылаемый Терминалом 1, должен пройти через процедуру DCF, т.е. через необходимость «борьбы» за КС. Но, аналогично пакету подтверждения ACK, кадр CTS, передаваемый точкой доступа, пропускает процедуру случайной задержки и перед тем, как быть переданным, должен выждать время, равное интервалу SIFS (рис.14). Приняв кадр CTS, все станции выжидают время, необходимое для передачи Терминалом 1 сообщения на точку доступа AP и получения обратно подтверждения ACK.

В свою очередь, Терминал 2, получив сообщение от AP, спустя время SIFS отправляет точке доступа пакет подтверждения ACK, хотя его собственный вектор NAV еще отличен от нуля.

Если пакет данных был искажен и требуется повторная передача, то терминал-источник должен снова получать доступ к КС на общих основаниях с другими станциями. При возникновении коллизии размер окна конкурентного доступа CW удваивается, но в итоге не может превысить установленное администратором сети значение CW_{max} . Это позволяет

увеличить разброс по времени ожидания и уменьшить вероятность выбора несколькими терминалами одного и того же времени обратного отсчета.

5.2.6. Принцип CSMA/CA: фрагментация пакетов

Фрагментация пакетов - это выполняемая на уровне MAC функция, назначение которой – повысить надежность передачи сообщений по широкополосному каналу. Под фрагментацией понимаются дробление пакета данных MSDU (*MAC Service Data Unit*) на меньшие фрагменты и передача каждого из них отдельно (рис. 15).

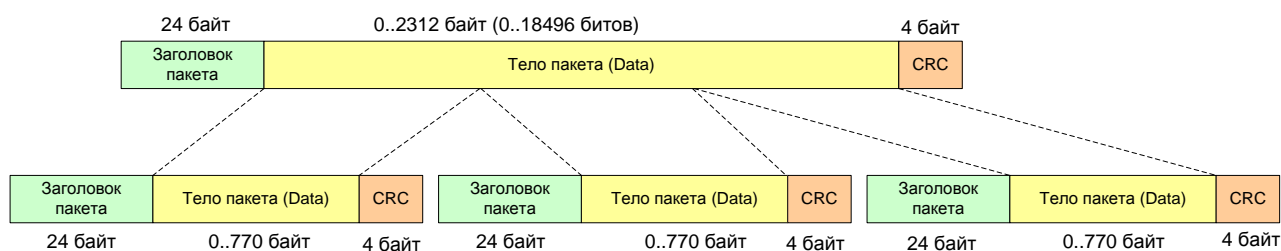


Рис. 15. Фрагментация пакета данных

Предполагается, что вероятность успешной передачи меньшего фрагмента через КС с помехами выше. Получение каждого фрагмента подтверждается отдельно; следовательно, если какой-либо фрагмент пакета будет передан с ошибкой или вступит в коллизию, то только его придется передавать повторно, а не весь пакет. Это увеличивает полезную пропускную способность зашумленного КС.

Размер фрагмента задается администратором сети. Фрагментации подвергаются только одноадресатные пакеты. Широковещательные пакеты (многоадресатные) должны передаваться целиком. Кроме того, фрагменты пакета передаются группой, с использованием только одной итерации процедуры DCF.

Фрагментация пакетов повышает надежность передачи сообщений по зашумленным КС, однако при этом увеличивается число служебных сигналов MAC-уровня, что снижает реальную производительность беспроводной станции. Таким образом, фрагментация – это баланс между надежностью передачи и непроизводительной загрузкой среды [4].

5.2.7. Принцип CSMA/CA: итоги

Перед началом передачи WLAN-терминал осуществляет измерение уровня радиосигнала в канале связи. Канал считается свободным при условии, что не обнаружено активности в течение определенного промежутка времени — межкадрового интервала DIFS. Если в течение этого промежутка канал оставался свободным, терминал ожидает еще в течение случайного числа

канальных интервалов и, если канал не был занят, передает подготовленный пакет. Если пакет предназначен конкретному устройству (не широковещательная или многоадресная передача), то терминал-адресат, успешно приняв пакет, посылает отправителю короткий кадр подтверждения получения АСК (ACKnowledge). Если станция-отправитель не приняла пакет АСК, она считает переданный ранее пакет утерянным и проводит вновь процедуру «захвата» КС для повторной передачи пакета.

При повторной передаче пакета для определения незанятости канала станция должна уже использовать увеличенный межпакетный интервал. Кроме того, время отсрочки выбирается случайным образом и кратное интервалу CW : при первой попытке передачи этот интервал минимален, при каждой последующей он удваивается до тех пор, пока не достигнет заданного предельного значения CW_{max} , установленного администратором сети.

Перед первой попыткой получить доступ к каналу станция-отправитель загружает длительность случайного интервала отсрочки в специальный счетчик. Его значение декрементируется с заданной частотой, пока канал свободен. Как только счетчик обнулится, терминал может занимать канал. Если до обнуления счетчика канал занимает другое устройство, счет останавливается, сохраняя достигнутое значение. При следующей попытке захвата КС отсчет начинается с сохраненной величины. В результате проигравшие в конкурентной борьбе терминалы получают больше шансов занять канал в следующий период конкуренции.

Описанный выше метод предотвращения конфликтов обеспечивает удовлетворительный доступ ко всем конкурирующим за доступ терминалам, однако он не гарантирует минимальной задержки при передаче пакета терминалам, поддерживающим услуги, имеющие ограничения по времени.

5.2.8. Точечная функция координации PCF

Точечная функция координации PCF (*Point coordination function*) - это опциональный, необязательный механизм доступа к КС, который используется дополнительно к механизму DCF. Механизм PCF обеспечивает не подверженную конкуренции за КС передачу пакетов к точке доступа и от нее. Необходимо отметить, что большинство производителей не обеспечивают поддержку механизма PCF в своих устройствах, поскольку он увеличивает служебную нагрузку на протокол взаимодействия сетевых устройств. Предполагается, что с повышением качества и класса предоставляемых услуг передачи данных (Quality of Service, QoS) в будущих спецификациях 802.11 будет использоваться другой механизм [4].

Необходимость в режиме централизованного управления PCF возникает при передаче чувствительной к задержкам информации, когда необходимо вводить приоритеты доступа к каналу связи. Для реализации этого режима требуется *центр координации* (*Point Coordinator* - **PC**), который управляет

доступом к каналу, опрашивая терминалы. Функции центра координации выполняет AP - точка доступа BSS.

Общим для PCF и DCF режимов является тот факт, что на MAC-уровне сети 802.11 существует единственный симплексный канал связи, который может быть занят только одной передающей станцией.

5.2.9. Механизм PCF: период отсутствия конкуренции

Все время работы сети поделено на циклы (рис. 14), состоящие из периодов отсутствия конкуренции за доступ CFP (*Contention-Free Period*) и периодов конкуренции CP. Период отсутствия конкуренции CFP – это временное окно, в течение которого осуществляется работа механизма PCF (рис. 16).

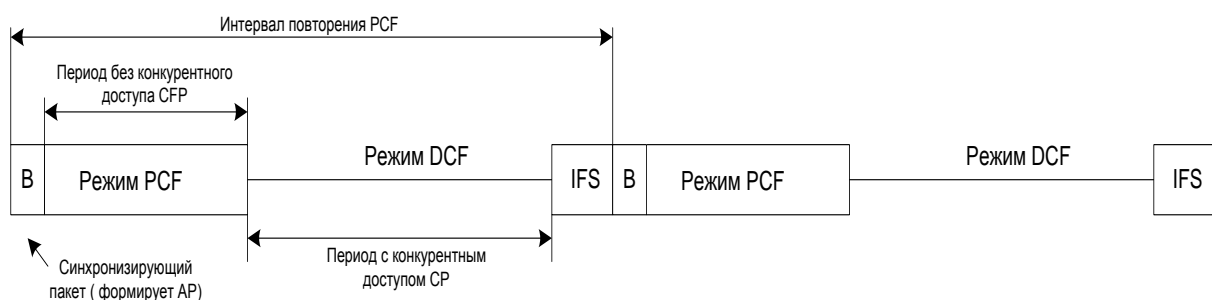


Рис. 16. Смешанный режим работы сети

Период CFP начинается с набора интервалов, следующих за сигнальным (маячковым) пакетом В (beacon frame). Частота следования периодов CFP определяется администратором сети. После начала CFP точка доступа начинает выполнять роль точки координации. После передачи сигнального пакета В (рис.16) все терминалы устанавливают значение NAV равным CFPMaхDuration (максимальное время продолжительности CFP). Точка координации может закончить работу в соответствии с механизмом CFP раньше, чем истечет время CFPMaхDuration. Для оперативного оповещения терминалов об оставшемся времени CFP точка доступа в течение CFP регулярно передает сигнальные пакеты, в которых содержится поле CFPDurationRemaining (оставшаяся продолжительность CFP). Посредством этого поля станции обновляют NAV-таймеры значением, соответствующим оставшейся продолжительности CFP.

В отличие от режима DCF при работе сети под управлением механизма PCF станции не имеют свободного доступа к КС и не могут свободно передавать данные. Станции могут передавать сообщения (по одному пакету за один раз) только тогда, когда точка координации проводит их опрос. Точка координации может посылать пакеты терминалам, опрашивать станции на предмет наличия сообщений для передачи, подтверждать получение пакетов или закончить период CFP.

5.2.10. Механизм PCF: работа точки координации

Рассмотрим работу сети в течение периода CFP (режим PCF, рис. 17). Точка координации прослушивает канал и ждет окончания текущей передачи данных. Когда начинается CFP, точка координации должна получить доступ к среде на общем основании и таким же образом, как это делается в DCF. Но в отличие от станций DCF точка координации пытается получить доступ к КС через интервал времени, называемый *преимущественным межкадровым интервалом* (*priority IFS, PIFS*). Интервал PIFS на один такт дольше интервала SIFS и на один такт короче промежутка DIFS. Это позволяет точке координации получать доступ к среде раньше станций DCF.

После ожидания в продолжение интервала PIFS точка координации посылает начальный сигнальный пакет В, содержащий информацию о периоде CFP и синхронизирующие сигналы. После получения этого кадра все терминалы сохраняют текущее значение вектора NAV и, в соответствии с полученной информацией, устанавливают новое значение NAV-таймера на весь период отсутствия конкуренции. Точка координации ожидает в течение интервала SIFS и затем посылает один из следующих пакетов:

- пакет данных (Data);
- пакет опроса (CF-Poll);
- комбинация пакетов данных и опроса (Data + CF-Poll);
- комбинация пакетов данных, подтверждения и опроса (Data + CF-Ack + CF-Poll);
- пакет завершения периода CFP (CF-End).

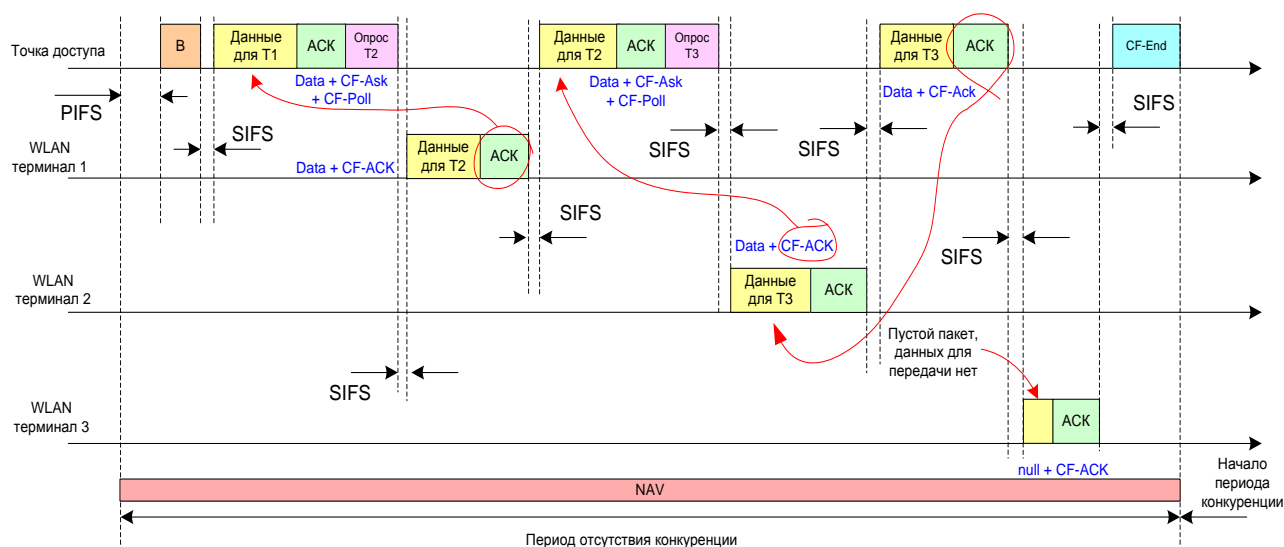


Рис. 17. Диаграмма работы сети в течение периода CFP

В течение периода CFP центр координации по очереди опрашивает терминалы, находящиеся в ее зоне обслуживания, передавая каждому данные из своего буфера (если они есть) и предоставляя возможность станциям отправить пакет с подготовленными данными.

Только опрошенный терминал может ответить на запрос по истечении промежутка SIFS, послав кадр подтверждения ACK или кадр **Data+ CF-ACK** (кадр с данными и подтверждением). Если передающий буфер опрашиваемого терминала пуст, то станция отвечает пакетом с нулевыми данными (null data frame), который не требует подтверждения со стороны точки доступа.

Период отсутствия конкуренции оканчивается кадром **CF-End**.

5.3. Операции, осуществляемые на уровне MAC стандарта 802.11

Операции, осуществляемые на MAC-уровне, помимо способов организации доступа к среде, изложенных в п. 5.2, решают задачу логического объединения терминалов в единую сеть. Эта задача решается на основе реализации различных режимов работы (процессов) с использованием обширного списка форматов пакетов.

5.3.1. Соединение станций стандарта 802.11

Для подключения любого абонентского терминала к сети 802.11 необходимо выполнение трех связанных процессов:

- 1) процесса запроса (зондирования);
- 2) процесса аутентификации;
- 3) процесса привязки.

Процесс запроса на подключение

Станция-клиент по всем доступным каналам физического уровня посылает специальный пакет запроса (probe request frame). Этот пакет содержит информацию о том, к какой зоне обслуживания она принадлежит (SSID) и какие скорости передачи она поддерживает. Пакеты запроса передаются с минимально возможной скоростью, составляющей 1 Мбит/с.

Когда точка доступа получает пакет запроса, она проверяет его контрольную последовательность CRC (или *frame check sequence*, **FCS**) и посылает ответ на запрос. Пакет ответа на запрос включает следующую информацию [4]:

- поле временной метки отправителя Timestamp;
- число тактов между маячковыми сигналами (один такт 1024 мкс);
- поле SSID – идентификатор зоны обслуживания;
- список поддерживаемых точкой доступа скоростей передач;
- особенности физического уровня - параметры PHY.

Принимая ответ точки доступа, терминал определяет уровень сигнала полученного пакета. Правило, в соответствии с которым станция-клиент

выбирает точку доступа, в спецификации 802.11 не описано – это реализуется поставщиком оборудования самостоятельно. Как правило, критерий выбора точки доступа может включать согласованное значение SSID (одно и то же у станции и точки доступа), максимальный уровень сигнала и поддерживаемый точкой доступа набор скоростей терминала.

После того как станция определила, с какой AP ей целесообразно ассоциироваться, она приступает к следующей фазе установления соединения - процессу аутентификации.

Процесс аутентификации

Процесс аутентификации по стандарту 802.11 может выполняться в двух режимах: аутентификация с открытым ключом и аутентификация с совместно используемым ключом [4]. В соответствии со спецификацией 802.11 задача аутентификации состоит в определении принадлежности станции-клиента локальной сети с идентификатором SSID. Подробнее с процессом аутентификации можно познакомиться в [4].

Процесс привязки к точке доступа

Процесс привязки по стандарту 802.11 позволяет точке доступа выделить для беспроводной станции логический порт или присвоить ей идентификатор ассоциации (*association identifier*, **AID**). Процесс привязки начинается беспроводной станцией с передачи пакета запроса на ассоциирование, содержащего информацию о возможностях терминала, и завершается пакетом ответа на ассоциирование, посылаемого точкой доступа. Ответ на ассоциирование может быть положительным или отрицательным и содержать код, указывающий на причины отказа. Можно выделить следующие ключевые поля пакета запроса на соединение.

- Интервал прослушивания (*listen interval*). Значение интервала прослушивания используется в режиме экономии энергопотребления и сообщается клиентской станцией точке доступа. Оно информирует AP о том, как часто эта станция "просыпается" (выходит из режима экономии энергопотребления), чтобы получить пакеты, накопленные для этой станции в точке доступа.
- Идентификатор SSID. Отражает идентификатор зоны обслуживания SSID клиентской станции для AP. В нормальном режиме работы AP не принимает запросы на ассоциацию от станций с SSID, отличающиеся от тех, которые сконфигурированы в точке доступа.
- Список поддерживаемых скоростей передачи. Указывает AP, какие скорости передачи поддерживает клиентская станция.

Ключевые поля пакета ответа на ассоциирование следующие.

- Код состояния (*status code*). Код состояния указывает на успешность или неуспешность реагирования точки доступа на полученный ранее запрос (например, 0 - успешно; 18 – ассоциация отклонена по причине неполной поддержки станцией скоростей передачи и т.д.).

- Идентификатор ассоциации AID. Идентификатор AID имеет смысл логического порта AP – как сетевого коммутатора. Клиентская станция должна знать это значение, когда она работает в режиме энергосбережения. В этом случае AP посылает оповещения в сигнальных (маячковых) пакетах, указывающие, каким AID предназначаются накопленные точкой доступа пакеты в ее оперативном буфере.
- Список поддерживаемых скоростей передачи. Указывает, какие скорости передачи поддерживает точка доступа.

5.3.2. Работа терминалов 802.11 в режиме энергосбережения

Чтобы продлить срок службы батарей портативных клиентов WLAN, стандарт 802.11 предусматривает их работу в режиме сниженного энергопотребления или в режиме энергосбережения (*power save operations*). Работа в режиме сниженного энергопотребления может осуществляться в двух вариантах:

- работа с одноадресными пакетами;
- работа с ширококестельными/многоадресными пакетами.

После перехода в режим энергосбережения терминала сети точка доступа накапливает пакеты, предназначенные для этой станции. Через определенный интервал времени клиент активизируется и принимает сигнал от AP, показывающий, имеются ли в буфере AP пакеты для данной клиентской станции.

При работе с одноадресными пакетами интервал прослушивания определяется терминалом. И наоборот, при работе в режиме энергосбережения с ширококестельными/многоадресными пакетами интервал прослушивания определяется точкой доступа и объявляется в ее сигнальных (маячковых) пакетах.

Терминал активизируется и принимает сигнальные пакеты AP, чтобы определить, накоплены ли для него пакеты. Если пакетов для него нет, клиент возвращается к режиму энергосбережения и пребывает в нем до истечения очередного периода активности.

Работа с одноадресными фреймами в режиме энергосбережения

Когда терминал связывается с AP, он указывает значение интервала прослушивания КС в пакете запроса на ассоциацию. Интервал прослушивания - это число сигнальных пакетов, которые терминал отсчитывает, прежде чем перейти в активный режим.

Сигнальный пакет включает поле, называемое *картой индикации трафика* (*traffic indication map*, TIM). Это поле содержит перечень всех AID, к которым имеются пакеты данных, принятые AP, когда терминалы, ассоциированные с этими портами, находились в «спящем» режиме. В соответствии со стандартом может быть до 2008 уникальных AID, так что размер поля TIM может достигать 251 бита. Чтобы минимизировать нагрузку на сеть, TIM использует

сокращенный метод перечисления AID.

Широковещание в режиме энергосбережения

Широковещание в режиме энергосбережения осуществляется в основном так же, как и одноадресатная передача в режиме с энергосбережением. Отличия состоят в следующем.

- Администратор сети определяет интервал, по истечении которого станция-клиент должна активизироваться и получить накопленный точкой доступа трафик широковещания или многоадресатной рассылки.
- Особый информационный элемент TIM, называемый DTIM, показывает, имеется ли в AP накопленный трафик широковещания или многоадресатной рассылки.
- Пакеты широковещания или многоадресатной рассылки накапливаются в буфере AP для всех станций (включая неэнергосберегающих), входящих в BSS, если хотя бы одна станция ассоциирована с точкой доступа.

Информационный элемент TIM имеет два поля, указывающие, накоплен ли трафик широковещания/многоадресатной рассылки и как скоро он будет передан в пределах BSS.

- Поле подсчета DTIM (*DTIM count field*). Указывает, сколько сигнальных пакетов должно быть передано, прежде чем будет передан накопленный трафик. Значение 0 указывает на то, что этот сигнальный пакет является последним и, если имеются накопленные AP пакеты, то они будут немедленно переданы следом за этим пакетом.

- Поле периода DTIM (*DTIM period field*). Указывает количество сигнальных пакетов, передаваемых между оповещениями DTIM. Например, значение 15 указывает на то, что каждый 15-й маячковый пакет будет содержать DTIM.

5.3.3. Структура кадров MAC уровня (кратко)

Существуют три типа кадров MAC. *Кадры управления (management frames)* используются для синхронизации, аутентификации, а также для установления и разрыва соединения терминала с данной точкой доступа. *Кадры контроля (control frames)* применяются в процедурах подтверждения приема и подтверждения готовности (*handshaking*), которые выполняются, как правило, в периоды конкуренции. Наконец, *кадры данных (data frames)* используются для передачи пользовательских данных и могут дополнительно содержать блоки подтверждения приема и опроса терминалов в периоды отсутствия борьбы за канал.

Передача данных на MAC-подуровне организована в виде MAC-кадров. На рис. 18 изображена типичная структура MAC-кадра в сетях стандарта 802.11. MAC-кадр содержит следующие поля:

- *поле управления кадром*, в котором указываются версия протокола и тип кадра (управления, контроля или данных). Это поле позволяет передавать информацию о необходимых действиях при организации приема-передачи данных в сети стандарта 802.11. В нем также указывается, фрагментирован ли кадр (вмещает кадр все данные или нет) и что означают адресные поля (например, направляется ли кадр в распределительную систему, прибывает из нее), имеется признак повторной передачи пакета;
- *поле идентификации длительности ID* указывает время в микросекундах, которое требуется для передачи MAC-кадра. Иногда в этом поле указывается идентификатор соединения;
- *адресные поля* с первого по четвертое указывают источник и пункт назначения передаваемого кадра, адрес передающей станции и адрес приемной станции; они интерпретируются в зависимости от значения поля управления кадром;
- *поле управления очередностью кадров* содержит порядковый номер кадра и предназначено для того, чтобы не допустить дублирования кадра при выполнении процедуры подтверждения получения данных. В этом поле указываются номер пакета (4 бита), который используется при разбиении исходного сообщения на пакеты и при последующей сборке, и порядковый номер (12 бит), который служит для нумерации кадров, передаваемых между конкретными АС;
- *поле данных*, содержащее блок данных размером до 2312 байтов. В поле данных передаются либо данные LLC-уровня, либо информация управления уровня MAC;
- *CRC-поле* длиной 32 бита, используемое для обнаружения ошибок в принимаемом кадре. Ошибки только обнаруживаются. Исправление ошибок достигается в необходимых случаях повторной передачей по запросу (процедура подтверждения ARQ).

Управление кадром (16)	Длительность идентификации (16)	Адрес 1 (48)	Адрес 2 (48)	Адрес 3 (48)	Управление очередностью кадров (16)	Адрес 4 (48)	Данные (0...18496)	CRC
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

Рис. 18. Структура MAC-кадра в сетях стандарта IEEE 802.11

Абонентская станция может также уведомлять другие АС и точку доступа АР о наличии в своем буфере данных сообщения и готовности к его передаче.

Такое уведомление приводит к переводу АС, которой предназначено сообщение, из режима пониженного энергопотребления в обычный режим функционирования.

6. Роуминг в сети стандарта 802.11

Роуминг в сети стандарта 802.11 осуществляется по принципу "сломай, прежде чем строить" (*break before make*), поскольку станция-клиент должна завершить сеанс своего обслуживания одной АР, прежде чем создавать ассоциацию с новой. Такой процесс оказывается целесообразным с точки зрения упрощения оборудования и алгоритмов работы абонентских терминалов, поскольку в противном случае станция должна была бы иметь возможность прослушивания и установления связи более чем по одному каналу одновременно.

Алгоритмы роуминга не отражаются в спецификации 802.11, они определяются поставщиками оборудования. В общем случае последовательность действий при роуминге такая.

1. Терминал должен обнаружить факт его перемещения к границе зоны обслуживания текущей АР. Для решения этой задачи могут использоваться уровень сигнала от АР, факт подтверждения пакета, вероятность ошибки приема пакета.
2. Станция-клиент должна обнаружить новую точку доступа АР. Это может быть сделано сканированием всех доступных КС на предмет наличия сигнальных пакетов от новой АР (пассивное сканирование) или началом процесса запроса (п. 5.3.1) – активное сканирование.

После обнаружения новой точки доступа и успешной ассоциации станции-клиента с ней должны быть выполнены следующие действия.

1. Предыдущая точка доступа должна определить, что станция-клиент уходит из ее области действия.
2. Предыдущая точка доступа должна буферизировать данные, предназначенные для клиента, осуществляющего роуминг.
3. Новая точка доступа должна сообщить предыдущей, что станция-клиент успешно переместилась в ее зону. Этот этап обычно выполняется с помощью одно- или многоадресных пакетов, передаваемых старой точкой доступа для новой и содержащих МАС-адрес источника, указывающий МАС-адрес перемещающегося клиента.
4. Предыдущая точка доступа должна послать накопленные данные новой точке доступа.
5. Предыдущая АР должна определить, что клиент покинул ее зону действия.
6. АР должна обновить таблицы МАС-адресов на коммутаторах сети, чтобы избежать потери данных перемещающегося клиента.

7. Стандарты IEEE 802.11a и Hiper LAN для частоты 5 ГГц

7.1. Краткая характеристика

Принципиальные сложности в реализации высоких скоростей обмена в рамках стандартов 802.11 и 802.11b привели к необходимости разработки оборудования с более высокими скоростями передачи информации. С целью преодоления ограниченности полосы частот 2,4...2,483 ГГц разработка оборудования проводилась в диапазоне 5 ГГц, где оказалось возможным выделить полосы частот, превышающих 100 МГц (рис. 19).

Продолжение работы над увеличением скоростей передачи данных в сетях WLAN привело к появлению нового расширения возможностей физического уровня IEEE 802.11a. Был установлен новый стандарт ETSI, который назвали Hiper LAN Type 2 (в США - IEEE 802.11a).

В России допустимо использование оборудования стандартов 802.11a и Hiper LAN 2 в полосе частот 400 МГц. Этой полосы достаточно для построения полноценных сетей радиодоступа на всей территории страны.

Стандарты определяют характеристики оборудования, применяемого в офисных или городских условиях, когда распространение сигнала происходит по многолучевым каналам из-за множества отражений. Для борьбы с замираниями, вызванными многолучевым распространением, используются сигналы с ортогональной частотной модуляцией (OFDM).

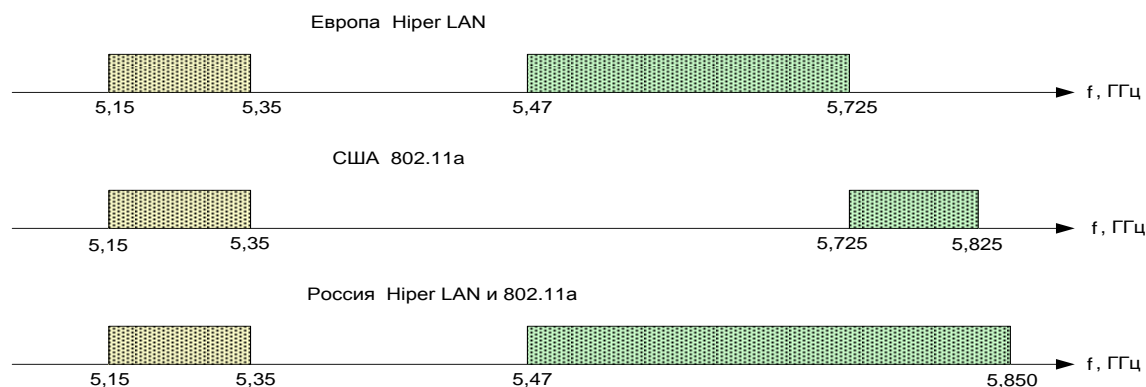


Рис. 19. Национальное распределение полос для оборудования стандарта 802.11a

Кроме этого, на физическом уровне стандарта стали доступны следующие возможности:

- *DFS (Dynamic Frequency Selection - динамический выбор частоты)* - метод адаптивного динамического выбора несущей частоты, используемый для предотвращения помех от других терминалов;
- *TPC (Transmit Power Control - регулировка мощности передатчика)* - регулировка мощности излучаемого радиосигнала, применяемая для

обеспечения надежного соединения между точкой доступа сети Hiper LAN и наиболее удаленным терминалом в зоне досягаемости этой точки доступа, а также между двумя устройствами Hiper LAN.

Необходимо заметить, что MAC-уровень беспроводных сетей стандартов **IEEE 802.11a** и Hiper LAN 2 не отличается от рассмотренного выше (п. 5.2), а физические уровни организации сетей очень похожи.

7.2. Физический уровень организации IEEE 802.11a

Стандарты 802.11a и Hiper LAN 2 определяют требования к физическому уровню (PHY) с использованием OFDM [5]. В стандартах обеспечивается передача данных с базовыми скоростями передачи 6, 9, 12, 18, 24, 36, 48 или 54 Мбит/с. В OFDM сигнале стандарта 802.11a используется всего 64 поднесущие. Из общего числа поднесущих для передачи данных используются 52 полосы, четыре из которых применяются для передачи вспомогательных пилот-сигналов. Таким образом, для передачи информации используется 48 поднесущих. Полоса частот на одну поднесущую составляет 0,3125 МГц:

$$\Delta f_{nn} = \Delta F_{\text{OFDM}} / N,$$

Высшие уровни OSI	
MAC-уровень	
Физический уровень 802.11a	PLCP
	PMD

где $\Delta F_{\text{OFDM}} = 20$ МГц - полоса частот, занимаемая сигналом OFDM в радиоканале; N - общее число поднесущих, равное 64.

Основная цель стандарта 802.11a - описание процесса передачи протокольных блоков данных уровня MAC **MPDU** через физический уровень с OFDM. Физический уровень разделен

Рис. 20. Структура протоколов 802.11a

на две составляющие: подуровень согласования с физическим уровнем **PLCP** и подуровень определения физической среды **PMD** (рис. 20).

MAC-уровень стандарта 802.11a осуществляет обмен с протоколом согласования **PLCP** посредством специальных служб физического уровня. Уровень **PLCP** преобразует пакеты данных MAC-уровня к виду, пригодному для передачи через физический уровень по команде от уровня MAC, а также переводит принятые на физическом уровне кадры в формат пакетов MAC-уровня.

Поток блоков данных **MPDU**, получаемый с MAC-уровня, подвергается скремблированию и помехоустойчивому кодированию (**FEC**). Затем кодовые слова перемежаются, и после разбивки потока данных на короткие блоки (по 2, 4 или 6 символов в зависимости от скорости передачи) выполняется их отображение в информационные символы. Этими символами модулируются поднесущие OFDM сигнала. После формирования пакета и сдвига спектра сигнала в область 5 ГГц, OFDM символ передается по радиоканалу.

Структура приемопередающего оборудования стандарта 802.11a приведена на рис. 21.

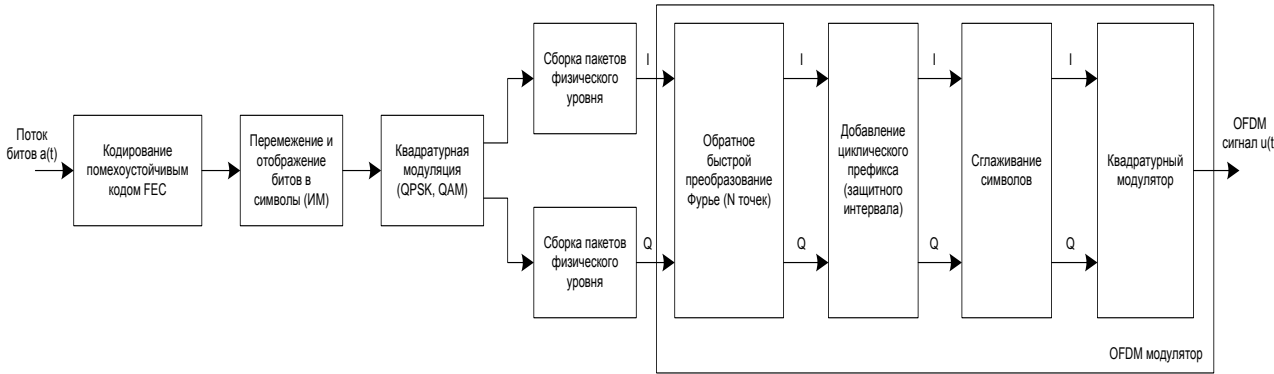


Рис. 21. Формирователь OFDM сигнала стандарта 802.11a

Структура пакетов физического уровня

На физическом уровне пакет представляет собой последовательность в виде преамбулы, заголовка (PLCP-заголовок) и поля данных, за которым следуют хвостовые биты (Tail, равны нулю и обозначают конец поля) и заполняющие биты (Pad), предназначенные для выравнивания длины пакета (рис. 22). Все поля заголовка, кроме поля SERVICE, передаются посредством одного OFDM-символа, причем с наименьшей из возможных скоростей (BPSK, номинальное значение 6 Мбит/с). Оставшаяся часть заголовка и поле данных транслируются с любой заданной скоростью из списка возможных (см. табл. 1).

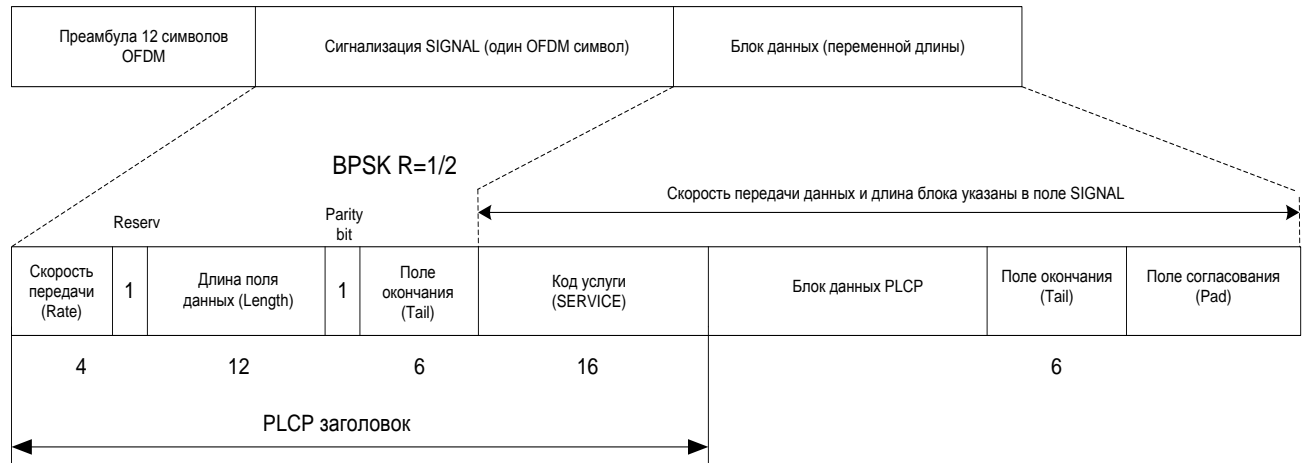


Рис. 22. Структура блока данных физического уровня PLCP

Собственно преамбула PLCP предназначена для обеспечения синхронизации и содержит 12 символов, 10 из которых — «короткие» символы ($\tau=12/\Delta f_{nn}$), а два - «длинные» ($\tau=53/\Delta f_{nn}$).

В коротких последовательностях OFDM-символы формируются на основе лишь 12 поднесущих, при этом применяется модуляция QPSK. Длительность короткой настроенной последовательности - 0,8 мкс, защитных интервалов

между символами нет (рис. 23). Короткие настроечные последовательности предназначены для автоматической настройки усилителей сигнала (APU), обнаружения OFDM сигнала, а также грубой временной и частотной синхронизации.

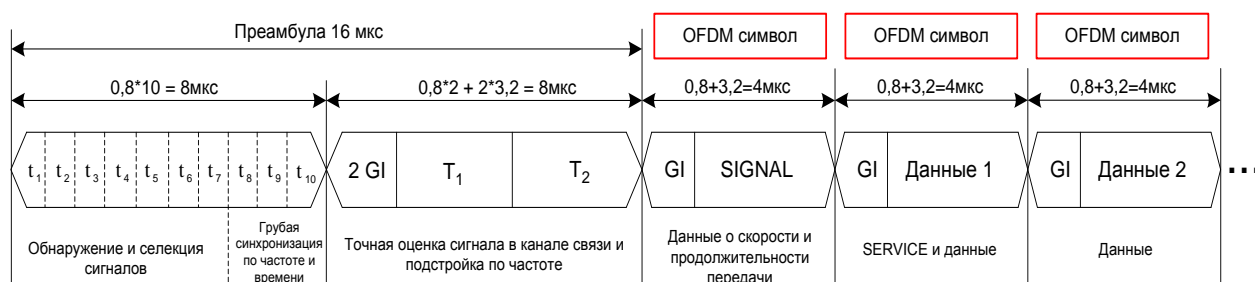


Рис. 23. Последовательность первых OFDM символов блока данных физического уровня PLCP

Две длинные настроечные последовательности следуют за короткими с промежутком в два защитных интервала $GI = 0,8$ мкс. Каждой из последовательностей соответствуют OFDM-символы, включающие 53 поднесущие, в том числе центральную f_0 . При формировании символов используются двоичная фазовая модуляция (BPSK) каждой поднесущей и сверточный код с кодовой скоростью $R = 1/2$, длительность символов - 3,2 мкс, защитных интервалов между символами нет. Длинные последовательности предназначены для оценки канала и точной частотной подстройки приемников. Таким образом, длительность передачи преамбулы составляет 16 мкс.

За преамбулой следует PLCP-заголовок физического пакета. Он состоит из двух фрагментов – сигнализации SIGNAL и поля услуг SERVICE. Фрагмент SIGNAL всегда занимает один OFDM-символ и передается без шифрования посредством BPSK-модуляции со скоростью кодирования $R = 1/2$. Во фрагменте SIGNAL передается информация о скорости передачи поля данных (поле RATE) и количестве байт в нем (LENGTH). Число бит в поле данных пропорционально числу бит на один символ OFDM (48, 96, 192 или 288). Для надежности используется бит контроля четности (Parity). Шесть последних бит (Tail), всегда равных нулю, обозначают завершение фрагмента SIGNAL.

Фрагмент SERVICE (16 бит) формально принадлежит заголовку, но входит в поле данных и передается с выбранной для передачи данных скоростью. Используются только младшие семь бит поля SERVICE (для инициализации генератора псевдослучайной последовательности в приемнике), перед скремблированием они всегда равны нулю. Остальные девять бит в стандарте 802.11a не задействованы.

Поле данных завершают 6 разделительных нулевых бит Tail. Они добавляются после шифрования и служат как дополнительное средство контроля ошибок, поскольку в приемнике после сверточного декодера их значения должны оказаться равными нулю. Кроме того, в конце пакета

добавляются специальные биты заполнения Pad (равны нулю), так чтобы общая длина поля данных (включая фрагмент SERVICE) оказалась кратной числу бит в OFDM-символе при выбранной скорости передачи данных.

Процесс формирования блока данных PLCP в 802.11a заключается в следующем [1,3,5].

Создается поле преамбулы, содержащее 10 коротких символов длительностью $\tau=12/\Delta f_{nn}$ и два длинные символа $\tau=53/\Delta f_{nn}$, служащие для настройки приемника терминала-получателя.

В соответствии с выбранной скоростью передачи данных определяются параметры OFDM сигнала, которые устанавливаются в поле услуг SERVICE блока данных (длина поля данных в символах, мощность излучения, скорость передачи данных, параметры преамбулы). Результирующая строка двоичных символов заполняется нулевыми символами, так чтобы общая длина строки была кратна числу бит, приходящихся на один OFDM-символ (N_0). Полученная строка объединяется с блоком данных MAC-уровня MPDU в пакет.

Над полученной строкой выполняется скремблирование сложением по модулю 2 с псевдослучайным сигналом. Скремблированию не подвергаются данные поля параметров сигнала. К N_0 битам скремблированной последовательности добавляются шесть концевых нулевых битов, опознаваемых сверточным кодером как «нулевое состояние» и обозначающих завершение информационной строки.

Далее полученная строка подвергается сверточному кодированию. Сверточный код имеет длину кодового ограничения $L = 7$ и порождается полиномами $g_1(x) = 133$ и $g_2(x) = 171$. Исходя из выбранной скорости передачи данных скорость кодирования может составлять $1/2$, $2/3$ и $3/4$. Скорость кодирования - это отношение числа бит в пакете до и после кодера (скорость кодирования $R= 1/2$ означает, что каждому входному биту после кодирования будет соответствовать два бита на выходе кодера). Значения скорости кодирования, отличные от $1/2$, получаются путем исключения из выходной последовательности отдельных битов (перфирирование).

Далее поток кодированных бит подвергается перемежению (Interliving) - изменяется порядок битов в последовательности в пределах OFDM-символа. Вся последовательность кодированных битов разбивается на блоки, длина которых равна числу бит в OFDM-символе (N_{CBPS}) при выбранной скорости передачи. В пределах блока биты нумеруются от 0 до $N_{CBPS} - 1$. Затем происходит двухэтапная перестановка битов. Цель первого этапа - добиться, чтобы смежные биты последовательности оказались на несмежных поднесущих OFDM-символа. Первый этап перемежения эквивалентен тому, что данные последовательно по строкам записываются в таблицу из 16 строк и $N_{CBPS} / 16$ столбцов, а затем последовательно считываются по столбцам.

После второго этапа перестановки смежные биты оказываются попеременно в старших и младших разрядах групп, определяющих модуляционный символ

квадратурной модуляции. Это делается для того, чтобы соседние биты не оказались в младших разрядах, надежность передачи которых наиболее низка.

При изменении скоростей сверточного кодирования и видов модуляции каждой поднесущей можно получить широкий диапазон скоростей передачи данных. В табл. 1 приведены скорости передачи данных, соответствующие конкретным скоростям кодирования и типам модуляции.

Таблица 1

Скорость передачи данных, Мбит/с	Вид модуляции	Скорость кодирования	Количество бит на поднесущую N_{CBPS}	Количество бит на символ OFDM $N_{\text{пн}}$	Количество бит данных на символ OFDM N_0
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

После перемежения и кодирования символы подвергаются модуляции в соответствии с табл. 1.

Как было отмечено выше, при передаче данных в стандарте 802.11a используются 52 поднесущие при общем числе поднесущих, равном 64. Последнее значение выбрано из соображений удобства преобразования Фурье – как ближайшее к 52 число, кратное степени 2. Таким образом, интервал между поднесущими $\Delta f_{\text{пн}} = \Delta F_{\text{OFDM}}/N = 312,5$ кГц, а сами поднесущие можно представить как $u(t) = U_{\text{пн}} \sin(2\pi(f_0 + n\Delta f_{\text{пн}})t + \varphi_n)$, где $n = -26, \dots, 26$; $U_{\text{пн}}$ – амплитуда n -й поднесущей, $f_0 + n\Delta f_{\text{пн}}$ – центральная частота поднесущей; φ_n – начальная фаза. Центральная поднесущая f_0 не используется, ее амплитуда всегда равна нулю.

После перемежения поток битов делится на группы по количеству $N_{\text{пн}}$ (табл. 1), а в пределах каждой группы – на блоки по N_{CBPS} битов в соответствии с заданным видом квадратурной модуляции. Блоки из $k=N_{CBPS}$ битов $B = \{b_0, b_1, \dots, b_k\}$ в квадратурных модуляторах отображаются в комплексные числа согласно сигнально-кодовому созвездию текущего вида модуляции (рис. 24).

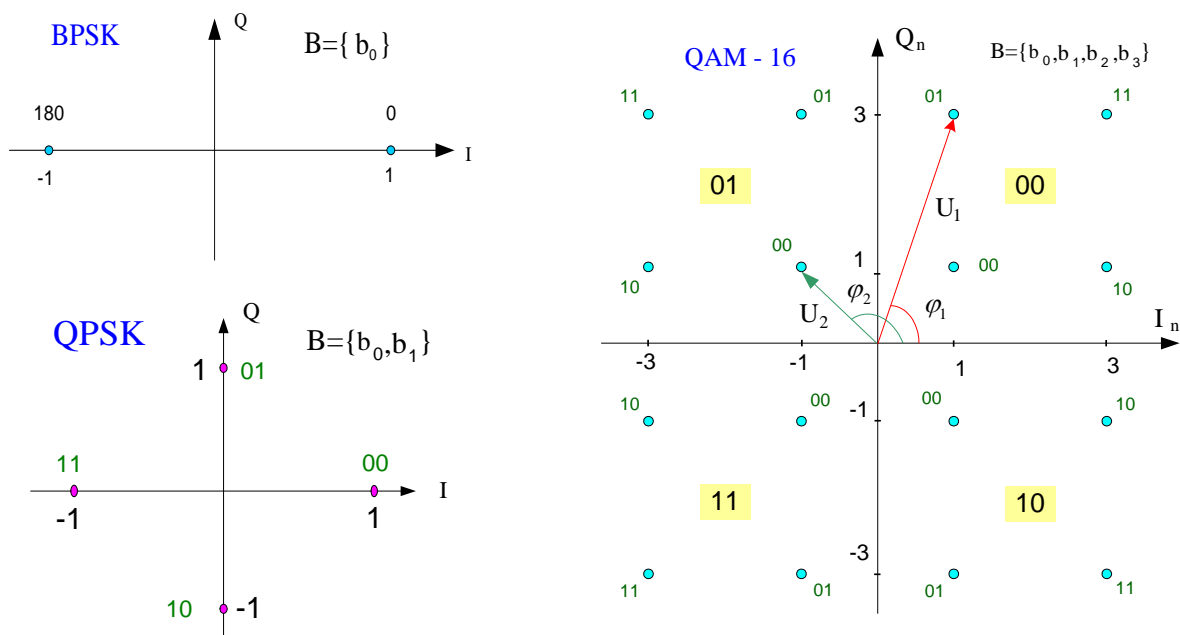


Рис. 24. Представление модуляционных символов

Поток комплексных чисел с выхода модулятора делится на группы по 48 символов. Каждая такая группа ассоциируется с OFDM-символом (48 информационных поднесущих). В каждой группе комплексные числа обозначаются 0...47 и отображаются на OFDM-поднесущие, нумеруемые -26...-22, -20...-8, -6...-1, 0, 1...6, 8...20, 22...26. Поднесущие с номерами -21, -7, 7 и 21 используются для передачи пилот-сигнала. Нулевая поднесущая соответствует центральной частоте OFDM сигнала и устанавливается в нулевое значение. Таким образом, общее число поднесущих $53 = 48 + 4 + 1$.

Группа из 53 символов (будущие поднесущие -26...26) дополняется слева 6-ю и справа 5-ю нулевыми символами (соответствующие этим символам крайние поднесущие информацию не переносят) (рис. 25). Над результирующей группой символов, состоящей из 64 символа (2^6), применяется обратное преобразование Фурье (ОБПФ) с целью формирования OFDM сигнала. При этом к каждому OFDM символу добавляется защитный интервал GI (циклический префикс).

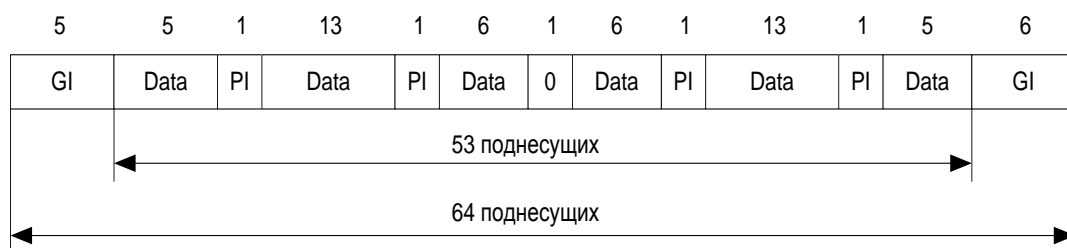


Рис. 25. Структура поднесущих (символ OFDM) стандарта 802.11a

Сформированные таким образом OFDM-символы переносятся в область 5 ГГц :

$$u_{OFDM}(t) = U_m e^{j\omega_0 t} \sum_{n=-N/2}^{N/2} C_n e^{j\varphi_n} e^{j2\pi f_n t}$$

и один за другим передаются в канал связи после символа SIGNAL, описывающего скорость передачи и длину блока данных MPDU (рис. 22, 23).

В табл. 2 даны значения параметров стандарта 802.11a для уровня PLCP.

Таблица 2

Параметр	Значение
Число поднесущих, используемых для передачи данных $N_{\text{пн}}$	48
Число пилот-сигналов N_{pi}	4
Общее число поднесущих	64
Ширина спектра OFDM сигнала	20 МГц
Полоса частот на поднесущую $\Delta f_{\text{пн}}$	0,3125 МГц (20 МГц/64)
Цикл быстрого прямого/обратного преобразования Фурье T_0	3,2 мкс ($1/\Delta f_{\text{пн}}$)
Длительность преамбулы PLCP	16 мкс
Период следования OFDM символов T_{OFDM}	4 мкс
Длительность защитного интервала $T_{\text{зи}}$	0,8 мкс
Длительность защитного интервала (преамбула)	1,6 мкс
Длительность обучающих «коротких» символов	8 мкс
Длительность обучающих «длинных» символов	8 мкс
Расстояние между наиболее удаленными поднесущими	16,25 МГц

Каждый OFDM-символ для обеспечения когерентного приема и повышения устойчивости к фазовому шуму содержит четыре пилот-сигнала, которые модулируются с помощью BPSK.

В соответствии со стандартом 802.11a диапазон частот 5 ГГц делится на 3 поддиапазона: нижний 5,15...5,25 ГГц, средний - 5,25...5,35 ГГц и верхний - 5,725...5,825 ГГц. Стандарт допускает три уровня излучения передатчика в соответствии с назначением диапазонов частот (табл. 3).

Таблица 3

Диапазон, ГГц	Номер канала	Частота, МГц	Максимальная выходная мощность, мВт
Нижний диапазон 5,15...5,25	36	5180	40 (2,5 мВт/МГц)
	40	5200	
	44	5220	
	48	5240	
Средний диапазон 5,25...5,35	52	5260	200 (12,5 мВт/МГц)
	56	5280	
	60	5300	
	64	5320	
Верхний диапазон 5,725...5,825	149	5745	800 (50 мВт/МГц)
	153	5765	
	157	5785	
	161	5805	

Спецификация 802.11a также определяет минимально допустимые параметры терминалов [4, 5]. В табл. 4 приведены минимальная чувствительность приемника, степень подавления помех от соседнего канала и степень подавления перекрестных помех от соседнего канала (alternate adjacent channel rejection) для возможных скоростей передачи данных при PER (packet error rate) менее 10% и длине PSDU 1000 байт. Кроме того, уровень полезного сигнала на входе приемника должен на 3 дБ превышать уровень минимальной чувствительности устройства и уровень сигнала помех, задаваемый указанным и таблице отношением.

Таблица 4

Скорость передачи данных, Мбит/с	Минимальная чувствительность, дБм	Подавление помех от соседнего канала, дБ	Подавление перекрестных помех от соседнего канала, дБ
6	-82	16	32
9	-81	15	31
12	-79	13	29
18	-77	11	27
24	-74	8	24
36	-70	4	20
48	-66	0	16
54	-65	-1	15

II. ЛАБОРАТОРНАЯ РАБОТА

ИЗУЧЕНИЕ СИГНАЛОВ ФИЗИЧЕСКОГО УРОВНЯ СТАНДАРТА 802.11A

Цель работы

Изучение общих принципов работы сети 802.11 и исследование особенностей работы устройств формирования и приема сигналов физического уровня стандарта 802.11a (WiFi).

Краткое описание модели физического уровня стандарта 802.11a

Работа проводится с использованием системы функционального моделирования System View. Модель физического уровня стандарта 802.11a включает в себя все необходимые компоненты, предусмотренные стандартом, и изображена на рис. 26.

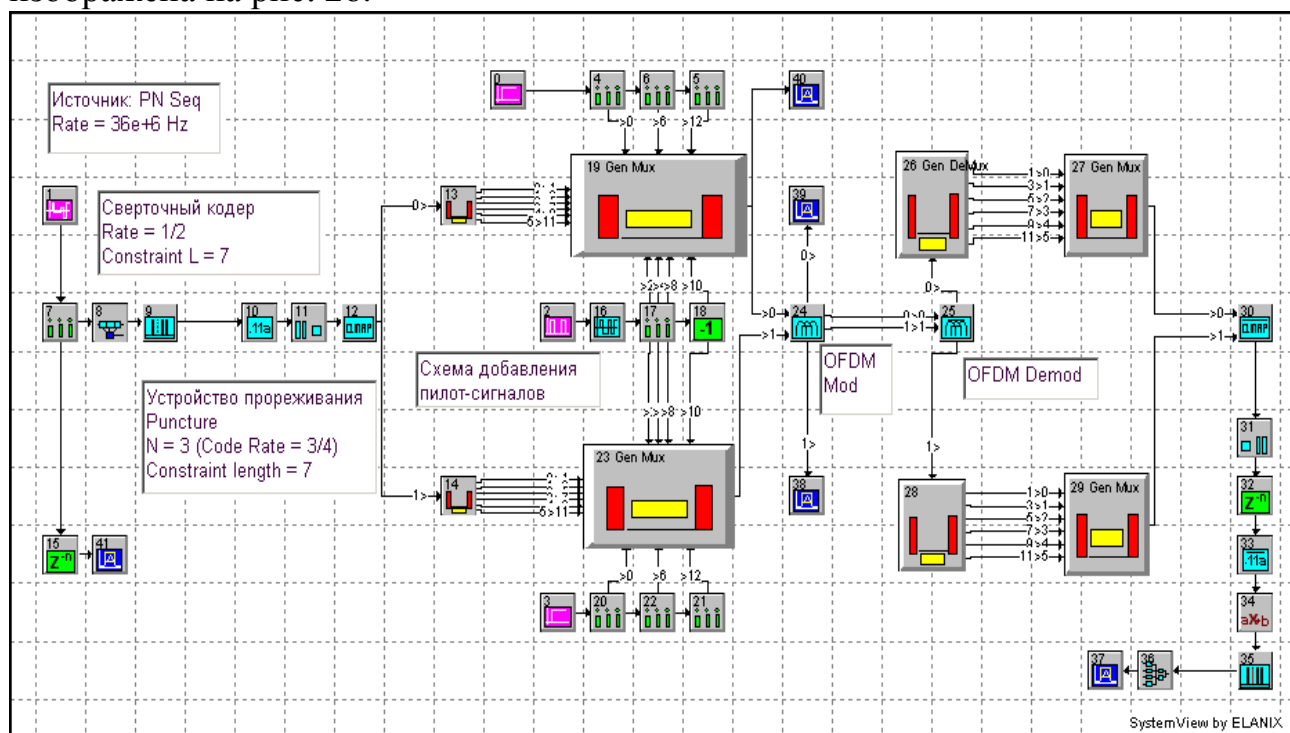


Рис. 26. Модель физического уровня стандарта 802.11a

Блок <1> формирует двоичную последовательность импульсов, следующих со скоростью R_b (в качестве примера $R_b=36$ Мбит/с). Данная модель может быть настроена на любую из доступных в стандарте 802.11a скоростей передачи данных (табл.1).

Модуль <7> осуществляет преобразование потока импульсов в поток битов – дискретизацию поступающего сигнала с частотой $R_b=36$ МГц. Тип выборки (*Sampler Type*): **Non-Interp Right**.

Сверточный кодер <8> (библиотека *Comm*, группа *Encode/Decode*, модуль *Cnv Coder*) работает со скоростью $\frac{1}{2}$, кодовое ограничение *Constraint* $L = 7$, длина блока *Code Length* $n = 2$, информационная часть *Info Bits* $k = 1$.

Устройство прореживания <9> выполняет функцию частичного прореживания потока битов с выхода сверточного кодера с целью получения требуемой скорости кодирования ($N=3$ и *Constraint length* $= 7$ для $R_{code}=\frac{3}{4}$ при $R_b=36$ Мбит/с, табл.1). Этот блок находится в дополнительной библиотеке *Comm*, группа *Encode/Decode*, блок *Puncture*.

Блок <10> (*Intrlv.11a*) осуществляет блоковое перемежение битов в соответствии со спецификацией 802.11a, размер блока $N_{\text{пп}}$ ($N_{\text{пп}}=192$ бита для $R_b=36$ Мбит/с, табл. 1). Единственный параметр модуля <10> – значение R_b . Этот блок находится в дополнительной библиотеке *Comm*, группа *Filters/Data*.

С выхода перемежителя поток битов поступает на импульсный модулятор <11> (библиотека *Comm*, группа *Encode/Decode*, модуль *Bit->Sym*), где осуществляется объединение битов в группы по $N_{CBPS}=k=\log_2 M$ символов (параметр *Bits/Symbol* блока <11>), M – позиционность модуляции (при $R_b=36$ Мбит/с согласно табл. 1 $M=16$, $N_{CBPS}=4$).

Модулятор <12> (*QAM Map*, располагается в дополнительной библиотеке *Comm*, группа *Processors*), используемый в модуле, реализует QAM-16: *Constellation Size* $= 16$. С выхода модулятора комплексный сигнал, имеющий 2 составляющие I и Q , по двум каналам поступает на формирователь OFDM символа. **Скорость следования символов на входе OFDM модулятора не зависит от значения R_b и составляет $12 \cdot 10^6$ симв/с = 48 инф. символа / 4мкс.**

Формирователь OFDM символа осуществляет формирование блока из 64 символов в соответствии с рис. 25. Модули <2>, <16>, <17>, <18> формируют биты, составляющие пилот-сигнал (4 поднесущие в одном OFDM символе). Группы модулей <3>, <20>, <22>, <23> и <0>, <4>, <5>, <6> заполняют нулевым значением соответствующие позиции блока символов (рис. 25, поле GI). Демультимплексоры <13> и <14> формируют 6 сегментов данных общим объемом 48 информационных символов (по количеству полей *Data*, рис. 25). В мультимплексорах к этим 6-ти сегментам добавляются 4 символа пилот-сигналов (поле PI, рис. 25) и сегменты, заполненные нулевыми битами (поля GI).

Сформированная таким образом строка символов отображается модулятором OFDM <24> (дополнительная библиотека *Comm*, группа *Modulators*, модуль *OFDM Mod*) в 64 поднесущие. Параметры модулятора должны соответствовать табл. 2 (*Samples Per Block* $= 64$, *Symbol Time* $= 4\text{e-}6$ sec, *Guard Time* $= 800\text{e-}9$ sec). С целью упрощения исследования смещение OFDM сигнала в область высоких частот не используется. Моделирование таким образом осуществляется на видеочастоте.

Остальная часть схемы реализует приемное устройство стандарта 802.11a и, в сущности, выполняет обратные действия. Отдельного пояснения требует блок задержки <32>, необходимый для обеспечения синхронной работы перемежителя <10> и деперемежителя <33>. Модуль <34> преобразует

двоичный поток битов (0,1) в бинарный (-1,1), это достигается линейной операцией $y = -1 + 2x$.

Поскольку в стандарте 802.11a используется прореживание битового потока, применение сверточного декодера, работающего по жесткой схеме, оказывается невозможным. Декодирование прореженного потока битов должно осуществляться по мягкой схеме (*Soft Decision*) на основе алгоритма Витерби. Параметры сверточного декодера <36> представлены в табл. 5.

Таблица 5

Soft Decision Code Length $n=2$ Info Bits $k = 1$	Constraint $L = 7$ Polynomial = oct Path Length = 15	Threshold = 0 v Offset = подлежит определению Bin Size = $100e-3$ v	Signal Mean = 1 v Eb/No = 10 dB Bits = 3
--	--	--	--

Домашнее задание

1. Ознакомиться с теоретическими сведениями о построении и принципах функционирования сети стандарта 802.11.
2. Изучить описание модели физического уровня стандарта 802.11a.
3. Провести анализ модели физического уровня стандарта 802.11a с целью ее настройки на максимальную скорость передачи данных 54 Мбит/с. Указать блоки модели, параметры которых надо изменить, обосновать новые значения параметров. Результат работы свести в таблицу.

Лабораторное задание

1. Запустить программу System View, загрузить шаблон проекта (... \G802.11a\template.svu). Шаблон проекта включает в себя настроенные модули формирования и разборки OFDM символов. Сохранить файл проекта под новым именем.


2. На основе шаблона проекта собрать модель системы в соответствии с рис. 26. Установить корректные параметры блоков (на основании краткого описания работы и в соответствии с табл. 1) за исключением модулей задержки (определяются в процессе работы). **Особое внимание необходимо уделить согласованному подключению квадратурных каналов приемника и передатчика.** Скорость передачи данных установить равной $R_b=36$ Мбит/с. Системную частоту дискретизации выбрать равной $2R_b$, количество выборок 16384.

3. Подключить окна анализа к модулятору OFDM <24>. Провести моделирование. Пронаблюдать спектр OFDM сигнала. Поскольку выходной сигнал <24> комплексный, то для выполнения этой задачи требуется построить спектр комплексного сигнала.

- /// Спектр комплексного сигнала получается с помощью многофункционального
- /// калькулятора Sink Calculator, группа Cmplx FFT. В таблице Complex FFT

- ✓ выбирается требуемый результат преобразования, в окнах справа – выходные
- ✓ квадратурные сигналы модулятора OFDM.

В рамках текущего задания требуется получить амплитудный спектр сигнала (значение $\text{Complex FFT} = \text{Magnitude}$) и спектр мощности ($\text{Complex FFT} = 20\lg|\text{FFT}|$). Указать размерности по осям, определить центральную частоту спектра, его ширину. Наложить на полученные рисунки теоретический «шаблон» спектра OFDM сигнала (64-х полосного), выявить и объяснить отличия.

4. Пронаблюдать OFDM символ. Для этого подключить к мультиплексору <19> окно анализа и после запуска системы выбрать Sink Calculator, группу *Style*, функцию *Slice*. Выбрав параметр *Samples*, указать в поле *Start* значение 0, в поле *length* значение 64. В окне справа выбрать соответствующее окно анализа. Получив изображение пакета, выбрать режим отображения отсчетов  и зафиксировать в виде числовой строки значения каждого из 64 наблюдаемых символов; при неоднозначном значении символа обозначить его константой c_i (т.е. использовать обозначения 0, ± 1 , $\pm c_i$).

5. Зафиксировать параметры демультимплексора <13>, мультиплексора <19>, блоков <0>, <4>, <5>, <6>, а также <2>, <16>, <17>, <18>. Объяснить значения установленных параметров. Построить схему формирования полей OFDM-символа.

6. Построить сигнально-кодовое созвездие QAM-16. Для этого подключить к выходам I и Q модулятора окна анализа (к блокам <19> и <23> соответственно) и, выполнив моделирование, перейти в раздел *Sink Calculator*, выбрать в группе *Style* функцию *Scatter Plot*, указав при этом в окнах выбора соответствующие источники.

7. Зафиксировать скорости цифровых потоков блоков <7> - <13>, <19>, <24>. Значение скорости соответствует параметру *Max Rate*, которое можно получить из меню контекстной подсказки путем наведения курсора мыши на соответствующий модуль. Привести объяснение.

8. Настроить приемное устройство. Настройка подразумевает установку значения задержки модуля <32> и параметра *Offset* сверточного декодера. Для этого требуется выполнить следующие действия:

- а) убедиться в правильности настройки OFDM демодулятора – построить сигнально-кодовое созвездие QAM-16, пользуясь выходными сигналами блоков <27> и <29>. Сравнить полученное созвездие с требуемым видом;
- б) настроить синхронную работу перемежителя и деперемежителя. Для этого установить фиксированную задержку в блоке <32>, равную $N_{\text{пн}} - N_{\text{CBPS}}$ отсчетам (табл. 1);
- в) определить значение параметра *Offset* сверточного декодера. Для этого подключить к <8> и <35> окна анализа и измерить задержку сигналов. Найденное значение присвоить параметру *Offset*;

г) найти общую задержку сигналов - с выходов блока <7> и <36>, найденное значение записать в модуль <15>. Зафиксировать и сравнить переданный и принятый сигналы. Сделать выводы.

9. Добавить в проект схему вычисления вероятности битовой ошибки (рис. 27). Проверить равенство нулю этой вероятности для текущих параметров модели.

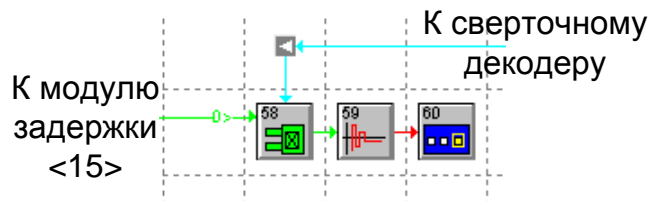


Рис. 27. Измеритель вероятности битовой ошибки

10. Добавить между модулятором и демодулятором модели многолучевого каналов связи (группа *Channel Models*, блок *Mpth Chn*) – для каждого квадратурного канала. Установить число лучей $No. Paths = 3$; К-фактор в диапазоне 30-50. Значение К-фактора определяет отношение мощности первого пришедшего луча к суммарной мощности всех остальных. Максимальную избыточную задержку *Max Delay* рассчитать исходя из размера области активных переотражений порядка 30-50м.

11. Зарисовать сигнально-кодовое созвездие QAM-16 принятого сигнала (выходные сигналы блоков <27> и <29>) в условиях многолучевого распространения для различных значений К-фактора (**значения менять одновременно для обоих квадратурных каналов**).

12. Провести измерение вероятности битовой ошибки в условиях многолучевого распространения. С этой целью убрать из проекта все ненужные окна анализа, увеличить количество системных выборок (установить, к примеру, $2^{20} = 1048576$) и получить вероятность битовой ошибки в диапазоне $10^{-4} \dots 10^{-2}$ для различных значений К-фактора.

13. Заменить модель многолучевого канала связи *Mpth Chn* моделью гауссовского канала связи (рис. 28). Дискретизаторы <67> и <69> осуществляют выборку значений шума с частотой 20МГц.

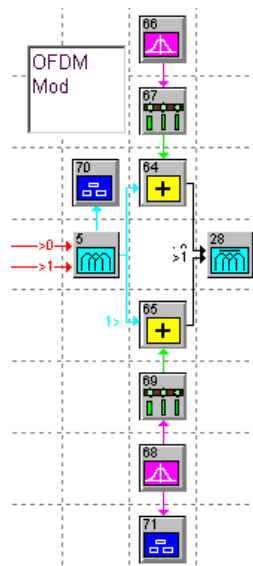


Рис. 28. Модель гауссовского канала связи

14. Уменьшить количество системных выборок до значения $2^{17} = 131072$. Подобрать значение *Pwr Density* источников шума таким образом, чтобы вероятность битовой ошибки была в пределах $10^{-4} \dots 10^{-3}$. Рассчитать полученное отношение сигнал-шум. Зарисовать сигнально-кодовое созвездие QAM-16 принятого сигнала.

Содержание отчета

1. Структурная схема модели физического уровня стандарта 802.11a.
2. Краткое пояснение работы модели.
3. Таблицы, графики, временные диаграммы, полученные в процессе выполнения задания.
4. Краткие выводы по работе с указанием причин расхождения теоретических и экспериментальных данных.

Библиографический список

1. Григорьев В. А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. - М.Эко-Трендз, 2005. -384 с.
2. Весоловский Кшиштоф. Системы подвижной радиосвязи. -М.: Горячая линия-Телеком, 2006.-536 с.
3. Шахнович И. В. Современные технологии беспроводной связи. -М.: Техносфера, 2006.-288 с.
4. Рошан П., Лиэри Д. Основы построения беспроводных локальных сетей стандарта 802.11. -М.: Издательский дом «Вильямс», 2004.-304 с.
5. IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. ANSI/IEEE Std 802.11, 1999 Ed.

Содержание

I. Теоретические сведения о построении и принципах функционирования сети стандарта 802.11	1
1. Введение	1
2. Конфигурации сетей WLAN	1
3. Проблема скрытой станции	4
4. Стандарты IEEE 802.11 для сетей WLAN	6
5. Стандарт IEEE 802.11	7
5.1. Физический уровень IEEE 802.11	9
5.1.1. Физический уровень DSSS	9
5.1.2. Физический уровень FHSS	10
5.1.3. Физический уровень инфракрасного диапазона	10
5.2. Подуровень MAC системы IEEE 802.11	11
5.2.1. Принцип доступа к среде стандарта 802.11	11
5.2.2. Принцип CSMA/CA: контроль несущей	12
5.2.3. Принцип CSMA/CA: распределенная функция координации DCF	13
5.2.4. Принцип CSMA/CA: пакет подтверждения	15
5.2.5. Принцип CSMA/CA: проблема скрытого узла и RTS/CTS	17
5.2.6. Принцип CSMA/CA: фрагментация пакетов	19
5.2.7. Принцип CSMA/CA: итоги	19
5.2.8. Точечная функция координации PCF	20
5.2.9. Механизм PCF: период отсутствия конкуренции	21
5.2.10. Механизм PCF: работа точки координации	22
5.3. Операции, осуществляемые на уровне MAC стандарта 802.11	23
5.3.1. Соединение станций стандарта 802.11	23
5.3.2. Работа терминалов 802.11 в режиме энергосбережения	25
5.3.3. Структура кадров MAC уровня (кратко)	26
6. Роуминг в сети стандарта 802.11	28
7. Стандарты IEEE 802.11a и Hiper LAN для частоты 5 ГГц	29
7.1. Краткая характеристика	29
7.2. Физический уровень организации IEEE 802.11a	30
II. Лабораторная работа. Изучение сигналов физического уровня стандарта 802.11a	38