БЕСПРОВОДНЫЕ ЛОКАЛЬНЫЕ СЕТИ

АНАТОМИЯ СТАНДАРТОВ IEEE 802.11

И.Шахнович

Беспроводные сети передачи данных – это атрибут и символ нового века. Простота развертывания таких сетей ограничена только необходимостью оформления разрешительной документации (в тех странах, где это требуется). А по пропускной способности они не уступают выделенным медным линиям. Помехоустойчивость, надежность и защищенность современных протоколов передачи сделали беспроводные локальные сети (WLAN) явлением повсеместным, а оборудование для них – массовым продуктом. Ежемесячно в мире продается около миллиона адаптеров стандарта IEEE 802.11b – по экспертным оценкам, их установлено уже свыше 20 миллионов. Вместе с тем, рынок массовых устройств беспроводных систем передачи данных очень молод. Первая версия стандарта IEEE 802.11 появилась в 1997 году. Но уже в 1999-м объем продаж устройств для беспроводных сетей достиг 600–770 млн. долл., а к 2004 году, по мнению аналитиков, он составит порядка 2,2–3 млрд. долл. Причем стремительно развиваются сами технологии передачи и оборудование для них – скорости выросли от 1–2 до 54 Мбит/с. С неменьшей стремительностью падает и стоимость оборудования. Ответвлений от родительского древа IEEE 802.11 уже так много, что не мудрено запутаться: в 1999 году появился первый отпрыск – IEEE 802.11b, а сегодня примериваются к оборудованию IEEE 802.11g. А тут еще европейские стандарты – HiperLan и HiperLan2. Разобраться во всем этом непросто, но разбираться надо – и пользователям, и производителям аппаратуры, поскольку отечественный рынок должен бы в первую очередь заполняться аппаратурой российской. А опыт последнего десятилетия подтверждает – в России есть фирмы, умеющие разрабатывать и производить качественную аппаратуру.

ИЗ НОВЕЙШЕЙ ИСТОРИИ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

Прежде всего оговоримся, что нас будут интересовать исключительно локальные вычислительные сети. Поэтому вне нашего внимания останутся такие стандарты персональных сетей, как HomeRF и Bluetooth (IEEE 802.15), с одной стороны, и синхронные широкополосные радиомодемы – с другой. А речь пойдет о Ethernet-подобных беспроводных сетях, принципиально асинхронных по своей природе.

Стартовой вехой беспроводных телекоммуникаций, видимо, следует считать исторический доклад "Об отношении металлических порошков к электрическим колебаниям", сделанный Александром Степановичем Поповым на заседании физического отделения Российского физико-химического общества 7 мая 1895 года. Почти через 80 лет свершилось не менее значимое событие – 22 мая 1973 года сотрудник исследовательского центра компании Xerox в Пало-Альто Роберт Меткалф подал докладную записку, в которой впервые ввел слово "ethernet" и изложил основные принципы работы новой локальной компьютерной сети, воплощенные позднее в стандарте IEEE 802.3, в простонародье именуемом сегодня Ethernet'ом. Интересно, выбирая название для новой технологии, автор сознательно остановился на слове "ether net" (эфирная сеть), предвидя, что через четверть века Ethernet рванется в эфир?

Сейчас устройства для беспроводных локальных сетей, появившиеся в начале-середине 90-х годов – это только история. Но тогда они означали технологический прорыв. Дело, как всегда, оставалось за малым – был необходим единый стандарт. И в июле 1997 года рабочая группа 11 Института инженеров по электротехнике и радиоэлектронике (IEEE) подвела первый итог работы, начатой в 1989 году, опубликовав 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 вытекающие из этого требования к функциям устройств, принципы доступа устройств к каналам связи, формат пакетов передачи, способы аутентификации и защиты данных. Хотя стандарт изначально задумывался как инвариантный по отношению к какому-либо частотному диапазону, на физическом уровне он определял 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 (FHSS) и методом прямой последовательности (DSSS). Скорости устанавливались на уровне 1 и 2 Мбит/с.

Однако в сентябре 1999 года появилось дополнение к стандарту IEEE 802.11 – спецификация IEEE 802.11b. Она рассматривала работу в диапазоне 2,4 ГГц только методом DSSS и расширяла диапа-

зон скоростей до 5,5 и 11 Мбит/с. Практически в то же время был опубликован и стандарт IEEE 802.11a, ориентированный на работу в 5-ГГц диапазоне и суливший скорости до 54 Мбит/с. В конце 1999 года были закончены основные работы по созданию европейского 5-ГГц стандарта беспроводных сетей – HiperLan2 (HiperLan type 2). Совсем недавно появилась черновая версия IEEE 802.11g – высокоскоростной (до 54 Мбит/с) стандарт в диапазоне 2,4 ГГц. А ведь с момента первой публикации IEEE 802.11 прошло чуть более пяти лет.

ОСНОВНЫЕ ПРИНЦИПЫ IEEE 802.11

Рассмотрим подробнее, что представляет собой IEEE 802.11 как базовый для всех последующих спецификаций. Как и все стандарты комитета IEEE 802, IEEE 802.11 рассматривает два нижних уровня модели взаимодействия открытых систем (OSI) – физический и уровень звена данных* (Data Link layer). Причем последний подразделяется на два подуровня. Более верхний – Logical Link Control (LLC) – описан в стандарте IEEE 802.2. Стандарт IEEE 802.11 рассматривает нижний подуровень – Medium Access Control (MAC), т.е. управление доступом к каналу (среде передачи). Иными словами, на физическом уровне стандарт определяет способ работы со средой передачи, скорость и методы модуляции. На MAC-уровне – принцип, по которому устройства используют общий канал, способы подключения и аутентификации устройств к точкам доступа, механизмы защиты данных. Поскольку стандарт IEEE 802.11 разрабатывался как "беспроводной Ethernet" (да и называют его так), он предусматривает пакетную передачу с 48-битовыми адресами пакетов, как и любая сеть Ethernet. Существенно, что все, находящееся в модели OSI "выше" среды передачи, одинаково для всех спецификаций семейства IEEE 802. В результате проводные и беспроводные сети группы IEEE 802 легко сопрягаются друг с другом.

Поскольку речь идет о радиотракте, ключевой вопрос – частотный диапазон. Как любой американский продукт, IEEE 802.11 привязан к действующим в США правилам. Изначально он был ориентирован на диапазон 2,400–2,4835 ГГц с шириной полосы 83,5 МГц. Определяемая стандартом спектральная маска для одного канала приведена на рис.1 (мощность отсчитывается относительно пиков функции sin(x)/x). Ширина канала по уровню –30 дБ составляет 22 МГц, следовательно, в полосе 83,5 МГц возможно три неперекрывающихся канала.

Стандарт предусматривает два основных способа организации локальной сети – по принципу "каждый с каждым" (ad-hoc-сеть) и в виде структурированной сети (рис.2). В первом случае связь устанавливается непосредственно между двумя станциями, все устройства ad-hoc-сети должны находиться в зоне радиовидимости, никакого администрирования не предусмотрено.

В случае структурированных сетей (а как показала практика, это основной способ построения сетей IEEE 802.11) в их составе появляется дополнительное устройство – точка доступа (AP – Access Point), как правило, стационарная и действующая на фиксированном канале. Связь между устройствами происходит только через AP. Через них же возможен выход во внешние проводные сети. В сети IEEE 802.11 может быть несколько AP, объединенных проводной сетью Ethernet. Фактически такая сеть представляет собой набор базовых станций с перекрывающимися зонами охвата. Стандарт IEEE 802.11 предусматривает возможность перемещения устройств из зоны одной AP в зону другой (роуминг), тем самым обеспечивая мобильность. Поскольку для мобильных станций важен вопрос ресурса элементов питания, в стандарте заложен специальный протокол управления энергопотреблением – непосредственно при обмене передающее устройство может перевести приемник в режим ожидания.

*В русскоязычной литературе его еще называют уровнем передачи данных, канальным уровнем.

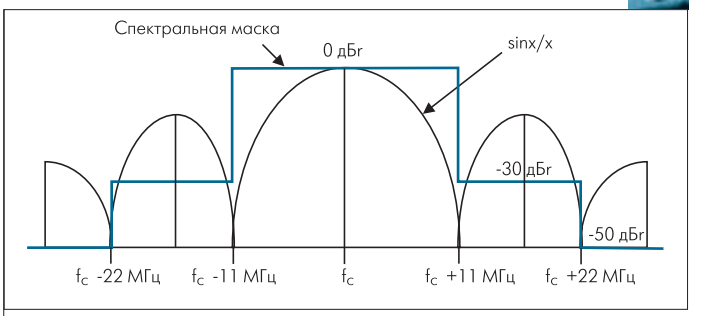

Рис.1. Спектральная маска канала сети 802.11 при модуляции методом DSSS

Как правило, функции управления распределены между всеми устройствами сети IEEE 802.11 – так называемый режим DCF (Distributed coordination function). Однако для структурированных сетей возможен режим Point coordination function (PCF), когда управление передано одной определенной точке доступа. Необходимость в режиме PCF возникает при передаче чувствительной к задержкам информации (например, потоков видеоинформации). Ведь сети семейства IEEE 802 действуют по принципу конкурентного доступа к каналу – приоритетов не существует. Чтобы их при необходимости задавать, и введен режим PCF. Однако работа в данном режиме может происходить только в определенные периодически повторяющиеся интервалы.

Важнейшее требование к стандартам беспроводной связи – это безопасность передачи данных. Памятуя об этом, разработчики на MAC-уровне предусмотрели 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, поэтому его назвали WEP (Wired Equivalent Privacy – эквивалент проводной конфиденциальности). 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 перемножение 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 (IV – initialization vector) и 40-разрядного секретного ключа. Существенно, что если секретный ключ известен устройствам сети и неизменен, то вектор IV может изменяться от пакета к пакету. Для защиты от несанкционированного изменения передаваемой информации каждый шифрованный пакет защища-

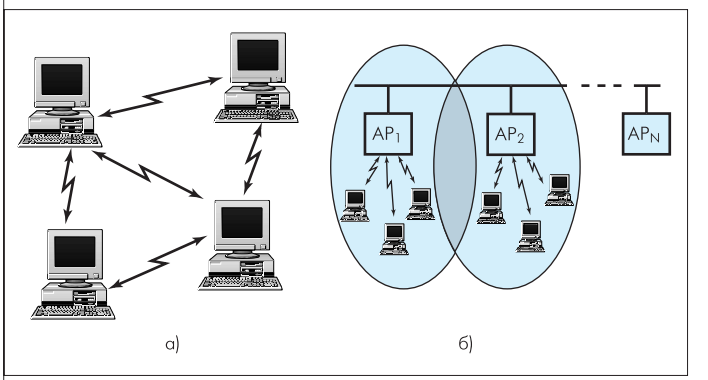

Рис.2. Архитектура сети 802.11: а – ad-hok-сеть, б – распределенная сеть

ется 32-разрядной контрольной суммой (ICV – integrity check value). 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). Отметим, что секретный ключ может быть гораздо длиннее – 64, 128 и т.д. бит. Это не противоречит стандарту, более того, такое оборудование выпускается, однако законодательство США препятствует экспорту устройств, поддерживающих шифрование данных с ключом длиннее 40 бит. Именно поэтому производители и ограничиваются 2^{40} вариантами ключа.

Вообще, защита информации в беспроводных сетях – это отдельная серьезная тема. Специальная группа работает над стандартом IEEE 802.11i, который также называют IEEE 802.X, поскольку закладываемые в него принципы применимы для различных сетей.

Отметим, что устройства, соответствующие исходной спецификации IEEE 802.11, практически не получили развития – не успели. Пропускная способность проводных сетей Ethernet сильно возросла, и максимальная скорость передачи по IEEE 802.11 – 2 Мбит/с – не удовлетворяла пользователей. Проблему на время решило появление стандарта IEEE 802.11b. Благодаря расширенному диапазону скоростей (1; 2; 5,5; 11 Мбит/с) он завоевал массовую популярность. В этой спецификации описаны механизмы передачи в диапазоне 2,4 ГГц только посредством DSSS. Поэтому далее, без умаления общности, будем рассматривать IEEE 802.11 с точки зрения именно IEEE 802.11b.

КАК ПОДЕЛИТЬ КАНАЛ (MAC-УРОВЕНЬ)

Отличия стандарта IEEE 802.11 от других спецификаций семейства IEEE 802 начинаются на MAC-уровне. Как известно, основной принцип Ethernet – это множественный доступ к каналу связи с контролем несущей и обнаружением конфликтов (CSMA/CD – Carrier Sense Multiple Acsses with Collision Detection). Станция может начать передачу, только если канал свободен. Если станции обнаруживают, что на одном канале пытаются работать несколько станций, все они прекращают передачу и пытаются возобновить ее через случайный промежуток времени. Таким образом, даже при передаче устройство должно контролировать канал, т.е. работать на прием.

Но то, что относительно просто при проводной связи, проблематично в беспроводных коммуникациях – затухание сигнала в эфире намного сильнее, чем в проводе. Поэтому возникают две основные проблемы. Во-первых, весьма сложна, если вообще разрешима, задача контроля несущей передающим устройством – когда оно вещает, то собственный сигнал заведомо намного мощнее, чем сигнал удаленного устройства. Во-вторых, возможна ситуация, когда два устройства (A и B) удалены и не слышат друг друга, однако оба попадают в зону охвата третьего устройства C (рис.3) – так называемая проблема скрытой точки. Напомним, в сетях семейства IEEE 802 с конкурентным принципом доступа два устройства не могут одновременно занимать канал. Если же оба устройства A и B начнут передачу, то ни они, ни устройство C методом прослушивания эфира принципиально не смогут обнаружить конфликтную ситуацию и определить, почему пакеты не проходят.

Для устранения подобных проблем в спецификации IEEE 802.11 принят механизм CSMA/CA (Carrier Sense Multiple Acsses with Collision Avoidance) – множественный доступ с контролем несущей и предотвращением коллизий. Перед началом передачи устройство слушает эфир и дожидается, когда канал освободится. Канал считается свободным при условии, что не обнаружено активности в течение определенного промежутка времени – межкадрового интервала (IFS) определенного типа. Если в течение этого промежутка канал оставался свободным, устройство ожидает еще в течение случайного промежутка времени и, если канал еще не занят, передает пакет. Если пакет предназначен конкретному устройству (не широковещательная или многоадресная передача), то приемник, успешно приняв пакет, посылает передатчику короткий пакет подтверждения получения ACK (ACKnowledge). Если передатчик не принял ACK, он считает посланный пакет утерянным и повторяет процедуру его передачи.

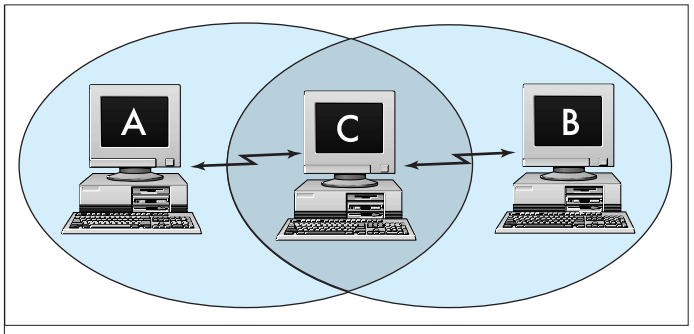

Рис.3. Иллюстрация проблемы скрытой точки

Примечательно, что если устройство повторно передает пакет, для определения незанятости канала оно должно использовать увеличенный межпакетный интервал (EIFS). Кроме того, время ожидания выбирается случайным образом на некотором интервале. При первой попытке передачи этот интервал минимален. При каждой последующей он удваивается до тех пор, пока не достигнет заданного предельного значения. Эти меры приводят к тому, что устройство, успешно передавшее пакет, имеет преимущества в захвате канала (кто ошибается, тот дольше ждет).

Перед первой попыткой получить доступ к каналу устройство загружает длительность случайного интервала ожидания в специальный счетчик. Его значение декрементируется с заданной частотой, пока канал свободен. Как только счетчик обнулится, устройство может занимать канал. Если до обнуления счетчика канал занимает другое устройство, счет останавливается, сохраняя достигнутое значение. При следующей попытке отсчет начинается с сохраненной величины. В результате неуспевший в прошлый раз получает больше шансов занять канал в следующий. В проводных сетях Ethernet подобного механизма нет.

Однако описанные процедуры доступа не избавляют от проблемы "скрытой точки". Для ее преодоления используются два дополнительных пакета – RTS (Request to Send – запрос на передачу) и CTS (Clear to Send – подтверждение готовности). Устройство, желающее отправить пакет данных, передает адресату короткий пакет RTS. Если приемное устройство готово к приему, оно выставляет передающему ответный пакет – CTS. Далее в соответствии с описанной выше процедурой передающее устройство отправляет пакет с данными и дожидается подтверждения ACK.

Стандарт IEEE 802.11 предусматривает два механизма контроля за активностью в канале (обнаружения несущей) – физический и виртуальный. Первый механизм реализован на физическом уровне и сводится к определению уровня сигнала в антенне и сравнению его с пороговой величиной. Виртуальный механизм обнаружения несущей основан на том, что в передаваемых пакетах данных, а также в управляющих пакетах ACK и RTS/CTS содержится информация о времени, необходимом для передачи пакета (или группы пакетов) и получения подтверждения. Все устройства сети получают информацию о текущей передаче и могут определить, сколько времени канал будет занят, – т.е. устройство при установлении связи всем сообщает, на какое время оно резервирует канал.

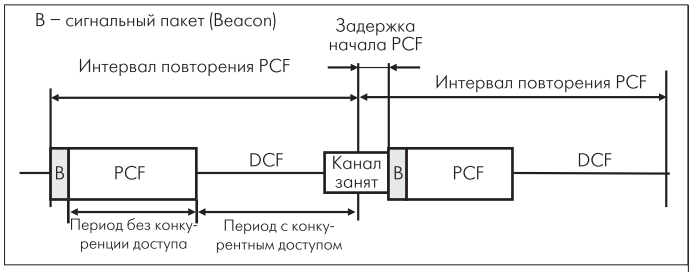

Рис.4. Циклы работы сети в режимах с концентрированным (PCF) и распределенным (DCF) управлением

Все описанные механизмы относятся к сети с распределенным управлением DCF. Однако в сети могут присутствовать и AP, наделенные полномочиями узурпировать управление, – тогда их называют точками координации (PC). Когда сеть переходит в режим PCF, в трафике появляются интервалы, в которых конкурентный доступ отменен, и весь обмен происходит под управлением PC (рис.4). По завершении такого интервала сеть возвращается в режим DCF. Интервалы под управлением PC следуют через строго определенный период, в начале каждого интервала PC выставляет особый сигнальный пакет (Beacon). PC не может передать очередной сигнальный пакет до тех пор, пока канал не освободится, т.е. очередной "свободный от конкуренции" интервал может начаться с задержкой.

Фактически режим PCF – это режим синхронной передачи, под который в асинхронной сети резервируются определенные интервалы. Этот режим позволяет использовать технологию IEEE 802.11 для таких приложений, как передача аудио/видео и других синхронных по своей природе данных.

FRAME'Ы РЕШАЮТ ВСЕ

Как мы уже говорили, весь обмен в сетях IEEE 802.11 происходит посредством отдельных пакетов (frame). По их структуре особенно четко видно разделение на физический и MAC-уровни. Фактически пакет формируется на MAC-уровне, на физическом уровне к нему добавляется заголовок физического уровня (PLCP). На MAC-уровень пакеты передаются от приложений верхнего уровня. Если их размер превышает максимально допустимый в IEEE 802.11, происходит дефрагментация – большой пакет разбивается на несколько меньших, которые передаются по специальной процедуре.

Пакеты MAC-уровня могут быть трех типов – пакеты данных, контрольные (ACK, RTS, CTS и т.п.) и пакеты управления (например, Beacon). Их структура одинакова (рис.5). Каждый пакет включает MAC-заголовок, информационное поле (Frame Body) и контрольную сумму CRC. В заголовке передается полная информация о версии протокола стандарта группы IEEE 802.11, типе пакета, системе защиты и т.д. (поле Frame Control); длительности процедуры передачи пакета (Duration/ID), адреса получателя/отправителя (Address1–4; четыре адресных поля необходимы, если пакеты передаются из подсети одной точки доступа в подсеть другой) и информация о последовательности связанных пакетов (Sequence Control). Информационное поле может быть различной длины или вовсе отсутствовать (в контрольных пакетах).

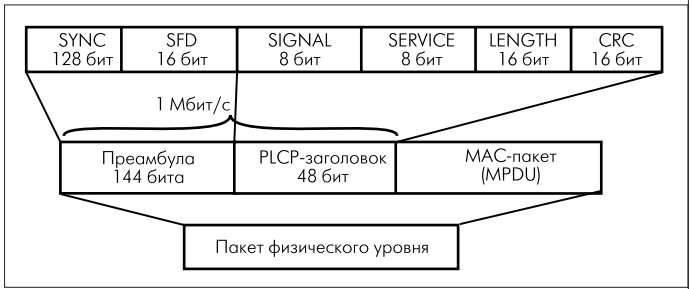

Рис.5. Структура пакетов сети 802.11 MAC-уровня

На физическом уровне к MAC-пакетам (MPDU) добавляется заголовок физического уровня, состоящий из преамбулы и собственно PLCP-заголовка (см. рис.5). Преамбула содержит стартовую синхропоследовательность (SYNC) для настройки приемника и 16-битный код начала пакета (SFD) – число $F3A0_{16}$. PLCP-заголовок включает поля SIGNAL (информация о скорости и типе модуляции), SERVICE (дополнительная информация, в том числе – о применении высокоскоростных расширений и PBSS-модуляции) и LENGTH (время в микросекундах, необходимое для передачи следующей за заголовком части пакета). Все три поля заголовка защищены 16-битной контрольной суммой CRC.

В стандарте IEEE 802.11b предусмотрено два типа заголовков – длинный и короткий (рис.6). Они отличаются длиной синхропоследовательности (128 и 56 бит), способом ее генерации, а также тем, что символ начала пакета в коротком заголовке передается в обратном порядке. Кроме того, если все поля длинного заголовка передаются со скоростью 1 Мбит/с, то при коротком заголовке преамбула транслируется на скорости 1 Мбит/с, другие поля заголовка – со скоростью 2 Мбит/с. Остальную часть пакета можно передавать на любой из допустимых стандартом скоростей передачи, указанных в полях SIGNAL и SERVICE. Короткие заголовки физического уровня предусмотрены спецификацией IEEE 802.1b для увеличения пропускной способности сети.

ГОНКИ ЗА СКОРОСТЬЮ

Из описания процедур связи сети IEEE 802.11 видно, что "накладные расходы" в этом стандарте выше, чем в проводной сети Ethernet. Поэтому крайне важно обеспечить высокую скорость передачи данных в канале. Повысить пропускную способность канала

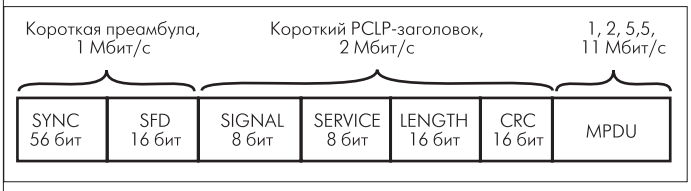

Рис.6. Короткий заголовок пакетов сети 802.11b

с заданной шириной полосы частот можно, разрабатывая и применяя более совершенные методы модуляции. По этому пути пошла группа разработчиков IEEE 802.11b.

Напомним, что изначально стандарт IEEE 802.11 предусматривал работу в режиме DSSS с использованием так называемой Баркеровской последовательности (Barker) длиной 11 бит: B_1 = (10110111000). Каждый информационный бит замещается своим произведением по модулю 2 (операция "исключающее ИЛИ") с данной последовательностью, т.е. каждая информационная единица заменяется на B_1, каждый ноль – на инверсию B_1. В результате бит заменяется последовательностью 11 чипов. Далее сигнал кодируется посредством дифференциальной двух- или четырехпозиционной фазовой модуляции (DBPSK или DQPSK, один или два чипа на символ, соответственно). При частоте модуляции несущей 11 МГц общая скорость составляет, в зависимости от типа модуляции, 1 и 2 Мбит/с.

Стандарт IEEE 802.11b дополнительно предусматривает скорости передачи 11 и 5,5 Мбит/с. Для этого используется так называемая CCK-модуляция (Complementary Code Keying – кодирование

комплементарным кодом). В основу данного метода легли работы специалистов компаний Intersil (ранее – Harris Semiconductor) и отчасти Agere Systems (полупроводниковое подразделение, выделенное из Lucent Technologies). Метод использует DQPSK-модуляцию в радиотракте. CCK-модуляция строится на выделении из последовательного информационного потока групп по 8 бит (d_0–d_7). Эти 8 бит определяют информационный символ C из 8 комплексных чипов $C=[c_0,...,c_7]$. Чипы являются комплексными, поскольку они определяют I- и Q- квадратурные составляющие сигнала для DQPSK. Восемь чипов информационного символа последовательно модулируют несущую с частотой модуляции 11 МГц. Фактически каждый чип представляет собой сигнал несущей частоты с фазовым сдвигом, определяемым формулой для всего символа

$$C=[c_0,...,c_7] = [\varphi_1+\varphi_2+\varphi_3+\varphi_4;\ \varphi_1+\varphi_3+\varphi_4;\ \varphi_1+\varphi_2+\varphi_4;$$
$$-(\varphi_1+\varphi_4);\ \varphi_1+\varphi_2+\varphi_3;\ \varphi_1+\varphi_3;\ -(\varphi_1+\varphi_2);\ \varphi_1]. \quad (1)$$

Элемент φ_1 входит в каждый чип символа, т.е. изменяет фазу всего символа. Фазовая модуляция сигнала называется дифференциальной, поскольку значение φ_1 текущего символа определяется относительно значения φ_1 предшествовавшего символа. Изменение фазы φ_1 задается как $\Delta\varphi_1 = (d_0\ d_1)\cdot\pi/2$ для четных символов, где ($d_0\ d_1$) – двухбитное двоичное число (0–3). Для нечетных символов значение φ_1 дополнительно смещают на π. Как мы уже отмечали, в стандарте IEEE 802.11b посредством CCK кодируют только MAC-пакет. Поэтому первый CCK-символ – тот, что следует сразу за символами заголовка физического уровня. Он имеет номер "0", т.е. является четным. Фаза последнего QPSK-символа заголовка пакета является опорной для определения φ_1 первого символа информационного поля – к нему добавляется $\Delta\varphi_1$. Остальные три параметра имеют абсолютные значения. Для скорости 11 Мбит/с они определяются как $\varphi_2 = (d_2\ d_3)\cdot\pi/2$; $\varphi_3 = (d_4\ d_5)\cdot\pi/2$; $\varphi_4 = (d_6\ d_7)\cdot\pi/2$, где ($d_i\ d_{i+1}$) – двухразрядные двоичные числа.

Для скорости 5,5 Мбит/с используется DBPSK-модуляция, и CCK-символ определяют не восемь, а четыре информационных бита (d_0–d_3), поэтому и скорость вдвое ниже. Параметр φ_1 вычисляется так же, как и для 11 Мбит/с, остальные – иначе: $\varphi_2 = d_2\cdot\pi + \pi/2$; $\varphi_3 = 0$; $\varphi_4 = d_3\cdot\pi$.

В чем достоинство CCK-модуляции? Как видно из формулы (1), чипы символа C определяются на основе последовательностей Уолша-Адамара. Для скорости 11 Мбит/с вектор входных данных $D = [d_0,...,d_7]$ можно представить в виде последовательности четверичных чисел m_1–m_4, где $m_1 = (d_0d_1)$, $m_2 = (d_2d_3)$,..., $m_4 = (d_6d_7)$. Пусть $\mathbf{M} = [m_1,...,m_4]$. Тогда вектор $\mathbf{C} = (\mathbf{M} \times \mathbf{WH} + \mathbf{B})\cdot\pi/2$, где **WH** – верхняя половина матрицы Уолша-Адамара:

$\{\mathbf{WH}\} =$

1	1	1	1	1	1	1	1
1	0	1	0	1	0	1	0
1	1	0	0	1	1	0	0
1	1	1	1	0	0	0	0

Вектор **B** = [0, 0, 0, 2, 0, 0, 2, 0], физически соответствующий повороту фазы чипов c_3 и c_6 на 180° (знаки "минус" в формуле (1)), необходим для улучшения корреляционных свойств кодовых последовательностей. Последовательности Уолша-Адамара хорошо изучены, обладают отличными автокорреляционными свойствами. Что немаловажно, каждая такая последовательность мало коррелирует сама с собой при фазовом сдвиге – очень полезное свойство при борьбе с переотраженными сигналами. Нетрудно заметить, что теоретическое операционное усиление CCK-модуляции – 3 дБ (в два раза), поскольку без кодирования QPSK-модулированный с частотой 11 Мбит/с сигнал может транслировать 22 Мбит в секунду. Как видно, CCK-модуляция представляет собой вид блочного кода, а потому достаточно проста при аппаратной реализации. Совокупность этих свойств и обеспечила CCK место в стандарте IEEE 802.11b в качестве обязательного вида модуляции.

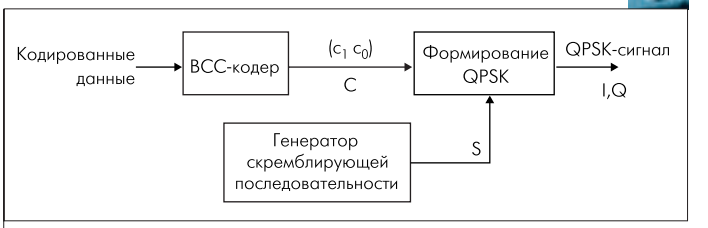

Рис.7. Общая схема PBCC-модуляции

На практике важно не только операционное усиление. Существенную роль играет и равномерность распределения символов в фазовом пространстве – они должны как можно дальше отстоять друг от друга, чтобы минимизировать ошибки их детектирования. И с этой точки зрения CCK-модуляция не выглядит оптимальной, ее реальное операционное усиление не превышает 2 дБ. Поэтому изначально прорабатывался другой способ модуляции – пакетное бинарное сверточное кодирование PBCC (Packet Binary Convolutional Coding). Этот метод вошел в стандарт IEEE 802.11b как дополнительная (необязательная) опция. Механизм PBCC (рис.7) был предложен специалистами фирмы Alantro Communications, в 2000 году вошедшей в состав компании Texas Instruments. PBCC позволяет добиваться в сетях IEEE 802.11b пропускной способности 5,5; 11 и 22 Мбит/с.

Как следует из названия, метод основан на сверточном кодировании. Для скоростей 5,5 и 11 Мбит/с поток информационных битов поступает в шестиразрядный сдвиговый регистр с сумматорами (рис.8а). В начальный момент времени все триггеры сдвигового регистра инициализируют нулем. В результате каждый исходный бит d заменяется двумя битами кодовой последовательности (c_0, c_1). При скорости 11 Мбит/с c_0 и c_1 задают один символ четырехпозиционной QPSK-модуляции. Для скорости 5,5 Мбит/с используют двухпозиционную BPSK-модуляцию, последовательно передавая кодовые биты c_0 и c_1. Если же нужна скорость 22 Мбит/с, схема кодирования усложняется (рис.8б), три кодовых бита (c_0–c_2) определяют один символ в 8-позиционной 8-PSK-модуляции.

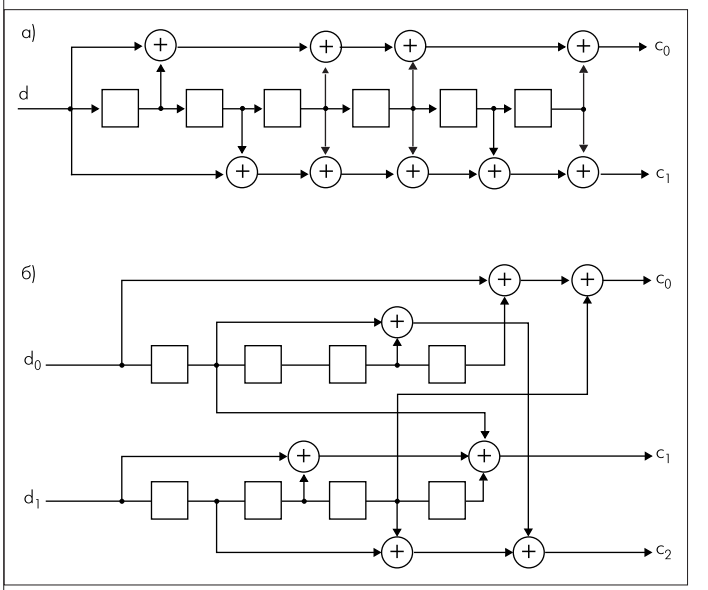

Рис.8. Схема сверточного BCC-кодирования: а – для скоростей 5,5 и 11 Мбит/с; б – для скорости 22 Мбит/с

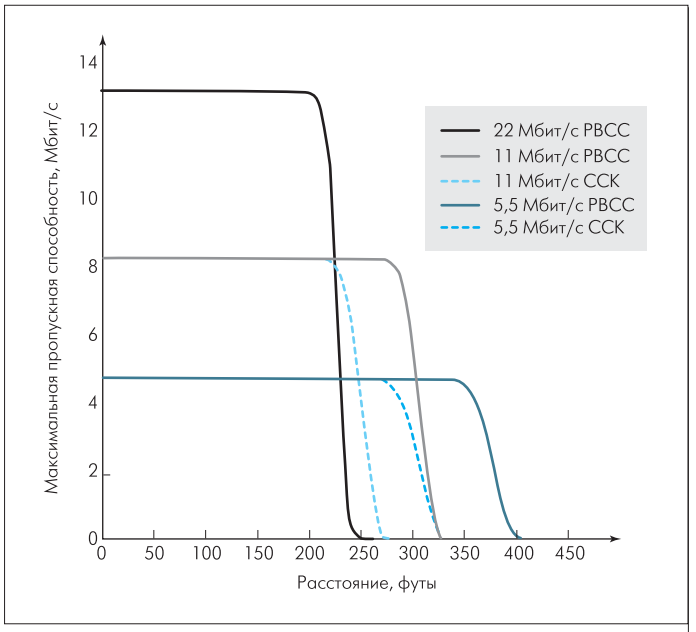

Рис.9. Дальность связи при различных способах модуляции и фиксированном затухании в канале (по материалам компании Texas Instruments о применении ИС ACX100)

После формирования PSK-символов происходит скремблирование. В зависимости от сигнала s (см. рис.7) символ остается без изменений (s=0) либо его фаза увеличивается на π/2 (s=1). Значение s определяет 256-битовая циклически повторяющаяся последовательность S. Она формируется на основе начального вектора $U=338B_{16}$, в котором равное число нулей и единиц. S представляет собой 16 последовательных векторов U_i (i=0, 15), причем каждый вектор U_i циклически сдвинут влево на 3i разряда.

У шестиразрядного сдвигового регистра, применяемого в PBCC для скоростей 11 и 5,5 Мбит/с, 64 возможных выходных состояния. Так что при модуляции PBCC информационные биты в фазовом пространстве оказываются гораздо дальше друг от друга, чем при CCK-модуляции. Поэтому PBCC и позволяет при одних и тех же соотношении сигнал/шум и уровне ошибок вести передачу с большей скоростью, чем в случае CKK (рис.9). Однако плата за более эффективное кодирование – сложность аппаратной реализации данного алгоритма. Видимо, не случайно продвигать PBCC-модуляцию стала компания Texas Instruments – ведущий производитель процессоров цифровой обработки сигнала.

АППАРАТНАЯ РЕАЛИЗАЦИЯ

Чипсеты для оборудования сетей IEEE 802.11b производят многие компании. Кроме упомянутой Texas Instruments, прежде всего сле-

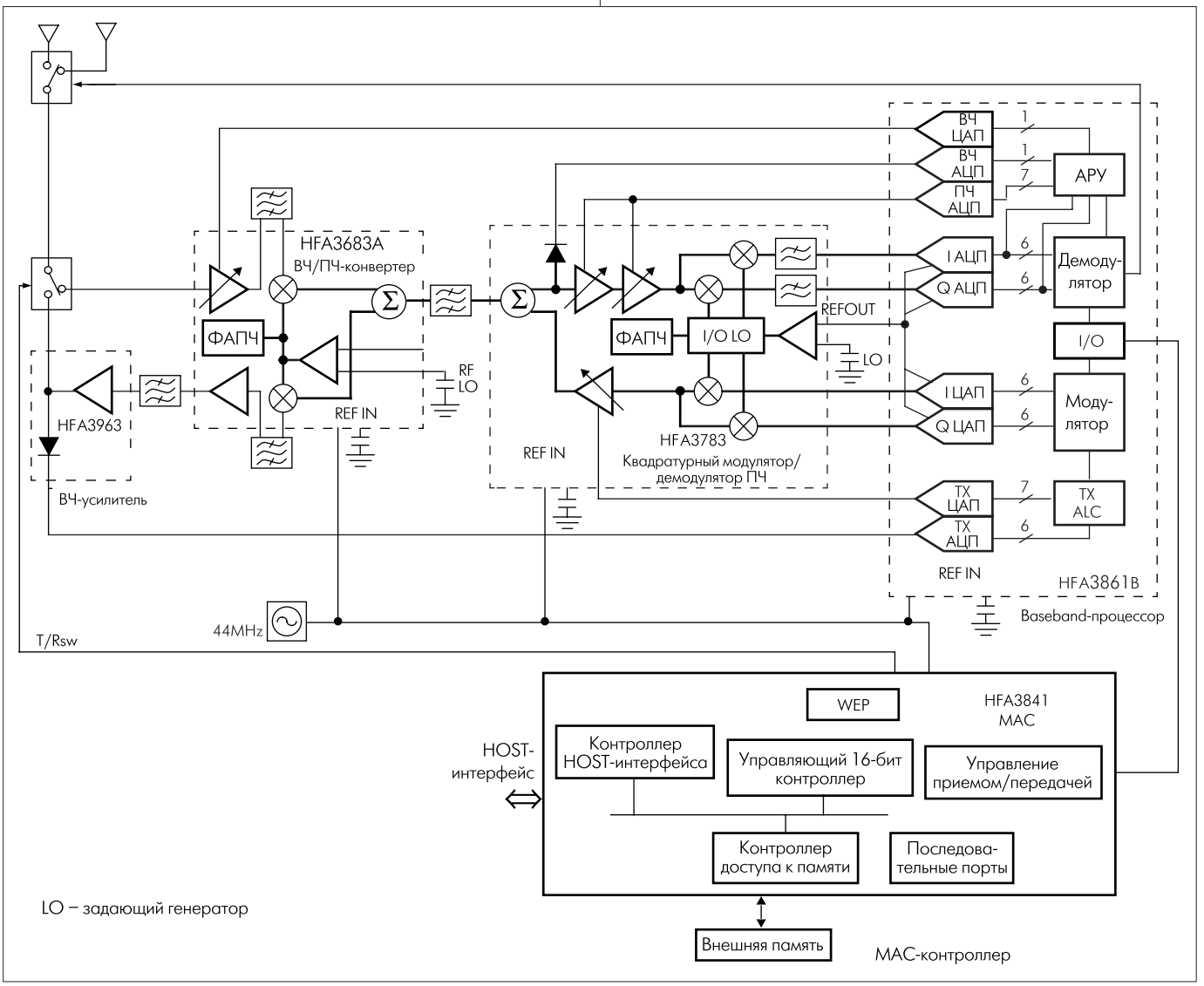

Рис.10. Структурная схема устройства на базе чипсета PRISM 2

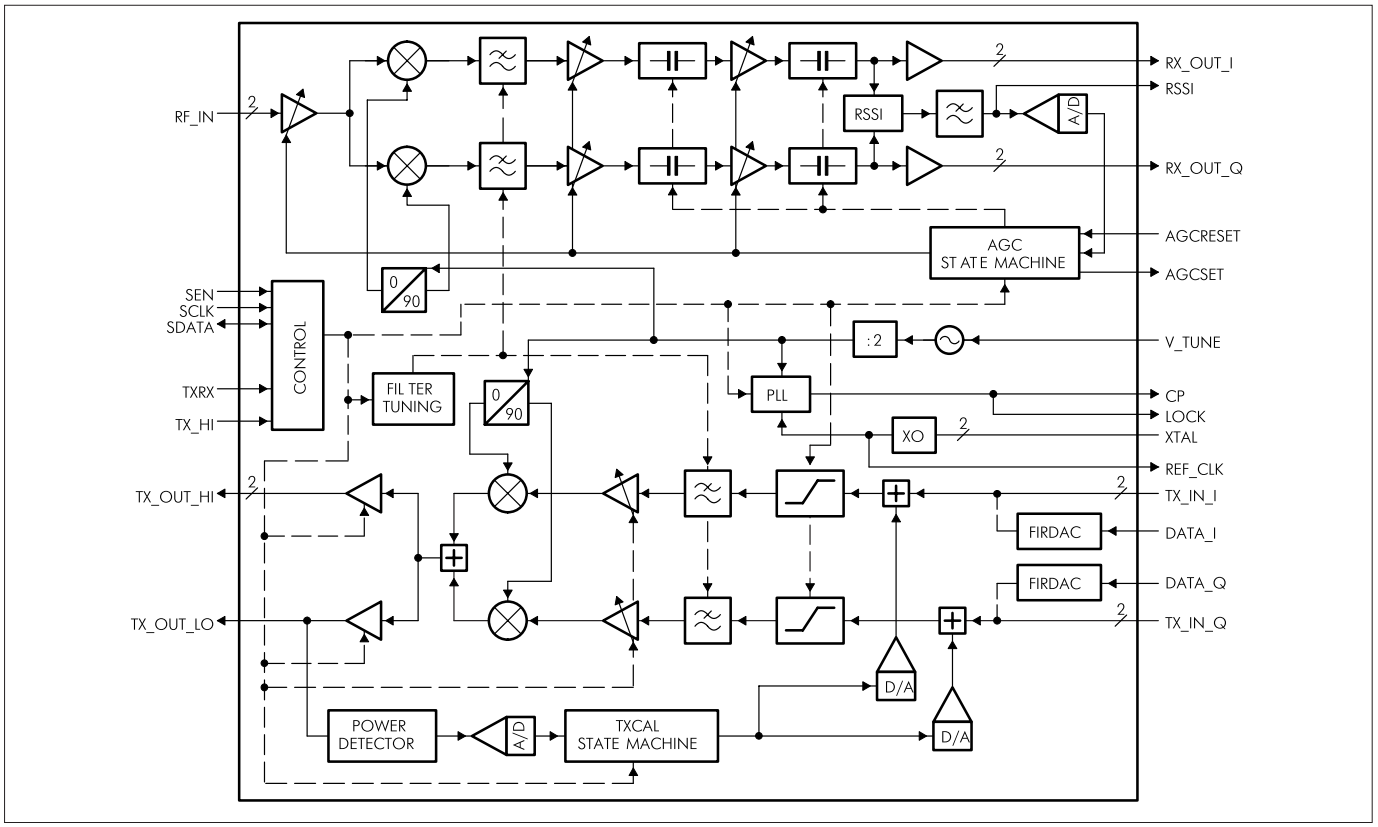

Рис.11. Структурная схема трансивера прямого преобразования SA2400

дует отметить линейку чипсетов PRISM корпорации Intersil. Первый ее чипсет для беспроводных ЛВС включал восемь основных микросхем и сразу привлек к себе внимание разработчиков аппаратуры. Выпущенный же более двух лет назад чипсет PRISM 2 можно рассматривать как базовый для последующих модификаций. В состав PRISM 2 (рис.10) входят четыре ИС – MAC-контроллер HFA3841, baseband-процессор* HFA3861B, квадратурный модулятор/демодулятор на промежуточной частоте (ПЧ) HFA3783 и ВЧ/ПЧ-конвертер HFA3683A. Как правило, для передачи требуется высокочастотный антенный усилитель, например HFA3963. Изначально компания Intersil поставляла данный чипсет по цене порядка 25 долл. (в партии 500 тыс. шт.) и утверждала, что полная стоимость всех необходимых компонентов адаптера IEEE 802.11b на основе PRISM 2 не превысит 50 долл. Но менее чем через год появилась модификация PRISM 2,5, в которой MAC-контроллер и baseband-процессор были интегрированы в одной ИС (ISL3873B), поддерживающей к тому же интерфейсы PCMCIA и USB.

Следующим шагом стало создание к лету 2001 года чипсета PRISM 3 на основе фирменной архитектуры прямого преобразования частоты ZIF (Zero IF, нулевая ПЧ), без использования ПЧ. В результате при цене чипсета 22 долл. стоимость всех компонентов для адаптера на его основе снижается, по мнению разработчиков, до 35 долларов.

Отметим и объявленный чипсет компании Philips Semiconductors, первая ИС которого – однокристальный трансивер SA2400 для диапазона 2,4 ГГц – была анонсирована в июле 2001 года. Данная ИС (рис.11) также построена по принципу прямого преобразования (без ПЧ) и содержит блоки приемника, передатчика, квадратурного модулятора/демодулятора, задающего генератора на основе ГУН и fractional-N-синтезатора, выходного малошумящего усилителя. В составе ИС – полностью интегрированные полосовые канальные фильтры, устройство автоматического контроля усиления, трехпроводная шина управления основными блоками устройства, интерфейс для сопряжения с baseband-процессором и т.д. Вторая микросхема чипсета – SA2440 – это интегрированные baseband-процессор и MAC-контроллер. Специалисты компании Philips утверждают, что устройство IEEE 802.11 на основе их чипсета можно сделать, затратив на все компоненты порядка 8,5 долл. Что ж, подождем появления SA2440. Об аналогичном чипсете (Alchemy, который включает трансивер Am1770 и baseband/MAC-процессор Am1771) объявила и компания AMD.

В ноябре 2002 года корпорация Agere Systems анонсировала свой новый чипсет, в состав которого входят две ИС – контроллер физического уровня и MAC-контроллер. ИС WL1141 – однокристальный контроллер физического уровня, включающий как baseband-процессор, так и аналоговую ВЧ-часть (рис.12). Вместе с MAC-контроллером WL60010 он образует полный чипсет для устройств IEEE 802.11b. Поставки должны начаться в 2003 году, объявленная цена на чипсет – 14 долл.

Надо отметить, что продукты компаний Intersil, Agere Systems, Philips поддерживают только CCK-модуляцию. PBCC реально присутствует практически только в продуктах компании Texas Instruments*.

Первой ИС, реализующей PBCC, стала ACX100 – однокристальный MAC-контроллер с baseband-процессором. Эта ИС, кроме обязательных для стандарта IEEE 802.11b опций, поддерживает PBCC-модуляцию со скоростями 5,5; 11 и 22 Мбит/с. Среди других осо-

*Baseband-процессор – "полосовой" процессор, выполняющий функции цифровой обработки сигнала на физическом уровне, т.е. работающий непосредственно с трактом обмена.

*Если быть точными, следует назвать и корпорацию Ubicom, продукты которой на основе Multi-Protocol-процессора IP2022 этой же компании поддерживают и PBCC. Но в данном случае речь идет исключительно о программной реализации, а не о специализированной ИС.

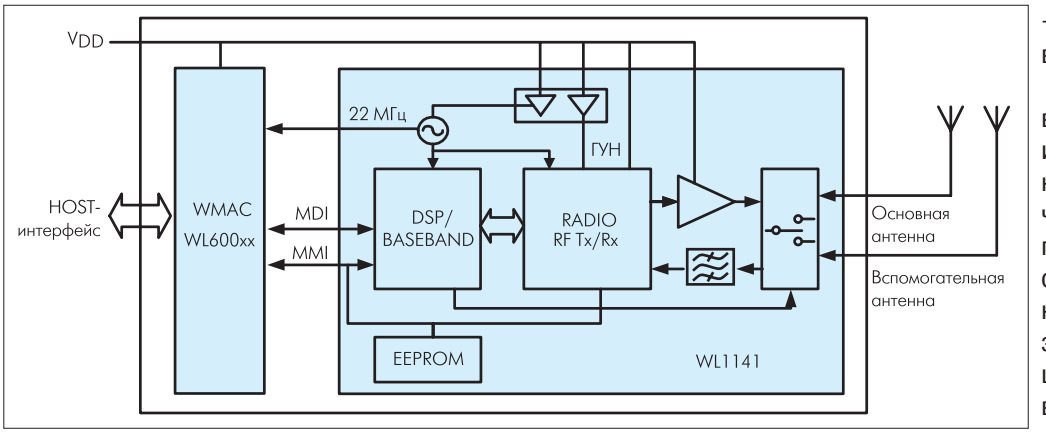

Рис.12. Чипсет компании Agere Systems

бенностей микросхемы – аппаратная поддержка 32-разрядных шин CardBus и PCI, последовательного интерфейса USB 1.1, а также интерфейса Ethernet. Интересно отметить, что при испытаниях устройств на основе этой схемы при одном и том же уровне пакетных ошибок (PER =10^{-2}) и скорости передачи 11 Мбит/с работа в режиме CCK была возможной при отношении сигнал/шум 8,5 дБ, а применение PBCC позволяло ухудшить это соотношение до 4,5 дБ.

Однако, несмотря на все усилия Texas Instruments, режим 22 Мбит/с так и не вошел в стандарт IEEE 802.11b – а ведь даже появилось обозначение "IEEE 802.11b+", устройства на основе ACX100 начали производить такие известные компании, как D-Link и NDC! Не получили распространения и 22-Мбит/с сети. Видимо, тут играют роль два обстоятельства. Прежде всего, процедура стандартизации – это фактически битва за огромный денежный

Рис.13. Структура заголовка физического уровня стандарта IEEE 802.11a

куш в виде лицензионных отчислений тому, чья технология стала стандартной. В данном случае столкнулись интересы двух гигантов полупроводниковой индустрии – компаний Intersil и Texas Instruments. Поддерживать одновременно два вида модуляции накладно, и производителям больше по душе (по карману) пришелся CCK-вариант.

С другой стороны, скорости порядка 22 Мбит/с стали мало интересны потребителям: перед ними открылись новые перспективы – до 54 Мбит/с. А аппаратура на базе PBCC в диапазоне 2,4 ГГц фактически ограничена скоростью 33 Мбит/с.

ВСЕ ВЫШЕ, И ВЫШЕ, И ВЫШЕ...

Стандарт IEEE 802.11a появился практически одновременно с IEEE 802.11b, в сентябре 1999 года. Эта спецификация была ориентирована на работу в 5-ГГц диапазоне. Видимо, в силу технологических проблем – более высокочастотные ИС сложнее в производстве и дороже – версия "a" как бы задержалась в развитии.

Стандарт IEEE 802.11a основывается на принципиально ином, чем описано выше, механизме кодирования данных – на частотном мультиплексировании посредством ортогональных несущих (OFDM). Метод достаточно хорошо известен, он используется, в частности, в системах цифрового телевизионного вещания DVB, поэтому мы не будем подробно описывать этот механизм*.

В IEEE 802.11a каждый пакет передается посредством 52 ортогональных несущих, каждая с шириной полосы порядка 300 кГц (20 МГц / 64). Ширина одного канала – 20 МГц. Несущие модулируют посредством BPSK, QPSK и 16- и 64-позиционной квадратурной амплитудной модуляции (QAM). В совокупности с различными скоростями кодирования r (1/2 и 3/4, для 64-QAM – 2/3 и 3/4)** образуется набор скоростей передачи 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с.

Из 52 несущих 48 предназначены для передачи информационных символов, остальные 4 – служебные. Структура заголовков физического уровня отличается от принятого в спецификации IEEE 802.11b, но не существенно (рис.13). Пакет включает преамбулу (12 символов синхропоследовательности), заголовок физического уровня (PLCP-заголовок) и собственно информационное поле, сформированное на MAC-уровне. В заголовке передается информация о скорости кодирования, типе модуляции и длине пакета. Преамбула и заголовок транслируются с минимально возможной скоростью (BPSK, r=1/2). Информационное поле – с указанной в заголовке, как правило максимальной, скоростью, в зависимости от условий обмена. OFDM-символы передаются через каждые 4 мкс, причем каждому символу длительностью 3,2 мкс предшествует 0,8-мкс защитный интервал (повторяющаяся часть символа). Последний необходим для борьбы с многолучевым распространением сигнала – отраженный и при-

*Конкурирующие стандарты цифрового телевизионного вещания. – ЭЛЕКТРОНИКА: НТБ, 2002, №1, с. 18–19.

**Скорость кодирования показывает отношение числа исходных битов к числу битов кодированной последовательности, т.е. r = 3/4 означает, что из трех исходных битов образуется четырехбитовая кодовая последовательность.

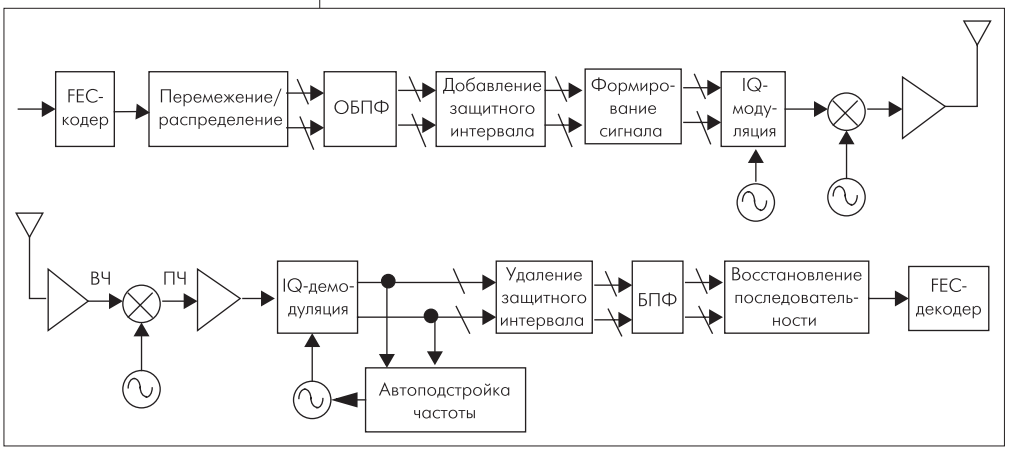

Рис.14. Функциональная схема трактов приема/передачи стандарта IEEE 802.11a

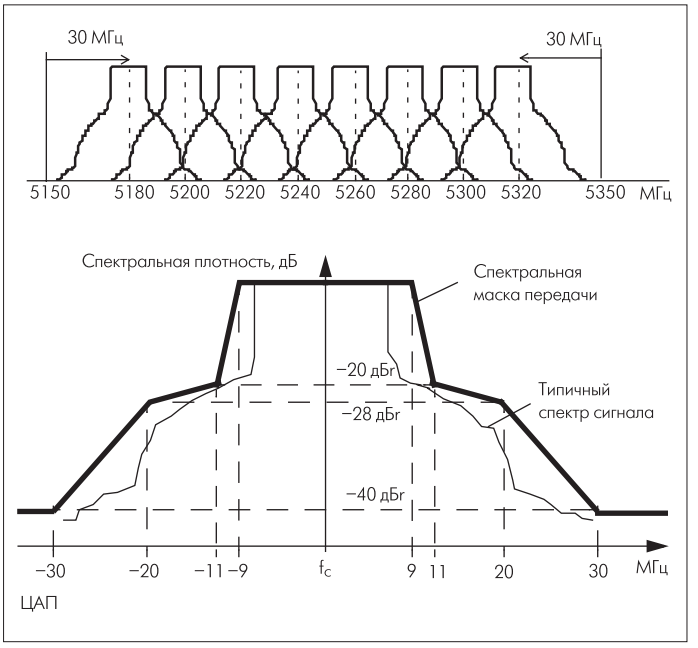

Рис.15. Спектральная маска и распределение неперекрывающихся каналов в диапазоне 5,15–5,35 ГГц для стандарта IEEE 802.11a

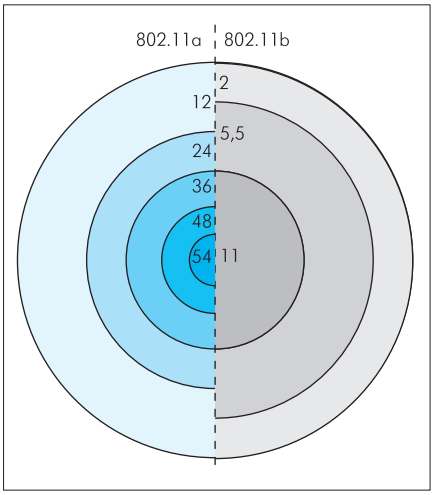

Рис.16. Соотношение скоростей передачи устройств стандартов 802.11a и 802.11b (по материалам компании Proxim)

шедший с задержкой символ попадет в защитный интервал и не повредит следующий символ.

Естественно, формирование/декодирование OFDM-символов происходит посредством быстрого преобразования Фурье (обратного /прямого, ОБПФ/БПФ). Функциональная схема трактов приема/передачи (рис.14) достаточно стандартна для данного метода и включает сверточный кодер, механизм перемежения/перераспределения (защита от пакетных ошибок) и процессор ОБПФ. Фурье-процессор, собственно, и формирует суммарный сигнал, после чего к символу добавляется защитный интервал, окончательно формируется OFDM-символ и посредством квадратурного модулятора/конвертера переносится в заданную частотную область. При приеме все происходит в обратном порядке.

Диапазон 5,1–5,9 ГГц хорош тем, что там гораздо проще найти широкую полосу для системы связи. В США для безлицензионной работы в этом диапазоне выделены полосы 5,15–5,35 и 5,725–5,825 ГГц – всего 300 МГц по сравнению с 83 МГц в диапазоне 2,4 ГГц. Вместо трех неперекрывающихся каналов для сетей IEEE 802.11b – только в нижнем поддиапазоне 5,15–5,35 ГГц восемь неперекрывающихся каналов (рис.15). Аналогичная ситуация и в Европе, и даже в России (только у нас нет безлицензионных диапазонов) – в более высокочастотной области места больше. В частности, если в Москве диапазон 2,4 ГГц разобран операторами достаточно давно, то 5-ГГц область еще только начинают осваивать, хотя свободных поддиапазонов там уже практически нет.

Кроме того, диапазон 2,4 ГГц перегружен различными системами – тут и беспроводные телефоны, и устройства Bluetooth, и многочисленное оборудование стандарта IEEE 802.11b. Взаимных помех избежать тяжело. Сравнительные испытания убедительно показывают, что в одних и тех же условиях устройства IEEE 802.11a по скорости обмена превосходят оборудование IEEE 802.11b (рис.16). И до недавнего времени казалось, что будущее принадлежит сетям стандарта IEEE 802.11a. Но возник ряд “но”.

Прежде всего, как быть с уже существующими сетями (и оборудованием) в диапазоне 2,4 ГГц? Как обеспечить столь необходимую всем обратную совместимость? С этой проблемой производители справились, разработав двухдиапазонные чипсеты. Характерный пример – компания Atheros, создавшая комплект из трех ИС AR5001X Combo. В его составе – ИС baseband-процессора и MAC-контроллера AR5211 и две аналоговые ИС трансиверов – на 2,4 и на 5 ГГц (AR2111 и AR5111, соответственно). Аналогичное решение предложено и компанией Intersil – чипсет PRISM Duette из двух ИС (рис.17): baseband/MAC-процессор ISL3890 и однокристальный двухдиапазонный трансивер ISL3690.

Однако когда данные решения стали технологически возможны и рентабельны, у стандарта IEEE 802.11a появились конкуренты. Во-первых, в Европе был разработан свой 5-ГГц стандарт – HiperLan2. Кроме того, работы по ускорению стандарта IEEE 802.11b в диапазоне 2,4 ГГц привели к появлению новой версии – IEEE 802.11g, предусматривающей скорости до 54 Мбит/с. Точнее, стандарта как такового официально пока нет, есть только черновой (draft) вариант, однако производители не стесняются указывать о его поддержке. В частности, рассмотренные выше чипсеты AR5001X Combo и PRISM Duette в диапазоне 2,4 ГГц поддерживают не только IEEE 802.11b, но и IEEE 802.11g. Однако об интриге высокоскоростных стандартов беспроводных сетей, которая разворачивается буквально у нас на глазах (PRISM Duette анонсирован в конце октября 2002 года на выставке Comdex), мы поговорим в следующий раз.

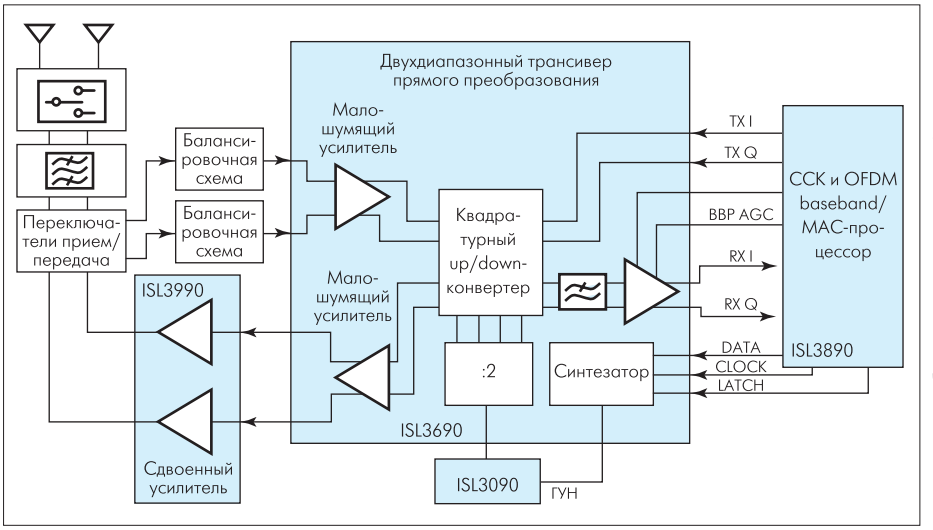

Рис.17. Чипсет PRISM Duette

Продолжение следует.