Беспроводные системы ПД
Передача данных в беспроводных сетях

Лекция 1
Общие понятия и классификация

Беспроводные технологии — подкласс информационных технологий, служат для передачи информации на расстояние между двумя и более точками, не требуя связи их проводами. Для передачи информации может использоваться инфракрасное излучение, радиоволны, оптическое или лазерное излучение.

В настоящее время существует множество беспроводных технологий, наиболее часто известных пользователям по их маркетинговым названиям, таким как Wi-Fi, WiMAX, Bluetooth. Каждая технология обладает определёнными характеристиками, которые определяют её область применения.

Классификация беспроводных технологий

По типу системы передачи:

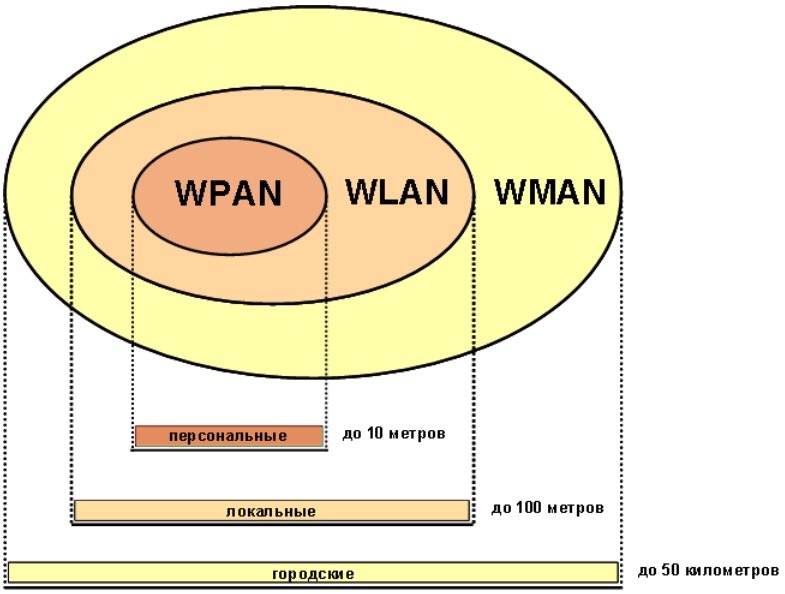
1. Радиоволны (Bluetooth, Wi-Fi, ...)
2. Оптическое/лазерное/ИК излучение (FSO, Li-Fi, IrDA)
3. Звуковые волны (передача данных ультразвуком, протокол Dhwani)

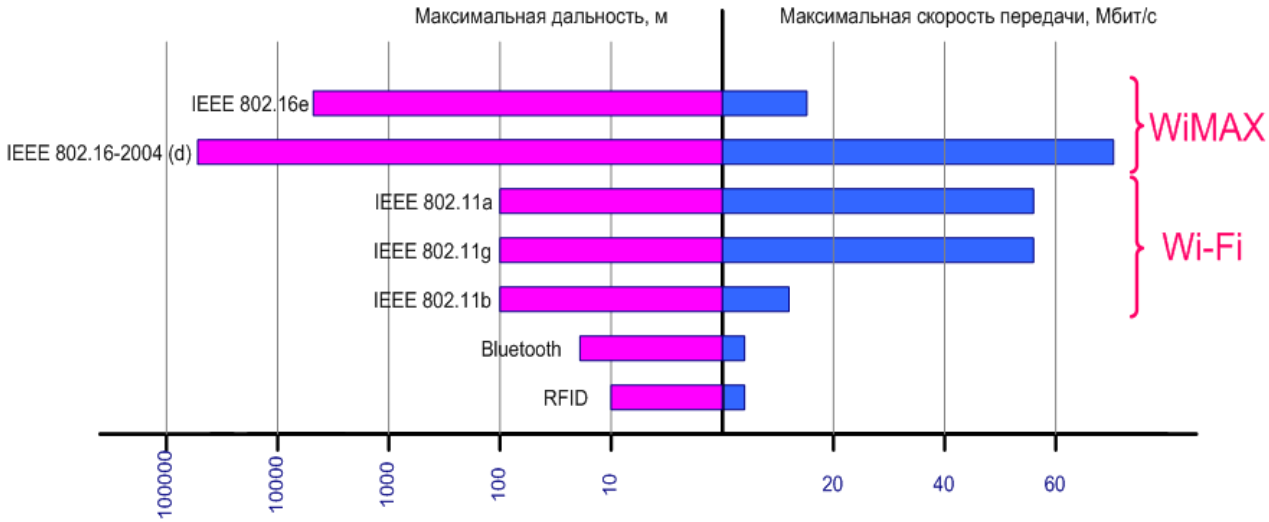
По дальности действия:

1. Беспроводные персональные сети (WPAN — Wireless Personal Area Networks). Примеры технологий — Bluetooth, ZigBee. Стандарт WPAN разработан рабочей группой IEEE 802.15. WPAN применяются для связи различных устройств, включая компьютерную, бытовую и оргтехнику, средства связи и т. д. Радиус действия WPAN составляет от нескольких метров до нескольких десятков сантиметров. WPAN используется как для объединения отдельных устройств между собой, так и для связи их с сетями более высокого уровня, например, глобальной сетью интернет.
2. Беспроводные локальные сети (WLAN — Wireless Local Area Networks). Примеры технологий — Wi-Fi.
3. Беспроводная сеть масштафа кампуса (WCAN — Wireless Campus Area Networks). Объединяет несколько близко расположенных зданий. Такой вариант выделяется далеко не всегда и обычно представляет собой увеличенную сеть, построенную по технологии WLAN с привлечением дополнительных технологий для обеспечения связи между зданиями. Например, в зданиях — Wi-Fi, а между зданиями — АОЛС (FSO).
4. Беспроводные сети масштаба города (WMAN — Wireless Metropolitan Area Networks). Примеры технологий — WiMAX. Предоставляют широкополосный доступ к сети через радиоканал. Основной стандарт — IEEE 802.16. Опубликован в 2002, описывает wireless MAN Air Interface. 802.16 — это так называемая технология «последней мили», которая использует диапазон частот

от 10 до 66 GHz. Так как это сантиметровый и миллиметровый диапазон, то необходимо условие «прямой видимости».

5. Беспроводные глобальные сети (WWAN — Wireless Wide Area Network). Для передачи данных в них используются технологии ПД по сетям мобильной связи — CSD, GPRS, EDGE, EV-DO, HSPA. Соответствующие услуги связи предлагаются, как правило, на платной основе операторами регионального, национального или даже глобального масштаба. С точки зрения видов коммутации в сетях передачи данных сети WWAN могут быть построены на основе коммутации пакетов (GPRS) или коммутации каналов (CSD, HSCSD).





По топологии:

1. «Точка-точка».
2. «Каждый-с-каждым» или «полносвязная топология».
3. «Звезда». В такой топологии все данные передаются через центральный узел — беспроводной коммутатор — точку доступа.
4. «Дерево» или «иерархическая звезда». Первый узел дерева принято называть корнем, следующие узлы высокого уровня — родительскими, а узлы более

низкого уровня — дочерними. Таким образом каждый дочерний узел, который имеет связь с более низкими узлами, является для этих узлов родительским.

5. «Ячеистая топология» или «mesh-сеть». Получается из полносвязной топологии путём удаления некоторых связей. построенная на принципе ячеек, в которой рабочие станции сети соединяются друг с другом и способны принимать на себя роль коммутатора для остальных участников. Данная организация сети является достаточно сложной в настройке, однако, в ней реализуется высокая отказоустойчивость. Большое количество связей обеспечивает широкий выбор маршрута следования трафика внутри сети — следовательно, обрыв одного соединения не нарушит функционирования сети в целом.

По области применения:

1. Корпоративные (ведомственные) беспроводные сети — создаваемые компаниями для собственных нужд.
2. Операторские беспроводные сети — создаваемые операторами связи для возмездного оказания услуг.
3. Беспроводные сенсорные сети или беспроводные сети датчиков (WSN — Wireless Sensor Networks). Примеры технологий — ZigBee. Это распределённая, самоорганизующаяся сеть множества датчиков и исполнительных устройств, объединённых между собой посредством радиоканала. Область покрытия подобной сети может составлять от нескольких метров до нескольких километров за счёт способности ретрансляции сообщений от одного узла к другому.

Беспроводная самоорганизующаяся сеть

Беспроводная ad-hoc-сеть (беспроводная динамическая сеть, беспроводная самоорганизующаяся сеть) — децентрализованная беспроводная сеть, не имеющая постоянной структуры. Клиентские устройства соединяются «на лету», образуя собой сеть. Каждый узел сети пытается переслать данные, предназначенные другим узлам. При этом определение того, какому узлу пересылать данные, производится динамически, на основании связности сети. Это является отличием от проводных сетей и управляемых беспроводных сетей, в которых задачу управления потоками данных выполняют маршрутизаторы.

Классификация

По иерархии
- одноранговые
- mesh-сети

По применению
- беспроводная сенсорная сеть
- транспортная ad hoc-сеть

По мобильности

- мобильные самоорганизующиеся сети

MANET (Mobile Ad hoc Network) — беспроводные мобильные децентрализованные самоорганизующиеся сети. Состоят из мобильных устройств. Каждое такое устройство может независимо передвигаться в любых направлениях, и, как следствие, часто разрывать и устанавливать соединения с соседями.

MANET относятся к одноранговым сетям. Такие сети состоят из однотипных узлов, где каждый узел обладает комплексом программно-аппаратных средств, позволяющих организовать передачу данных от источника к получателю напрямую при физическом наличии такого пути и тем самым распределить нагрузку на сеть и повысить суммарную пропускную способность сети. ПД между двумя абонентами может происходить, даже в случае если они находятся вне зоны прямой радио видимости. В этих случаях пакеты данных этих абонентов ретранслируются другими узлами сети, которые имеют связь с корреспондирующими абонентами. Сети с многократной ретрансляцией называются многопролетными или многоскачковыми (multihop). При разработке таких сетей основными проблемами являются маршрутизация пакетов от узла источника к узлу получателю, масштабируемость сетей, адресация оконечных устройств, поддержание связности в условиях переменной топологии.

Вариантом MANET являются сети VANET — Vehicular Ad Hoc Network, предназначенные для ПД между движущимися автомобилями. Также используют и другой термин — IVC — inter-vehicle communication — межавтомобильная передача данных. Считается, что сети VANET будут одним из ключевых компонентов интеллектуальной транспортной системы.

Главным препятствием к организации сетей MANET является отсутствие беспроводной технологии, позволяющей решить все проблемы, возникающие при работе и организации сети. Существующие беспроводные технологии обладают теми или иными ограничениями, например, большинство этих технологий не предназначены для работы одноранговой сети.

Классификация радиосетей

По частотному диапазону:

МСЭ	Длины волн	Название волн	Диапазон частот	Название частот	Применение
ELF	100-10 Мм	Декамегаметровые (СДВ)	3-30 Гц	Крайне низкие (КНЧ)	Связь с подводными лодками, геофизические исследования
SLF	10-1 Мм	Мегаметровые (СДВ)	30-300 Гц	Сверхнизкие (СНЧ)	
ULF	1000-100 км	Гектокилометровые (СДВ)	300-3000 Гц	Инфранизкие (ИНЧ)	Связь с подводными лодками
VLF	100-10 км	Мириаметровые (СДВ)	3-30 кГц	Очень низкие (ОНЧ)	Служба точного времени, радиосвязь с подводными лодками

МСЭ	Длины волн	Название волн	Диапазон частот	Название частот	Применение
LF	10-1 км	Километровые (ДВ)	30-300 кГц	Низкие (НЧ)	Радиовещание, радиосвязь земной волной, навигация
MF	1000-100 м	Гектометровые	300-3000 кГц	Средние (СЧ)	Радиовещание и радиосвязь земной волной и ионосферная
HF	100-10 м	Декаметровые (КВ)	3-30 МГц	Высокие (ВЧ)	Радиовещание и радиосвязь ионосферная, загоризонтная радиолокация, рации
VHF	10-1 м	Метровые волны (УКВ)	30-300 МГц	Очень высокие (ОВЧ)	Телевидение, радиовещание, радиосвязь тропосферная и прямой волной, рации
UHF	1000-100 мм	Дециметровые (УКВ)	300-3000 МГц	Ультравысокие (УВЧ)	Телевидение, радиосвязь тропосферная и прямой волной, мобильные телефоны, рации, УВЧ-терапия, микроволновые печи, спутниковая навигация.
SHF	100-10 мм	Сантиметровые (УКВ)	3-30 ГГц	Сверхвысокие (СВЧ)	Радиолокация, интернет, спутниковое телевещание, спутниковая- и радиосвязь прямой волной, беспроводные компьютерные сети.
EHF	10-1 мм	Миллиметровые	30-300 ГГц	Крайне высокие (КВЧ)	Радиоастрономия, высокоскоростная радиорелейная связь, радиолокация (метеорологическая, управление вооружением), медицина, спутниковая радиосвязь.
THF	1-0,1 мм	Децимиллиметр.	300-3000 ГГц	Гипервысокие частоты, длинноволновая область инфракрасного излучения	Экспериментальная «терагерцовая камера», регистрирующая изображение в длинноволновом ИК (которое излучается теплокровными организмами, но, в отличие от более коротковолнового ИК, не задерживается диэлектрическими материалами).

По ширине канала:

1. UWB (Ultra-Wide Band, сверхширокая полоса, СШП). Для целей радиосвязи, согласно определению Федеральной комиссии по связи (FCC) США (2002 г.), сверхширокополосными предлагается считать сигналы с относительной шириной полосы не менее 20-25 %, то есть $\mu = \Delta F/(f_{lower} + f_{upper}) \geqslant 0{,}2...0{,}25$ либо сигналы с абсолютной шириной полосы $\Delta F \geqslant 500$ MHz (в диапазоне частот 3,1 — 10,6 ГГц).
2. UNB (Ultra-Narrow Band, сверхузкополосные сигналы). Полоса обычно составляет десятки или сотни Гц. Скорости передачи — порядка 100 бит/с или ниже.

Источники:

1. Беспроводные технологии. https://ru.wikipedia.org
2. Сетевая топология. https://ru.wikipedia.org
3. Беспроводная ad-hoc-сеть. https://ru.wikipedia.org
4. Беспроводная сенсорная сеть. https://ru.wikipedia.org
5. MANET. https://ru.wikipedia.org
6. Что такое MANET или почему WiFi не решение всех телекоммуникационных проблем. https://habrahabr.ru

Беспроводные системы ПД

Лекция 02
Технология Wi-Fi (семейство IEEE 802.11)

Wi-Fi — торговая марка организации Wi-Fi Alliance для локальных беспроводных сетей WLAN на базе спецификаций семейства IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity — «беспроводное качество») понимают целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Любое оборудование, соответствующее одному из стандартов семиейства IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

Wi-Fi Alliance или — объединение крупнейших производителей компьютерной техники и беспроводных устройств, работающих по технологии Wi-Fi. Альянс разрабатывает семейство стандартов 802.11 и методы построения WLAN. Основан в 1999 компаниями 3Com, Aironet (Cisco), Harris Semiconductor (Intersil), Lucent (Agere), Nokia и Symbol Technologies как альянс **WECA (Wireless Ethernet Compatibility Alliance)**. В 2000 переименован в Wi-Fi Alliance. На сегодняшний день альянс объединяет около 600 компаний, работающих в области беспроводных технологий.

IEEE 802.11 — набор стандартов связи для коммуникации в WLAN в частотных диапазонах 0,9; 2,4; 3,6 и 5 ГГц.

Список стандартов (частично)

При описании стандарта в скобках указан год его принятия. Скорость указана брутто, т. е. с учетом служебного трафика. Как правило, в самых идеальных условиях полезная скорость передачи данных по Wi-Fi не превышает 50% канальной.

- **802.11** — изначальный 1 Мбит/с и 2 Мбит/с, 2,4 ГГц и ИК стандарт (1997).
- **802.11a** — 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001).
- **802.11b** — улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с, 2,4 ГГц (1999).
- **802.11g** — 54 Мбит/с, 2,4 ГГц стандарт (обратно совместим с **b**) (2003).
- **802.11n (Wi-Fi 4)** — увеличение скорости передачи данных (600 Мбит/с). 2,4 или 5 ГГц. Обратно совместим с **802.11a/b/g** (сентябрь 2009).
- **802.11u** — взаимодействие с не-802 сетями (например, сотовыми).
- **802.11v** — управление беспроводными сетями.
- **802.11y** — дополнительный стандарт связи, работающий на частотах 3,65–3,70 ГГц. Обеспечивает скорость до 54 Мбит/с на расстоянии до 5000 м на открытом пространстве.
- **802.11ac (Wi-Fi 5)** — Скорость передачи данных — до 6,77 Гбит/с для устройств, имеющих 8 антенн. (январь 2014).
- **802.11ad** — новый стандарт с дополнительным диапазоном 60 ГГц (частота не требует лицензирования). Скорость передачи данных — до 7 Гбит/с.

- **802.11ah** — стандарт, предназначенный для работы в диапазоне ~900 МГц. Предполагается, что он позволит обеспечить скорость до 40 Мбит/с. Основное назначение — интернет-вещей. (2007). В 2016 Wi-Fi Alliance анонсировал расширение стандарта, получившее название Wi-Fi HaLow.
- **802.11ax (Wi-Fi 6)** — High-Efficiency Wireless, HEW — предназначен для работы в спектрах 2,4 и 5 ГГц, но может включать дополнительные полосы частот в диапазонах от 1 до 7 ГГц по мере их появления. В дополнение к MIMO и MU-MIMO вводится режим OFDMA для улучшения спектральной эффективности, и модуляция 1024-QAM для увеличения пропускной способности. Максимальная скорость до 11 Гбит/с.

Первый стандарт 802.11 предусматривал два типа среды передачи: радиочастота 2,4 ГГц и инфракрасный диапазон 850–950 нм. ИК-устройства не были широко распространены и в будущем развития не получили. В диапазоне 2,4 ГГц было предусмотрено два способа расширения спектра:

- методом скачкообразного изменения частоты (FHSS) :: 79 каналов по 1 МГц
- методом прямой последовательности (DSSS).

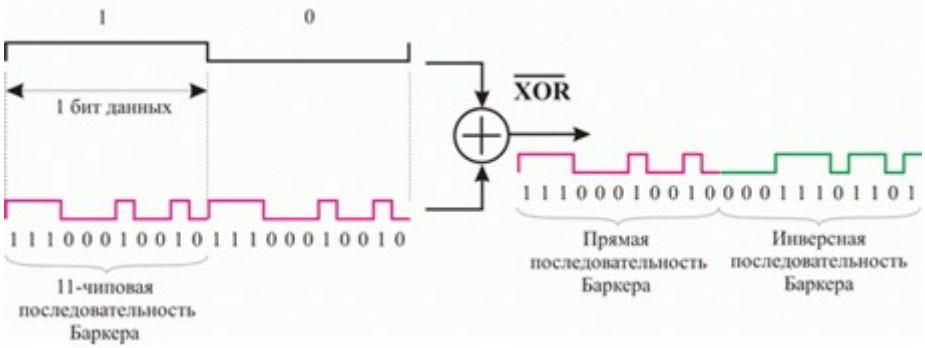
В первом случае (FHSS) все сети используют одну и ту же полосу частот, но с различными алгоритмами перестроения.

Согласно методу FHSS данные передаются только по одному каналу, но сам канал с частотой не более 20 мс изменяется псевдослучайным образом. Причем схема изменения канала определяется и согласовывается между передатчиком и приемником заранее, на этапе соединения. Подобный подход позволяет значительно уменьшить вероятность того, что передаче данных что-то может помешать. Даже если в один из моментов передачи данных какое-то другое беспроводное оборудование займет нужный канал, сигнал об этом поступит отправителю, и необходимый фрагмент данных будет отправлен повторно.

По сравнению с DSSS метод FHSS является более помехозащищенным. Причиной является ширина канала, который используется для передачи данных. Так, возможность возникновения помехи для передачи, которая ведется с помощью 79 каналов шириной в 1 МГц, гораздо ниже, чем вероятность появления помехи для передачи, которая использует канал шириной в 22 МГц. Даже если рассмотреть вариант узкополосных помех, то случайное изменение несущей частоты, то есть смена каналов, делает такое влияние некритичным и приводит лишь к незначительному падению скорости передачи данных за счет отсылки дополнительных частей данных.

По этой причине на практике системы FHSS оказываются более устойчивыми к широкополосным помехам и могут продолжать работать (хотя и с пониженной пропускной способностью) в условиях, когда системы DSSS уже не способны нормально воспринимать полезный сигнал.

Во втором случае (DSSS) появляются частотные каналы от 2412 МГц до 2472 МГц с шагом 5 МГц, сохранившиеся по сей день. В качестве расширяющей последовательности используется последовательность Баркера длиной 11 чипов.



Важно: ***Под чипом понимается элементарный символ последовательности.*** *Этот термин введен, чтобы не путать его с реальным битом данных.*
При этом максимальная скорость передачи данных (канальная, брутто) составляла от 1 до 2 Мбит/с. Таким образом чиповая скорость составляет 22 Мбит/с. Для передачи сигнала в 802.11 использовалась 2-х и 4-х позиционная манипуляция, при последней за один такт передачи передаются 2 бита (4 уровня сигнала).

На смену 802.11 пришёл **стандарт 802.11b**, в котором скорость передачи данных была увеличена до 5,5; 11 и 22 (опционально) Мбит/с. Увеличение скорости было достигнуто путём уменьшения избыточности помехоустойчивого кодирования с 1/11 до 1/2 и даже 2/3 за счёт внедрения блочных и сверточных кодов. Кроме того, максимальное число ступеней модуляции было увеличено до 8 на символ (3 бита на 1 бод). Ширина канала и используемые частоты не изменились, но при уменьшении избыточности и увеличении глубины модуляции выросли требования к соотношению сигнал/шум. Из-за невозможности увеличения мощности устройств по причине экономии энергии мобильных устройств и законодательных ограничений,пришлось сократить зону обслуживания на новых скоростях. Площадь обслуживания на унаследованных скоростях 1–2 Мбит/с не изменилась. От способа расширения спектра методом скачкообразной перестройки частоты было решено полностью отказаться. Больше в семействе Wi-Fi он не использовался.

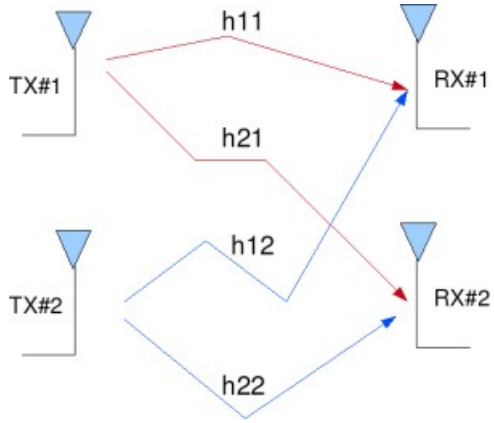
Следующее увеличение скорости до 54 Мбит/с было реализовано в стандарте **802.11a** (начал разрабатываться раньше, чем 802.11b, но финальная версия была выпущена позже, стандарты 802.11b и 802.11a не совместимы). Увеличение скорости в основном было достигнуто за счёт увеличения глубины модуляции до 64 уровней на символ (6 бит на 1 бод). Кроме того, была радикально пересмотрена радиочастотная часть: расширение спектра методом прямой последовательности было заменено на расширение спектра методом разделения последовательного сигнала на параллельные ортогональные поденсущие (OFDM). Использование параллельной передачи на 48 подканалах позволило снизить межсимвольную интерференцию за счёт увеличения длительности отдельных символов. Передача данных осуществлялась в диапазоне 5 ГГц. При этом ширина одного канала составляет 20 МГц. В отличие от стандартов 802.11 и 802.11b, даже частичное перекрытие этой полосы может привести к ошибкам передачи. В диапазоне 5 ГГц расстояние между каналами составляет именно 20 МГц.

Стандарт 802.11g был утверждён в октябре 2002 года. Он стал компиляцией 802.11a и 802.11b в диапазоне 2,4 ГГц: в нём поддерживались скорости обоих стандартов. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая

скорость соединения до 54 Мбит/с (при модуляции OFDM) и гарантируя обратную совместимость со стандартом 802.11b, для чего он поддерживает также режим модуляции DSSS (скорость при этом 11 Мбит/с).

В **стандарте 802.11n** (в обоих диапазонах 2,4 и 5 ГГц) скорость была увеличена до 72 Мбит/с за счёт уменьшения защитных интервалов между передаваемыми символами. Для увеличения пропускной способности можно было объединить два канала по 20 МГц и получить 150 Мбит/с. При этом в диапазоне 2,4 ГГц может поместиться всего один расширенный канал в 40 МГц. Также, согласно стандарту, если в диапазоне 2,4 ГГц на котором используется канал удвоенной ширины появляется устройство, работающее на канале стандартной ширины, то устройство 802.11n обязано перейти на работу с каналом стандартной ширины. Соответственно, использовать каналы по 40 МГц рекомендуется только в диапазоне 5 ГГц. Для сосуществования каналов шириной 20/40 МГц точка доступа стандарта 802.11n должна переходить на другой канал или переключаться на использование канала шириной в 20 МГц, если соседняя точка доступа начинает передачу в одной из половин канала 40 МГц. Главным недостатком широких каналов является большее влияние на них помех и, соответственно, меньшее расстояние передачи данных. Существует также обратная модификация каналов производителями — уменьшение их ширины до 5 или 10 МГц, что позволяет увеличить дальность передачи ценой меньшей скорости.

Ещё одним способом повышения скорости стала технология MIMO: использование нескольких приёмопередатчиков, работающих на одной и той же частоте. Разделение каналов происходит за счёт пространственного разнесения антенн и математических операций над сигналом, принятым на разные антенны: он будет различаться в силу многолучевого распространения радиоволн. Стандарт 802.11n поддерживает MIMO 4x4:4 (четыре независимых канала) и обеспечивает скорость до 600 Мбит/с.



Однако данная технология требует высокого качества изготовления радио части устройств. Кроме того, данные скорости принципиально не реализуемы на мобильных терминалах (основной целевой группе стандарта Wi-Fi): наличие 4-х антенн на достаточном разнесении не может быть реализовано в малогабаритных устройствах как по соображениям отсутствия места, так и из-за отсутствия достаточного на 4 приёмопередатчика энергии.

В большинстве случаев скорость 600 Мбит/с является не более, чем маркетинговой уловкой и нереализуема на практике, так как фактически её можно добиться только между стационарными точками доступа, установленными в пределах одной комнаты при хорошем соотношении сигнал/шум.

Стандарт 802.11ac предусматривает максимальную скорость до 6,93 Гбит/с, однако фактически такая скорость ещё не достигнута ни на одном оборудовании, представленном на рынке. Увеличение скорости достигнуто за счёт увеличения полосы пропускания до 80 и даже до 160 МГц. Такая полоса не может быть предоставлена в диапазоне 2,4 ГГц, поэтому стандарт 802.11ac функционирует только

в диапазоне 5 ГГц. Ещё один фактор увеличения скорости – увеличение глубины модуляции до 256 уровней на символ (8 бит на 1 бод) Такая глубина модуляции может быть получена только вблизи точки из-за повышенных требований к соотношению сигнал/шум. Указанные улучшения позволили добиться увеличения скорости до 867 Мбит/с. Остальное увеличение получено за счёт потоков MIMO 8x8:8. 867x8=6,93 Гбит/с. Технология MIMO была усовершенствована: впервые в стандарте Wi-Fi информация в одной сети может передаваться двум абонентам одновременно с использованием различных пространственных потоков.

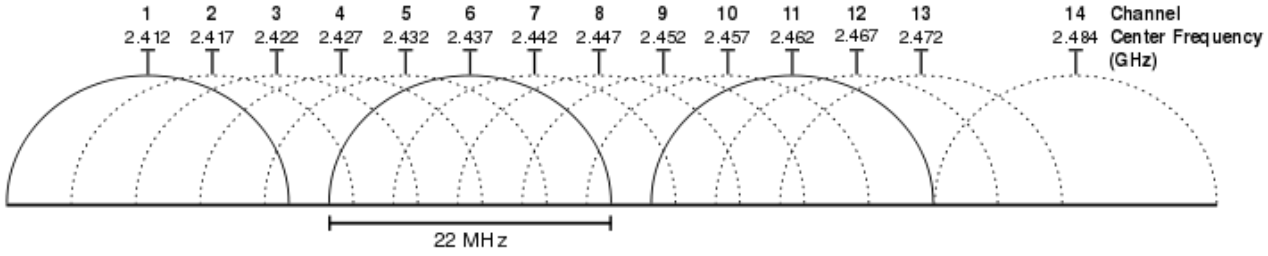
Частотная сетка 802.11

Как было указано ранее, сети 802.11 работают в частотных диапазонах 0,9; 2,4; 3,6 и 5 ГГц. Каждый из этих диапазонов разделяется на ряд поддиапазонов, или каналов. В разных странах существуют свои ограничения по использованию частотных диапазонов, поэтому и число доступных для нелицензированного использования каналов в каждой стране различно. В РФ для нелицензированного использования на сегодня разрешены каналы из диапазонов 2,4 и 5 ГГц.

- ***Диапазон 2,4 ГГц***

Диапазон 2,4 ГГц используется в стандартах 802.11b/g/n. Это часть так называемого ISM диапазона, отведенного в большинстве стран для гражданских целей (ISM – Industrial, Science, Medicine). Помимо 802.11b/g/n в этом диапазоне работают технологии Bluetooth и ZigBee.

Диапазон 2,4 ГГц содержит всего 14 перекрывающихся каналов шириной 22 МГц каждый. Для стандарта 802.11g и более поздних ширина каждого канала установлена равной 20 МГц. Суммарно они занимают полосу частот от 2,401 ГГц до 2,495 ГГц.



В зависимости от законодательства страны, разрешенными для использования могут быть только некоторые из каналов. В России и на Украине разрешено использовать каналы 1–13, в Японии все 14. Во Франции и Испании разрешено использовать только 4 канала (2,457–2,472 ГГц — 10–13 каналы).

В РФ частотный диапазон 2,4 ГГц регламентируется следующими документами

1. Решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия»
2. Решение ГКРЧ от 20 ноября 2014 г. № 14-29-01 «О внесении изменений в решение ГКРЧ от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия»

Если рассмотреть разрешенный в РФ диапазон, то в нем одновременно доступны всего 3 неперекрывающихся 22 МГц канала, например 1, 6 и 11. Точки доступа, работающие на неперекрывающихся каналах не создают друг другу помех. При работе в стандарте 802.11g/n, где используются каналы 20 МГц, одновременно доступно 4 неперекрывающихся канала — 1, 5, 9 и 13. Учитывая, что оборудование 802.11b используется очень редко, имеет смысл ориентироваться именно на эти каналы.

Для оценки ситуации в эфире используются такие программы, как inSSIDer или LinSSID. Они позволяют проверить на каких каналах работают точки доступа, в зоне действия которых находится ноутбук-измеритель и выбрать канал для работы вновь устанавливаемой точки доступа.

- ***Диапазон 5 ГГц***

Диапазон 5 ГГц используется в стандартах 802.11a/n/ac. При этом, в РФ используются только технологии 802.11n/ac.

Unlicensed National Information Infrastructure (**U-NII**)

Диапазон 5 ГГц разделен на четыре поддиапазона.

1. **UNII-1:** 5150–5250 МГц (доступно 4 частотных канала).
2. **UNII-2:** 5250–5350 МГц (доступно 4 частотных канала).
3. **UNII-2 Extended:** 5470–5725 МГц (доступно 11 частотных каналов).
4. **UNII-3:** 5725–5825 МГц (доступно 4 частотных канала).

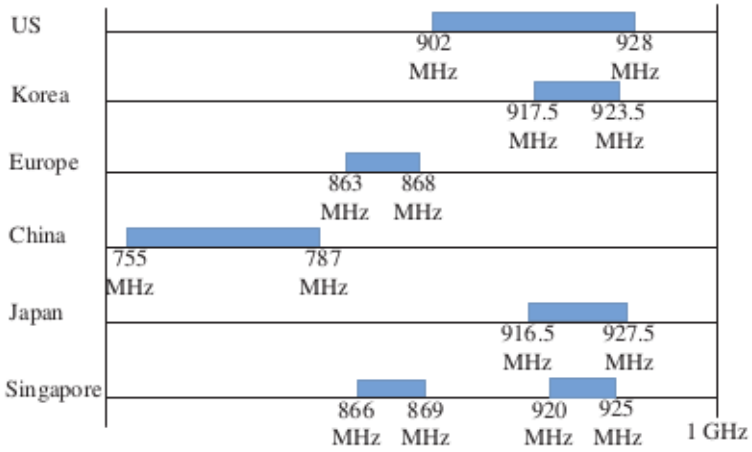
Ширина каждого канала установлена равной 20 МГц.

Номер канала	**Частота, МГц**	**Номер канала**	**Частота, МГц**	**Номер канала**	**Частота, МГц**	**Номер канала**	**Частота, МГц**
Поддиапазон UNII-1							
36	5180	40	5200	44	5220	48	5240
Поддиапазон UNII-2							
52	5260	56	5280	60	5300	64	5320
Поддиапазон UNII-2 Extended							
100	5500	112	5560	124	5620	136	5680
104	5520	116	5580	128	5640	140	5700
108	5540	120	5600	132	5660		
Поддиапазон UNII-3							
149	5745	153	5765	157	5785	161	5805

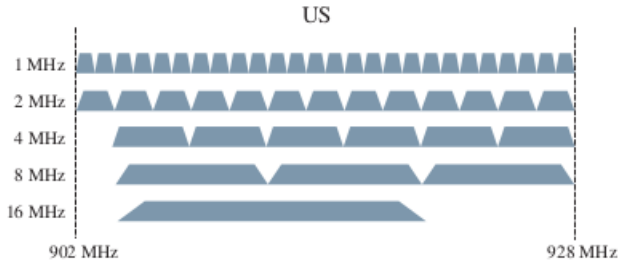
На территории РФ в диапазоне 5 ГГц для нелицензированного использования внутри помещений разрешены каналы с 36 по 64. При этом, оборудование, работающее в диапазоне 5250–5350 МГц должно быть зарегистрировано в установленном в РФ порядке. Регламентируется теми же решениями ГКРЧ, что и диапазон 2,4 ГГц.

- ***Диапазон 0,9 ГГц***

Диапазон 0,9 ГГц или, так называемый субгигагерцовый диапазон, применяется в стандарте 802.11ah. Во многих странах этот частотный диапазон является нелицензируемым. На территории РФ частоты 900 МГц частично отданы сотовым операторам.



Субгигагерцовый диапазон в разных странах исторически широко используется для различных радиотехнологий, поэтому в спец. 802.11ah предложены различные диапазоны для разных стран.



Выделенная полоса частот разбивается на каналы по 1 МГц, которые могут объединяться в более широкие каналы 2, 4, 8 и 16 МГц для увеличения скорости передачи данных. Здесь работает тот же принцип, что и в протоколе 802.11n.

Для примера приведено распределение каналов в диапазоне 902–928 МГц, используемом в США. В зависимости от выделенной полосы частот и особенностей законодательства максимальная полоса пропускания объединенных каналов в разных странах может отличаться.

- Южная Корея — 4 МГц
- Европа — 2 МГц
- Китай — 8 МГц
- Япония — 1 МГц
- Сингапур — 4 МГц

Для передачи данных в каналах технология 802.11ah использует те же принципы, что и 802.11ac. Для работы в каналах шириной 2, 4, 8 и 16 МГц используется модуляция OFDM с числом несущих, аналогичным каналам 20, 40, 80 и 160 МГц в 802.11ac. Например, в 2 МГц канале используется 64 поднесущих OFDM, из которым 52 используются для передачи данных. В каждом из каналов может быть использована одна из 10 кодовых схем MCS 0–9.

MCS	Модуля-ция	Скорость кода	MCS	Модуля-ция	Скорость кода	MCS	Модуля-ция	Скорость кода
0	BPSK	1/2	4	16-QAM	3/4	8	256-QAM	3/4
1	QPSK	1/2	5	64-QAM	2/3	9	256-QAM	5/6
2	QPSK	3/4	6	64-QAM	3/4			
3	16-QAM	1/2	7	64-QAM	5/6			

В каналах 1 МГц используется OFDM с 24 поднесущими и схема кодирования MCS 10, представляющая собой MCS 0 с двукратным повторением передаваемых данных, что обеспечивает большую дальность при той же помехоустойчивости.

- ***Диапазон 3,6 ГГц***

Диапазон 3,6 ГГц применяется в стандарте 802.11y. В нем применяются каналы 5, 10 и 20 МГц.

Канал	Частота (МГц)	5 МГц	10 МГц	20 МГц	Канал	Частота (МГц)	5 МГц	10 МГц	20 МГц
131	3657,5	Да	Нет	Нет	135	3677,5	Да	Нет	Нет
132	3662,5	Да	Нет	Нет	136	3682,5	Да	Нет	Нет
132	3660,0	Нет	Да	Нет	136	3680,0	Нет	Да	Нет
133	3667,5	Да	Нет	Нет	137	3687,5	Да	Нет	Нет
133	3565,0	Нет	Нет	Да	137	3685,0	Нет	Нет	Да
134	3672,5	Да	Нет	Нет	138	3689,5	Да	Нет	Нет
134	3670,0	Нет	Да	Нет	138	3690,0	Нет	Да	Нет

Принцип работы

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети SSID (Service set identification) с помощью специальных сигнальных кадров-маяков на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала, согласно принятым кадрам-маякам.

По способу объединения ТД в единую систему можно выделить:

- Автономные ТД (самостоятельные, децентрализованные, умные)
- ТД под управлением контроллера («легковесные», централизованные)
- Бесконтроллерные, но не автономные (управляемые без контроллера)

В случае *автономной архитектуры* сеть строится как набор несвязанных ТД, каждая из которых конфигурируется и обслуживается независимо. Поэтому сложность обслуживания сети, построенной подобным образом, растет линейно с ростом количества устройств. Обычно такие сети содержат не более 3–5 ТД.
Существуют исключения, которые облегчают создание более масштабных сетей, например, технология кластеризации ТД. Такое решение предлагает Cisco в линейке ТД для малого бизнеса (Cisco WAP 321, WAP 121). Но такая архитектура в любом случае не имеет полноценного управления радиоресурсами, т. к. нет единого центра. Все сводится к упрощению задачи конфигурирования сети.
Развитием автономной архитектуры явились *псевдо-централизованные решения*, в которых в относительно небольшой группе ТД одна точка выделяется как контроллер группы. По сути такой мини-контроллер может выполнять многие функции полноценного контроллера сети Wi-Fi. Однако процессор ТД имеет ограниченную производительность и масштабирование таких решений невелико. Подобные решения и ТД предлагает, например, компания Aruba (Aruba Instant).

В случае *централизованной архитектуры* сети Wi-Fi полное управление инфраструктурой сети радиодоступа выполняется контроллером сети WLAN. Например, у Cisco подобная архитектура называется CUWN (Cisco Unified Wireless Network). Контроллер в централизованном решении сети стандарта Wi-Fi управляет загрузкой/изменением ПО, изменениями конфигурации, RRM (динамическое управление радиоресурсами), управляет связью с внешними серверами (AAA, DHCP, LDAP и т. п.), управляет аутентификацией пользователей, управляет профилями качества обслуживания QoS. Контроллеры могут объединяться в группы для обеспечения бесшовного роуминга клиентов между различными точками доступа в зоне покрытия.

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- Со статическими настройками радиоканалов
- С динамическими (адаптивными) настройками радиоканалов
- Со «слоистой» или многослойной структурой радиоканалов

Ad-hoc-сеть (беспроводная динамическая/самоорганизующаяся сеть) — децентрализованная беспроводная сеть, не имеющая постоянной структуры. Клиентские устройства соединяются «на лету», образуя собой сеть. Каждый узел сети пытается переслать данные, предназначенные другим узлам. При этом определение того, какому узлу пересылать данные, производится динамически, на основании связности сети.

Построение сети

При проектировании беспроводной сети в помещениях применяют различные подходы, которые почти всегда содержат несколько этапов.

1. Оценка количества точек доступа в зависимости от предполагаемого числа пользователей Wi-Fi и услуг, которые должны быть им предоставлены.
2. Размещение точек доступа на план-схеме помещения с учетом его размеров, материалов, из которых изготовлены стены и мебель, а также размещения пользователей.

Одним из самых простых способов определения количества точек доступа является задание фиксированного количества пользователей на точку. Например, существует рекомендация использовать одну точку доступа на 20 пользователей при отсутствии шифрования и одну точку на 15 пользователей при использовании какого-либо шифрования. Такой подход очень прост, но имеет ряд недостатков. Во-первых, такое количество точек доступа может оказаться избыточным, что приведет к лишним тратам как на само беспроводное оборудование, так и на организацию его размещения (электропитание, подключение к проводной локальной сети). Во-вторых, при большом количестве точек доступа, размещённых в одном помещении, рассчитанном на большое число пользователей (например, конференц-зал или лекторий), они могут мешать друг другу и их потребуется разносить по разным каналам, что может быть сложным при использовании диапазона 2,4 ГГц (например, если используется технология 802.11g).

Второй способ исходит из требований по уровню сигнала. Например, считается, что для доступа в Интернет (электронная почта и веб-серфинг) достаточно обеспечить на всей территории помещения уровень сигнала не хуже, чем −(68–70) дБм. Такой подход как правило требует применения специализированного программного обеспечения для предварительного расчета, либо использования измерений на месте, когда предполагаемая к использованию точка доступа размещается в разных местах помещения, и производится измерение ее сигнала на возможных точках размещения пользователей. Как правило этот способ предлагает заниженное число точек доступа, благодаря чему на практике построенная сеть может не справиться с нагрузкой. К тому же, полное покрытие помещения может оказаться не нужным в том случае, когда пользователи компактно размещаются в одной части помещения, а другая часть помещения не используется.

Третий способ предварительного определения количества точек доступа исходит из требований по скорости доступа в зависимости от необходимых пользователям услуг. В результате таких расчетов может получиться некоторое усредненное количество точек доступа. Однако вопрос неравномерности размещения пользователей также необходимо учитывать на этапе размещения точек доступа на план-схеме помещения.
При проведении планирования необходимо также провести энергетический расчет и составить частотный план, чтобы размещенные в помещении точки доступа не влияли друг на друга, а их сигнал не выходил за границы помещения и не влиял на беспроводные сети, расположенные снаружи помещения.

Влияние препятствий на зону покрытия сети 802.11

При размещении точек доступа очень важно определить, из каких материалов сделаны стены, перекрытия, конструкционные элементы и мебель в помещении, и уже с учетом этого проводить размещение оборудования и выбор антенн, которые будут использоваться вместе с точками доступа.
Например, одной из распространенных ошибок при размещении точек доступа, является установка точки с всенаправленной (омни) антенной возле металлической или железобетонной стены или конструкции. В этом случае металлическая поверхность будет отражать сигнал. Диаграмма направленности антенны изменится став направленной. Вдобавок возникнет мощное многолучевое распространение (multipath), так как половина излучаемой мощности будет уходить к металлической стене/поверхности и, отражаясь обратно, создаст интерференцию своему же полезному излучению. Другим примером может являться размещение точки возле емкостей и труб в водой, которая интенсивно поглощает высокочастотное излучение (особенно в частотном спектре 2,4 ГГц).

Основным методом решения является вынесение точек доступа с внутренними антеннами (или самих внешних антенн) за пределы преград, обеспечивая беспрепятственное излучение с учетом диаграммы направленности антенн.

Также необходимо учитывать, что уровень сигнала убывает пропорционально квадрату расстояния, потому скорость быстро падает естественным путем по мере удаления от точки доступа.

Модель OSI

Wi-Fi охватывает первые два уровня модели OSI, каждый из которых разделен на два подуровня.

2. Канальный	Подуровень LLC
	Подуровень MAC
1. Физический	Подуровень PLCP
	Подуровень PMD

Физический уровень:

1. PLCP (Physical Layer Convergence Protocol) — выполняет процедуру отображения PDU уровня MAC во фрейм, соответствующий версии протокола и используемому типу разделения каналов. Также на этом подуровне выполняются передача, обнаружение несущей и прием сигнала;
2. PMD (Physical Medium Dependent) — "подуровень, зависящий от среды передачи". Он различен для разных скоростей передачи и разных стандартов из серии 802.11. Подуровень PMD обеспечивает данные и сервис для подуровня PLCP и функции радиопередачи и приема, результатом которых является поток данных, информация о времени, параметры приема.

Основным рабочим состоянием уровней PLCP является обнаружение несущей и оценка незанятости канала. Для выполнения передачи PLCP переключает PMD из

режима "прием" в режим "передача" и посылает элемент данных PPDU (PLCP Data Unit).

Второй уровень (Data Link):

1. LLC (Logical Link Control) — идентичен для всех сетей платформы 802.
2. MAC (Media Access Control) — идентичен для всех сетей платформы 802.11.

Метод доступа к сети

Для доступа к общей разделяемой среде передачи используется метод доступа **CSMA/CA — «Carrier Sense Multiple Access With Collision Avoidance»** («Carrier sensing multiple access with collision avoidance») — «множественный доступ с контролем несущей и избеганием коллизий» («многостанционный доступ с контролем несущей и предотвращением конфликтов»).

Для предотвращения коллизий используется следующая последовательность действий:

- используется схема прослушивания несущей волны
- станция, которая собирается начать передачу, посылает jam signal (сигнал преднамеренной помехи)
- после продолжительного ожидания всех станций, которые могут послать jam signal, станция начинает передачу кадра
- если во время передачи станция обнаруживает jam signal от другой станции, она останавливает передачу на отрезок времени случайной длины и затем повторяет попытку

В 802.11 для реализации CSMA/CA используются кадры Request to Send (запрос на отправку) и Clear to Send (готовность к отправке).

Функция RTS/CTS является опциональной и разработана для уменьшения количества коллизий при пересылке кадров, когда присутствуют скрытые устройства с Wi-Fi, имеющие ассоциацию с той же точкой доступа (пример: в зоне покрытия точки доступа есть капитальная стена и два смартфона с двух сторон «слышат» эту точку, но «не слышат» друг друга). Мобильные устройства отправляют RTS кадр (играет роль jam-сигнала) к другому устройству, как первую фазу в двухшаговом процессе, необходимом до отправки кадра данных. Мобильное устройство (или точка доступа) с WiFi отвечает на кадр RTS кадром CTS, подтверждая тем самым для запрашивающего устройства чистоту канала для отправки кадра данных. Кадр CTS включает параметр времени, на которое все другие устройства в сети не должны передавать какие-либо кадры в течении периода, который требуется запрашивающему устройству на передачу его кадра. Данная функция минимизирует коллизии даже при наличии скрытых устройств.

Кадры Request to Send и Clear to Send относятся к так называемым кадрам контроля.

Фреймы сети 802.11

Стандарт 802.11 определяет три типа кадров:

1. Кадры управления (Management frames),
2. Кадры контроля (Control frames),
3. Кадры данных (Data frames).

Каждый кадр имеет контрольное поле, которое определяет версию протокола 802.11, тип кадра и различные индикаторы (например: WPA включен, управление энергосбережением активно и т. п.). Дополнительно к этому все кадры содержат MAC-адреса источника и получателя, номер кадра в последовательности, тело кадра и контрольную сумму. Кадры 802.11 инкапсулируют пакеты верхних уровней модели OSI.

Кадры управления (Management Frames)

Кадры управления 802.11 позволяют устанавливать и поддерживать соединения в сети стандарта WiFi.

Пользовательские устройства могут работать в двух режимах поиска сети:
1. Режим *Пассивного сканирования* (Passive Scanning) — прослушивание эфира.
Медленный режим, т. к. пользовательское устройство должно последовательно прослушивать все частотные каналы поддерживаемого диапазона для выявления кадров-маяков точек доступа.
2. Режим *Активного сканирования* (Active Scanning) — активная отправка запросов в эфир.
Устройство посылает кадры типа Probe Request по всем частотным каналам в поддерживаемом диапазоне часто с указанием искомого SSID сети (direct probe request) или без SSID (null probe request). Активное сканирование значительно повышает динамику работы с сетью и позволяет обеспечить быстрый роуминг, но при этом создает дополнительную нагрузку на сеть.

Всего стандарт 802.11 определяет 14 типов кадров управления:
1. Association request,
2. Association response,
3. Reassociation request,
4. Reassociation response,
5. Probe request,
6. Probe response,
7. Beacon,
8. ATIM (Announcement traffica indication mesage),
9. Disassiciation,
10. Authentication,
11. Deauthentication,
12. Action,
13. Action No Ack,
14. Timing advertisement

Кадр аутентификации (Authentication frame)

В стандарте IEEE 802.11 требуется выполнить два обязательных последовательных шага до начала пересылки трафика: аутентификация и ассоциация.

Аутентификация в сети 802.11 — это процесс в ходе которого точка доступа разрешает или отвергает идентификационные данные от конечного устройства (при наличии в сети AAA-сервера ТД может перенаправлять эти запросы на него). Конечное устройство начинает процесс путем отправки кадра аутентификации, содержащего его идентификационную информацию, к точке доступа. При открытой аутентификации, радиокарта конечного устройства отправляет кадр аутентификации и ТД отвечает кадром аутентифкации, означающим подтверждение (или отказ). В случае схем аутентифкации с ключом конечное устройство отправляет начальный кадр аутентификации и ТД отвечает кадром аутентифкации, содержащим специальную тестовую последовательность (challenge text). Конечное устройство должно далее отправить обратно зашифрованную версию тестовой последовательности (шифруется своим ключем) в кадре аутентификации. ТД проверяет корректность ключа и отвечает пользовательскому устройству фреймом аутентификации, содержащим результат аутентификации.

Кадр деаутентификации (Deauthentication frame)

Пользовательское устройство отправляет кадр деаутентификации к другому устройству, если хочет прервать безопасное соединение. Фрейм деаутентификации это уведомление, а не запрос. При получении кадра деаутентификации ни одна принимающая сторона не может отказаться его выполнить, за исключением случая когда включен режим защиты кадров (802.11w: MFP или Management Frame Protection) и не удалось успешно выполнить контроль от подделки кадра MIC (Message Integrity Check). Если кадр уведомления деаутентификации не услышан на другом конце, то правила управления на MAC-уровне позволяют трактовать такое состояние как потерю коммуникаций.

Кадр запроса на ассоциацию (Association request frame)

Ассоциация 802.11 указывает ТД выделить и занять ресурсы для заданной новой сессии и синхронизироваться с радиокартой устройства пользователя. Радиокарта пользовательского устройства начинает процесс ассоциации путем отправки кадра запроса на ассоциацию к точке доступа. Этот кадр содержит информацию о радиокарте устройства пользователя (например, поддерживаемые скорости передачи данных и т. п.) и SSID сети WLAN, с которой устройство хочет быть ассоциировано. После получения запроса на ассоциацию точка доступа решает вопрос по ассоциированию с радиокартой и, если принято положительное решение, резервирует область памяти и формирует идентификатор сессии AID (Association Identifier) для данной радиокарты.

Кадр ответа на запрос ассоциации (Association response frame)

ТД отправляет кадр ответа на запрос ассоциации, который содержит уведомление о подтверждении или отказе на запрос радиокарты об ассоциации. Если точка доступа подтверждает ассоциацию пользовательского устройства, то кадр ответа включает информацию о данной ассоциации, например идентификатор ассоциации и поддерживаемые скорости передачи данных. Если результат ответа положителен, то радиокарта пользовательского устройства может использовать данную ТД для взаимодействия с другими радиокартами на других пользовательских устройствах в сети.

Кадр повторного запроса ассоциации (Reassociation request frame)

Если мобильное устройство пользователя выполняет роуминг от текущей ТД к другой ТД, которая имеет больший уровень сигнала, определяемого по кадру-маяку, то радиокарта мобильного устройства будет отправлять кадр повторного запроса на ассоциацию к новой ТД. Новая ТД затем координирует пересылку данных, которые могут все ещё находиться в буфере предыдущей ТД и ожидать передачи на данное мобильное устройство.

Кадр ответа на повторный запрос ассоциации (Reassociation response frame)

ТД отправляет кадр ответа на повторный запрос ассоциации, который содержит сообщение подтверждения или отказа для радиокарты мобильного устройства, запрашивающего ассоциацию с сетью. Подобно процессу ассоциации фрейм включает информацию относительно ассоциации, как, например, идентификатор сессии ассоциации и поддерживаемые скорости передачи данных.

Кадр остановки ассоциации (Disassociation frame)

Мобильное устройство отправляет кадр остановки ассоциации другому устройству, если оно хочет закончить ассоциацию. Например, радиокарта, которая была выключена правильным образом, может отправить кадр остановки ассоциации для того чтобы известить точку доступа, что данное устройсто выключается.

Кадр-маяк (Beacon frame)

Это один из наиболее важных кадров управления. ТД периодически отправляет маяки для анонсирования своего присутствия и предоставления необходимой информации (SSID, частотный канал, временные маркеры для синхронизации устройств по времени, поддерживаемые скорости, возможности обеспечения QoS и т. п.) всем устройствам в зоне ее покрытия. Радиокарты пользовательских устройств периодически сканируют все каналы 802.11 и слушают маяки, как основу для выбора лучшей ТД для ассоциации. Пользовательские устройства обычно не посылают маяки, за исключением ситуации, когда выполняется процедура участия в одноранговом соединении типа Ad-hoc.

Кадр пробы (Probe request frame)

Мобильные устройства с Wi-Fi отправляют пробу, чтобы получить информацию от другого устройства. Например радиокарта мобильного устройства отправлет пробу, чтобы определить какие точки доступа находятся внутри зоны покрытия.

Кадр ответ на пробу (Probe response frame)

Ответ на пробу содержит информацию о функциональности, поддерживаемых скоростях передачи данных и т. п.

Кадры Контроля Wi-Fi (Control Frames)

Кадры контроля 802.11 помогают в доставке кадров данных между станциями и между станциями и ТД. Всего стандарт 802.11 определяет 9 типов кадров контроля:
1. PS-Poll (Power Save Poll),
2. RTS (Request to Send),
3. CTS (Clear to Send),
4. ACK (Acknolegement),
5. CF-End (Contention Free-End),
6. CF-End + CF-ACK,
7. Block ACK Request (BlockAckReq),
8. Block ACK (BlockAck),
9. Control wrapper.

Кадр подтверждения (Acknowledgement (ACK) frame)

После получения кадра данных устройство-получатель запускает процесс проверки кадра на ошибки. Если ошибок не обнаружено, то устройство-получатель отправит кадр подтверждения к устройству-отправителю. Если устройство-отправитель не получило кадр подтверждения после определенного периода времени, то отправитель должен посылает кадр заново (в сети 802.11 все кадры данных unicast должны быть подтверждены, иначе устройство-отправитель будет посылать их заново, снижая производительность системы).

Кадры Данных (Data Frames)

Стандарт WiFi IEEE 802.11 определяет 15 типов фреймов данных:

1. Data frame (простой фрейм данных),

Простой кадр данных это наиболее распространенный тип кадров данных.
Необходимо отметить, что существует кадр специальной нулевой функции (Null function frame), который используется пользовательскими устройствами для информирования ТД об изменениях статуса режима сохранения энергии (Power Save). Когда пользовательское устройство решает выйти из частотного канала для проведения активного сканирования, то устройство должно отправить такой фрейм нулевой функции с битом управления энергией (Power Management), выставленным в

1. После получения такого фрейма ТД должна буферизовать все, что поступает в адрес этого клиента. Когда клиентское устройство возвращается на свой частотный канал, оно должно снова отправить кадр нулевой функции с битом управления энергией, выставленным в 0. После этого точка доступа передаёт все буферизированные ранее данные клиенту.

2. Null function (без данных),
3. Data + CF-ACK (для режима Point Coordination Function),

В режиме Point Coordination Function (PCF) ТД посылает «сигнальные» фреймы через постоянные промежутки времени (обычно 0.1 секунды). Между этими фреймами, PCF определяет два периода: Contention Free Period (CFP) и Contention Period (CP). В CP используется режим Distributed Coordination Function (DCF), основанный на CSMA/CA. А в CFP ТД посылает Contention Free — Poll (CF-Poll) пакеты каждой станции по одному за раз, чтобы дать им право посылать пакеты.

4. Data + CF Poll (PCF only),
5. Data + CF-ACK + CF-Poll (PCF only),
6. CF-ACK (без данных) (PCF only),
7. CF-Poll (без данных) (PCF only),
8. CF-ACK + CF-Poll (без данных) (PCF only),
9. QoS Data (для режима Hybrid Coordination Function),

HCF работает во многом схоже с PCF: интервалы между сигнальными фреймами делятся на два периода, CFP и CP. Во время CFP, Hybrid Coordinator (HC) контролирует доступ в эфир. Во время CP, все станции функционируют по EDCF (DCF с приоретизацией трафика). Главное различие от PCF заключается в том, что присутствуют Traffic Classes (TC). Также HC может координировать трафик любым выбранным им способом (а не только циклически). Кроме того станции дают информацию о длине их очередей для каждого TC. HC может использовать эту информацию для того, чтобы дать одной станции больший приоритет. Другое отличие заключается в том, что станциям дается Transmit Opportunity (TXOP): они могут посылать несколько пакетов друг за другом, в выделенный им период времени выбранный HC.

10. QoS Null (без данных) (HCF),
11. QoS Data + CF-ACK (HCF),
12. QoS Data + CF-Poll (HCF),
13. QoS Data + CF-ACK + CF-Poll (HCF),
14. QoS CF-Poll (без данных) (HCF),
15. QoS CF-ACK + CF-Poll (без данных) (HCF).

Безопасность в 802.11

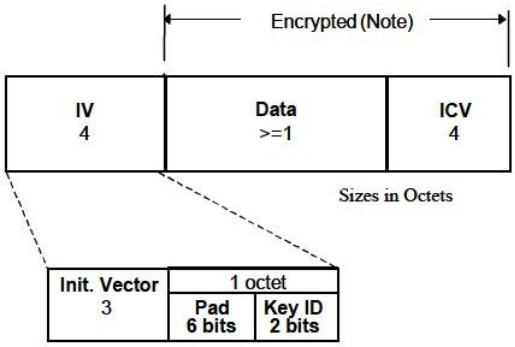
Для обеспечения безопасности в сетях Wi-Fi, т. е. для защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания и

невозможности подключения к сети неавторизованных пользователей используются два основных алгоритма — WEP и WPA.

Wired Equivalent Privacy (WEP)

Существует две основные разновидности WEP: WEP-40 (WEP-64), одобренная IEEE в 1997, и WEP-104 (WEP-128), вышедшая в 2001. Эти версии различаются только длиной ключа. Некоторые производители предлагают реализации WEP с большей длиной ключа — WEP-152 и WEP-256. В настоящее время WEP является устаревшей технологией, так как ее взлом хорошо отработан и может быть осуществлен за малое время. Тем не менее, она продолжает широко использоваться. WEP часто неправильно называют Wireless Encryption Protocol.

Для шифрования в WEP используется поточный шифр RC4. Для подсчета контрольных сумм используется CRC32.



Кадр WEP включает в себя следующие поля:
Незашифрованная часть:

1. Вектор инициализации (Init. Vector, IV) (24 бита)
2. Пустое место (Padding) (6 бит)
3. Идентификатор ключа (Key ID) (2 бита)

Зашифрованная часть:

4. Данные
5. Контрольная сумма (32 бита)

В WEP-40 (WEP-64) используется 40-битный ключ, который вместе с 24-битным вектором инициализации (IV) образует ключ шифрования RC4. 40-битный ключ может быть введен как строка из 10 шестнадцатеричных цифр или как 5 символов ASCII (8 бит/символ), однако, ограничение символов ASCII только печатаемыми символами значительно снижает пространство возможных ключей.

104-битный ключ в WEP-104 (WEP-128) представляется либо как 26 шестнадцатеричных цифр, либо как 13 символов ASCII. В совокупности с IV он образует 128-битный ключ для RC4.

WEP-152 и WEP-256 работают полностью аналогично. Отличается только длина ключа — 128 + 24 = 152 и 232 + 24 = 256, соответственно.

Инкапсуляция данных в кадр WEP:

1. Контрольная сумма от поля «данные» вычисляется по алгоритму CRC32 и добавляется в конец кадра.
2. Данные с контрольной суммой шифруются алгоритмом RC4.
3. Проводится операция XOR над исходным текстом и шифротекстом.
4. В начало кадра добавляется вектор инициализации и идентификатор ключа.

Декапсуляция данных из кадра WEP:

1. К используемому ключу добавляется вектор инициализации.
2. Происходит расшифрование.
3. Проводится операция XOR над полученным текстом и шифротекстом.
4. Проверяется контрольная сумма.

Методы аутентификации WEP

В WEP используется два метода аутентификации:
1. Аутентификация с открытой системой (Open System auth.)
2. Аутентификация с общим ключом (Shared Key auth.)

При открытой системе любой клиент может подключиться к ТД. Процедура аутентификации не производится. Ключ WEP используется только для шифрования трафика.

При аутентификации с общим ключом используется т. н. четырехэтапное рукопожатие:
1. Клиент посылает ТД запрос на аутентификацию.
2. ТД отправляет в ответ некий контрольный текст.
3. Клиент шифрует текст ключом и отправляет обратно.
4. ТД дешифрует полученный шифротекст и сверяет его с оригинальным сообщением, если все верно, то отправляется положительный ответ.

Несмотря на кажущееся увеличение безопасности, метод с общим ключом менее безопасен, поскольку перехват кадров рукопожатия с оригинальным текстом и шифротекстом позволяет упростить процедуру определения ключа. Таким образом, несмотря на то, что при открытой системе к ТД может подключиться любой клиент, для большей безопасности рекомендуется использовать именно этот метод.

Ограничение доступа к ТД может быть осуществлено другими методами, например, списком разрешенных клиентских MAC-адресов.

Wi-Fi Protected Access (WPA и WPA2)

Механизмы WPA и WPA2 одобрены IEEE в 2004. В WPA обеспечена поддержка стандартов 802.1X, а также протокола EAP (Extensible Authentication Protocol — расширяемый протокол аутентификации). Для шифрования в WPA используется усовершенствованный RC4. а в WPA2 поддерживается шифрование AES (Advanced Encryption Standard)с более стойким криптоалгоритмом.

Wi-Fi Alliance даёт следующую формулу для определения WPA, как суммы технологий:

$$WPA = 802.1X + EAP + TKIP + MIC$$

Как упомянуто выше, в стандарте WPA используется Расширяемый протокол аутентификации (EAP) как основа для механизма аутентификации пользователей. Непременным условием аутентификации является предъявление пользователем свидетельства (мандата), подтверждающего его право на доступ в сеть. Для этого пользователь проходит проверку по базе зарегистрированных пользователей. База зарегистрированных пользователей и система проверки в больших сетях, как правило, расположены на специальном сервере (чаще всего RADIUS).

Также WPA имеет упрощённый режим. Он получил название Pre-Shared Key (WPA-PSK или EAP-PSK). При применении режима PSK необходимо ввести один пароль для каждого отдельного узла беспроводной сети (беспроводные маршрутизаторы, точки доступа, мосты, клиентские адаптеры). Если пароли совпадают с записями в базе, пользователь получит разрешение на доступ в сеть.

IEEE 802.1X — стандарт Института инженеров электротехники и электроники, описывающий процесс инкапсуляции данных EAP, передаваемых между запрашивающими устройствами (клиентами), системами, проверяющими подлинность (коммутаторами, точками беспроводного доступа), и серверами проверки подлинности (RADIUS).

Для усиления шифрования используются механизмы TKIP и MIC.

TKIP (Temporal Key Integrity Protocol — протокол целостности временного ключа) отвечает за увеличение размера ключа с 40 до 128 бит, а также за замену одного статического ключа WEP ключами, которые автоматически генерируются и рассылаются сервером аутентификации. Кроме того, в TKIP используется специальная иерархия ключей и методология управления ключами, которая убирает излишнюю предсказуемость, которая использовалась для несанкционированного снятия защиты WEP ключей.

Сервер аутентификации, после получения сертификата от пользователя, использует 802.1X для генерации уникального базового ключа для сеанса связи. TKIP осуществляет передачу сгенерированного ключа пользователю и точке доступа, после чего выстраивает иерархию ключей плюс систему управления. Для этого используется двусторонний ключ для динамической генерации ключей шифрования данных, которые в свою очередь используются для шифрования каждого пакета данных. Подобная иерархия ключей TKIP заменяет один ключ WEP (статический) на 500 миллиардов возможных ключей, которые будут использованы для шифрования данного пакета данных.

Другим важным механизмом является проверка целостности сообщений (Message Integrity Check, MIC). Её используют для предотвращения перехвата пакетов данных, содержание которых может быть изменено, а модифицированный пакет вновь передан по сети. MIC построена на основе мощной математической функции, которая применяется на стороне отправителя и получателя, после чего сравнивается результат. Если проверка показывает на несовпадение результатов вычислений, данные считаются ложными и пакет отбрасывается.

При этом механизмы шифрования, которые используются для WPA и WPA-PSK, являются идентичными. Единственное отличие WPA-PSK состоит в том, что аутентификация производится с использованием пароля, а не по сертификату пользователя.

В WPA2 помимо более надежного шифрования AES вместо TKIP используется CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol — протокол блочного шифрования с кодом аутентичности сообщения (MAC) и режимом сцепления блоков и счётчика) — протокол шифрования 802.11i.

Источники:

1. Wi-Fi. https://ru.wikipedia.org
2. WECA. https://ru.wikipedia.org
3. IEEE 802.11. https://ru.wikipedia.org
4. CSMA/CA. https://ru.wikipedia.org
5. Беспроводная ad-hoc-сеть. https://ru.wikipedia.org
6. WEP. https://ru.wikipedia.org
7. Wired Equivalent Privacy. https://en.wikipedia.org
8. WPA. https://ru.wikipedia.org
9. Материалы с сайта http://www.wi-fi.org
10. Эволюция скорости передачи данных в сетях Wi-Fi. https://habrahabr.ru
11. Кое-что о Wi-Fi. https://habrahabr.ru
12. IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz / Weiping Sun, Munhwan Choi and Sunghyun Choi // Journal of ICT Standardization. 2013. Vol. 1. 83–108.
13. Wi-Fi и IEEE 802.11. http://www.bookasutp.ru
14. Типы фреймов сети стандарта IEEE 802.11. http://wi-life.ru

Беспроводные системы ПД

Лекция 03
Технология WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) — телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов). Основана на стандарте IEEE 802.16, который также называют Wireless MAN (WiMAX следует считать жаргонным названием, так как это не технология, а название форума, на котором Wireless MAN и был согласован).

Название «WiMAX» было создано организацией WiMAX Forum, которая была основана в июне 2001 года с целью продвижения и развития технологии WiMAX. Форум описывает WiMAX как «основанную на стандарте технологию, предоставляющую высокоскоростной беспроводной доступ к сети, альтернативный выделенным телефонным линиям и DSL». Максимальная скорость — до 1 Гбит/сек на ячейку.

Много писалось о том, что системы WiMAX могут передавать данные на расстояние до 50км со скоростью 70Мбит/с. Но, по данным корпорации Intel, максимальная скорость передачи данных, примерно равная 70Мбит/с, реализуется при использовании 20МГц-канала и высокоуровневой модуляции 64QAM¾ и при такой модуляции радиус соты не может быть равным 50км (в реальной системе SkyMAX фирмы Siemens он составляет только 4...6км в зависимости от условий распространения радиосигналов). Другие системы WiMAX работают в частотных полосах шириной от 3,5 до 10МГц, а в полосе частот 10МГц максимальная расчетная скорость передачи данных получается примерно 37Мбит/с. Требуется учитывать и тот факт, что, по разным экспертным оценкам, реальная скорость передачи данных составляет 30–65% от максимальной и абонентам не стоит рассчитывать на 70Мбит/с.

Варианты WiMAX

- ***802.16-2004 (802.16d**, фиксированный WiMAX или WiMAX^{pre}).* Спецификация утверждена в 2004 году. Используется ортогональное частотное мультиплексирование (OFDM), поддерживается фиксированный доступ в зонах с наличием либо отсутствием прямой видимости. Пользовательские устройства представляют собой стационарные модемы для установки вне и внутри помещений, а также PCMCIA-карты для ноутбуков. В большинстве стран под эту технологию отведены диапазоны 3,5 и 5 ГГц.
- ***802.16-2005 (802.16e**, мобильный WiMAX).* Спецификация утверждена в 2005 году. Является развитием технологии фиксированного доступа (802.16d). Оптимизирована для поддержки мобильных пользователей и поддерживает ряд специфических функций, таких как хэндовер, idle mode и роуминг. Применяется масштабируемый OFDM-доступ (SOFDMA), возможна работа при наличии либо отсутствии прямой видимости. Частотные диапазоны для сетей Mobile WiMAX: 2,3–2,5; 2,5–2,7; 3,4–3,8 ГГц.

Основное различие двух технологий состоит в том, что фиксированный WiMAX позволяет обслуживать только «статичных» абонентов, а мобильный ориентирован на работу с пользователями, передвигающимися со скоростью до 150 км/ч. Мобильность означает наличие функций роуминга и «бесшовного» переключения между базовыми станциями при передвижении абонента (как происходит в сетях сотовой связи). В частном случае мобильный WiMAX может применяться и для обслуживания фиксированных пользователей. WiMAX-системы, основанные на версиях стандарта IEEE 802.16 e и d, практически несовместимы.

Методы ПД в WiMAX

На физическом уровне в стандарте IEEE 802.16-2004 определены 4 метода передачи данных:

- Single Carrier (WirelessMAN-SC) — символы модуляции передаются на несущей частоте — ориентирован на работу в условиях прямого распространения сигнала на частоте несущей в диапазоне 10-66 ГГц;
- Single Carrier a (WirelessMAN-SCa) — модификация WirelessMAN-SC для работы в условиях непрямого распространения сигнала на частоте несущей до 11 ГГц;
- Orthogonal Frequency Division Multiplexing (WirelessMAN-OFDM) — символы модуляции передаются на множестве поднесущих с использованием технологии OFDM — предназначен для работы в условиях непрямого распространения сигнала на частоте несущей до 11 ГГц;
- Orthogonal Frequency Division Multiple Access (WirelessMAN-OFDMA) — множественный доступ с частотно-временным разделением с использованием технологии OFDM — предназначен для работы в условиях непрямого распространения сигнала на частоте несущей до 11 ГГц.

Таблица

Основные режимы в стандарте IEEE 802.16-2004

Режим	Частотный диапазон, ГГц	Опции	Метод дуплексирования
WirelessMAN-SC	10-66		TDD/FDD
WirelessMAN-SCa	<11	AAS/ARQ/STC	TDD/FDD
WirelessMAN-OFDM	<11	AAS/ARQ/STC/Mesh	TDD/FDD
WirelessMAN-OFDMA	<11	AAS/ARQ/STC	TDD/FDD
WirelessHUMAN	<11, безлиценз. диапазон	DFS/AAS/ARQ/Mesh/STC	TDD

- ARQ (automatic repeat request) – автоматический запрос повторной передачи;
- AAS (adaptive antenna system) – работа с адаптивными антенными системами;
- STC (space time coding) – пространственно-временное кодирование;
- MESH – режим взаимодействия АС друг с другом;
- DFS (dynamic frequency selection) – режим динамического распределения частот.

WirelessMAN-SC

Физический уровень WirelessMAN-SC предназначен для работы в условиях прямого распространения сигнала на частоте несущей в диапазоне 10-66 ГГц. Стандарт IEEE 802.16 жестко не регламентирует полосу частот для WirelessMAN-SC. Задаются три наиболее типичных значения - 20, 25 и 28 МГц.

Физический уровень WirelessMAN-SC поддерживает два вида дуплекса: частотный FDD (Frequency Division Duplex) и временной TDD (Time Division Duplex). При частотном дуплексе поддерживаются как полнодуплексные пользовательские станции: которые могут принимать и передавать одновременно, так и полудуплексные пользовательские станции, которые одновременно могут либо передавать, либо принимать.

Передача данных в прямом (от базовой станции к пользовательской) и в обратном каналах имеет кадровую структуру. Стандарт регламентирует три размера кадра: 0.5, 1 и 2мс.

Рассмотрим подробнее структуру кадра. Он содержит кадр прямого канала, и кадр обратного канала. В случае частотного дуплекса кадры прямого и обратного каналов передаются одновременно на различных частотах:

Рис. 2. Кадры прямого и обратного каналов в случае частотного дуплекса.

При временном дуплексе в кадре вначале передают кадр прямого канала, а за ним кадр обратного канала. Сам кадр имеет фиксированный размер, а доли кадра, занимаемые кадрами прямого и обратного каналов, могут адаптивно меняться от кадра к кадру.

Рис. 3. Кадры прямого и обратного каналов в случае временного дуплекса.

При частотном дуплексе кадр прямого канала имеет структуру, показанную на рис. 4. и включает в себя следующие элементы:
преамбулу кадра прямого канала;

- DL-MAP (Dowlink Map)- расписание кадра прямого канала;
- UL-MAP (Uplink Map)- расписание кадра обратного канала;
- TDM-часть:
  - TDM-пакеты с пользовательскими данными;
- TDMA-часть:
  - TDMA – пакеты с пользовательскими данными, перед каждым из которых передаётся преамбула.

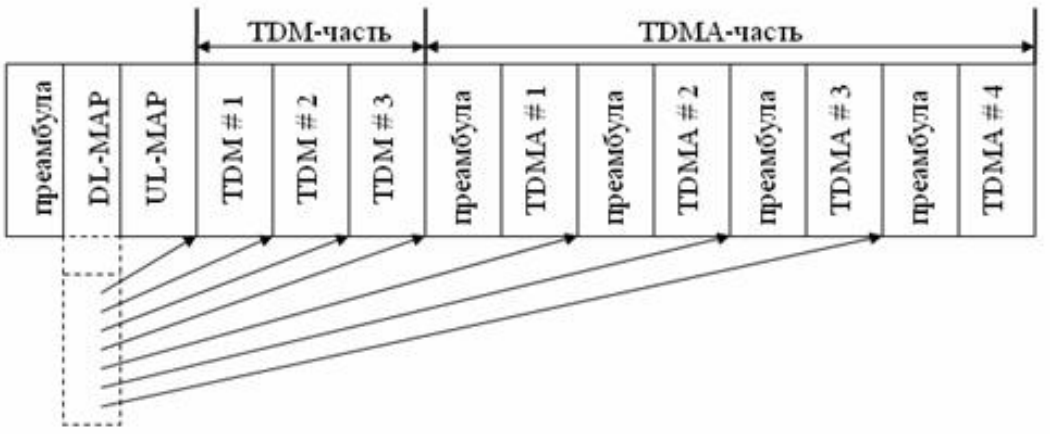


Рис. 4. Структура кадра прямого канала в случае частотного дуплекса.

Данные разных пользовательских станций в прямом канале разделяются по времени. При этом предусмотрено два подхода: TDM (Time Division Multiplexing) - временное мультиплексирование; TDMA (Time Division Multiple Access) - множественный доступ с временным разделением. Последний подход предусмотрен для поддержки полудуплексных станций.

Сообщение DL-MAP задаёт расписание пакетов разных пользователей внутри кадра прямого канала, а сообщение UL-MAP — внутри кадра обратного канала.
Преамбулы служат для измерений, частотно-временной синхронизации и оценки канала.

В случае временного дуплекса кадр прямого канала имеет структуру, показанную на рисунке 5. Она проще, так как отсутствует TDMA-часть. Добавлен временной интервал TTG (Transmit/Receive Transition Gap) - защитный интервал, предназначенный для перестройки от передачи к приёму (на базовой станции) и от приёма к передаче (на пользовательской станции).

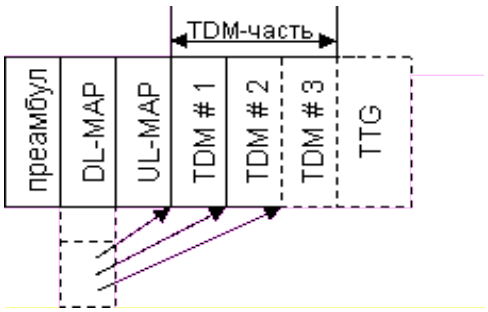


Рис. 5. Структура кадра прямого канала в случае временного дуплекса

Структура кадра обратного канала показана на рис. 6. Она практически одинакова для частотного и временного дуплекса. Отличие заключается в наличии временного интервала RTG (Receive/Transmit Transition Gap)- защитного интервала, как и TTG.

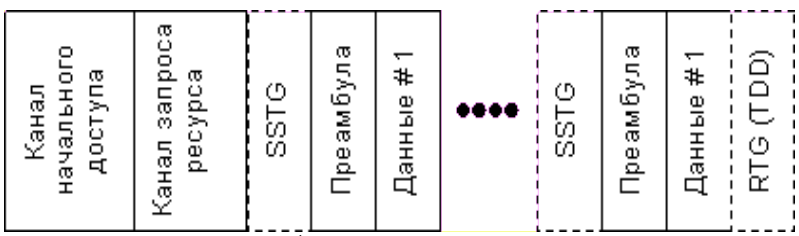


Рис. 6. Структура кадра обратного канала

Кадр обратного канала содержит следующие основные элементы:

- канал начального доступа;
- канал запроса частотно-временного ресурса;
- пакеты с пользовательскими данными .

Последние в случае временного дуплекса имеют SSTG (Subscriber Station Transition Gap) – защитный временной интервал между пакетами разных пользовательских станций и состоят из преамбулы; пользовательских данных. Длительность канала начального доступа и канала запроса частотно-временного ресурса плюс расписание отправки пакетов с данными задаёт сообщение UL-MAP текущего или одного из предыдущих кадров прямого канала.

Для физического уровня WirelessMAN-SC стандарта IEEE 802.16 определены четыре схемы кодирования:

- код Рида-Соломона (Reed-Solomon Code);
- код Рида-Соломона и блочный свёрточный код (Block Convolutional Code);
- код Рида-Соломона и проверка чётности (Parity Check);
- блочный турбокод (Block Turbo Code).

Определены три вида модуляции: QPSK; 16-QAM; 64-QAM. Применение разных схем кодирования и видов модуляции позволяют реализовать адаптивное кодирование и модуляцию. Скорости передачи для размера кадра 1мс для трёх рекомендованных полос частот физического уровня WirelessMAN-SC приведены в табл. 3.

Таблица 3. Канальные скорости передачи WirelessMAN-SC

Полоса частот, МГц	Скорость передачи, QPSK, Мбит/с	Скорость передачи, 16-QAM, Мбит/с	Скорость передачи, 64-QAM, Мбит/с
20	32	64	96
25	40	80	120
28	44.8	89.6	134.4

Для нормальной работы станций стандарт предусматривает начальную и периодическую частотно-временную синхронизацию. Выполняется по сигналу базовой станции.
Предусмотрена регулировка мощности передатчика пользовательской станции .
Для реализации функций адаптивного кодирования и модуляции, а также для регулировки мощности стандарт IEEE 802.16 предусматривает периодические измерения уровня принимаемого сигнала и отношения сигнал/шум (RSSI).

WirelessMAN-SCa

Физический уровень WirelessMAN-SCa предназначен для работы в условиях не прямого распространения сигнала на частоте несущей до 11 ГГц.

Определены следующие схемы кодирования:

- код Рида-Соломона+перемежитель+совместное кодирование и модуляция с переменной скоростью на базе свёрточного кода (rate-compatible TCM from K=7, R=1/2 CC);
- кодирование не применяется;
- блочный турбокод;
- свёрточный код.

Определены следующие виды модуляции: BPSK с расширением спектра; BPSK; QPSK; 16-QAM; 64-QAM; 256-QAM.

В кадр добавлены пилотные символы для оценки канала; разрешена возможность повторной передачи (ARQ); определена разнесённая передача на основе пространственно-временных кодов; реализована поддержка адаптивных антенных систем.

Пилот-сигнал (пилот-тон) — сигнал с априорно известными на приёмной стороне параметрами (например, определённой частоты). Пилот-сигналы могут передаваться как вместе с информационным сигналом, так и в режиме временного, кодового, частотного разделения. Пилот-сигналы используются для синхронизации, оценки параметров канала распространения, адаптации параметров приёма, обработки сигналов телекоммуникационной системой.

WirelessMAN-OFDM

Спецификация физического уровня WirelessMAN-OFDM является наиболее интересной с точки зрения практической реализации. Она базируется на технологии OFDM, что значительно расширяет возможности оборудования, в частности, позволяет работать на относительно высоких частотах в условиях отсутствия прямой видимости. Кроме того, в нее включена поддержка топологии «каждый с каждым» (mesh), при которой абонентские устройства могут одновременно функционировать и как базовые станции, что упрощает развертывание сети и помогает преодолеть проблемы прямой видимости.

Физический уровень WirelessMAN-OFDM предназначен для работы в условиях не прямого распространения сигнала на частоте несущей до 11 ГГц и основан на технологии OFDM.

Метод OFDM является сочетанием модуляции и мультиплексирования. Обычно, мультиплексирование относится к независимым сигналам, произошедшим от разных источников. Поэтому возникает вопрос о том, как разделить спектр частот между этими сигналами. В OFDM задача мультиплексирования применяется для отдельных сигналов, но эти отдельные сигналы являются подмножеством одного основного сигнала. Иногда можно встретить наименование *FDM на нескольких несущих (multi-carrier FDM)*.

OFDM-символ содержит 256 поднесущих, из которых используется 200 поднесущих. Из них на 8 поднесущих передают пилот-сигналы, а остальные используют для передачи данных.

При формировании OFDM-сигнала цифровой поток данных делится на несколько подпотоков (каналов), в каждом канале поднесущая модулируется своим подпотоком данных, а затем каналы мультиплексируются для создания OFDM несущей. Амплитуда и фаза поднесущей вычисляются на основе выбранной схемы модуляции.

Одним из главных преимуществ метода OFDM является его устойчивость к эффекту многолучевого распространения. Эффект вызывается тем, что излученный сигнал, отражаясь от препятствий, приходит к приемной антенне разными путями, вызывая межсимвольные искажения. Этот вид помех характерен для городов с разноэтажной застройкой из-за многократных отражений радиосигнала от зданий и других сооружений. Для того чтобы избежать межсимвольных искажений, перед каждым OFDM-символом вводится защитный интервал, называемый циклическим префиксом. Циклический префикс представляет собой фрагмент полезного сигнала, что гарантирует сохранение ортогональности поднесущих (но только в том случае, если отраженный сигнал при многолучевом распространении задержан не больше, чем на длительность циклического префикса). Кроме того, циклический префикс позволяет выбрать окно для преобразования Фурье в любом месте временного интервала символа.

Стандарт IEEE 802.16 традиционно не регламентирует полосу частот для WirelessMAN-OFDM, но определяет значения, одному из которых должна быть кратна полоса частот: 1,25; 1,5; 1,75; 2 и 2,75 МГц.

WirelessMAN-OFDM поддерживает два вида дуплекса: частотный и временной. Для частотного дуплекса стандарт поддерживает и полнодуплексные и полудуплексные пользовательские станции.

Регламентируются следующие размеры кадра WirelessMAN-OFDM: 2,5; 4; 5; 8; 10; 12,5 и 20 мс.
Рассмотрим структуру кадров прямого и обратного каналов для режима «точка-многоточка». Кадр прямого канала показан на рисунке 7.

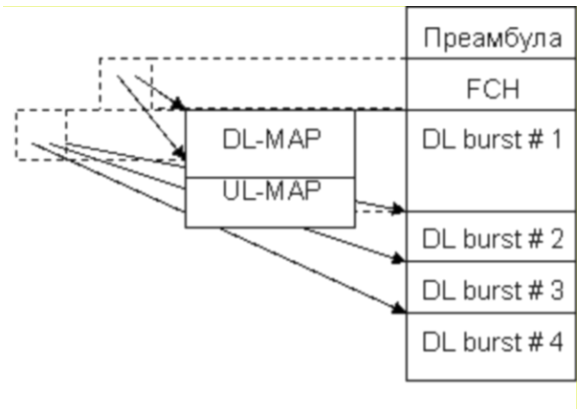


Рис. 7. Структура кадра прямого канала

Кадр прямого канала содержит: преамбулу; FCH(Frame Control Header) – заголовок, указывающий местоположение, вид кодирования и модуляцию сообщений DL-MAP и UL-MAP; DLburst#1 – первый пакет прямого канала содержит DL-MAP-расписание кадра прямого канала и UL-MAP-расписание кадра обратного канала; Dlburst#n – остальные пакеты прямого канала.

Вид кодирования и модуляции - одинаковый внутри одного пакета прямого канала и может изменяться от пакета к пакету. Пакет может передавать данные, как одному, так и разным пользователям.

Сообщение DL-MAP задаёт расписание пакетов разных пользователей внутри кадра прямого канала, а сообщение UL-MAP- внутри кадра обратного канала.

Преамбула служит для измерений, частотно-временной синхронизации и оценки канала.

Кадр обратного канала показан на рисунке 8.

Рис. 8. Структура кадра обратного канала

Кадр обратного канала содержит: канал начального доступа; канал запроса частотно-временного ресурса; пакеты с данными пользователей, которые имеют преамбулу и сами данные.
Как и в предыдущих физических уровнях для временного дуплекса предусмотрены защитные интервалы для разделения кадров прямого и обратного каналов и для разделения пакетов каналов разных пользовательских станций.
Длительность каналов начального доступа и запроса частотно-временного ресурса, а так же расписание передачи пакетов с пользовательскими данными задаёт UL-MAP текущего или одного из предыдущих кадров прямого канала.

WirelessMAN-OFDM определяет три схемы кодирования:

- код Рида Соломона и блочный свёрточный код;
- блочный турбокод;
- свёрточный турбокод (Convolutional Turbo Code).

Предусмотрено четыре типа модуляции: BPSK; QPSK; 16-QAM; 64-QAM. Это позволяет применить адаптивное кодирование и модуляцию.
Определена синхронизация, регулировка мощности пользовательской станции и измерения RSSI, предусмотрена поддержка адаптивных антенных систем.

WirelessMAN-OFDMA

Этот уровень предназначен для работы в условиях не прямого распространения сигнала на частоте несущей до 11 ГГц и использует OFDMA (Orthogonal Frequency Division Multiple Access) - множественный доступ с частотно-временным разделением на базе технологии OFDM.

В OFDM-символе предусмотрены 2048 поднесущих, из них часть используется для передачи и на части поднесущих передают пилот-сигналы.
Определены рекомендованые для WirelessMAN-OFDMA полосы частот: 1,25; 1,5; 1,75; 2 и 2,75 МГц и два вида дуплекса: частотный и временной с поддержкой полнодуплексных и полудуплексных пользовательских станций.
Регламентированы размеры кадра WirelessMAN-OFDMA: 2,5; 4; 5; 8; 10; 12,5 и 20мс.

Кадры прямого и обратного каналов могут содержать разное количество зон (рисунок 9). Зоны отличаются количеством пилот-сигналов и схемами перемежения поднесущих.

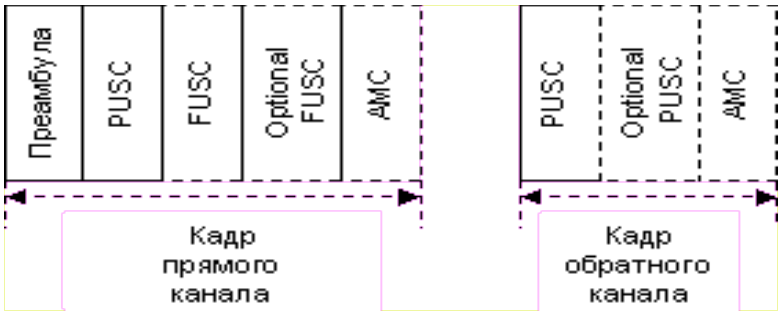


Рис. 9. Структура кадров прямого и обратного канала

Для прямого канала определены следующие зоны:

- PUSC (Partial Usage of Subcarriers) - зона, использующая частотное разнесение при передаче и предусматривающая три частотных сегмента, при этом базовая станция может использовать 1/3, 2/3 или всю полосу частот;
- FUSC (Full Usage of Subcarriers) - зона, использующая частотное разнесение при передаче и предусматривающая только один частотный сегмент;
- Optional FUSC- отличается от зоны FUSC только количеством пилот-сигналов;
- AMC (Adaptive Modulation and Coding) - зона, не использующая частотного разнесения (предполагается использование многопользовательского разнесения).

В обратном канале зоны определены так:

- PUSC - аналогичная верхней PUSC-зоне;
- Optional PUSC - отличается от зоны PUSC только количеством пилот-сигналов;
- AMC - аналогичная верхней AMC-зоне.

Все зоны имеют примерно одинаковые логические структуры. Например рассмотрим зону PUSC прямого канала и зону PUSC обратного канала. При этом будем предполагать, что базовая станция (сектор) использует всю полосу частот. На рисунке 10 показана структура этих зон.

Зона PUSC прямого канала включает следующие элементы:

- Преамбула (так как это первая зона в кадре прямого канала);

- FCH - заголовок кадра, указывающий на местоположение и вид кодирования и модуляции сообщения DL-MAP;
- DL-MAP - расписание кадра прямого канала;
- UL-MAP - расписание кадра обратного канала;
- DL burst #n - пакеты прямого канала.

Зона PUSC обратного канала содержит пакеты обратного канала.
DL-MAP задаёт расписание зон внутри кадра прямого канала, а так же расписание пакетов данных внутри каждой зоны прямого канала. UL-MAP задаёт расписание зон внутри кадра обратного канала, а так же расписание пакетов данных внутри каждой зоны обратного канала.
Зоны PUSC и Optional PUSC обратного канала могут содержать каналы начального доступа и запроса частотно-временного ресурса.

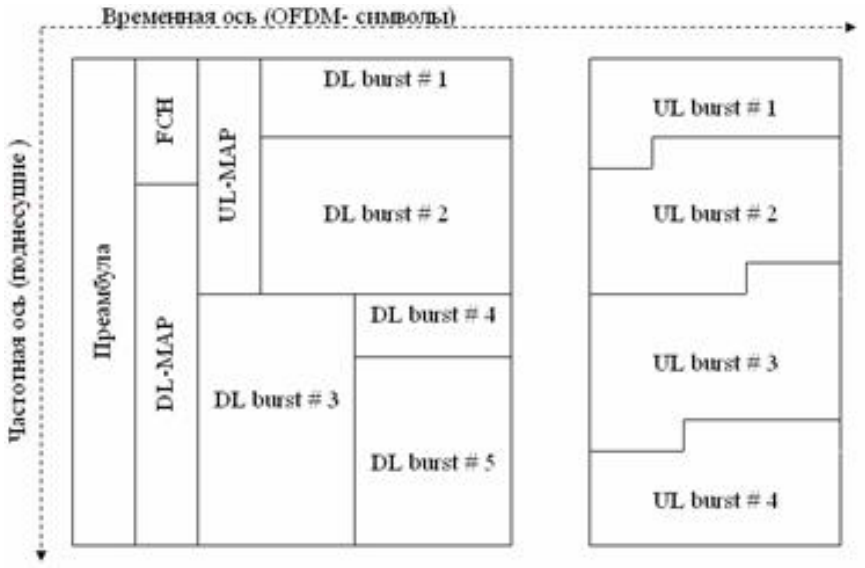


Рис. 10. Структура зоны PUSC прямого и обратного каналов

Для уровня WirelessMAN-OFDMA определены три схемы кодирования: блочный свёрточный код; блочный турбокод; свёрточный турбокод. Предусмотрено три вида модуляции: QPSK; 16-QAM; 64-QAM. Несколько схем кодирования и видов модуляции позволяют осуществлять адаптивное кодирование и модуляцию.

Канальные скорости передачи для полос частот 6 и 7 МГц- для уровня WirelessMAN-OFDMA, для циклического префикса и для разных видов кодирования и модуляции приведены в таблице 4.

Таблица 4. Канальные скорости передачи для WirelessMAN-OFDMA

Полоса частот, МГц	QPSK 1/2	QPSK 3/4	16-QAM 1/2	16-QAM 3/4	64-QAM 2/3	64-QAM 3/4
6	4,99	7,48	9,97	14,96	19,95	22,44
7	5,82	8,73	11,64	17,45	23,27	26,18

Предусмотрена начальная и периодическая частотно-временная синхронизация по сигналу базовой станции. Имеется регулировка мощности пользовательской станции. Для адаптивного кодирования и модуляции, а так же для регулировки мощности определены периодические измерения уровня принимаемого сигнала, а также отношения сигнал/шум.

Предусмотрена возможность повторной передачи (ARQ) и гибридной повторной передачи (H-ARQ), а также разнесённая передача и поддержка адаптивных антенных систем.

MAC-уровень

Уровень MAC выполняет управление доступом к среде передачи различных пользовательских станций, а также управление параметрами передачи.
Основные функции уровня MAC базовой и пользовательской станции показаны на рисунках 11, 12 и 13.

В стандарте IEEE 802.16 реализован уровень MAC с централизованным управлением. Управление передачей данных в прямом и обратном канале осуществляется на базовой станции. Уровни MAC пользовательских станций при передаче данных в обратном канале выполняют решения, принятые на базовой станции.
На базовую и на пользовательские станции поступают пакеты данных SDU (Service Data Unit) с верхних уровней от разных источников или приложений. Поток данных от одного источника (приложения) называют сервисным потоком (Service Fow). Он определен требованиями по качеству обслуживания QoS (Quality of Service). На уровне MAC каждый сервисный поток обрабатывается отдельно.

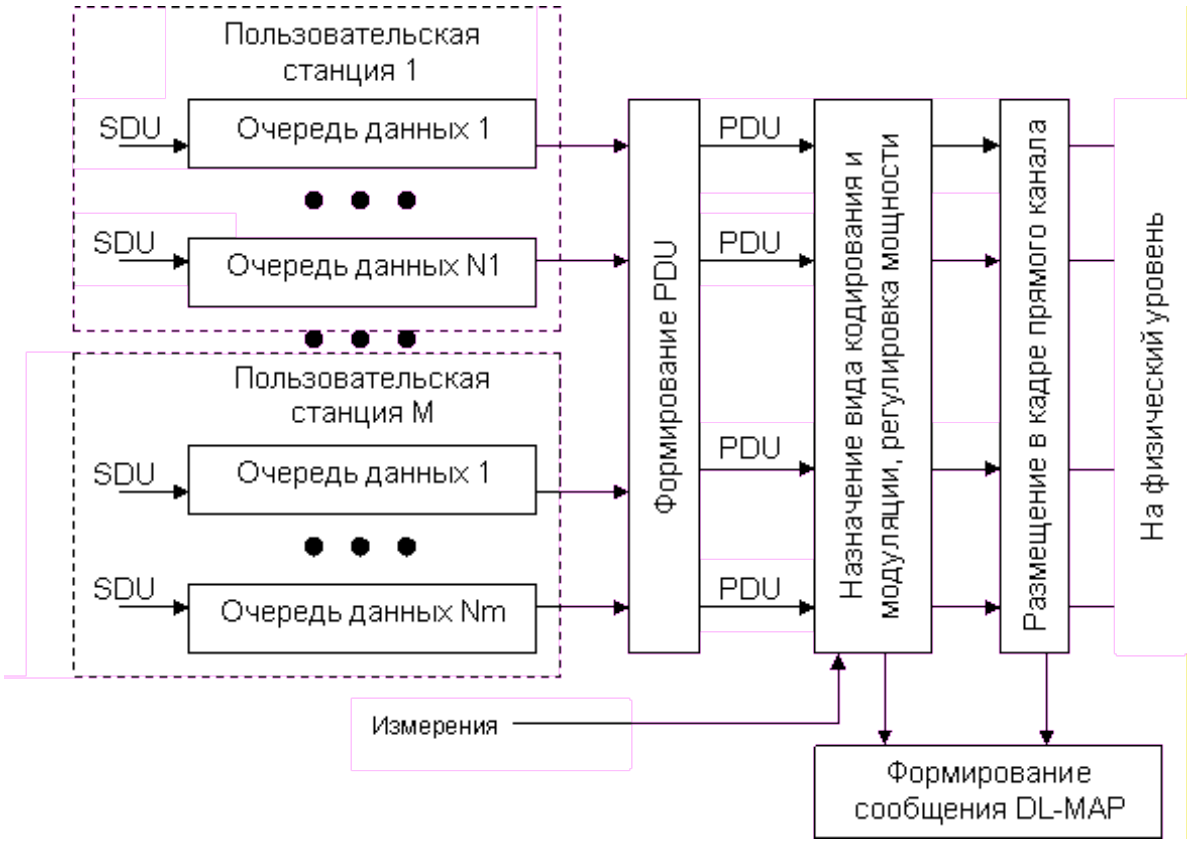


Рис. 11. Основные функции уровня MAC базовой станции при управлении передачей в прямом канале

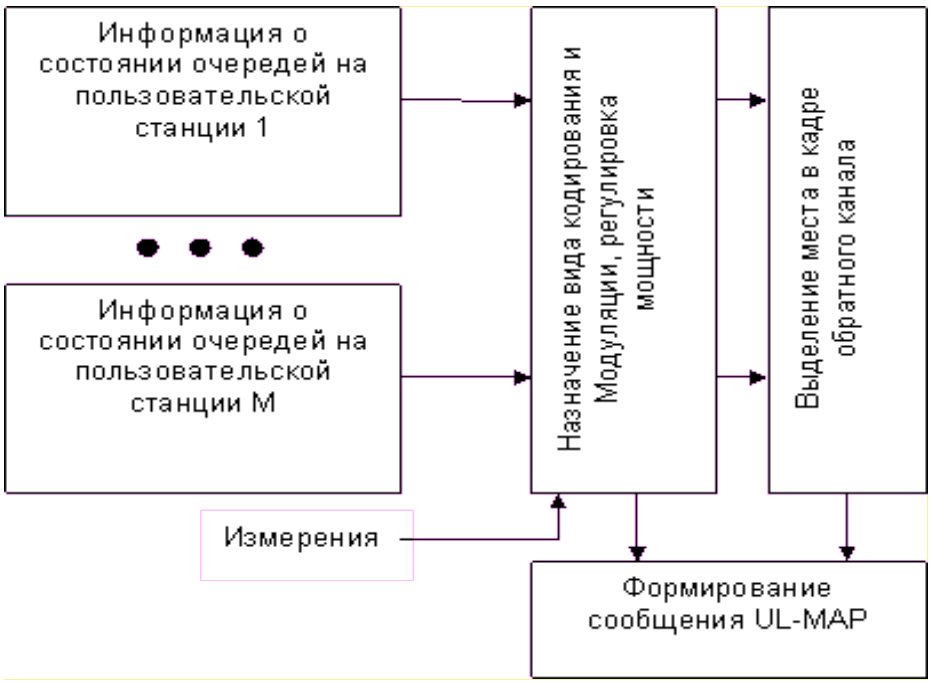


Рис. 12. Основные функции уровня MAC базовой станции при управлении передачей в обратном канале

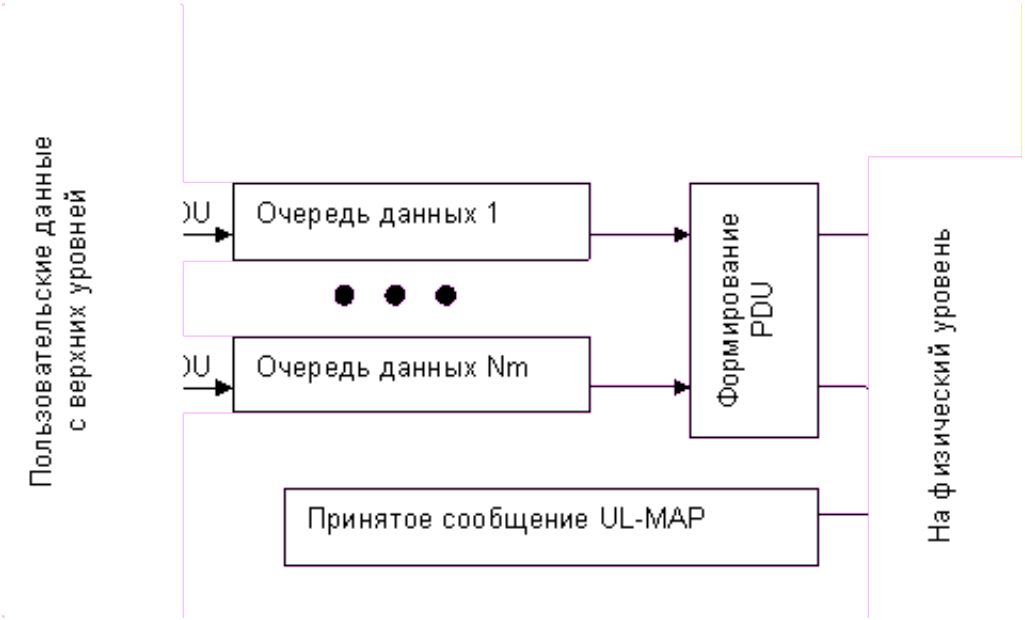


Рис. 13. Основные функции уровня MAC пользовательской станции при управлении передачей

Уровень MAC базовой станции при управлении передачей в прямом канале выполняет следующие функции:

- Хранит пакеты данных SDU, поступившие с верхних уровней, в очередях (отдельная очередь для каждого сервисного потока);
- Принимает решения о том, сколько данных и из каких очередей будет передано в текущем кадре;
- Преобразует пакеты данных SDU в пакеты данных PDU (Protocol Data Unit);
- Отдельно назначает каждому набору пакетов данных PDU одного сервисного потока вид кодирования и модуляции, а также излучаемую мощность (при этом используется информация о требованиях QoS этого сервисного потока,

количестве и структуре сформированных пакетов данных PDU, а также результаты измерений состояния канала передачи RSSI);
- Логически размещает сформированные наборы пакетов данных PDU сервисных потоков в кадре прямого канала.

Производит формирование сообщения DL-MAP текущего кадра прямого канала: количество наборов пакетов данных PDU; их вид кодирования и модуляции; их положение в кадре; передает пакеты данных PDU на физический уровень.

Уровень MAC базовой станции при управлении передачей в обратном канале выполняет следующие функции:

- Принимает решение о том, сколько данных и из каких очередей будет передано в текущем кадре (при этом используется информация о размере очередей на пользовательских станциях);
- Назначает отдельно каждому сервисному потоку вид кодирования и модуляции, а также излучаемую мощность (при этом используется информация о требованиях QoS этого сервисного потока, размер его очереди на пользовательской станции, а также результат измерений состояния канала передачи);
- Выделяет место для передачи сервисным потокам в кадре обратного канала.

Выполняет формирование сообщения UL-MAP, содержащее для текущего кадра обратного канала следующую информацию: количество выделенных мест; назначенные виды кодирования и модуляции; положение выделенных мест в кадре обратного канала.

Уровень MAC пользовательской станции при управлении передачей в обратном канале выполняет следующие функции:

- Хранит пакеты данных SDU, поступившие с верхних уровней, в очередях (отдельная очередь для каждого сервисного потока);
- Принимает информацию из сообщения UL-MAP;
- Принимает решение о том, сколько данных будет взято из очередей, под которые выделено место для передачи в текущем кадре обратного канала;
- Преобразует пакеты данных SDU в пакеты данных PDU;
- Передает сформированные наборы пакетов данных PDU, а также информацию из сообщения UL-MAP на физический уровень.

Средства запроса и выделения частотно-временного ресурса

Согласно предыдущих разделов управление передачей в стандарте IEEE 802.16 осуществляется на уровне MAC базовой станции. Для управления передачей в обратном канале в стандарте предусмотрены следующие средства запроса и выделения частотно-временного ресурса:

- Запросы (Request);
- Выделение ресурса для передачи данных (Grant);
- Выделение ресурса для передачи запроса (Poll);
- Канал запроса ресурса (Bandwidth Request Subchannel).

Эти средства используются в соответствии с одной из предусмотренных в стандарте процедур (Scheduling Service). В стандарте IEEE 802.16 предусмотрено четыре процедуры:

- Выделение ресурса без предварительного запроса UGS (Unsolicited Grant Service);
- Выделение ресурса под запрос с высокой частотой rtPS (Real Time Polling Service);
- Выделение ресурса под запрос со средней частотой nrtPS (non real time Polling Service);
- Запросы со случайным доступом BE (Best Effort).

Каждому сервисному потоку в обратном канале назначается одна из четырёх процедур исходя из требований QoS и других параметров этого сервисного потока.

Процедура UGS предназначена для передачи сервисного потока с постоянной скоростью поступления пользовательских данных и постоянным размером пакетов данных SDU. Она заключается в том, что сервисному потоку на периодической основе выделяется ресурс в кадре обратного канала под передачу данных.

Процедуры rtPS и nrtPS очень схожи между собой. В соответствии с ними сервисному потоку на периодической основе выделяют в кадре обратного канала ресурс под передачу запроса, который содержит информацию о размере очереди этого сервисного потока на пользовательской станции. После приёма этого запроса уровень MAC базовой станции выделяет ресурс в кадре обратного канала под передачу данных из очереди этого сервисного потока. Отличия процедур rtPS и nrtPS следующие - как следует из названия, при использовании процедуры rtPS ресурс под запрос выделяется чаще, чем при использовании процедуры nrtPS и сервисным потокам, использующим процедуру nrtPS, дополнительно разрешается передавать сообщения в канале запроса ресурса.

Процедура BE предназначена для передачи сервисных потоков, практически не чувствительных к задержке. При этом минимальная скорость передачи также не гарантируется. В соответствии с процедурой BE уровень MAC пользовательской станции передаёт сообщение в канале запроса ресурса. Этот канал использует случайный доступ. В случае успешного приёма сообщения на базовой станции она выделяет ресурс для передачи запроса в кадре обратного канала. Запрос содержит информацию о размере очереди сервисного потока. После приёма запроса уровень MAC базовой станции выделяет ресурс для передачи данных этого сервисного потока.

Вход в сеть и синхронизация

Для входа в сеть пользовательской станции предусмотрен канал начального доступа. Он идентичен каналу запроса ресурса за исключением того, что использует другой набор сообщений. Во время процедуры входа в сеть пользовательская станция

осуществляет начальную частотно-временную синхронизацию и регулировку мощности (Initial Ranging). Также пользовательская и базовая станции обмениваются информацией о сервисных потоках, которые надо будет поддерживать в прямом и обратном каналах.
При входе в сеть происходит аутентификация пользовательской станции. Стандарт IEEE 802.16 поддерживает шифрование предаваемых данных для обеспечения безопасности.
В процессе работы пользовательская станция осуществляет периодическую частотно-временную синхронизацию (Periodic Ranging).

Мобильность WiMAX

Стандарт IEEE 802.16e является дополнение к стандарту IEEE 802.16 для обеспечения мобильности. Рассмотрим основные дополнительные механизмы стандарта IEEE 802.16e.

Для физического уровня

Стандарт IEEE 802.16e поддерживает работу мобильных пользователей со следующими физическими уровнями стандарта IEEE 802.16: WirelessMAN-SCa; WirelessMAN-OFDM; WirelessMAN-OFDMA.
Основные дополнения коснулись физического уровня WirelessMAN-OFDMA. Из них можно выделить два основных дополнения. Во-первых, кроме OFDM- символа с 2048 поднесущими, в стандарте IEEE 802.16e предусмотрены OFDM-символы с 1024, 512 и 128 поднесущими. Во-вторых, предусмотрен новый вид кодирования- код с низкой избыточностью и проверкой чётности LDPC (LowDensity Parity Check).

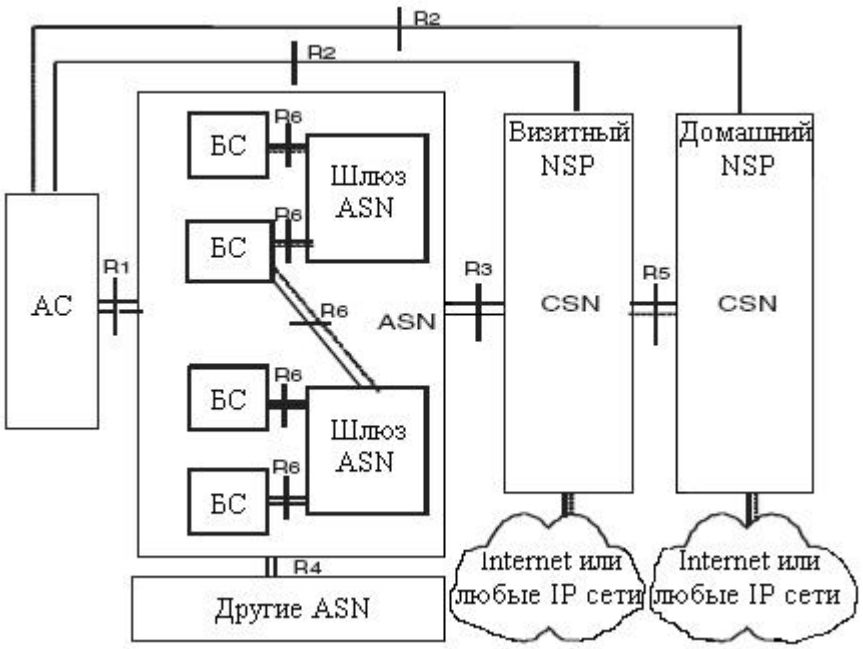
Для MAC-уровня

Уровень MAC стандарта IEEE 802.16e содержит ряд существенных дополнений для поддержки мобильных пользовательских станций.
Для экономии расхода батареи мобильных пользовательских станций предусмотрен спящий режим (Sleep Mode). В этом режиме мобильная пользовательская станция осуществляет приём и передачу только в заранее согласованные интервалы времени, а в остальное время отключается.
В стандарте IEEE 802.16e предусмотрены различные виды Handover (передача обслуживания мобильной пользовательской станции между базовыми станциями) для поддержания непрерывности соединений при движении мобильной пользовательской станции. Предусмотрены следующие виды Handover: жесткий (Hard); быстрая смена обслуживающей базовой станции (FBSS- Fast Base Station Switching); мягкий (Soft).
В стандарте IEEE 802.16e предусмотрен режим ожидания (Idle Mode). В случае если у мобильной пользовательской станции нет активных соединений, то она может перейти в режим ожидания. Это существенно уменьшает нагрузку на сеть как в прямом, так и в обратном каналах, а также экономит ресурс батареи мобильной пользовательской станции. В этом режиме предусмотрен поиск мобильной пользовательской станции (Paging).

Базовая модель сети WiMAX

Спецификации стандарта WiMAX описывают передачу трафика и сигнальный обмен только на радиоинтерфейсе. Относительно соединения БС с Интернетом, сетями беспроводного доступа и сетями сторонних операторов, решения по структуре сети принимает оператор совместно с вендором (поставщиком оборудования). В целях унификации и оптимизации WiMAX Forum предложена базовая структура сети

WiMAX — NRM (Network Reference Model) — являющаяся логическим представлением сетевой архитектуры.



NRM подразделяет систему на три логические части:

- Абонентские станции (AC, SS/MS — the Subscriber Station/Mobile Station), используемые клиентами для получения доступа к сети;
- ASN (Access Services Network) — сеть доступа к услугам, являющаяся собственностью оператора доступа к сети (NAP — Network Access Provider); ASN включает одну или несколько базовых станций (БС), которыми управляет один или несколько шлюзов ASN (ASN-GW).
- CSN (Connectivity Services Network) — подсеть оператора, способствующая выходу на IP и другие сети для реализации абонентских услуг. Эта подсеть реализует необходимые коммутационные функции и функции безопасности. Абонента может обслуживать оператор домашней сети NSP (Network Services Provider). Кроме того, абонент может находиться в роуминге. В данном случае его обслуживает оператор визитной сети; при этом осуществляется обмен сигнальной информацией CSN визитного и домашнего оператора.

Функции ASN:

- соединение на уровне L2 с AC;
- поиск и выбор сети, основываясь на предпочтениях абонента о CSN/NSP;
- реализация безопасности: передача информации об устройствах, пользователях и услугах серверу безопасности, временное хранение профилей абонентов;
- создание сквозных IP-соединений между AC и CSN;
- управление радиоресурсом (RRM) в соответствии с классом трафика и требуемым QoS;
- поддержка мобильности, т. е. выполнение процедур хэндовера, локализации и пейджинга.

WiMAX Forum определил различные способы организации ASN, которые получили название профилей. Специфицированы профили **A, B, C**. Шлюз ASN – это логическое устройство, которое может быть реализовано по-разному. Профиль **B** ASN представляет простую организацию, которая состоит из БС и шлюза ASN. Профили **A**

и **С** разделяют функции между БС и шлюзом ASN по-разному, а именно в управлении мобильностью и радиоресурсами.

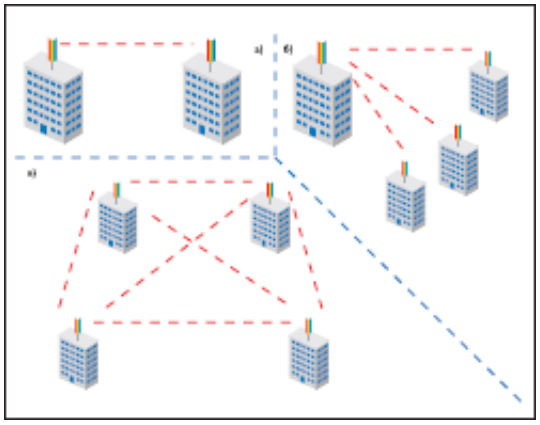
Функционально БС представляет собой один сектор с выделенным частотным диапазоном, обеспечивающим интерфейс IEEE 802.16e с абонентской станцией. Дополнительные функции, выполняемые БС в обоих профилях, включают распределение для восходящего и нисходящего каналов, классификацию трафика и SFM (управление сервисным потоком). При этом должны быть выполнены требования по QoS для различных классов трафика, передаваемых по радиоинтерфейсу. БС также управляет статусом абонентской станции (активный, неработающий), поддерживает туннельный протокол в направлении к шлюзу ASN, обеспечивает с помощью сервера DHCP динамическими адресами. БС также передает сигнальный обмен, обеспечивая все уровни защиты, предусмотренные стандартом. БС может быть подключена одновременно к двум шлюзам для баланса нагрузки.

Шлюз ASN – это основной элемент сети. Во время сеансов связи шлюз организует хэндовер абонентов и пейджинг абонентской станции, управляет доступом к сети. Шлюз объединяет трафик и сообщения сигнализации от БС и передает их в сеть CSN. Для любого подсоединенного абонента в шлюзе открыта база данных, включающая профили абонента и ключи шифрования. На шлюз возложены задачи авторизации потока услуг согласно профилю абонентов и QoS. В направлении БС шлюз поддерживает туннельное соединение; в направлении ядра сети (CSN) шлюз осуществляет соединение по стандартному IP протоколу.

Для соединения базовой станции с абонентской используется высокочастотный диапазон радиоволн от 1,5 до 11 ГГц. В идеальных условиях скорость обмена данными может достигать 70 Мбит/с, при этом не требуется обеспечения прямой видимости между базовой станцией и приёмником.

Между базовыми станциями устанавливаются соединения (прямой видимости), использующие диапазон частот от 10 до 66 ГГц, скорость обмена данными может достигать 140 Мбит/с. При этом, по крайней мере одна базовая станция подключается к сети провайдера с использованием классических проводных соединений. Однако, чем большее число БС подключено к сетям провайдера, тем выше скорость передачи данных и надёжность сети в целом.

Топология сети



- Для соединения «точка–точка» используются две направленные друг на друга антенны; так строятся, например, радиорелейные линии передач, в которых расстояние между соседними релейными вышками может исчисляться десятками километров.
- При топологии «точка–многоточка» в центре «ячейки» помещается базовая станция со всенаправленной или секторной антенной, а все обслуживаемые ей абоненты снабжаются сфокусированными на нее направленными антеннами.
- Другой тип связи получится при использовании только всенаправленных антенн. В этом случае будет достигнута возможность соединения «каждого с каждым», или «многоточка–многоточка» (mesh).

Защита информации в WiMAX

В соответствии со стандартом, для предотвращения несанкционированного доступа и защиты пользовательских данных осуществляется шифрование всего передаваемого по сети трафика. БС WiMAX представляет собой модульный конструктив, в который при необходимости можно установить несколько модулей со своими типами интерфейсов, но при этом должно поддерживаться административное программное обеспечение для управления сетью. Данное программное обеспечение обеспечивает централизованное управление всей сетью. Логическое добавление в существующую сеть абонентских комплектов осуществляется также через эту административную функцию.

Абонентская станция (АС) представляет собой устройство, имеющее уникальный серийный номер, MAC-адрес, а также цифровую подпись (сертификат) X.509, на основании которой происходит аутентификация АС на БС. Сертификат уникален для каждого абонента, подписан hash-функцией SHA-1 и не может быть изменен, поскольку «зашит» в само устройство. При этом, согласно стандарту, срок действительности цифровой подписи АС составляет 10 лет. После установки АС у клиента и подачи питания АС авторизуется на БС, используя определенную частоту радиосигнала, после чего БС, основываясь на перечисленных выше идентификационных данных, передает абоненту конфигурационный файл по TFTP-протоколу. В этом конфигурационном файле находится информация о поддиапазоне передачи (приема) данных, типе трафика и доступной полосе, расписание рассылки ключей для шифрования трафика и прочая необходимая для работы АС информация. Необходимый файл с конфигурационными данными создается автоматически, после занесения администратором системы АС в базу абонентов, с назначением последнему определенных параметров доступа.

После процедуры конфигурирования аутентификация АС на базовой станции происходит следующим образом:

1. Абонентская станция посылает запрос на авторизацию, в котором содержится сертификат X.509, описание поддерживаемых методов шифрования и дополнительная информация.
2. Базовая станция в ответ на запрос на авторизацию (в случае достоверности запроса) присылает ответ, в котором содержится ключ на аутентификацию, зашифрованный открытым ключом абонента, 4-битный ключ для определения последовательности, необходимый для определения следующего ключа на авторизацию, а также время жизни ключа.

3. В процессе работы АС через промежуток времени, определяемый администратором системы, происходит повторная авторизация и аутентификация, и в случае успешного прохождения аутентификации и авторизации поток данных не прерывается.

В стандарте используется протокол PKM (Privacy Key Management), в соответствии с которым определено несколько видов ключей для шифрования передаваемой информации:

- Authorization Key (AK) — ключ, используемый для авторизации AK на базовой станции;
- Traffic Encryption Key (TEK) — ключ, используемый для криптозащиты трафика;
- Key Encryption Key (KEK) — ключ, используемый для криптозащиты передаваемых в эфире ключей.

Согласно стандарту, в каждый момент времени используются два ключа одновременно, с перекрывающимися временами жизни. Данная мера необходима в среде с потерями пакетов (а в эфире они неизбежны) и обеспечивает бесперебойность работы сети. Имеется большое количество динамически меняющихся ключей, достаточно длинных, при этом установление безопасных соединений происходит с помощью цифровой подписи. Согласно стандарту, криптозащита выполняется в соответствии с алгоритмом 3-DES, при этом отключить шифрование нельзя. Опционально предусмотрено шифрование по более надежному алгоритму AES.

Оборудование WiMAX на базе SoC («система на кристалле»)

Современные тенденции развития телекоммуникационного рынка диктуют разработку так называемых System-on-Chip. Под устройствами класса SoC в общем случае понимаются устройства, на едином кристалле которых интегрированы один или несколько процессоров, некоторый объем памяти, ряд периферийных устройств и интерфейсов, — то есть максимум того, что необходимо для решения поставленных перед системой задач. Разработка SoC предполагает оптимизацию разрабатываемой схемотехники, что непосредственно сказывается на потребляемой мощности, площади кристалла и, как следствие, стоимости.

На текущий момент ведущие мировые производители сосредоточились на разработке SoC, в которых интегрированы основные функции физического и MAC уровней стандарта WiMAX. Первые образцы, разработанные на основе спецификации IEEE 802.16-2004, были представлены компаниями Fijitsu, Intel, Sequans Communications, Wavesat и PicoChip. В предлагаемых этими компаниями решениях на физическом уровне используется модуляция OFDM с 256 поднесущими и основная схема кодирования, в которой для внутреннего кода применяется сверточное кодирование и декодирование по алгоритму Витерби, а для внешнего — коды Рида-Соломона.

Функционально оборудование WiMAX разделяется на базовое и абонентское. Первое поколение чипов для базовых станций обладает меньшим уровнем интеграции, чем для абонентских станций. Для реализации MAC-протокола базовой станции требуется увеличение производительности этих решений. Для этой цели используются внешние процессоры, служащие для выполнения верхнего уровня MAC-протокола. Таким образом, чипсеты WiMAX реализуют функции физического уровня и функции нижнего уровня MAC-протокола.

Источники:

1. WiMAX. https://ru.wikipedia.org
2. Стандарт WiMAX: техническое описание, варианты реализации и специфика применения / А. Архипкин // Беспроводные технологии. № 3. 2006. http://www.wireless-e.ru
3. Учебное пособие по методу Мультиплексирования с Ортогональным Частотным Разделением сигналов (OFDM) / Charan Langton, пер. с англ. А. Бабуров, В. Едренкин. https://www.scribd.com
4. Структура сети WiMAX. http://1234g.ru

Беспроводные системы ПД

Лекция 04
Технология DECT

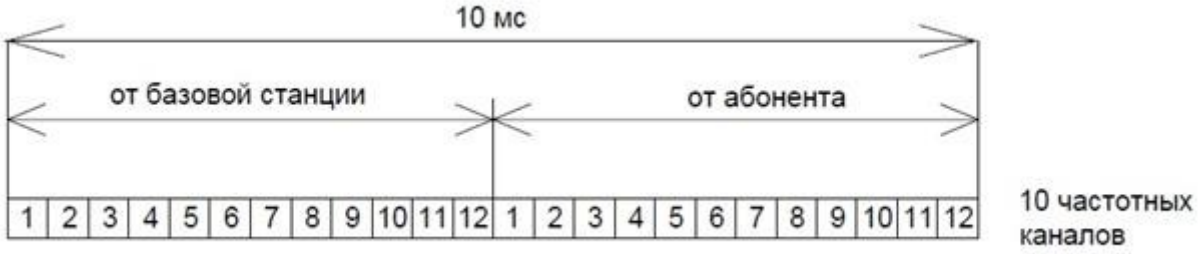
DECT (Digital Enhanced Cordless Telecommunication) — технология беспроводной связи на частотах 1880–1900 МГц с модуляцией GMSK (BT = 0,5), используется в современных радиотелефонах. Стандарт DECT является наиболее популярным стандартом беспроводного телефона в мире благодаря простоте развёртывания DECT-сетей, широкому спектру пользовательских услуг и высокому качеству связи. По оценкам 1999 года, DECT принят более чем в 100 странах, а число абонентских устройств DECT в мире приближается к 50 миллионам.

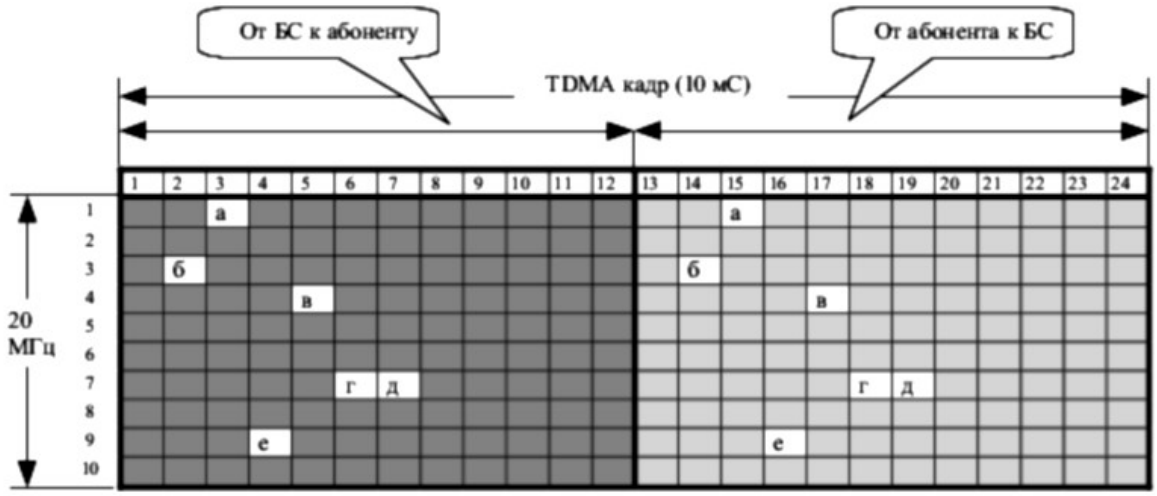
В России массовое использование оборудования стандарта DECT официально было разрешено в 1998 г. решением ГКРЧ России "Об использовании полосы радиочастот 1880–1900 МГц для оборудования DECT" и приказом Госкомсвязи России "О порядке внедрения оборудования DECT на российских сетях электросвязи".

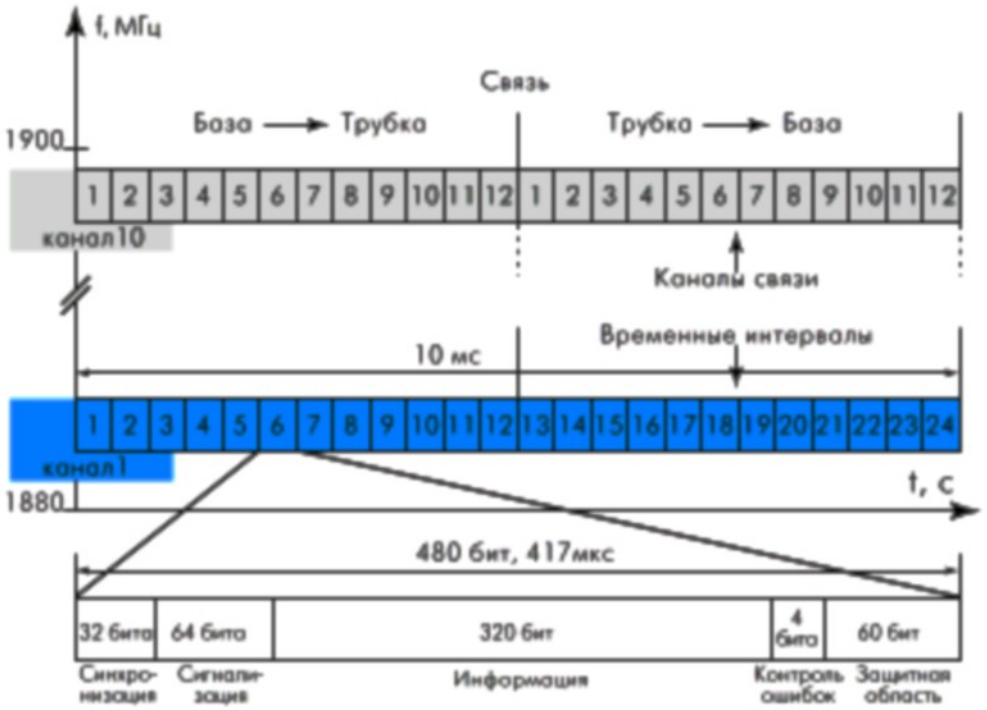
Рабочий спектр (частота DECT)	1880–1900 МГц
Количество несущих частот	10
Разнос частот	1.728 МГц
Метод доступа	MC/TDMA/TDD
Кол-во каналов на одну частоту	24 (12 дуплексных каналов)
Длительность фрейма	10 мс
Скорость передачи данных	1.152 Мб/с
Вид модуляции	GMSK (BT = 0.5)
Сжатие голоса	ADPCM (АДИКМ)
Допустимое отношение сигнал/шум	12 Дб
Мощность передатчика	10 мВт (средняя), 240 мВт (пиковая)
Достижимая дальность	до 20 км
Гарант. (разрешенная) дальность	до 5 км
Мобильность	полная в рамках одной системы (без перерыва разговора – хэндовер), в нескольких системах - роуминг

Радиоинтерфейс DECT основывается на методологии радиодоступа с использованием нескольких несущих, принципа множественного доступа с разделением времени, дуплекса с разделением времени (Multy Carrier/Time-Division Multiple Access/Time-Division Duplexing — MC/TDMA/TDD). Выделение базовой частоты DECT использует 10 частотных каналов (MC) в диапазоне 1880–1900 МГц. Временной спектр для DECT подразделяется на временные фреймы, повторяющиеся каждые 10 мс. Фрейм состоит из 24 временных слотов, каждый из которых индивидуально доступен (TDMA), слоты могут использоваться либо для передачи либо для приема. В базовой речевой услуге DECT два временных слота — с разделением в 5 мс — образуют пару для обеспечения поддерживающей емкости обычно для

полнодуплексных 32 kbps соединений (ADPCM — адаптивная дифференциальная ИКМ — аудиокодек G.726). Поэтому информационная часть каждого слота – 320 бит. При передаче данных возможно объединение временных слотов. Для облегчения реализаций базового стандарта DECT временной фрейм в 10 мс разделяется на две половины (TDD); первые 12 таймслотов используются для передачи фиксированной части (downlink), а остальные 12 — для передачи носимой части (uplink).







Структурой TDMA обеспечивается до 12 одновременных голосовых соединений DECT (полный дуплекс) на каждый трансивер, что дает значительные ценовые преимущества по сравнению с технологиями, позволяющими только одно соединение на трансивер. Благодаря усовершенствованному радиопротоколу, DECT может предлагать полосы частот различной ширины, соединяя несколько каналов в одну несущую. Для целей передачи данных достигаются защищенные от ошибок чистые скорости в n × 24 kbps максимально до 552 kbps, при этом, как оговорено стандартом DECT, обеспечивается полная безопасность.

GMSK (Gaussian Minimum Shift Keying) *— это гауссовская двухпозиционная частотная манипуляция (ЧМн) с минимальным сдвигом*, обладающая двумя особенностями, одна из которых — "минимальный сдвиг", другая — гауссовская фильтрация. Обе особенности направлены на сужение полосы частот, занимаемой GMSK-сигналом. Использование GMSK в системе сотовой радиосвязи GSM регламентируется стандартом ETSI (Европейский институт стандартов связи)

В общем случае, при ЧМн (FSK), спектр сигнала шире, чем при амплитудной манипуляции. Расширение спектра, свойственное угловой модуляции, частным случаем которой является ЧМн, зависит от *индекса модуляции — величины, характеризующей изменение фазы, обусловленное модуляцией*. Для ЧМн индекс равен ß = Δf/F (в радианах), где Δf — девиация (сдвиг) частоты, а F — частота манипуляции. Характер изменения фазы зависит от формы модулирующей функции частоты. Для обычной ЧМн функция прямоугольна, а для ЧМн с гауссовской фильтрацией, сглаживающей фронты посылок, близка к синусоидальной (при последовательности чередующихся посылок "0" и "1"). При синусоидальной модулирующей функции индекс модуляции является амплитудой изменения фазы. ЧМн подразделяют на узкополосную (ß < 0,5) и широкополосную. В основе GMSK лежит MSK — узкополосная ЧМн "с минимальным сдвигом", характеризуемая ß = 0,5. При формировании сигналов с GMSK используется гауссовская низкочастотная фильтрация модулирующих посылок, которую осуществляют обычно в цифровом процессоре (DSP), в котором формируется сигнал модуляции.

Различные компании выпускают микросхемы приемопередатчиков DECT с встроенным GMSK-модемом. Фирма Analog Devices выпускает микросхему приемопередатчика AD6411. Infineon Technologies выпускает микросхемы PMB 6720, PMB 6610 и PMB 6818/9.

При использовании принципа MC/TDMA/TDD для базового DECT (частотные и временные измерения), устройству DECT в любой момент доступен общий спектр из 120 дуплексных каналов. При добавлении третьего измерения (пространства) — при условии, что емкость DECT ограничивается помехами от сопряженных сот и достигается соотношение C/I (Carrier-to-Interface) = 10 дБ — можно получить очень низкий коэффициент повторного использования канала. Различные каналы связи в прилегающих сотах могут использовать тот же канал (комбинация частота/временной слот). Следовательно, при высокой плотности установки базовых станций DECT (например, на расстоянии 25 м в идеальной модели покрытия в форме шестиугольника) можно достичь емкости трафика для базовой технологии DECT приблизительно до 10 000 Эрланг/кв.км./этаж при отсутствии необходимости частотного планирования. Инсталляция оборудования DECT упрощена, так как необходимо учитывать только требования к покрытию и трафику.

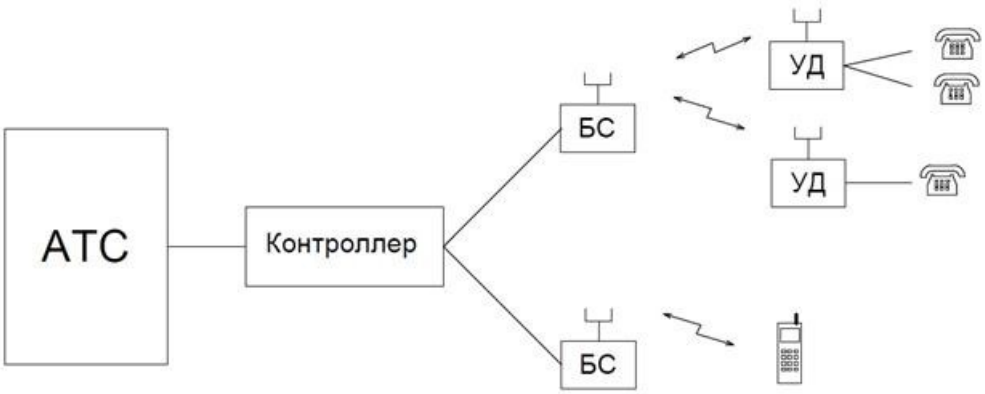
1 Эрланг равен средней нагрузке трафика, вызываемой одним речевым соединением DECT с использованием одной пары "частота/временной слот" 100% времени.

Архитектура DECT

Основными составными частями любой DECT-системы являются:

- контроллер управления;
- базовые станции (ретрансляторы);
- переносные (мобильные) телефоны.

Благодаря параметрам базовых станций систем DECT возможна организация зон обслуживания (сот), размеры которых составляют 10–30 м в зданиях и до 300 м на открытом пространстве. При использовании направленных антенн (вытянутая сота) дальность связи увеличивается до нескольких километров, что обеспечивает широкое применение систем DECT — от построения домашних односотовых систем до микросотовых сетей общего доступа.



БС — базовая станция DECT обеспечивает требуемое радиопокрытие. БС подключается к контроллеру по одной или двум парам проводов. Она представляет собой приемопередатчик, обеспечивающий одновременную работу по 4–12 частотным каналам, работающий на две пространственно разнесенные антенны. БС выполняются в двух вариантах — для внутреннего и наружного размещения.

УД — устройства доступа представляют собой мобильную трубку или стационарный абонентский терминал, который иногда именуется «радиорозеткой». Встречается также название — абонентский радиоблок (АРБ).

БС DECT постоянно передает сигнал, по крайней мере, по одному каналу, таким образом выступая в качестве маяка для соединения с УД. Передача может быть частью активной связи, а может быть холостой. Передача маяка БС содержит служебную информацию об идентификации БС, возможностях системы, статусе БС и пейджинговую информацию для установления входящей связи. УД, подключенные к передаче маяка, проанализируют передаваемую информацию и определят, есть ли у УД права доступа к системе (только те УД, у которых есть права доступа, могут установить связь), соответствуют ли возможности системы услугам, требующимся УД и — в том случае, если связь необходима — есть ли у БС свободная емкость для установления радиосвязи с УД.

Динамическое распределение и выбор канала

Вместо частотного планирования сети используется механизм Непрерывного Динамического Выбора и Распределения Каналов (CDCS/CDCA). Суть этого механизма заключается в том, что каналы выбираются динамически из всего набора каналов по следующим показателям: качество прохождения сигнала и уровень помех. Причём канал не закрепляется за соединением на всё время, он может меняться по мере необходимости. Происходит это следующим образом:
Каждая базовая станция DECT непрерывно сканирует все 120 частотных каналов, измеряет уровень принятого сигнала (RSSI — Received Signal Strength Indicator) (низкие значения мощности сигнала означают свободные каналы без помех, а высокие значения означают занятые каналы или каналы с помехами) и выбирает канал с минимальным уровнем помех. В этом частотном канале БС DECT излучает служебную информацию, которая, в числе прочих, содержит данные:
1) Для синхронизации телефона DECT (АРБ);
2) Об идентификаторе системы;
3) О возможности системы;
4) О свободных каналах;
5) Пейджинг.

Анализируя эту информацию, телефон DECT находит свою БС и прописывается к ней. При выходе из зоны действия одной БС DECT происходит поиск следующей. Т. о., телефон всегда приписан к той или иной БС своей или дружественной системы. Далее телефон синхронно с БС начинает непрерывно сканировать все 120 каналов и измерять силу сигнала в каждом из них. Номера каналов с наименьшими RSSI заносятся в память. Одновременно в памяти находятся не менее двух таких каналов.

При необходимости организации исходящей связи телефон направляет запрос БС DECT, к которой он в данный момент приписан, предлагая установить связь в одном из свободных, с точки зрения телефона, каналов. Если этот канал отвергается БС, то телефон предлагает следующий из списка свободных. После согласия БС на установление соединения по одному из предложенных каналов происходит обмен

сигнализационной и другой служебной информацией, а затем установление соединения и разговор.

Организация входящей связи осуществляется аналогичным образом. Радиотелефон DECT непрерывно анализирует «пейджинговое» сообщение на наличие «своего» входящего вызова. После распознавания входящего вызова он посылает запрос на установление связи в одном из свободных каналов. Таким образом, выбор канала для установления соединения происходит динамически и только по инициативе и под управлением телефонной трубки DECT. Этот механизм называется непрерывным динамическим выбором канала (CDCS).

Канал, в котором происходит разговор, не является выделенным на всё время соединения. По тем или иным причинам (например, ухудшение качества связи при перемещении трубки в зону «тени») радиотелефон может сменить его. При этом радиотелефон DECT выбирает канал из списка свободных и предлагает его БС. При согласовании с БС DECT происходит переход на новый канал. Переход может происходить и по инициативе БС. При этом она о своем желании перейти на новый канал сообщает радиотелефонной трубке, далее всё происходит так, как описано выше, т.е. выбор нового канала осуществляется радиотелефоном. Этот механизм называется непрерывным динамическим распределением каналов (CDCA).

Хендовер в DECT системе происходит мягким способом. Это значит, что во время хендовера между АРБ и системой (несколько БС) одновременно работают два канала: «старый» и «новый». В какой-то момент времени информация между АРБ и системой передается одновременно по этим двум каналам. Только после успешного перехода на «новый» канал происходит деактивация «старого». Надо отметить, что хендовер происходит не только при ухудшении качества связи или при разрыве соединения, но и в том случае, когда АРБ находит лучший с его точки зрения канал. Таким образом, для соединения всегда используется лучший свободный канал.

Механизм CDCS/CDCA существенно отличает DECT от сотовых систем связи - управление каналами осуществляется не центральным контроллером, а мобильными терминалами. Эта способность DECT позволяет сосуществовать нескольким системам в одной и той же полосе частот, при сохранении в каждой из них высокого качества и безопасности связи. Кроме того, этот механизм существенно увеличивает емкость трафика системы за счет минимизации каналов с несколькими путями распространения. Особенно это важно для помещений, где происходит многократное отражение радиосигнала от стен.

Защита систем DECT от несанкционированного доступа

Перечень штатных процедур по обеспечению безопасности в системах стандарта DECT включает в себя:

- прописку АРБ;
- аутентификацию АРБ;
- аутентификацию БС;
- взаимную аутентификацию АРБ и БС;
- аутентификацию пользователя;
- шифрование данных.

Прописка

Прописка — это процесс, благодаря которому система допускает конкретную мобильную DECT-трубку (АРБ) к обслуживанию. Оператор сети или сервис-провайдер обеспечивает пользователя секретным ключом прописки (PIN-кодом), который должен быть введен как в БС, так и в трубку до начала процедуры. До того, как трубка инициирует процедуру фактической прописки, она должна также знать идентификацию БС, в которой она должна прописаться. Время проведения процедуры обычно ограничено, и ключ прописки может быть применен только один раз, это делается специально для того, чтобы минимизировать риск несанкционированного использования. Прописка в DECT может осуществляться "по эфиру", после установления радиосвязи с двух сторон происходит верификация того, что используется один и тот же ключ прописки. Происходит обмен идентификационной информацией, и обе стороны просчитывают секретный аутентификационный ключ, который используется для аутентификации при каждом установлении связи. Секретный ключ аутентификации не передается по эфиру.

АРБ может быть прописан на нескольких БС. При каждом сеансе прописки, трубка просчитывает новый ключ аутентификации, привязанный к сети, в которую он прописывается. Новые ключи и новая информация идентификации сети добавляются к списку, хранящемуся в трубке и используемому в процессе соединения. Трубки могут подключиться только к той сети, в которую у них есть права доступа.

Аутентификация

Аутентификация АРБ позволяет предотвратить его неправомочное использование (например, с целью избежать оплаты услуг) или исключить возможность подключения похищенного или незарегистрированного АРБ. Аутентификация происходит по инициативе БС при каждой попытке установления соединения (входящего и исходящего), а также во время сеанса связи. Вначале БС формирует и передает запрос, содержащий некоторый постоянный или сравнительно редко меняющийся параметр (64 бита), и случайное число (64 бита), сгенерированное для данной сессии. Затем в БС и АРБ по одинаковым алгоритмам с использованием аутентификационного ключа вычисляется так называемый аутентификационный ответ (32 бита). Этот вычисленный (ожидаемый) ответ в БС сравнивается с принятым от АРБ, и при совпадении результатов считается, что аутентификация АРБ прошла успешно.

Аутентификация БС исключает возможность неправомочного использования станции. С помощью этой процедуры обеспечивается защита служебной информации (например, данных о пользователе), хранящейся в АРБ и обновляемой по команде с БС, также блокируется угроза перенаправления вызовов абонентов и пользовательских данных с целью их перехвата. Алгоритм аутентификации БС аналогичен последовательности действий при аутентификации АРБ.

Взаимная аутентификация может осуществляться двумя способами:

- при прямом методе последовательно проводятся две процедуры аутентификации АРБ и БС;
- косвенный метод в одном случае подразумевает комбинацию двух процедур
  - аутентификации АРБ и шифрования данных (поскольку для шифрования информации необходимо знание аутентификационного ключа),
  - шифрование данных с использованием статического ключа SCK (Static Cipher Key), известного обеим станциям.

Аутентификация пользователя позволяет выяснить, знает ли пользователь АРБ свой персональный идентификатор. Процедура инициируется БС в начале вызова и может быть активизирована во время сеанса связи. После того, как пользователь вручную наберет свой персональный идентификатор UPI (User Personal Identity), и в АРБ с его помощью будет вычислен аутентификационный ключ, происходит процедура, аналогичная последовательности действий при аутентификации АРБ.

Аутентификационный ключ.
Во всех описанных процедурах аутентификационный ответ вычисляется по аутентификационному запросу и ключу аутентификации в соответствии со стандартным алгоритмом (DSAA – DECT Standard Authentication Algorithm). Алгоритм DSAA является конфиденциальной информацией и поставляется по контракту с ETSI (The European Telecommunications Standards Institute). Использование другого алгоритма ограничивает возможности абонентских станций из-за трудностей при роуминге в сетях общего пользования DECT.

Аутентификационный ключ является производной от одной из трех величин или их комбинаций, приведенных ниже.

1. Абонентский аутентификационный ключ UAK (User Authentication Key) длиной до 128 бит. UAK является уникальной величиной, содержащейся в регистрационных данных пользователя. Он хранится в ПЗУ абонентской станции или в карточке DAM (DECT Authentication Module).
2. Аутентификационный код AC (Authentication Code) длиной 16-32 бита. Он может храниться в ПЗУ абонентской станции или вводиться вручную, когда это требуется для проведения процедуры аутентификации. Необходимо отметить, что нет принципиальной разницы между параметрами UAK и AC. Последний обычно используется в тех случаях, когда требуется довольно частая смена аутентификационного ключа.
3. Персональный идентификатор пользователя UPI (User Personal Identity) длиной 16-32 бита. UPI не записывается в устройства памяти абонентской станции, а вводится вручную, когда это требуется для проведения процедуры аутентификации. Идентификатор UPI всегда используется вместе с ключом UAK.

Шифрование данных обеспечивает криптографическую защиту пользовательских данных и управляющей информации, передаваемых по радиоканалам между БС и АРБ. В АРБ и БС используется общий ключ шифрования CK (Cipher Key), на основе которого формируется шифрующая последовательность KSS (Key Stream Segments), накладываемая на поток данных на передающей стороне и снимаемая на приемной.

KSS вычисляется в соответствии со стандартным алгоритмом шифрования DCS (DECT Standard Cipher) или любым другим алгоритмом, отвечающим требованиям криптографической стойкости. Алгоритм DSC является конфиденциальной информацией и поставляется по контракту с ETSI.

В зависимости от условий применения систем DECT могут использоваться ключи шифрования двух типов:

- вычисляемый – DCK (Derivation Cipher Key);
- статический – SCK (Static Cipher Key).

Статические ключи SCK вводятся вручную абонентом, а вычисляемые DCK обновляются в начале каждой процедуры аутентификации и являются производной от аутентификационного ключа. В ПЗУ абонентской станции может храниться до 8 ключей.

Статический ключ обычно используется в домашних системах связи. В этом случае SCK является уникальным для каждой пары "абонентская /базовая станция", формирующей домашнюю систему связи. Рекомендуется менять SCK один раз в 31 день (период повторения номеров кадров), иначе риск раскрытия информации существенно возрастает.

Организация протоколов DECT

Архитектура протоколов DECT включает:

- физический уровень (PHL Layer);
- уровень доступа к среде (MAC Layer);
- уровень управления звеном передачи данных (DLC layer);
- сетевой уровень (NWK. layer);
- прикладные уровни (Application profiles).

Физический уровень обеспечивает среду для связи АРБ с БС и описан в стандарте ETS 300 174-2 и он определяет параметры радиотракта DECT (см. выше). Именно PHL уровень отвечает за механизм MC/TDMA/TDD.

Для обеспечения передачи данных до 2Мбит/с базовый стандарт ETS 300 175 был дополнен методом высокоскоростной передачи на основе фазовой модуляции. Используются две схемы модуляции: 4-уровневая (π/4-DQPSK) и 8-уровневая (π/8—D8PSK). Высокоуровневая модуляция (4-х и 8-ми уровневая) используется только для модуляции информационного канала (информация или данные пользователя), а для модуляции каналов синхронизации и управления используется частотная манипуляция. Таким образом, обеспечивается совместимость новых систем с высокоуровневой модуляцией с существующими системами.

Каждый таймслот содержит защитный интервал длительностью 25мкс, 32 бита синхронизации, 64 бита управления и биты данных (информация). Поскольку биты синхронизации присутствуют в каждом физическом канале, синхронизация может проводиться перед каждым физическим каналом. Биты управления и данных

образуют 2 логических канала соответственно для управления и передачи пользовательских данных (как и в ISDN).

Уровень доступа к среде (MAC Layer) отвечает за установление радиоканала между АРБ и БС и основными функциями этого уровня являются:
- установление соединений;
- обеспечение сигнализации;
- управление хендовером.

Именно MAC уровень отвечает за "мягкий" хендовер и механизм CDCS/CDCA. Кроме того, MAC уровень обеспечивает канал для передачи пейджинговой информации и сигнализации.

Уровень управления звеном передачи данных (DLC layer) отвечает за надежную передачу управляющей информации по физическому каналу. На этом уровне решаются задачи по:
- защите передаваемых данных от ошибок;
- управлению качеством физического соединения;
- управлению процедурой выбора канала на MAC-уровне.

На уровнях MAC и DLC используются так называемые протокольные блоки данных, состоящие из:
- заголовка;
- поля данных MAC уровня;
- поля данных DLC уровня;
- циклического проверочного кода (CRC).

Заголовок сообщения определяет тип сообщения и тип DECT системы (домашняя, офисная или общего пользования). Кроме того, передается идентификатор системы, информация о поддерживаемых функциях системы и пейджинговая информация.

Сетевой уровень (NWK Layer) отвечает за сигнализацию и осуществляет:
- управление уровнями MAC и DLC;
- управление вызовами;
- управление мобильностью (внешний хендовер, роуминг и т.д.);
- передачу информации с/без установления соединения;
- обеспечение ДВО.

Для обеспечения внутреннего хендовера не требуется участие третьего уровня, т.к. этот процесс отрабатывает второй уровень. В этом заключается основное (принципиальное) отличие технологии DECT от GSM.

Прикладные уровни (Application profiles) содержат дополнительные спецификации протокольного стека о способах применения эфирного интерфейса в конкретной системе радиосвязи и назначаются следующими основными профилями DECT определенными ETSI с целью обеспечения возможности реализации широкого спектра услуг при обеспечении максимальной совместимости оборудования разных производителей:
- GAP (Generic Access Profile);
- CAP (CTM Access Profile);

- IAP и IIP (DECT/ISDN Interworking profiles);
- GIP (DECT/GSM Interworking Profile);
- DSP (Data Service Profile);
- RAP (Radio Local Loop Access Profile);
- DMAP (DECT Multimedia Access Profile);
- DPRS (DECT Packet Radio Services).

GAP определен, как основной профиль доступа для приложений DECT (и единственный для домашних и офисных систем). GAP является главным профилем доступа DECT, предназначенным для использования в системах, поддерживающих телефонные услуги независимо от типа присоединенной сети. Он определяет минимум необходимых требований к АРБ и БС, которые обеспечивают их совместимость. В GAP определены процедуры для установления и завершения входящих и исходящих соединений, для поддержания мобильности, включая роуминг.

Стандарт DECT определяет технологию радиодоступа, обеспечивающую мобильность, поэтому сама радиотехнология DECT может быть использована для доступа в любые сети.

GIP описывает способ подключения сетей DECT к сети GSM. Такой доступ обеспечивается интерфейсом типа А сети GSM (к MSC). При этом сеть GSM воспринимает DECT как систему базовых станций (BSC) и этот профиль обеспечивает два преимущества.

1. Появилась возможность строительства мобильных сетей DECT на основе наземной инфраструктуры сетей GSM. При этом существенно снижаются затраты на создание инфраструктуры сети DECT поскольку сети GSM имеют практически глобальное распространение и постоянно увеличивают охват территорий.
2. Для операторов сети GSM появилась возможность использования дуальных мобильных терминалов GSM/DECT для увеличения трафика, так как сети DECT в отличие от GSM поддерживают очень высокую плотность трафика. Сети, построенные на основе DECT и GSM, обладают такими качествами, как высокая плотность трафика для малоподвижных абонентов в местах наибольшего скопления абонентов за счет подсистемы базовых станций DECT, большая площадь радиопокрытия и высокая мобильность за счет подсистемы базовых станций GSM.

Кроме этого есть и другой способ взаимодействия сетей GSM и DECT через ISDN сети. Этот подход основан на протоколе DSS1+, являющимся расширением протокола DSS1 и определен профилями IAP и IIP. Оба профиля поддерживают одинаковый набор услуг. Основное отличие между ними заключается в способе соединения.

Первый из них ориентирован на доступ к услугам сети ISDN посредством стандартного терминала DECT - при этом со стороны сети ISDN терминал DECT виден как обычный терминал ISDN с соответствующими возможностями. Преимущества профиля IAP заключаются в том, что для получения услуг ISDN используется только один трафиковый канал DECT. Информационный канал ISDN (B канал) шириной 64 кБит/с передается в канал «данных пользователя» DECT (рис. 1)

путем преобразования кодирования PCM в ADPCM. Очевидно, что этот профиль может обслуживать только речевые терминалы.

Второй профиль IIP называется профилем промежуточной системы и используется для подключения стандартного терминала ISDN к сети ISDN посредством радиоинтерфейса DECT. При этом появляется возможность подключения и терминалов передачи данных на скорости до 64 кбит/с. Недостатком этого профиля является неэффективное использование радиоспектра. Для организации информационного канала используются два трафиковых канала DECT. Кроме того, для отображения канала сигнализации (D канала ISDN) выделяется еще один канал. Таким образом, для одного соединения используются 3 трафиковых канала DECT.

В рамках этого профиля возможна организация стандартной канальной структуры 2B+D базового доступа ISDN-BRI путем выделения 5 трафиковых каналов DECT. При этом DECT обеспечивает стандартное сетевое окончание ISDN с интерфейсом S. Преимуществом данного профиля является возможность использования любого стандартного терминала ISDN, в том числе и терминалов передачи данных.

Для систем абонентского радиодоступа (WLL) на основе DECT разработан профиль RAP, который определяет протоколы и возможность предоставления услуг ЦСИО конечным пользователям. RAP определяет два типа сервиса:

- базовые телефонные услуги, включая ПД с помощью модемов на скоростях вплоть до V.34;
- широкополосные услуги, включая ISDN и ПД с коммутацией пакетов.

Услуги предоставляются через стандартный АРБ DECT, аналогично ISDN.

В связи с тем, что WLL на основе DECT распространен в мире, в ETSI рассмотрен вопрос о расширении возможностей стандарта DECT для удаленных терминалов (более 5км). Реализован механизм "усовершенствованной схемы синхронизации", обеспечивающий связь на расстояниях до 16км при сохранении совместимости с существующими системами.

При строительстве сетей доступа на основе DECT определен профиль доступа в сети мобильных терминалов (CTM). CTM обеспечивает роуминг терминалов между сетями DECT в местах, где обеспечивается радиопокрытие DECT системой (домашней, офисной или общего пользования), беспроводный телефон может обслуживать как входящие, так и исходящие вызовы. При этом мобильный терминал регистрируется только в одной системе с одним телефонным номером. Таким образом, обеспечивается связь в любом месте, где присутствует DECT. Причем для терминала во всех сетях сохраняется один и тот же сетевой номер и входящие звонки не теряются.

Основное отличие CAP от GIP заключается в том, что CTM обеспечивает мобильность не только в пределах сети GSM, но может взаимодействовать с любой сетью, поддерживающей мобильность. Примерами таких сетей являются сети ISDN с расширением поддержки мобильности (протокол DSSI+) и сети ОКС-7 (INAP и MAP). Профиль CAP является надмножеством GAP, и это обеспечивает совместимость с GAP терминалами, т.е. сохраняется преемственность между GAP и CAP.

Интеграция DECT с сетями передачи данных (СПД) обеспечена рядом профилей передачи данных DSP, отличающихся по предоставляемым услугам и степени мобильности. По степени мобильности профили подразделяются на два класса:

- без поддержки мобильности в пределах одной БС;
- с поддержкой мобильности в частных сетях и сетях общего пользования.

По услугам СПД профили передачи данных делятся на 6 типов:

- низкоскоростная ПД с frame relay (до 24,6кБит/с);
- высокоскоростная ПД с frame relay (до 552кБит/с, в ETS-300-175 -до 2МБит/с);
- передача данных на основе коммутации пакетов;
- прозрачная передача данных;
- передача коротких сообщений с/без подтверждения;
- услуги телесервиса (например, FAX).

Мультимедийный профиль DMAP разработан для организации беспроводного доступа в сети Internet через ISDN сети и поддержания речевых терминалов и терминалов ПД DECT. Поэтому базируется DMAP на протоколах ISDN, GAP и DSP. Этот профиль тесно связан с компьютерами, в частности ноутбуками. Потому для обеспечения совместимости и упрощения доступа в терминале эмулируется клиент CAPI, а в базовой станции — сервер CAPI.

Профиль DPRS создал основу для сопряжения всех услуг беспроводной пакетной передачи данных, которые предоставляются через интерфейс DECT, независимо от того, в каком приложении (домашний сектор, домашний офис, малый офис, корпоративный сектор, системы общего пользования) он используется.

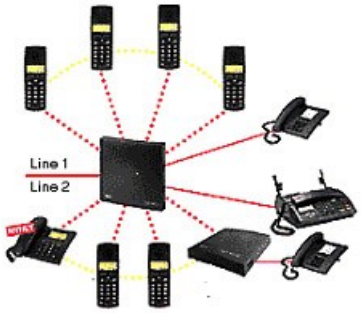
Виды сетей DECT

Системы DECT различаются по размерам и количеству подключаемых абонентских устройств. Основными являются:

- ***Домашние многотерминальные системы (Home)*** — односотовые системы домашнего использования, подключаемые непосредственно к ТфОП, с ограниченным количеством абонентских трубок.
- ***Бизнес-системы (Business)*** применяются для построения беспроводных офисных и учрежденческих сетей связи, как правило, с использованием одного контроллера и нескольких базовых станций.
- ***Системы уровня предприятия (Enterprise)*** используются для построения территориально-распределенных корпоративных сетей связи и обеспечивают беспроводную связь для большого количества абонентов на ограниченной территории.
- ***Микросотовые системы общего пользования (Cordless Terminal Mobility — CTM)*** позволяют обслуживать большое количество мобильных абонентов, перемещающихся с небольшой скоростью (до 30 км/ч).
- ***Системы фиксированного абонентского радиодоступа (Wireless Local Loop — WLL, Radio Local Loop — RLL)*** используются для быстрого беспроводного подключения абонента или группы абонентов к ТфОП в местах, где не развиты

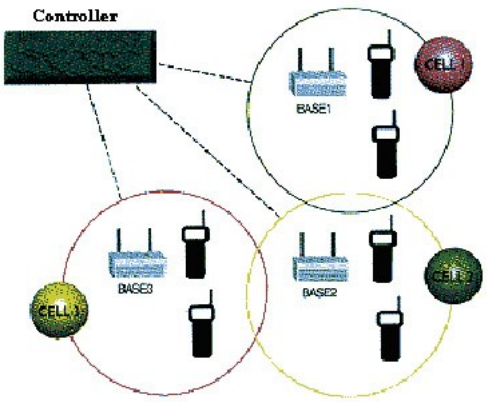
кабельные линии связи, или в местах с малой плотностью абонентов, когда прокладка кабелей экономически нецелесообразна или физически невозможна.

Классическая Home System состоит из одного базового блока, подключаемого обычно через обыкновенную аналоговую линию (1 или 2 линии).

	Устанавливается обычно в частных квартирах. Доступно к подключению до 8–10 мобильных трубок. Обеспечивают в рамках одной базы 2 соединения между 2 трубками и 1 соединение между одной трубкой и аналоговой линией одновременно. Имеют расширенный сервис, такой как автоответчик или АОН. Часто интегрируется с факсимильным аппаратом. Примеры такой системы: Siemens Gigaset и Goodwin Lund.

Подобные системы выпускают также LG и Sagem. Все эти системы объединяет одно неприятное свойство — Home System не поддерживают хэндовер (handover) — способность системы "передавать" мобильного абонента из БС в БС и способность мобильной трубки переключиться из БС в БС при ухудшении сигнала. Также существующая способность DECT-трубок регистрироваться во многих системах это функция, отличная от хэндовера.

Стандартная Business System состоит из одного DECT контроллера (часто контроллер интегрирован в УАТС) и достаточно большого количества БС.



БС подключаются к контроллеру по разным протоколам и разным линиям. Например, компания Matra Telecom подключает свои БС по ISDN-BRI со скорость 128 кбит/с, что с учетом 32 kbps кодирование ADPCM G.726 обеспечивает четыре речевых канала. Компания DeTeWe подключает базовые станции по своему собственному протоколу, аналогичному ISDN-BRI. К БС возможно подключить до 2 таких линий, обеспечивающих в сумме 8 одновременных соединений на базу.

Компания Philips разработала 6 и 12 канальные базы, подключающиеся к контроллеру по 2 Mbps G.703. Максимальное удаление БС от контроллера определяется характеристиками интерфейса соединительной линии и может быть от 1,7 км до 5 км в зависимости от производителя. Способы электропитания также отличаются: где-то оно подается дистанционно, а где-то — от отдельного источника.

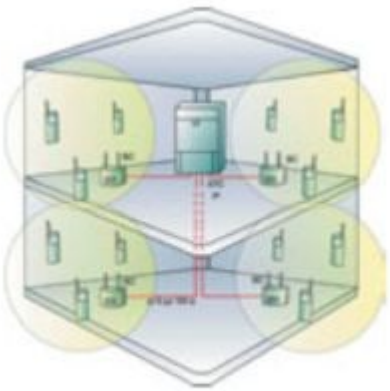


Рис. 1. Типовая схема организации учрежденческой сети связи

Enterprise System отличается от варианта Business наличием *роуминга — способности системы передавать вызов в другую систему и присваивать класс обслуживания роуминговому абоненту*.

Классификация DECT-систем по типу интеграции с опорной АТС

Типы интеграции DECT контроллеров с опорной АТС различаются по типу стыка с АТС (цифровой или аналоговый канал), по типу интеграции (внешний или интегрированный в АТС контроллер) и по способности коммутировать вызовы.

Основные проблемы, возникающие в разных вариантах интеграции:

1. *Контроллеры, стыкующиеся с АТС по аналоговым линиям*, обеспечивают DECT абоненту сервис аналогового аппарата, но исключают такие сервисы, как отображение фамилий и прочей доп. информации на дисплее. Подобные системы слабо расширяемы и роуминга не имеют.
2. *Контроллеры, стыкующиеся с АТС по цифровым линиям, но являющиеся по сути своей радиоудлинителями*, обеспечивают абоненту в случае удачной интеграции весь сервис современной цифровой АТС. Каждый абонент имеет свой класс обслуживания и т. д. Однако такие системы очень недешевы, и, как правило, для полноценной интеграции требуют покупки всей линейки оборудования у одного поставщика, из-за чего теряется выгода в использовании открытой технологии, которой и является DECT. Плюсом подобных систем является огромная расширяемость системы. Примером может служить Definity Dect R2 (Avaya Comm.). Эта система расширяется до 16320 DECT абонентов и поддерживает роуминг начиная с ПО v.8.4. Минусом является проблемность в стыке со сторонними АТС.
3. *Внешние микросотовые системы, умеющие самостоятельно коммутировать каналы* — достаточно дешевы, хорошо расширяемы, достаточно мобильны, но у них имеется недостаток, заключающийся в том, что эта система и является отдельной системой. Максимальный сервис — это базовый вызов и, при условии использования сигнализаций типа ISDN QSIG, AutoCallBack. Основные функции, использующиеся в современной АТС, будут недоступны абоненту микросотовой системы DECT. Класс обслуживания на всю систему будет один.

4. Наилучшим решением являются *встроенные в АТС контроллеры*. В этом случае DECT абонент получает максимально доступный сервис, сравнимый с сервисом системных телефонов. Минусом является незначительная масштабируемость и относительная дороговизна. Плюсами является наличие роуминга, реализующегося средствами АТС по межстанционным каналам. Также, в таких системах затруднен мониторинг подсистемы DECT. Такие системы выпускала компания Intracom в рамках высоконадежной универсальной системы связи iAS-W. Такие системы предлагались как для гражданского применения, так и для военного. В частности, в войсках НАТО (в основном США) iAS использовалось для быстрого развертывания связи на военных базах. Гражданское применение этих систем реализовано в США и Канаде для обеспечения связью фермерских хозяйств.

Источники:

1. DECT. https://ru.wikipedia.org
2. Описание стандарта DECT. http://www.abc-tel.ru
3. Обзор стандарта DECT. http://1234g.ru
4. Стандарт DECT: обзор оборудования / Ю.В. Радионова, А.В. Власов // Технологии и средства связи. http://www.tssonline.ru
5. Основные принципы работы систем стандарта DECT. http://www.t-service.ru
6. MSK сигналы с гауссовой огибающей (GMSK). http://www.dsplib.ru
7. Модуляция GMSK в современных системах радиосвязи / В. Голуб. http://www.chipinfo.ru

Беспроводные системы ПД

Лекция 05
Технология LoRa и сеть LoraWAN

LoRa (Long Range) — радиотехнология и одноимённый метод модуляции, разработанные и запатентованные компанией Semtech.

Технология LoRa и построенная на ее основе сеть LoraWAN были представлены широкой публике в 2015 году компанией Semtech и исследовательским центром IBM Research. Также на Всемирном мобильном конгрессе MWC 2015 в Барселоне было заявлено о создании консорциума LoRa Aliance, в который вошли Semtech, IBM, Cisco и многие другие компании. На сегодня в консорциум входят более 500 компаний производителей электроники и операторов связи. В частности в консорциум входят оператор МТТ и инженерная компания «Россма».

LoRa основывается на модуляции с расширением спектра (коэффициент расширения от 6 до 12, обычно используется от 7 до 12) и вариации линейной частотной модуляции (ЛЧМ, Chirp Spread Spectrum, CSS) с интегрированной прямой коррекцией ошибок. ЛЧМ — это вид частотной модуляции, при которой частота несущего сигнала изменяется по линейному закону с использованием т. н. чирплет-преобразования. LoRa значительно повышает чувствительность приемника и, аналогично другим методам модуляции с расширенным спектром, использует всю ширину полосы пропускания канала для передачи сигнала, что делает его устойчивым к канальным шумам и нечувствительным к смещениям, вызванным неточностями в настройке частот при использовании недорогих опорных кварцевых резонаторов. Считается, что технология LoRa позволяет осуществлять демодуляцию сигналов с уровнями на 19,5 дБ ниже уровня шумов.

LoRa является именно технологией радиопередачи. Она обеспечивает физический уровень, поверх которого можно строить радиосети различного типа.

Зона покрытия сети LoRa определяется радиусом действия базовых станций (шлюзов LoRa) до 2,5 км внутри города и до 15 км в сельской местности. Дальность работы приемопередатчиков сильно зависит от типа и размещения антенн.

Для работы LoRa, как правило, использует нелицензируемые частоные диапазоны, которые определены согласно региональным ограничениям:

- 430 МГц – Азия;
- 780 МГц – Китай;
- 433 МГц – Европа;
- 866 МГц – Европа;
- 915 МГц – США.

В России для LoRa выделен диапазон 864–870 МГц. Это согласуется с решением Государственной комиссии по радиочастотам от 07.05.2007 №07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия», согласно которому разрешенный

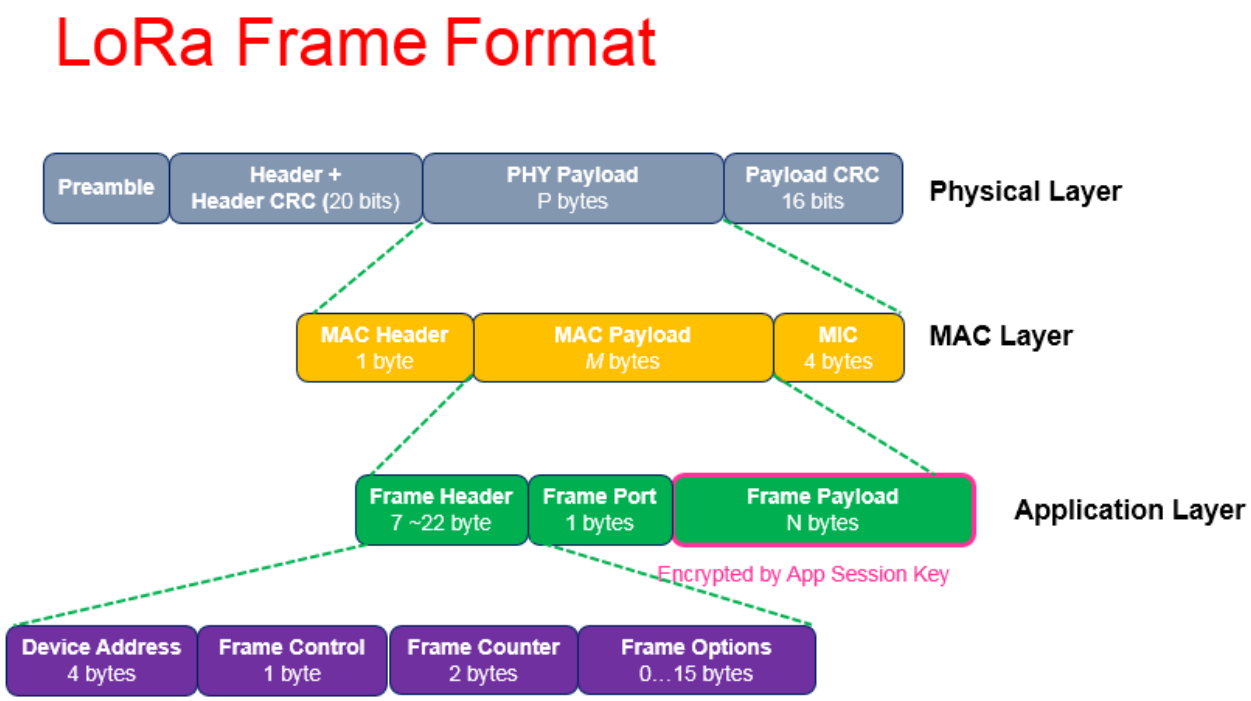
частотный диапазон для работы по протоколу LoRaWAN (а также LPWAN и по другим протоколам) состоит из двух разрешенных поддиапазонов: 864–865 МГц и 868,7–869,2 МГц.

Также можно использовать LPD диапазон 433,05–434,79 МГц. Но в нём присутствует значительная помеховая обстановка.

Как правило используются каналы с шириной полосы **125**, 250 и 500 кГц. Допускается использование более узких каналов (7.8, 10.4, 15.6, 20.8, 31.2, 41.7, 62.5 кГц). Скорость передачи от 250 бит/с до 50 кбит/с. Таким образом технология является низкоскоростной.

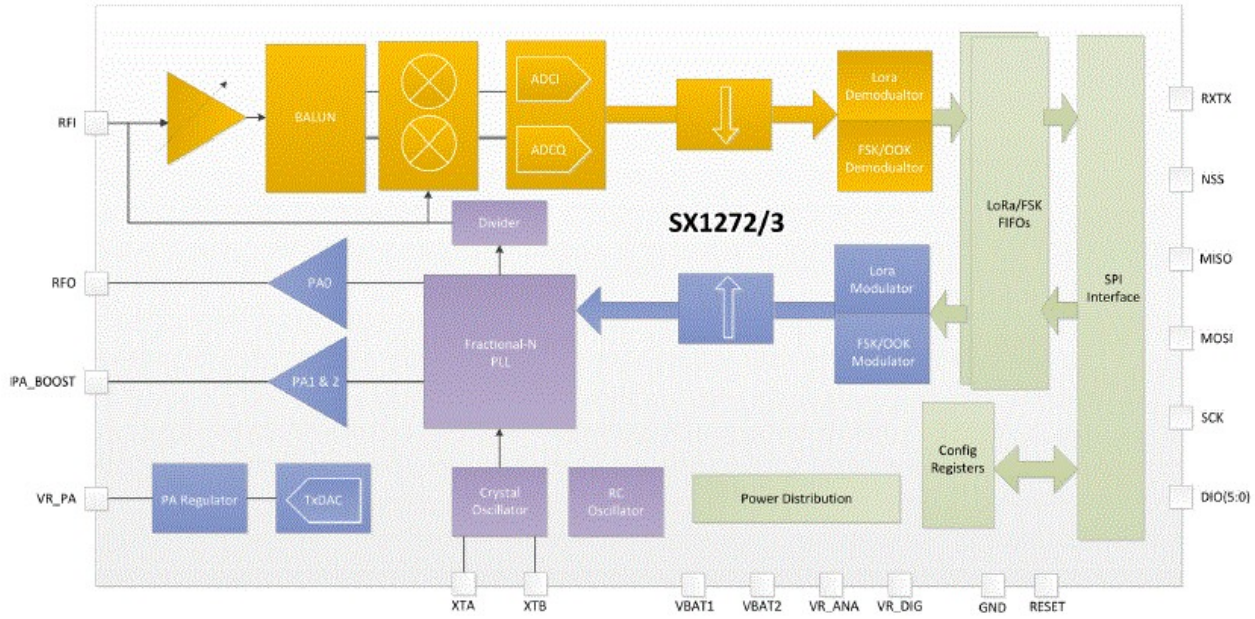
В связи с большой дальностью работы и низкой скоростью LoRa как правило используется для сенсорных радиосетей и систем обмена короткими сообщениями.

Максимальный размер пакета данных для передачи равен 256 байт. Однако, рекомендуется использовать более короткие пакеты. Это позволяет обеспечить лучшую помехоустойчивость при передаче.



Формат кадра LoRa

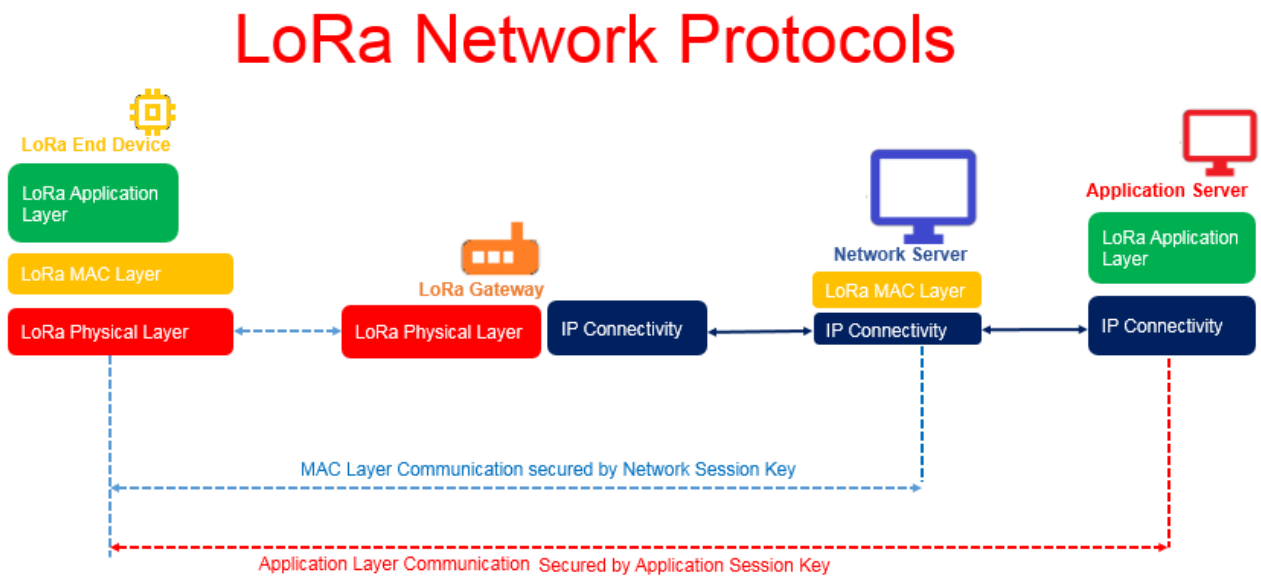
Оборудование LoRa делают компании Semtech Corp., Ingenu, Sensus, Microchip, Silicon Labs и Kerlink. Для оконечных устройств наиболее популярны чипы SX126x и SX127x от компании Semtech (SX1261, SX1272, SX1276, SX1278 и др.). Для базовых станций используются модули SX1301 и SX1257.



Блок-схема чипа SX1272

Сеть и протокол LoraWAN

Сеть и одноименный протокол LoraWAN позволяют сформировать беспроводную сеть передачи данных для обмена информацией между оконечными узлами LoRa и клиентскими приложениями.



Взаимодействие в сети LoraWAN

Типичная сеть LoRaWAN состоит из следующих элементов:

1. **Конечный узел (End Node/Device)** предназначен для осуществления управляющих или измерительных функций. Он содержит набор необходимых датчиков и управляющих элементов.
2. **Шлюз LoRa (Gateway/Concentrator)** — устройство, принимающее данные от конечных устройств с помощью радиоканала и передающее их в транзитную сеть. В качестве такой сети могут выступать Ethernet, WiFi, сотовые сети и любые другие

телекоммуникационные каналы. Шлюз и конечные устройства образуют сетевую топологию типа звезда. *Обычно данное устройство содержит многоканальные приёмопередатчики для обработки сигналов в нескольких каналах одновременно или нескольких сигналов в одном канале — частотное, временное и кодовое разделения.* Соответственно, несколько таких устройств обеспечивает зону покрытия сети и прозрачную двунаправленную передачу данных между конечными узлами и сервером.

3. **Сетевой сервер (Network Server)** предназначен для управления сетью: заданием расписания, адаптацией скорости, хранением и обработкой принимаемых данных.
4. **Сервер приложений (Application Server)** может удаленно контролировать работу конечных узлов и собирать необходимые данные с них.

Для решения различных задач и применений в сети LoRaWAN предусмотрено три класса устройств:

1. **Двунаправленные конечные устройства «класса А» (Bi-directional end-devices, Class A).** Устройства этого класса применяются, когда необходима минимальная потребляемая мощность при преобладании передачи данных к серверу. В качестве инициатора сеанса связи выступает конечный узел, отправляя пакет с необходимыми данными, а затем выделяет два окна, в течении которых ждёт данных от сервера. Таким образом, передача данных от сервера возможна только после выхода на связь конечного устройства.
2. **Двунаправленные конечные устройства «класса Б» (Bi-directional end-devices, Class B).** Основное отличие от устройств «класса А» заключается в выделении дополнительного окна приёма, которое устройство открывает по расписанию. Для составления расписания конечное устройство осуществляет синхронизацию по специальному сигналу от шлюза. Благодаря этому дополнительному окну сервер имеет возможность начать передачу данных в заранее известное время.
3. **Двунаправленные конечные устройства «класса С» с максимальным приемным окном (Bi-directional end-devices, Class C).** Устройства этого класса имеют почти непрерывное окно приёма данных и закрывает его лишь на время передачи данных, что позволяет их применять для решения задач, требующих получения большого объёма данных.

Источники:

1. Semtech LoRa Technology Overview / Semtech // Сайт компании Semtech. URL: https://www.semtech.com/lora
2. Материалы с сайта https://lora-alliance.org/
3. IBM и Semtech представили новую сетевую технологию LoRaWAN для M2M-коммуникаций / IBM // Habr. URL: https://habr.com/ru/company/ibm/blog/254827/
4. Технология LoRa / RealTrac Technologies // Habr. URL: https://habr.com/ru/company/realtrac/blog/304312/
5. Технология LoRa в вопросах и ответах / К. Верхулевский // Беспроводные технологии. №1. 2016.
6. Технология LoRa: перспективы внедрения на сетях IoT / В.Тихвинский, В.Коваль, Г.Бочечка // Первая миля. №6. 2016.
7. Материалы с сайта Lo-Ra.ru

8. Материалы с сайта IoT.ru
9. Known and Unknown Facts of LoRa: Experiences from a Large Scale Measurement Study / J. C. Liando and others // ACM Trans. Sensor Netw. Article 19. 2018.
10. Modeling the energy performance of LoRaWAN / L. Casals and others // Sensors. Vol. 17. 2017.
11. Материалы с сайта Codeplayon.com

Беспроводные системы ПД

Лекция 06

Протокол ZigBee

ZigBee® — это открытый стандарт беспроводной связи для систем сбора данных и управления. Технология ZigBee позволяет создавать самоорганизующиеся и самовосстанавливающиеся беспроводные сети с автоматической ретрансляцией сообщений, с поддержкой батарейных и мобильных узлов. Базируется на беспроводном стандарте IEEE 802.15.4. Технология относится к беспроводным персональным вычислительным сетям (WPAN).

Спецификация ZigBee ориентирована на приложения, требующие гарантированной безопасной передачи данных при относительно небольших скоростях и возможности длительной работы сетевых устройств от автономных источников питания (батарей).

У истоков протокола стоит организация **ZigBee Alliance**, основанная в 2002 и включающая в себя более 300 компаний. Альянс отвечает за развитие и продвижение стандарта, а также за сертификацию оборудования. Спецификация ZigBee 1.0 была ратифицирована 14 декабря 2004 и доступна для членов альянса ZigBee. Через год спецификации первой версии протокола были утверждены, и он стал внедряться в конечные устройства. Сейчас первый вариант спецификации известен под названием ZigBee 2004. Второй выпуск стека называется ZigBee 2006. 30 октября 2007 г., была размещена спецификация ZigBee 2007, обеспечивающая полную совместимость с устройствами ZigBee 2006. В ZigBee 2007 разработчики представили сразу две реализации стандарта: простую ZigBee и продвинутую ZigBee Pro (ZigBee Pro Feature Set). Большинство современных устройств для автоматизации дома базируется именно на Pro-версии от 2007 года.

Протокол ZigBee имеет ряд ответвлений: в 2009 году был представлен стандарт ZigBee RF4CE (Radio Frequency for Consumer Electronics), а позднее появилась спецификация ZigBee IP, предназначенная для использования IPv6 в сенсорных сетях. Она позволяет развернуть сеть 6LoWPAN поверх маломощных устройств с поддержкой IEEE 802.15.4.

Большое количество версий протокола вкупе с тем, что производством коммуникационных чипов с поддержкой ZigBee занимается множество компаний, каждая из которых интерпретирует спецификации по-своему, а также вносит определенные оптимизации в работу протокола, приводит к проблемам с совместимостью. В литературе указывается, что оборудование разных стандартов в рамках одной сети лучше не использовать, и вероятность того, что устройства от разных производителей откажутся работать друг с другом, весьма велика.

Программный интерфейс ZigBee

Для интерфейса ZigBee нет единого для всех платформ прикладного протокола API. Сделано это намеренно, чтобы предоставить совершенствование протоколов API производителю платформы. Для разработчика это означает, что при переходе на другую платформу необходимо вносить поправки в программное обеспечение. Чтобы упростить эту задачу, рекомендуется выполнять часть кода, отвечающую за обмен со стеком, на отдельном МК.

В стандарте прописаны только функции ZigBee. Команды, вызывающие ту или иную функцию, имеют разную структуру в зависимости от используемой платформы. Например, команда передачи данных APSDE-DATA.request на оборудовании Freescale вызывается инструкцией AF_DataRequest(), а на платформе Ember — инструкцией emberSendDatagram(). Хотя обе функции называются по-разному и имеют неодинаковый набор аргументов, они производят одно и то же действие — передачу октета.

Сеть ZigBee не может сама определить тип оборудования того или иного узла, разработчику приходится догадываться об этом по косвенным признакам и особенностям поведения устройства. Оборудование с меткой ZigBee-certified является полностью совместимым, вне зависимости от производителя.

Применение

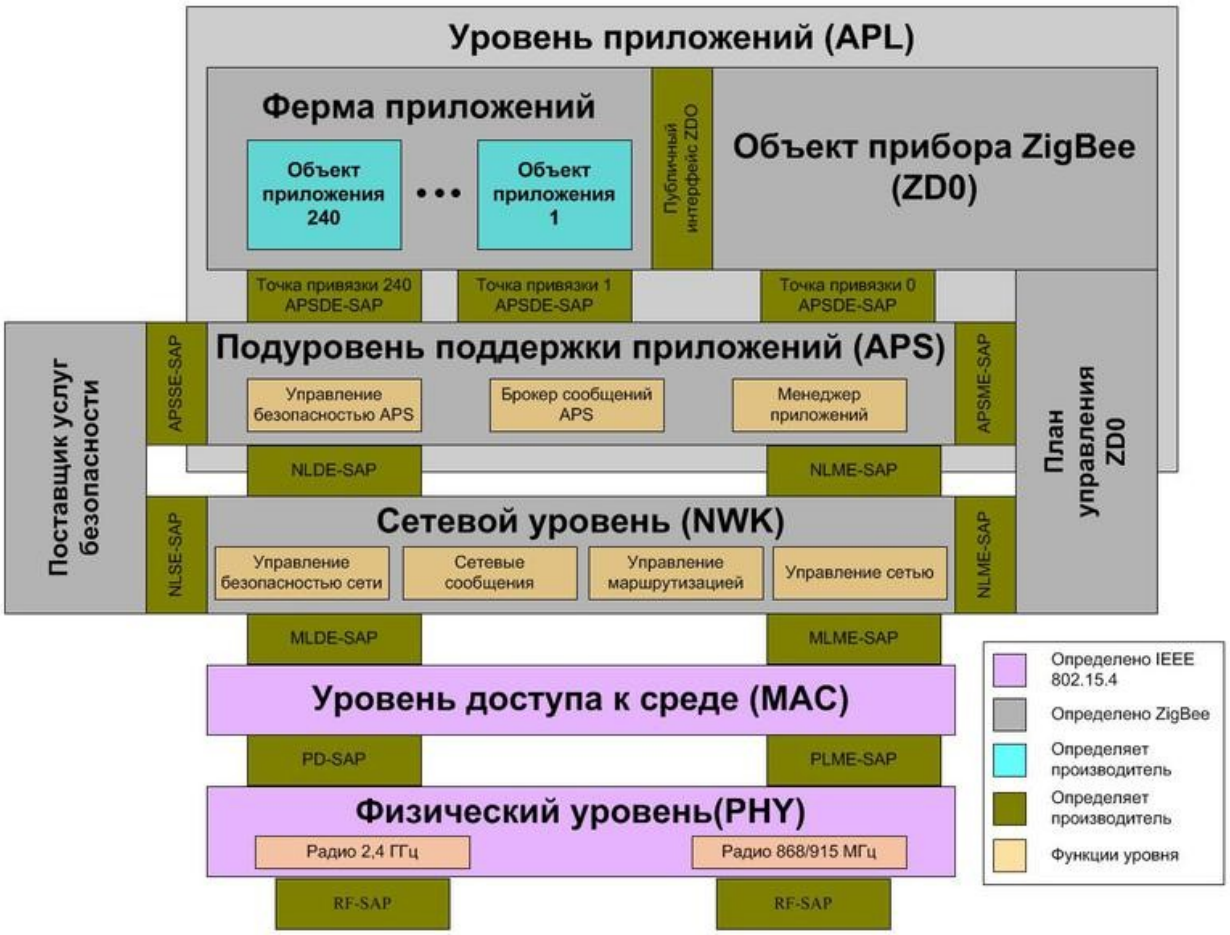
Протоколы ZigBee разработаны для использования во встроенных приложениях, требующих низкую скорость передачи данных и низкое энергопотребление. Цель ZigBee — это создание недорогой, самоорганизующейся сети с ячеистой топологией предназначенной для решения широкого круга задач. Сеть может использоваться в промышленном контроле, встроенных датчиках, сборе медицинских данных, оповещении о вторжении или задымлении, строительной и домашней автоматизации и т. д. Созданная в итоге сеть потребляет очень мало энергии — индивидуальные устройства согласно данным сертификации ZigBee позволяют энергобатареям работать два года.

Типовые области применения:

- Домашние развлечения и контроль — рациональное освещение, продвинутый температурный контроль, охрана и безопасность, фильмы и музыка.
- Домашнее оповещение — датчики воды и энергии, мониторинг энергии, датчики задымления и пожара, рациональные датчики доступа и переговоров.
- Мобильные службы — мобильные оплата, мониторинг и контроль, охрана и контроль доступа, охрана здоровья и телепомощь.
- Коммерческое строительство — мониторинг энергии, HVAC (Heating, Ventilation, & Air Conditioning – Отопление, вентиляция и кондиционирование – ОВК), света, контроль доступа.
- Промышленное оборудование — контроль процессов, промышленных устройств, управление энергией и имуществом.

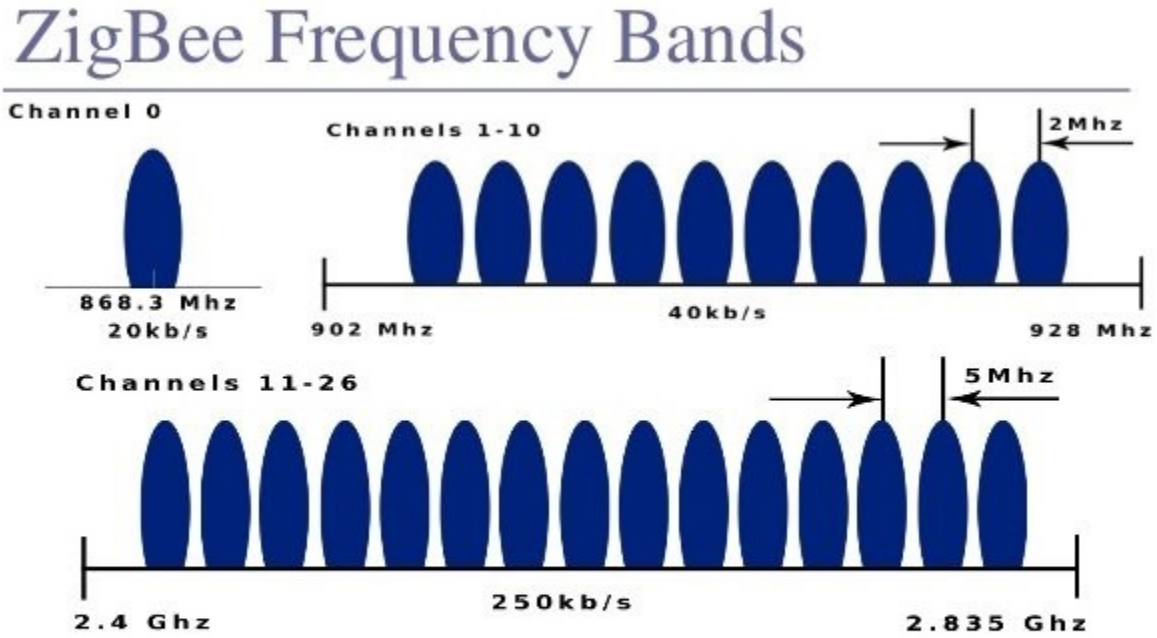
Сетевые протоколы

Протоколы, регламентированные стандартами IEEE 802.15.4 и ZigBee 2007 Specification, обеспечивают формирование и функционирование беспроводной сенсорной сети.
Стандарт IEEE 802.15.4 определяет физический и MAC уровни, а спецификация ZigBee определяет сетевой уровень и уровень приложений. На рисунке показан стек протоколов ZigBee.



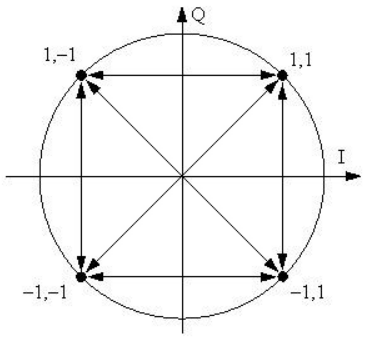
Используемые частоты

Передача данных в рамках сети осуществляется по радиоканалу. Используемые частоты зависят от региона: для Европы выбрано значение 868 МГц, для США и ряда других стран — 915 МГц. Кроме того, стандарт предусматривает работу на частоте 2,4 ГГц — она не имеет привязки к географическому положению. При этом, подобное обилие вариантов мало сказывается на вопросах совместимости: по факту, практически все ZigBee-оборудование использует частоту 2,4 ГГц. Этот вариант обеспечивает наибольшую пропускную способность — в теории, она может достигать значения в 250 Кбит/с. Дальность передачи сигнала внутри помещения составляет 10–20 метров.



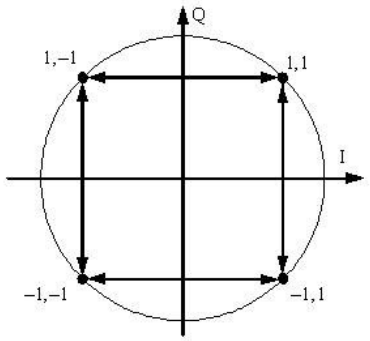
PHY (MHz)	Frequency Band (MHz)	Modulation	Bit Rate	Number of Channels
868 / 915	868-868.6	BPSK	20	1
	902-928	BPSK	40	10
2450	2400-2483.5	O-QPSK	230	16

ZigBee на полосе 2,4 ГГц использует каналы 11–26, разделенные интервалом 5 МГц. В устройствах Freescale каналы имеют номера 0–15, поэтому их надо транслировать в каналы 11–26. В сетях ZigBee используется уплотнение спектра (DSSS — Direct Sequence Spread Spectrum). Передача производится в полудуплексном режиме. В каждый момент времени доступен только один канал. Обычно в протоколах ZigBee не используется переключение канала. Высокое качество работы даже в условиях сильной зашумленности обеспечивается модуляцией O-QPSK и уплотнением DSSS.



При **квадратурной фазовой манипуляции QPSK (Quadrature Phase Shift Keying или 4-PSK)** используется созвездие из четырёх точек, размещённых на равных расстояниях на окружности. На символ приходится два бита. Скорость может быть увеличена в два раза относительно BPSK при той же полосе сигнала, либо оставить скорость прежней, но уменьшить полосу вдвое.

Хотя QPSK можно считать квадратурной манипуляцией (QAM-4), иногда её проще рассматривать в виде двух независимых модулированных несущих, сдвинутых на 90°. При таком подходе чётные (нечётные) биты используются для модуляции синфазной составляющей I, а нечётные (чётные) — квадратурной составляющей несущей Q. Так как BPSK используется для обеих составляющих несущей, то они могут быть демодулированы независимо.



В **четырехпозиционной фазовой модуляции со сдвигом квадратур (OQPSK – Offset QPSK)** битовые потоки, подаваемые на модуляторы квадратур I и Q, сдвинуты друг относительно друга на длительность одного бита (половина символьного интервала). Поэтому в конкретно взятый момент времени только один из квадратурных битовых потоков может изменять свое значение. Это создает диаграмму переходов состояний, существенно отличающуюся от диаграммы переходов состояний модуляции QPSK. В OQPSK сигнальные траектории не проходят рядом с началом координат квадратурной плоскости. В результате максимальное изменение амплитуды передаваемого сигнала достигает 3 дБ. Это существенно меньше изменения амплитуды в сигналах двоичной и квадратурной модуляции. В результате удается получить существенный выигрыш по коэффициенту полезного действия усилителя мощности радиопередатчика.

Метод прямой последовательности для расширения спектра DSSS (Direct Sequence Spread Spectrum) — широкополосная модуляция с прямым расширением спектра. Исходный двоичный сигнал преобразуется в псевдослучайную последовательность, используемую для модуляции несущей. Вся используемая «широкая» полоса частот делится на некоторое число подканалов (в ZigBee этих подканалов 32). По стандарту 802.15.4 каждый передаваемый байт информации делится на два полубайта (4-битных символа), каждый из которых по таблице перекодируется в 32-битную ПСП, которая передается как бы одновременно и параллельно (физически сигналы передаются последовательно), используя все 32 подканала. При этом сильно уменьшается отношение уровня передаваемого сигнала к уровню шума, (то есть случайных или преднамеренных помех), так что передаваемый сигнал уже как бы неразличим в общем шуме. Но благодаря его избыточности принимающее устройство все же может его распознать.

Symbol	Chip sequence (C_0, C_1, C_2, … , C_{31})
0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 1 0 1 1 0 1
8	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1
11	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

Выбор канала производится пользователем. Устройство при подключении к сети сканирует все каналы. При формировании сети сканирование проводится дважды: в пассивном и активном режимах. Разработчику предоставляется возможность использовать два режима работы сети: с «маяком» (beacon-enabled) и без него (beacon-disabled). Режим beacon-enabled обеспечивает строго структурированную по времени передачу данных в рамках суперциклов, что позволяет определить время задержки на отсылку пакета. Маяком в сети является координатор, который рассылает сообщения синхронизации.

Пассивное сканирование позволяет выбрать наиболее свободный канал, а при активном сканировании координатор рассылает найденные в сети запросы маяка (beacon request), чтобы определить занятые идентификаторы PAN. По умолчанию сеть ZigBee выбирает канал с наименьшим количеством сетей и с самым низким уровнем шума. При подключении устройства к сети проводится только активное сканирование. Если сеть уже сформирована и подключаемое устройство получило ответный кадр маяка (beacon response), то канал считается достаточно тихим.

Лицензирование

Спецификация ZigBee доступна для широкой публики при условиях некоммерческого использования. Входной уровень членства в альянсе ZigBee, называемый Adopter, обеспечивает доступ к ещё не опубликованным спецификациям и разрешает создавать продукты для коммерческого использования спецификации. Регистрация в ходе использования спецификации ZigBee требует от коммерческого разработчика присоединения к альянсу ZigBee.

Государственное регулирование

Согласно Решению ГКРЧ при Мининформсвязи России от 07.05.2007 № 07-20-03-001 на территории РФ применение сетей ZigBee в частотном диапазоне 2400–2483,5 МГц не требует получения частотных разрешений и дополнительных согласований.

Топология сети ZigBee

ZigBee поддерживает простые топологии сети, такие как «точка-точка», «дерево» и «звезда». Однако, основным вариантом топологии является самоорганизующуюся и самовосстанавливающуюся *ячеистую (mesh) топологию* с ретрансляцией и маршрутизацией сообщений. В такой сети, каждое устройство может связываться с любым другим устройством как напрямую, так и через промежуточные узлы сети. Ячеистая топология предлагает альтернативные варианты выбора маршрута между узлами. Сообщения поступают от узла к узлу, пока не достигнут конечного получателя. Возможны различные пути прохождения сообщений, что повышает доступность сети в случае выхода из строя того или иного звена.

В сети ZigBee существует 3 типа узлов: координатор (ZC), роутер/маршрутизатор (ZR), конечные устройства (ZED), которые делятся на спящие устройства и мобильные устройства.

Главное устройство в ZigBee-сети – это координатор. В каждой сети есть один координатор ZigBee. Координатор выполняет функции по формированию сети, а также является одновременно доверительным центром (trust-центром). Доверительный центр устанавливает политику безопасности, хранит ключи безопасности и задает настройки во время подключения устройства к сети.

Конечное устройство обменивается информацией с материнским узлом (координатором или маршрутизатором). Оно не может передавать данные с других устройств. Из-за этого узел большую часть времени может пребывать в спящем состоянии (режим пониженного энергопотребления), что позволяет экономить энергоресурс батарей (как правило такие устройства имеют автономное питание). Обычно конечные устройства выполняют роль датчиков или контроллеров каких-либо исполнительных устройств. Их количество диктуется потребностью конкретного приложения.

Роутеры осуществляют маршрутизацию пакетов по сети и должны быть готовы к передаче данных в любой момент времени. Поэтому эти узлы не используют режимов пониженного энергопотребления и имеют стационарное питание. Их количество в сети должно быть достаточным для обслуживания требуемого количества спящих и мобильных узлов. Максимальное количество спящих или мобильных узлов, обслуживаемых одним роутером - 32.

Обмен данными и задержки

При индивидуальной рассылке сначала между узлами автоматически выбирается маршрут. После подтверждения пакет посылается повторно до трех раз. Иногда маршрут передачи изменяется, если промежуточный узел выходит из строя. Широковещательные данные передаются всем узлам сети, находящимся в пределах досягаемости. Групповая передача осуществляется в пределах определенной группы узлов.

ZigBee — асинхронный протокол, поэтому каждый узел может инициировать передачу в любой момент времени. Например, когда пользователь включает свет, данные посылаются мгновенно, независимо от быстродействия выключателя. *Недостаток ZigBee заключается в том, что нельзя предсказать задержку пакета.* Обычно принимается, что для передачи пакета требуется по 10 мс на каждый промежуток между абонентами. Сложности возникают, когда требуется повторная посылка или вычисление маршрута. Для выбора маршрута производится широковещательная рассылка, а устройство, начавшее передачу, должно ждать.

Повторные посылки делятся на пошаговые — MAC и между конечными устройствами — APS. Если один узел инициирует передачу другому, находящемуся на расстоянии четырех скачков, то в среднем пакет будет принят через 40 мс, а подтверждение придет через 80 мс.

При индивидуальной передаче с подтверждением может быть произведено до трех повторных передач с интервалом 1.5 с, т. е. в худшем случае задержка может составить около 5 с. Размер пакета не влияет на задержку, если канал относительно свободен, поскольку время ожидания выбирается случайным образом, уменьшая время передачи. Но если канал загружен, то вероятность повторной посылки экспоненциально возрастает с увеличением длины пакета. В связи с этим рекомендуется пересылать короткие пакеты, чтобы сократить задержку и уменьшить занимаемую полосу, освобождая ресурс для других приложений. Передача в больших пакетах целесообразна только в случае, если данные имеют очень большой объем.

Адресация сети

Типы адресов ZigBee и диапазон их значений приведены в таблице 1. Сетевой адрес, обозначаемый NwkAddr, представляет собой 16-разрядное число, уникально определяющее узел в сети, то есть один координатор, теоретически, может взять под свою опеку порядка 65 000 устройств. Вместе с тем, предусмотрена возможность одновременного использования нескольких сетей. Например, в отеле Aria (Лас-Вегас) одновременно используется около 75 тыс. устройств с поддержкой ZigBee. Координатор всегда имеет адрес 0x0000. На одном канале могут существовать два координатора с одинаковыми адресами, поскольку они имеют разные PAN ID (Personal Area Network ID – идентификатор сети).

Таблица 1

Адреса ZigBee

Название	Диапазон	Описание
Канал	`11–26`	Физическая часть РЧ–спектра
Идентификатор PAN	`0x0000–0x3fff`	Адрес сети в канале
Сетевой адрес (NwkAddr)	`0x0000–0xfff7`	Адрес узла в сети
Конечная точка	`1–240`	Адрес приложения в узле
Кластер	`0x0000–0xffff`	Объект внутри приложения
Команда	`0x00–0xff`	Действие внутри кластера
Атрибут	`0x0000–0xffff`	Единица данных внутри кластера
Расширенный PAN ID Extended PAN ID (EPID)	`0x0000000000000000–0xffffffffffffffff`	Уникальный 64-разрядный идентификатор сети
Группа	`0x0000–0xffff`	Выбранная часть узлов сети
Идентификатор профиля	`0x0000–0xffff`	Профиль ZigBee

В стеке ZigBee (0x01) поле NwkAddr характеризует расположение узла в сети. Например, устройство с NwkAddr = 0x0001 является первым подключившемся к сети

ZR, а узел с адресом NwkAddr = 0x796F — это первое конечное устройство. В стеке ZigBee Pro (0x02) адрес присваивается произвольным образом.

MAC-адрес

MAC-адрес — это расширенный адрес, представляющий собой уникальный 64-разрядный номер, присвоенный устройству. Между адресом MAC и NwkAddr нет связи. При отключении устройства от сети и подсоединении его к другой MAC-адрес обязательно останется прежним, а NwkAddr может измениться.

Приемники ZigBee не содержат MAC-адрес. Он назначается производителем и записывается во флэш-память микроконтроллера, расположенного на плате. MAC-адрес записывается от младшего бита к старшему, поэтому во флэш-память устройства он заносится в обратном порядке.

MAC-адрес может иногда использоваться вместо короткого адреса узла, например, если узел перемещается и меняет свой короткий адрес. Так, когда пульт дистанционного управления выходит из зоны охвата своего родителя, он ищет новое родительское устройство, чтобы быть доступным для узлов сети.

Идентификаторы PAN

Идентификаторы PAN ID используются для логического отделения узлов одной сети ZigBee от узлов другой, если сети расположены на одной и той же территории либо работают в одном канале. Благодаря разным ID несколько сетей могут существовать в непосредственной близости друг от друга без интерференции.

Идентификатор ZigBee представляет собой 16-разрядное число от 0x0000 до 0x3fff. В стандарте 802.15.4 идентификаторы имеют значения в диапазоне 0x0000–0xfffe. В версии ZigBee 2006 идентификаторы имеют уникальное значение на данном канале, т. е. в разных каналах могут работать устройства с одинаковым ID. В ZigBee 2007 это запрещено из-за применения функции быстрой подстройки частоты (frequency agility), которая разрешает сети переключать каналы для поиска лучшего.

При формировании сети PAN ID принимает значение 0xffff, которое говорит о том, что приложение запрашивает у стека случайный идентификатор, не конфликтующий с ID других, работающих поблизости, сетей. При подключении к сети ID = 0xffff означает, что узел хочет подключиться к любой сети. Идентификатор выбирается пользователем.

Расширенный идентификатор PAN

Расширенные идентификаторы (EPID — Extended PAN ID) представляют собой 64-разрядные числа, которые уникальным образом идентифицируют персональную сеть. Обмен данными производится с использованием 16-разрядного идентификатора, кроме одного случая. Ответный кадр, посланный на запрос маяка, содержит

расширенный идентификатор сети, чтобы узел, который хочет подключиться к сети, выбрал нужный ID.

Когда узел ZigBee хочет подключиться к сети, он всегда высылает запрос маяка. Затем он анализирует все полученные ответные маяки и выбирает подходящий. Расширенные идентификаторы не устанавливаются ни одним комитетом стандартов. Для старших 24 разрядов EPID рекомендуется использовать OUI — уникальный номер, присвоенный сетевому устройству производителем. Расширенные ID абсолютно не связаны с 16-разрядными идентификаторами и MAC-адресами и используются исключительно для нахождения узлом нужной сети.

Адресация внутри узла

Выше были приведены параметры узла, необходимые для его определения в сети. Однако ZigBee обеспечивает также совместимость на уровне приложения за счет использования кластеров, конечных точек, команд, атрибутов и профилей. Каждый пакет должен содержать PAN ID (поле MAC), NwkAddr (поле NWK), адрес конечной точки приемника и передатчика, ID профиля и кластера (поле APS).

Конечные точки

Конечные точки позволяют относить один узел к различным профилям или объединять несколько ZigBee-устройств в узел. Каждый узел сети может содержать 1–240 конечных точек в соответствии с количеством выполняемых приложений. Номера конечных точек могут идти не по порядку.

Например, выключатель может быть предназначен как для внутреннего, так и для внешнего освещения. Соответственно, он представляет собой две конечные точки. Такие устройства как термостат могут содержать несколько независимых устройств с точки зрения сети (датчик, интерфейс пользователя, нагревательный и охладительный элементы).

Кластеры

Кластер похож на класс в объектно-ориентированном программировании и представляет собой совокупность:

- *описания стандартного устройства ZigBee* (осветительное устройство, диммер, выключатель, счетчик)
- *описания стандартных атрибутов* для этого устройства (вкл./выкл., яркость, показания счетчика)
- *описания стандартных команд* для этого устройства (установить уровень яркости, считать показания, включить/выключить)

Кластеры имеют клиент-серверную природу. ZigBee-сервер – это устройство, которое хранит значение атрибута, в то время, как ZigBee-клиент дистанционно считывает или записывает значение этого атрибута. Например, пара стандартных устройств лампочка и выключатель могут вместе реализовать функционирование стандартного кластера включить/выключить. При этом лампочка будет ответственна за серверную часть

кластера. Она хранит значение атрибута включено/выключено. Выключатель дистанционно устанавливает значение этого атрибута и реализует, таким образом, клиентскую часть кластера. Одно и то же устройство может содержать клиентские части одних кластеров и серверные части других. Например, выключатель в нашем примере может дополнительно содержать серверную часть кластера конфигурация, при помощи которого он будет получать информацию о режимах своей работы от конфигурирующего устройства.

Кластеры определяются 16-разрядным идентификатором и являются объектами приложения. В то время как NwkAddr и конечные точки относятся к адресации, кластер определяет назначение приложения. Например, кластер включения и выключения On/Off выполняет действие перевода устройства из одного состояния в другое. При этом тип исполнительного устройства неважен.

Текущее состояние устройства определяется приложением по атрибуту внутри кластера. Некоторые кластеры, определенные в ZigBee, приведены в таблице 2. Кластеры определены только внутри конкретного профиля. Например, в одном профиле кластер 0x0000 может выполнять отключение сети (Off), а в другом — содержать основные установки (Basic). Кроме идентификатора кластеры имеют направление. В свойстве SimpleDescriptor конечной точки кластер обозначается как вход или выход.

Таблица 2

Кластеры ZigBee

Наименование	**ID**
Basic (основной)	0x0000
Power Configuration (регулировка мощности)	0x0001
Temperature Configuration (настройка температуры)	0x0002
Identify (кластер распознавания)	0x0003
Groups (кластер группы)	0x0004
Scenes (кластер сцен)	0x0005
On/Off (включение/выключение)	0x0006
On/Off Configuration (настройка включения и выключения)	0x0007
Level Control (управление уровнем)	0x0008
Time (время)	0x000a
Location (местоположение)	0x000b

В стандартных профилях (Public profile) используется библиотека кластеров ZigBee (ZigBee Cluster Library, ZCL), содержащая команды и атрибуты. С помощью библиотеки легко получить или присвоить атрибут, используя общий набор команд. Библиотека ZCL группирует кластеры по функциональному признаку: общего назначения, для работы с датчиками, для управления осветительными устройствами, вентиляцией и т. д. Использование стандартных кластеров для пересылки сообщений является обязательным требованием спецификации ZigBee PRO Feature Set.

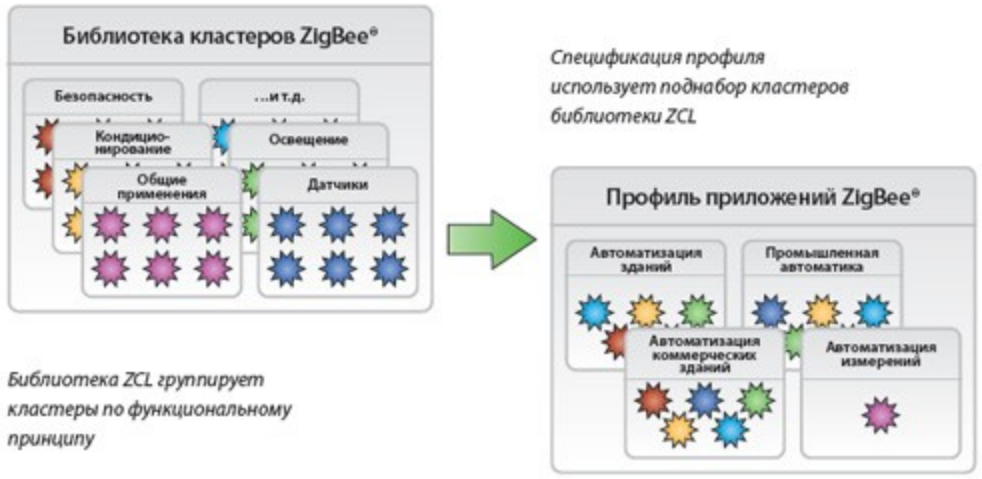
Команды представляют собой 8-разрядное число и могут быть внутрикластерными или межкластерными. Кластерные команды зависят от номера кластера и обычно

начинаются с 0x00. Например, 0x00 — команда выключения в кластере On/Off и команда движения к заданному уровню в кластере LevelControl.

В индивидуальных профилях использовать библиотеку кластеров необязательно. Это позволяет сократить программный код. Атрибуты являются 16-разрядными числами и описывают текущее состояние кластера. Совокупность атрибутов всех кластеров, поддерживаемых устройством, определяет состояние устройства.

Профили

Профилем называется совокупность настроек программного обеспечения узлов сети, обеспечивающая их совместную работу. Спецификация профиля определяет такие параметры, как способы задания идентификационных параметров сети, режимы образования сети, способы защиты данных, используемый поднабор кластеров, который включает кластеры из разных функциональных групп библиотеки ZCL.



Все запросы данных посылаются в профиль приложения. Для этого используются идентификаторы профиля — 16-разрядные числа в диапазоне 0x0000–0x7fff для стандартных профилей и 0xbf00–0xffff — для профилей, определенных производителем.

Профиль относится к приложению или устройству. Стандартные профили определяются альянсом ZigBee, индивидуальные — производителем.

Home Automation (автоматизация дома) — *стандартный профиль для объединения в сеть бытовых устройств, в т.ч. осветительных приборов, выключателей, розеток, пультов управления, кондиционеров, термостатов, нагревателей*. Другой пример — стандартный профиль Commercial Building Automation, который определяет такие устройства ZigBee как *сложные осветительные приборы и многопозиционные выключатели, системы отпирания дверей без использования ключа и системы безопасности*.

В одной сети может существовать несколько стандартных и индивидуальных профилей. В ZigBee Alliance постоянно идет работа над расширением набора стандартных профилей, чтобы удовлетворить все потребности клиентов. Именно

производители определяют, каких профилей не хватает в первую очередь. Краткий список стандартных профилей приведен в таблице 3.

Таблица 3

Стандартные профили ZigBee

ID проф.	Название профиля
0101	Industrial Plant Monitoring (IPM, мониторинг предприятия)
0104	Home Automation (HA, автоматизация жилых помещений)
0105	Commercial Building Automation (CBA, автоматизация коммерческих помещений)
0107	Telecom Applications (TA, телекоммуникация)
0108	Personal Home & Hospital Care (PHHC, амбулаторное или стационарное лечение)
0109	Advanced Metering Initiative (AMI, дополнительные измерения)

Профили позволяют соединять устройства различных производителей без дополнительной настройки. Индивидуальные профили, также называемые профилями производителей (Manufacturer Specific Profiles, MSP), не закреплены альянсом ZigBee. Они создаются для таких приложений, которые рассчитаны на взаимодействие с устройствами только одного производителя.

Профили, определенные производителем, позволяют задавать любой набор кластеров, конечных точек и устройств. Стандарт не накладывает каких бы то ни было ограничений на тип передаваемых данных при условии, что скорость передачи находится в допустимом диапазоне и приложение не перегружает канал.

ZigBee Alliance по запросу производителя — члена организации — присваивает идентификатор предложенному им профилю. Чтобы задать кластеры в индивидуальном профиле, необходимо сначала составить карту всех устройств сети и определить, какого типа информацию они должны обрабатывать. В этом случае структура будет наиболее прозрачна и легка в управлении.

Идентификаторы устройств

Каждая конечная точка содержит идентификатор профиля и идентификатор устройства. Как уже говорилось, одно физическое устройство может представлять собой несколько устройств ZigBee. Идентификаторы устройств ZigBee принимают значения от 0x0000 до 0xffff (см. табл. 4). Идентификаторы устройств имеют двойное назначение. Они позволяют отображать на дисплее пользователя иконки, соответствующие типу устройства, и в то же время помогают сделать инструменты ZigBee более совершенными.

Таблица 4

Идентификаторы устройств для профиля Home Automation

Устройство	Идентиф.	Устройство	Идентиф.
Расширитель диапазона	0x0008	Датчик света	0x0106
Розетка электросети	0x0009	Затенитель	0x0200

Выключатель света	0x0100	Контроллер затенителя	0x0201
Лампа с регулируемой яркостью	0x0101	Нагревательно-охладительный элемент	0x0300
Выключатель света	0x0103	Термостат	0x0301
Регулятор яркости	0x0104	Датчик температуры	0x0302

Рассмотрим двухпозиционный переключатель и штепсельную розетку. В плане удаленного мониторинга и управления эти устройства идентичны. Они принадлежат одному кластеру — 0x0006 (On/Off). Однако, с точки зрения пользователя, розетка относится к инструменту для ввода в эксплуатацию электронных устройств, а переключатель позволяет включить или выключить свет.

Сеть ZigBee не устанавливает интерфейса между человеком и устройствами. Выключателем может быть кнопка, тумблер, пластина датчика электрического поля, датчик ускорения и т. д. Во всех стандартных профилях ZigBee содержится список устройств. Производители могут расширить его, используя поле Manufacturer Specific Extension, которое является частью интерфейса библиотеки кластеров ZigBee. Они также могут создать устройство в индивидуальном профиле (MSP), тогда оно будет взаимодействовать с устройствами из стандартного профиля через идентификаторы устройств и кластеры.

Формирование сети

Сеть ZigBee – самоорганизующаяся, и ее работа начинается с формирования. Устройство, назначенное при проектировании координатором персональной сети (PAN координатор), определяет канал, свободный от помех, и ожидает запросов на подключение.
Устройства, пытающиеся присоединиться к сети, рассылают широковещательный запрос. Пока PAN координатор – единственное устройство в сети, отвечает на запрос и предоставляет присоединение к сети только он. В дальнейшем присоединение к сети могут предоставлять также присоединившиеся к сети маршрутизаторы.
Устройство, получившее ответ на широковещательный запрос, обменивается с присоединяющим устройством сообщениями, чтобы определить возможность присоединения. Возможность определяется способностью присоединяющего маршрутизатора обслужить новые устройства в дополнение к ранее подключенным.

Вступление в сеть (присоединение)

Существует два способа присоединения: MAC ассоциация и повторное сетевое присоединение (NWK rejoin).

MAC ассоциация доступна любому устройству ZigBee и осуществляется на MAC уровне. Механизм MAC ассоциации следующий:

1. Устройство, позволяющее присоединиться к нему, выставляет на MAC уровне разрешение на присоединение.
2. Устройство, вступающее в сеть, выставляет на MAC уровне запрос на присоединение и передает широковещательный запрос маячка.

3. Получив маячок от устройств, готовых подключить присоединяемое устройство, последнее определяет, в какую сеть и к какому устройству оно желает присоединиться, и выставляет на MAC уровне требование о вступлении с флажком «повторное присоединение» в значении FALSE.
4. Затем вступающее устройство направляет на выбранное для присоединения устройство запрос присоединения и получает ответ с присвоенным ему сетевым адресом.

При MAC ассоциации данные передаются не зашифрованными, поэтому MAC ассоциация не является безопасной.

Повторное сетевое присоединение вопреки названию может применяться и при первичном присоединении. Оно выполняется на сетевом уровне. При этом, если вступающее устройство знает текущий сетевой ключ, обмен пакетами может быть безопасным. Ключ может быть получен, например, при настройке.
При повторном подключении присоединяющееся устройство выставляет на сетевом уровне запрос присоединения и обменивается с подключающим устройством пакетами «запрос присоединения» – «ответ на запрос присоединения».

Динамика сети

Кроме случаев присоединения новых устройств структура сети меняется и в случаях, когда устройства покидают сеть и повторно присоединяются в других местах (это происходит, например, в случае перезагрузки устройства). Каждый раз такое устройство получает адрес из имеющегося в распоряжении присоединяющего маршрутизатора диапазона адресов.

Источники:

1. Материалы с сайта http://www.zigbee.org
2. ZigBee. https://ru.wikipedia.org
3. В. Лекнин Сети ZigBee. Зачем и почему? https://habrahabr.ru
4. Протокол ZigBee: беспроводные технологии на службе «умного» дома. Н. Жогов. http://www.ferra.ru
5. Беспроводные сети ZigBee и Thread. http://www.wless.ru
6. А. Павлов Адресация и профили ZigBee. http://www.russianelectronics.ru
7. Дрю Гисласон (Drew Gislason). Приложения ZigBee: обмен данными, API и PAN [перевод]. http://www.russianelectronics.ru
8. Четырехпозиционная фазовая модуляция (QPSK). http://digteh.ru
9. Четырехпозиционная фазовая модуляция со сдвигом квадратур (OQPSK). http://digteh.ru

Беспроводные системы ПД

Лекция 07
Протокол Bluetooth

Bluetooth — производственная спецификация беспроводных персональных сетей WPAN. Bluetooth обеспечивает обмен информацией между оконечными пользовательскими устройствами, такими как персональные компьютеры, мобильные телефоны, принтеры, цифровые фотоаппараты, устройства ввода, наушники, гарнитуры на радиочастоте для ближней связи.

Протокол Bluetooth относится к физическому уровню модели OSI и в настоящее время определяется спецификацией IEEE 802.15.1.

Bluetooth	Логотип Bluetooth является сочетанием двух нордических («скандинавских») рун: «хагалаз» (Hagall) — аналог латинской H и «беркана» (Berkanan) — латинская B.

Работы по созданию Bluetooth начала компания Ericsson в 1994 году как беспроводную альтернативу кабелям RS-232. Проект получил название BlueTooth в честь короля Норвегии и Дании Гарольда Голубой Зуб (Harald Blaatand, 940–981 годы). Проект являлся конкурентом стандарта IEEE 802.11 (оба стандарта используют один и тот же частотный диапазон, одни и те же 79 каналов). Первая спецификация Bluetooth была разработана группой Bluetooth Special Interest Group (Bluetooth SIG), которая была основана в 1998 году. В неё вошли компании Ericsson, IBM, Intel, Toshiba и Nokia. Впоследствии в 2000 году Bluetooth SIG и IEEE достигли соглашения, на основе которого спецификация Bluetooth стала частью стандарта IEEE 802.15.1 (14 июня 2002 года).

Спецификации

Bluetooth 1.0

Устройства версий 1.0 (1998) и 1.0B имели плохую совместимость между продуктами различных производителей. В 1.0 и 1.0B была обязательной передача адреса устройства (BD_ADDR) на этапе установления связи, что делало невозможной реализацию анонимности соединения на протокольном уровне и было основным недостатком данной спецификации.

Bluetooth 1.1

В Bluetooth 1.1 было исправлено множество ошибок, найденных в 1.0B, добавлена поддержка для нешифрованных каналов, индикация уровня мощности принимаемого сигнала (RSSI).

Bluetooth 1.2

Главные улучшения включают следующее:

- Быстрое подключение и обнаружение.
- Адаптивная перестройка частоты с расширенным спектром (AFH), которая повышает стойкость к радиопомехам.
- Более высокие, чем в 1.1, скорости передачи данных, практически до 1 Мбит/с.
- Расширенные Синхронные Подключения (eSCO), которые улучшают качество передачи голоса в аудиопотоке, позволяя повторную передачу повреждённых пакетов, и при необходимости могут увеличить задержку аудио, чтобы оказать лучшую поддержку для параллельной передачи данных.
- В Host Controller Interface (HCI) добавлена поддержка трёхпроводного интерфейса UART.
- Введены режимы управления потоком данных (Flow Control) и повторной передачи (Retransmission Modes) для L2CAP.

Утверждён как стандарт IEEE Standard 802.15.1-2005.

Bluetooth 2.0 + EDR

Bluetooth версии 2.0 был выпущен 10 ноября 2004 г. Имеет обратную совместимость с предыдущими версиями 1.x. Основным нововведением стала поддержка Enhanced Data Rate (EDR) для ускорения передачи данных. Номинальная скорость EDR около 3 Мбит/с, однако на практике это позволило повысить скорость передачи данных только до 2,1 Мбит/с. Дополнительная производительность достигается с помощью различных радиотехнологий для передачи данных.

Стандартная (базовая) скорость передачи данных использует GFSK-модуляцию радиосигнала при скорости передачи в 1 Мбит/с. EDR использует сочетание модуляций GFSK и PSK с двумя вариантами, π/4-DQPSK и 8DPSK. Они имеют большие скорости передачи данных по воздуху — 2 и 3 Мбит/с соответственно.

Bluetooth SIG издала спецификацию как «Технология Bluetooth 2.0 + EDR», которая подразумевает, что EDR является дополнительной функцией. Кроме EDR, есть и другие незначительные усовершенствования к 2.0 спецификации, и продукты могут соответствовать «Технологии Bluetooth 2.0», не поддерживая более высокую скорость передачи данных.

Согласно 2.0 + EDR спецификации, EDR обеспечивает следующие преимущества:

- Увеличение скорости передачи в 3 раза (2,1 Мбит/с) в некоторых случаях.
- Уменьшение сложности нескольких одновременных подключений из-за дополнительной полосы пропускания.
- Снижение потребления энергии благодаря уменьшению нагрузки.

Bluetooth 2.1

2007 год. Добавлена технология расширенного запроса характеристик устройства (для дополнительной фильтрации списка при сопряжении), энергосберегающая технология Sniff Subrating, которая позволяет увеличить продолжительность работы устройства от одного заряда аккумулятора в 3—10 раз. Кроме того обновлённая спецификация существенно упрощает и ускоряет установление связи между двумя устройствами, позволяет производить обновление ключа шифрования без разрыва соединения, а также делает указанные соединения более защищёнными, благодаря использованию технологии Near Field Communication.

Bluetooth 2.1 + EDR

В августе 2008 года Bluetooth SIG представил версию 2.1+EDR. Новая редакция Bluetooth снижает потребление энергии в 5 раз, повышает уровень защиты данных и облегчает распознавание и соединение Bluetooth-устройств благодаря уменьшению количества шагов, за которые оно выполняется.

Bluetooth 3.0 + HS

3.0+HS была принята Bluetooth SIG 21 апреля 2009 года. Она поддерживает теоретическую скорость передачи данных до 24 Мбит/с. Её основной особенностью является добавление AMP (Alternate MAC/PHY), дополнение к 802.11 как высокоскоростное сообщение. Для AMP были предусмотрены две технологии: 802.11 и UWB, но UWB отсутствует в спецификации.

Модули с поддержкой новой спецификации соединяют в себе две радиосистемы: первая обеспечивает передачу данных в 3 Мбит/с (стандартная для Bluetooth 2.0) и имеет низкое энергопотребление; вторая совместима со стандартом 802.11 и обеспечивает возможность передачи данных со скоростью до 24 Мбит/с (сравнима со скоростью сетей Wi-Fi). Выбор радиосистемы для передачи данных зависит от размера передаваемого файла. Небольшие файлы передаются по медленному каналу, а большие — по высокоскоростному. Bluetooth 3.0 использует более общий стандарт 802.11 (без суффикса), то есть не совместим с такими спецификациями Wi-Fi, как 802.11b/g или 802.11n.

Bluetooth 4.0

Bluetooth SIG утвердил спецификацию Bluetooth 4.0 30 июня 2010 года. Bluetooth 4.0 включает в себя протоколы:

- Классический Bluetooth,
- Высокоскоростной Bluetooth
- Bluetooth с низким энергопотреблением (Bluetooth low energy, Bluetooth LE).

Высокоскоростной Bluetooth основан на Wi-Fi, а Классический Bluetooth состоит из протоколов предыдущих спецификаций Bluetooth.

Полоса частот: 2,402–2,48 ГГц (мощность не более 0,0025Вт).

Протокол Bluetooth с низким энергопотреблением предназначен, прежде всего, для миниатюрных электронных датчиков (использующихся в спортивной обуви, тренажёрах, миниатюрных сенсорах, размещаемых на теле пациентов и т. д.). Низкое энергопотребление достигается за счёт использования особого алгоритма работы. Передатчик включается только на время отправки данных, что обеспечивает возможность работы от одной батарейки типа CR2032 в течение нескольких лет. Стандарт предоставляет скорость передачи данных в 1 Мбит/с при размере пакета данных 8–27 байт. В новой версии два Bluetooth-устройства смогут устанавливать соединение менее чем за 5 миллисекунд и поддерживать его на расстоянии до 100 м. Для этого используется усовершенствованная коррекция ошибок, а необходимый уровень безопасности обеспечивает 128-битное AES-шифрование.

Первый чип с поддержкой Bluetooth 3.0 и Bluetooth 4.0 был выпущен компанией ST-Ericsson в конце 2009 года.

Bluetooth 4.1

В конце 2013 года Bluetooth SIG представила спецификацию Bluetooth 4.1. Одно из улучшений, реализованных в спецификации Bluetooth 4.1, касается совместной работы Bluetooth и мобильной связи четвёртого поколения LTE. Стандарт предусматривает защиту от взаимных помех путём автоматического координирования передачи пакетов данных.

Bluetooth 4.2

3 декабря 2014 Bluetooth SIG представила спецификацию Bluetooth 4.2. Основные улучшения — повышение конфиденциальности и увеличение скорости передачи данных.

Bluetooth 5.0

16–17 июня 2016 года Bluetooth SIG представила спецификацию Bluetooth 5.0 Изменения коснулись в основном режима с низким потреблением и высокоскоростного режима.

В режиме Low Energy (LE) пропускная способность по сравнению с Bluetooth 4.2 будет увеличена в два раза. Эффективная дальность возрастёт в четыре раза. В высокоскоростном режиме, на этот раз основанном на более быстром стандарте Wi-Fi, скорость будет увеличена в два-три раза. В классическом режиме сохранится совместимость с предыдущими спецификациями Bluetooth. Но при этом увеличится энергоэффективность модулей. Так же обещается увеличение в восемь раз количества одновременных подключений к одному модулю

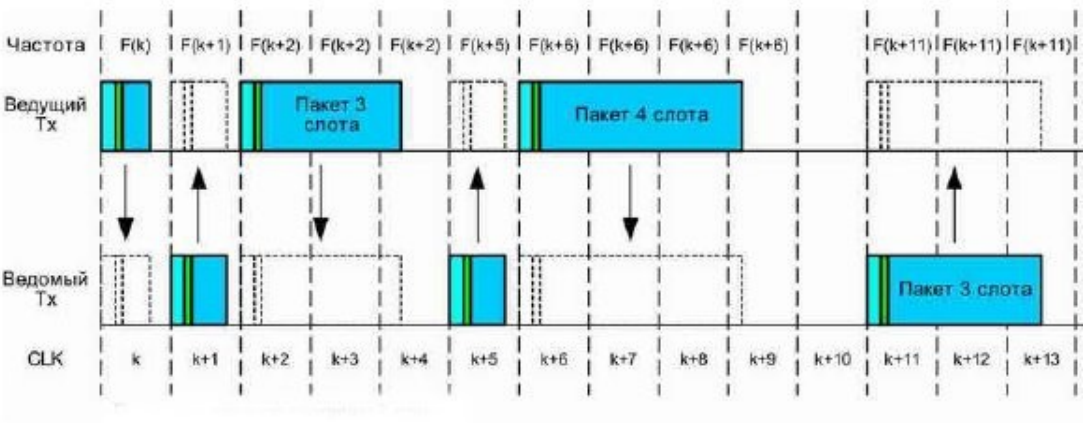
Принцип действия Bluetooth

Принцип действия основан на использовании радиоволн. Радиосвязь Bluetooth осуществляется в свободном от лицензирования ISM-диапазоне 2,4–2,4835 ГГц (Industry, Science and Medicine), который используется в различных бытовых приборах и беспроводных сетях. Используются широкие защитные полосы: нижняя граница частотного диапазона составляет 2 ГГц, а верхняя — 3,5 ГГц. Точность заданий частоты (положение центра спектра) задается с точностью ±75 кГц. Кодирование сигнала осуществляется по двухуровневой схеме GFSK (Gaussian Frequency Shift Keying).

ISM диапазон — несколько частотных диапазонов (433, 900, 2400, 5800 МГц), отведенных в большинстве стран для гражданских целей, то есть, для систем промышленного, научного и медицинского применения (ISM – Industrial, Science, Medicine). Диапазон 2400 МГц используется в оборудовании беспроводного широкополосного доступа. В эту категорию относятся Bluetooth, ZigBee, Radio-Ethernet (IEEE 802.11).

GFSK (Gaussian Frequency-Shift Keying) — вид частотной манипуляции модуляцией, при которой используется фильтр Гаусса для сглаживания положительных и отрицательных частотных перестроек, представляющих собой бинарный информационный код — «1» или «0». Принцип работы модулятора GFSK похож на FSK, за исключением того, что сначала полоса импульсов (−1, 1) проходит через фильтр Гаусса для сглаживания, что обеспечивает уменьшения ширины его спектра, а уже после попадает в FSK. Фильтрация Гаусса — один из самых распространенных способов уменьшения ширины спектра.
Если мы используем −1 для $f_c - f_d$ и 1 для $f_c + f_d$, то тогда, когда мы переходим от −1 к 1 или от 1 к −1, модулированный сигнал изменяется быстро, что приводит к появлению помех за пределами диапазона. Если мы разобьем импульс перехода от −1 к 1 например так: −1, −0,98, −0,93 ..... 0,96, 0,99, 1 и будем использовать этот сглаженный импульс для модуляции несущей, то количество помех за пределами диапазона будет уменьшено.

В Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum, FHSS). Согласно алгоритму FHSS, в Bluetooth несущая частота сигнала скачкообразно меняется 1600 раз в секунду. Таким образом, время разделяется на интервалы (так называемые слоты) продолжительностью 625 мкс. Скачкообразное переключение частоты отводит на переходные процессы 250–260 мкс. Длительность тика часов мастера равна 312,5 мкс, что определяет частоту часов — 3,2 кГц. Допускается временная неопределенность при приеме, равная ±20 мкс. В течение каждого интервала передача осуществляется по определенному подканалу (всего выделяется 79 рабочих частот шириной в 1 МГц, а в Японии, Франции и Испании полоса у́же — 23 частотных канала). Данные между устройствами Bluetooth передаются пакетами. Пакет может быть передан как за один, так и за несколько слотов. Если передача пакета к началу интервала уже завершена, то, синхронно в передатчике и приемнике, происходит смена подканала (изменение несущей частоты). Смена подканала осуществляется в заранее определенной для всех устройств пикосети псевдослучайной последовательности. Последовательность смены частот определенным образом вычисляется исходя из значений часов и адреса ведущего устройства Bluetooth.



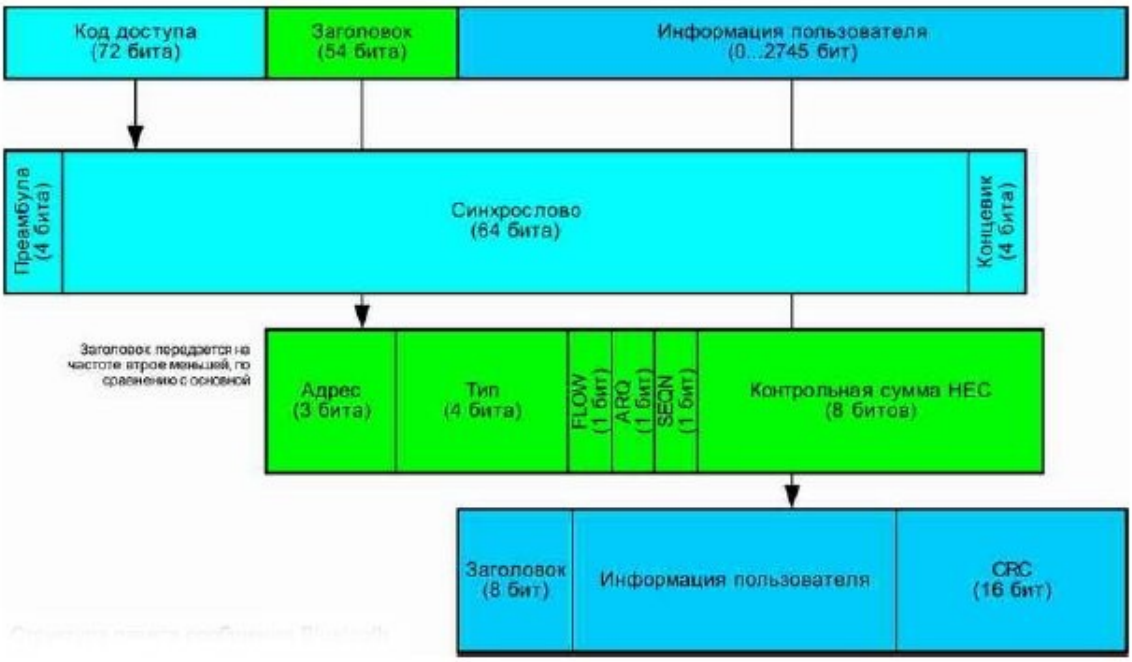
Таким образом, если рядом работают несколько пар приёмник-передатчик, то они не мешают друг другу. Этот алгоритм является также составной частью системы защиты конфиденциальности передаваемой информации: переход происходит по псевдослучайному алгоритму и определяется отдельно для каждого соединения. При передаче цифровых данных и аудиосигнала (64 кбит/с в обоих направлениях) используются различные схемы кодирования: аудиосигнал не повторяется (как правило), а цифровые данные в случае утери пакета информации будут переданы повторно.

Протокол Bluetooth поддерживает не только соединение «point-to-point», но и соединение «point-to-multipoint».

Формат пакета Bluetooth

Состав пакета:

- код доступа,
- заголовок пакета,
- информация пользователя.



Код доступа идентифицирует пакеты, принадлежащие одной пикосети, а также используется для синхронизации и процедуры запросов. Он включает преамбулу (4 бита), синхрослово (64 бита) и концевик – 4 бита контрольной суммы.

Заголовок содержит информацию для управления связью и состоит из шести полей:

- Адрес (3 бита) – адрес активного элемента;
- Тип (4 бита) – код типа данных;
- FLOW (1 бит) – управление потоком данных, показывает готовность устройства к приему;
- ARQ (1 бит) – подтверждение правильного приема;
- SEQN (1 бит) – служит для определения последовательности пакетов;
- HEC (8 бит) – контрольная сумма.

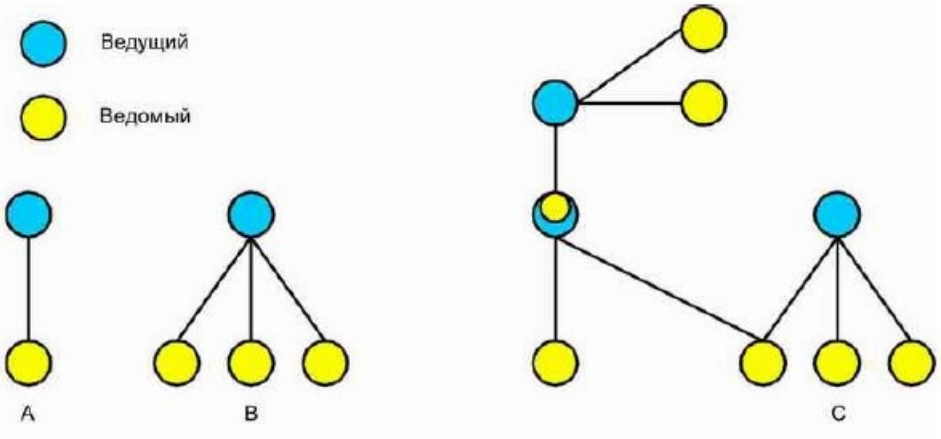
Информация пользователя состоит из трех сегментов: заголовок информации пользователя, непосредственно информация пользователя и контрольная сумма (CRC). Заголовок (8 бит) определяет логический канал, управление потоком в логических каналах, а также имеет указатель длины информации пользователя. Информация пользователя. CRC (16 бит) – от передаваемой информации вычисляется 16 бит циклического избыточного кода, после чего он прикрепляется к информации.

Класс мощности

В зависимости от мощности передатчика устройства Bluetooth делятся на три класса. Устройства класса 1 имеют максимальную выходную мощность 100 мВт (20 dBm) и обеспечивают дальность связи до 100 метров. Устройства класса 2 имеют мощность до 2,5 мВт (4 dBm) и обеспечивают дальность связи до 10 метров. Устройства класса 3 имеют мощность до 1 мВт (0 dBm) и дальность связи до 1 метра.

Пикосеть

В процессе работы физический радиоканал совместно используется (в режиме временного разделения) группой устройств, которые синхронизированы на общие часы и общую последовательность смены частот. Одно из них, выполняющее функции ведущего устройства, формирует сигналы синхронизации. Все другие устройства являются ведомыми. Группа устройств, синхронизированных таким образом, образует *пикосеть*. Пикосеть является фундаментальной формой коммуникации в технологии Bluetooth. Пикосеть является сетью категории “Ad Hoc” (т. е. обычно создается самопроизвольным способом, не имеет формальной структуры и ограничена как во времени своего существования, так и в занимаемом ею пространстве). Пикосеть может содержать до 7 активных ведомых устройств. Кроме того, в окрестности (зоне уверенного приема) ведущего устройства могут находиться неактивные (так называемые «припаркованные») ведомые устройства, которые также синхронизированы на общие часы и общую последовательность смены частот, но не могут обмениваться данными до тех пор, пока ведущее устройство не активирует их.



A - пикосеть с одним ведомым устройством;
B - пикосеть с несколькими ведомыми устройствами;
C - скаттернет

Адрес устройства Bluetooth (BD_ADDR) – неизменяемое 48-ми разрядное значение, предназначенное для идентификации любого доступного устройства Bluetooth, которое присваивается при изготовлении устройства.

Ведущее устройство пикосети – устройство в пикосети, значения адреса устройства и часов Bluetooth которого были использованы для синхронизации пикосети (определения общей для пикосети последовательности смены подканалов). Ведущее устройство пикосети должно находиться в одной окрестности (зоне уверенного приема) с каждым из ведомых устройств, входящих в пикосеть. Ведущее устройство одной пикосети может входить в другую пикосеть только на правах ведомого устройства.

Ведомое устройство пикосети – любое устройство в пикосети, которое не является ведущим пикосети, но подключено к ней. Ведомое устройство должно находиться в одной окрестности (зоне уверенного приема) с ведущим устройством пикосети. Ведомое устройство обменивается данными только с ведущим устройством, непосредственный обмен между двумя ведомыми устройствами спецификация Bluetooth не предусматривает.

Активное ведомое устройство пикосети имеет свой временный номер (от 1 до 7), под которым оно функционирует в пикосети. Если активное ведомое устройство деактивируется (паркуется), то оно отдает свой временный номер другому ведомому устройству. При последующей активации оно может получить и другой временный номер.

Доступное устройство Bluetooth – устройство пикосети (ведущее или активное ведомое), которое имеет возможность осуществлять связь, в соответствии со спецификацией Bluetooth.

Запаркованное устройство – устройство, работающее в основном режиме пикосети, то есть, синхронизированное с ведущим устройством, но не имеющее временного номера (параметры его логического транспорта сброшены в исходные).

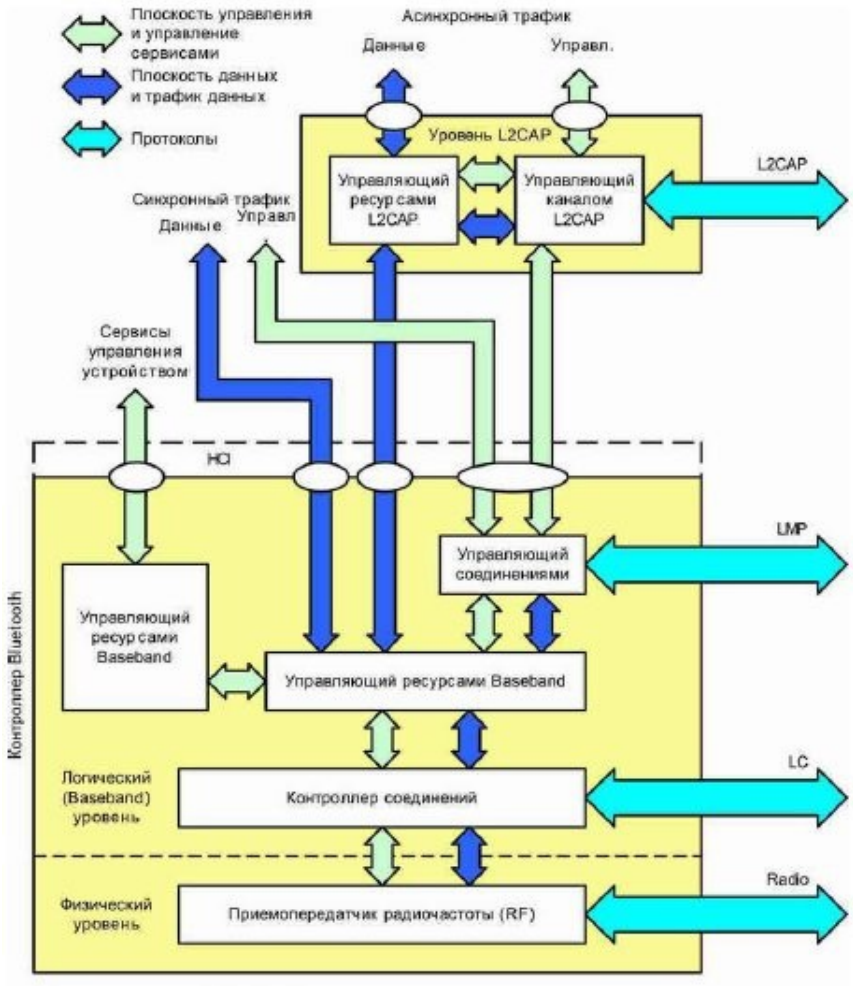
Окрестность (зона уверенного приема) – пространственная область, в которой два устройства Bluetooth могут обменяться сообщениями с приемлемым качеством и производительностью. В пределах одной пространственной области может существовать множество независимых пикосетей. Каждая из них имеет свой физический канал пикосети.

Устройство-участник множества пикосетей (PMP) является одновременно элементом более чем одной пикосети. Это возможно при использовании временного разделения каналов. PMP чередует свою работу на физическом канале каждой пикосети.

Скаттернет – две или более пикосетей, которые включают одно или более устройств, действующих как PMP. Пикосети, входящие в скаттернет, не синхронизированы между собой.

Ядро системы Bluetooth

Иерархия ядра Bluetooth содержит ряд уровней. Самый низкий – физический уровень. Далее – логический уровень (или Baseband). Наиболее высокий уровень – уровень L2CAP (Протокол управления логическим подключением и адаптацией – Logical Link Control and Adaptation Protocol).



Физический и логический уровни ядра Bluetooth принято группировать в подсистему, называемую *контроллером Bluetooth*. Таким образом, контроллер Bluetooth содержит следующие ресурсы: на физическом уровне – приемопередатчик радиочастоты (RF) и на логическом – контроллер соединений (Link Controller), управляющий ресурсами Baseband (Baseband Resource Controller), управляющий соединениями (Link manager), управляющий устройством (Device Manager).

Хост Bluetooth включает наиболее высокий уровень – уровень L2CAP и ряд сервисов. В этом качестве может выступать компьютер, вычислительное устройство, периферийное устройство, мобильный телефон, точка доступа к локальной сети или к сети PSTN (коммутируемая телефонная сеть общего пользования) и т.д. Хост Bluetooth, подключенный к контроллеру Bluetooth, может взаимодействовать с другими хостами Bluetooth, которые также подключены к своим контроллерам Bluetooth. Контроллер Bluetooth и хост Bluetooth взаимодействуют между собой посредством интерфейса HCI (Host Controller Interface).

Интерфейс хост-контроллер HCI (Host Controller Interface) Bluetooth обеспечивает командный интерфейс между логическим уровнем (Baseband) и уровнем L2CAP. Этот интерфейс обеспечивает унифицированный метод доступа к ресурсам логического уровня (Baseband).

Протоколы ядра системы Bluetooth. Устройства Bluetooth взаимодействуют между собой по протоколам обмена в соответствии со спецификацией Bluetooth. Протоколы ядра системы Bluetooth – протокол физического уровня (RF), протокол контроллера соединений (LC), протокол управления соединениями (LMP) и адаптированный протокол управления логическими связями (L2CAP). Кроме того, существует протокол обнаружения обслуживания (SDP), необходимый для всех приложений Bluetooth.

Логический уровень (Baseband) ядра системы – уровень ядра системы Bluetooth, который осуществляет доступ к среде и процедурам физического уровня. Он обеспечивает обмен потоками данных и звуковой информацией в режиме реального времени между устройствами Bluetooth, входящими в пикосеть. Этот уровень предоставляет два различных способа физического подключения – синхронный, ориентированный на соединение (SCO) и асинхронный без установления соединения (ACL).

Синхронные подключения (связи) с установлением соединения используются для передачи изохронного трафика (например, оцифрованного звука). Это связи типа «точка–точка». Их предварительно устанавливает ведущее устройство с выбранными ведомыми устройствами, и для каждой связи определяется период (в слотах), через который для нее резервируются слоты. Связи получаются симметричные двусторонние. Повторные передачи пакетов в случае ошибок приема не используются.

Асинхронные подключения (связи) без установления соединения реализуют коммутацию пакетов по схеме «точка–множество точек» между ведущим устройством и одним или несколькими (всеми) ведомыми устройствами пикосети.

Ведущее устройство может связываться с любым из ведомых устройств пикосети в слотах, не занятых под SCO, послав ему пакет и потребовав ответ. Ведомое устройство имеет право на передачу, только получив обращенный к нему запрос ведущего устройства (декодировав при этом свой адрес). Для большинства типов пакетов предусматривается повторная передача в случае обнаружения ошибки приема. Ведущее устройство может посылать и безадресные широковещательные пакеты для всех ведомых устройств своей пикосети.

Стек протоколов Bluetooth

Bluetooth имеет многоуровневую архитектуру, состоящую из основного протокола, протоколов замены кабеля, протоколов управления телефонией и заимствованных протоколов. *Обязательными протоколами* для всех стеков Bluetooth *являются: LMP, L2CAP и SDP.* Кроме того, устройства, связывающиеся с Bluetooth *обычно используют протоколы HCI и RFCOMM.*

- **LMP — Link Management Protocol** — используется для установления и управления радиосоединением между двумя устройствами. Реализуется контроллером Bluetooth.
- **HCI — Host/Controller interface** — определяет связь между стеком хоста (компьютера или мобильного устройства) и контроллером Bluetooth.
- **AVRCP — A/V Remote Control Profile** — обычно используется в автомобильных навигационных системах для управления звуковым потоком через Bluetooth.
- **L2CAP — Logical Link Control and Adaptation Protocol** — используется для мультиплексирования локальных соединений между двумя устройствами, использующими различные протоколы более высокого уровня. Позволяет фрагментировать и пересобирать пакеты.
- **SDP — Service Discovery Protocol** — позволяет обнаруживать услуги, предоставляемые другими устройствами, и определять их параметры.
- **RFCOMM — Radio Frequency Communications** — протокол замены кабеля, создаёт виртуальный последовательный поток данных и эмулирует управляющие сигналы RS-232.
- **BNEP — Bluetooth Network Encapsulation Protocol** — используется для передачи данных из других стеков протоколов через канал L2CAP. Применяется для передачи IP-пакетов в профиле Personal Area Networking.
- **AVCTP — A/V Control Transport Protocol** — используется в профиле A/V Remote Control для передачи команд по каналу L2CAP.
- **AVDTP — A/V Distribution Transport Protocol** — используется в профиле Advanced Audio Distribution для передачи стереозвука по каналу L2CAP.
- **TCS — Telephony Control Protocol** — протокол, определяющий сигналы управления вызовом для установления голосовых соединений и соединений

для передачи данных между устройствами Bluetooth. Используется только в профиле Cordless Telephony.

Заимствованные протоколы включают в себя: Point-to-Point Protocol (PPP), TCP/IP, UDP, Object Exchange Protocol (OBEX), Wireless Application Environment (WAE), Wireless Application Protocol (WAP).

Реализации стека протоколов Bluetooth

Bluetooth-стеки можно условно разделить на две группы:

- Универсального назначения. Написаны с упором на функциональность и гибкость, как правило, для настольных компьютеров. Поддержка дополнительных профилей Bluetooth может быть добавлена через драйверы.
- Для встроенных систем. Предназначены для использования в периферийных Bluetooth-устройствах, где ресурсы ограничены, а требования ниже.

Универсального назначения

1 Windows
  1.1 Widcomm. Реализация компании Widcomm Inc. была первой для операционной системы Windows. Widcomm Inc. прошла слияние с Broadcom Corporation в апреле 2004 года. Компания Broadcom продолжает лицензировать стек для включения со многими Bluetooth-устройствами конечного пользователя.
  1.2 Стек Microsoft Windows. Поддерживаются только встроенные Bluetooth-адаптеры или внешние, присоединённые через интерфейс USB. Не поддерживается соединение Bluetooth через PCI, I^2C, Serial, PC Card и другие интерфейсы. Также поддерживается только один передатчик Bluetooth. Windows XP включает в себя встроенный Bluetooth стек, начиная с SP2.
  1.3 Toshiba. Toshiba лицензирует стек для других производителей оригинального оборудования (OEM) и поставляется вместе с некоторыми ноутбуками Fujitsu Siemens, ASUS, Dell и Sony. Для получения API производитель должен подписать соглашение о неразглашении. Стек от Toshiba поддерживает один из наиболее полных перечней профилей Bluetooth: SPP, DUN, FAX, LAP, OPP, FTP, HID, HDP, HCRP, PAN, BIP, HSP, HFP, A2DP, AVRCP.
2 Linux
  2.1 BlueZ. Стек BlueZ поддерживает все основные протоколы и уровни Bluetooth. Был первоначально разработан Qualcomm, и доступен для ядра Linux версии 2.4.6 и выше. Используется как низкоуровневыми утилитами (пакеты bluez-utils и bluez-firmware), так и более дружелюбными к пользователю программами (Blueman).
  2.2 Affix. Разработан Исследовательским центром Nokia (Nokia Research Center).
3 OS X. Содержит интегрированный Bluetooth-стек, начиная с версии 10.2. Включает профили DUN, SPP, FAX, HID, HSP, SYNC, PAN, BPP и OBEX. В версии 10.5 добавлена поддержка A2DP и AVRCP.

Для встроенных систем

1. BlueMagic. Стек BlueMagic 3.0 (Qualcomm) используется в iPhone от Apple и устройствах Qualcomm, таких как Motorola RAZR. Протокол BlueMagic также используется в продуктах Logitech, Samsung, LG, Sharp, Sagem, и многих других. BlueMagic 3.0 был первым полностью сертифицированным (все протоколы и профили) Bluetooth-стеком протоколов в спецификации 1.1.
2. lwBT. Облегченный протокол Bluetooth-стека для встраиваемых систем с открытым исходным кодом. Он действует как сетевой интерфейс для lwIP стека протоколов.
3. Bluetopia. Реализация от Stonestreet One для верхних слоёв протокола Bluetooth-стека выше интерфейса HCI и отвечает условиям версии 2.1+EDR и более ранним версиям спецификации Bluetooth. API обеспечивает доступ для всех протоколов верхнего уровня и профиля, может напрямую взаимодействовать с наиболее популярными Bluetooth чипами от Broadcom, TI и другими. Bluetopia была портирована на множество операционных систем, таких как Windows Mobile / Windows CE, Linux, QNX, Nucleus, uCOS, ThreadX, NetBSD, и другие. Bluetopia в настоящее время используется в устройствах таких компаний, как Motorola, Kodak, Honeywell, Garmin, VTech и Harris.
4. Стек Symbian OS встроен в соответствующую ОС. Все телефоны на базе платформы Nokia S60 и Sony Ericsson / Motorola платформы UIQ используют этот стек.

Профили Bluetooth

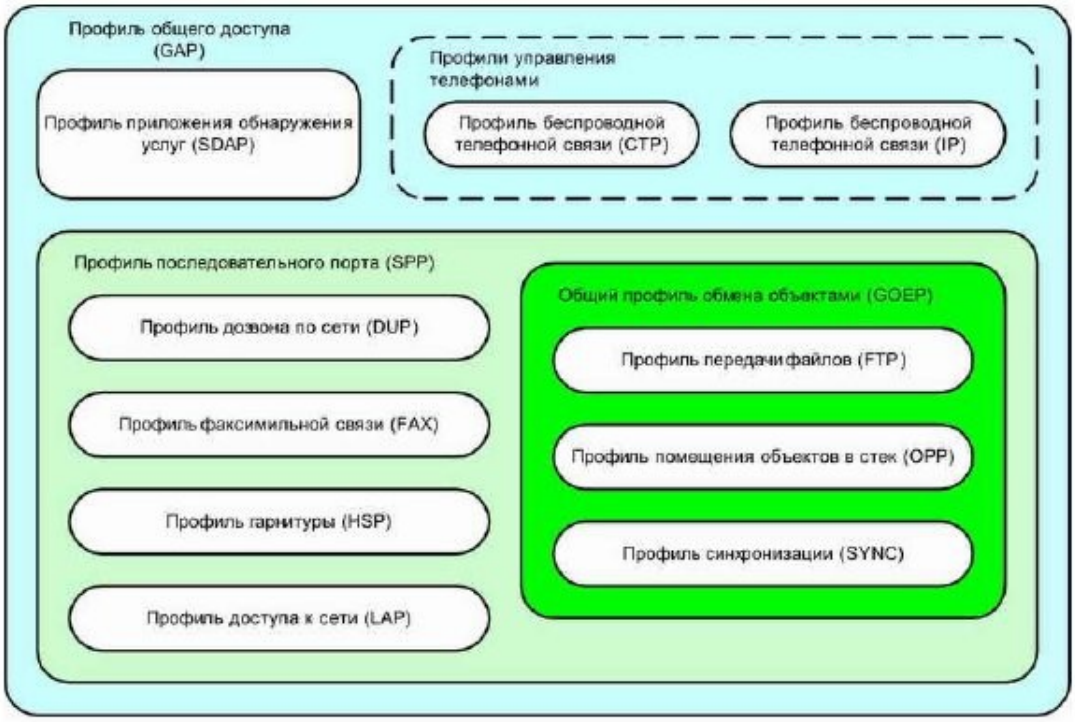
Профиль — набор функций или возможностей, доступных для определённого устройства Bluetooth. Для совместной работы Bluetooth-устройств необходимо, чтобы все они поддерживали общий профиль.

Технология Bluetooth определяет широкий диапазон профилей, которые описывают множество различных моделей применения. Профили определяют области возможного применения устройства Bluetooth.

Если устройства от различных производителей соответствуют одному профилю, определенному в спецификации Bluetooth, они смогут взаимодействовать друг с другом. Для всех моделей применения обязательно наличие профиля общего доступа (GAP), который сам по себе, однако, недостаточен для работы какого-либо реального устройства. Остальные профили добавляются в зависимости от назначения устройства и выполняемых им функций.

Три профиля общего назначения применяются для всех моделей применения, связанных с передачей данных. Это профиль последовательного порта (SPP), профиль приложения обнаружения услуг (SDAP) и профиль общего обмена объектами (GOEP).

В зависимости от назначения устройства к ним добавляются до девяти возможных профилей: DUP, FAX, HSP, LAP, FTP, OPP, SYNC, CTP и IP. Эти 13 профилей образуют основную конфигурацию профилей.



Ниже указаны некоторые профили, определенные и одобренные группой разработки Bluetooth SIG:

- Advanced Audio Distribution Profile (A2DP) — разработан для передачи двухканального стерео аудиопотока, например, музыки, к беспроводной гарнитуре или любому другому устройству. Профиль полностью поддерживает низкокомпрессированный кодек Sub_Band_Codec (SBC) и опционально поддерживает MPEG-1,2 аудио, MPEG-2,4 AAC и ATRAC, способен поддерживать кодеки, определённые производителем.
- A/V Remote Control Profile (AVRCP) — разработан для управления стандартными функциями телевизоров, Hi-Fi оборудования и прочего. То есть позволяет создавать устройства с функциями дистанционного управления. Может использоваться в связке с профилями A2DP или VDPT.
- Basic Imaging Profile (BIP) — разработан для пересылки изображений между устройствами и включает возможность изменения размера изображения и конвертирование в поддерживаемый формат принимающего устройства.
- Basic Printing Profile (BPP) — позволяет пересылать текст, сообщения электронной почты, vCard и другие элементы на принтер. Не требует от принтера специфических драйверов.
- Common ISDN Access Profile (CIP) — для доступа устройств к ISDN.
- Cordless Telephony Profile (CTP) — профиль беспроводной телефонии.
- Device ID Profile (DIP) — позволяет идентифицировать класс устройства, производителя, версию продукта.
- Dial-up Networking Profile (DUN) — протокол предоставляет стандартный доступ к Интернету или другому телефонному сервису через Bluetooth.
- File Transfer Profile (FTP_profile) — обеспечивает доступ к файловой системе устройства. Включает стандартный набор команд FTP, позволяющий получать список директорий, изменения директорий, получать, передавать и удалять файлы. В качестве транспорта используется OBEX, базируется на GOEP.

- General A/V Distribution Profile (GAVDP) — база для A2DP и VDP.
- Generic Access Profile (GAP) — база для всех остальных профилей.
- Hard Copy Cable Replacement Profile (HCRP) — предоставляет простую альтернативу кабельного соединения между устройством и принтером. Для принтера необходимы специфичные драйвера, что делает профиль неуниверсальным.
- Human Interface Device Profile (HID) — обеспечивает поддержку устройств с HID (Human Interface Device), таких как мыши, джойстики, клавиатуры и проч. Использует медленный канал, работает на пониженной мощности.
- Headset Profile (HSP) — используется для соединения беспроводной гарнитуры (Headset) и телефона. Поддерживает минимальный набор AT-команд GSM для обеспечения возможности совершать звонки, отвечать на звонки, завершать звонок, настраивать громкость.
- Intercom Profile (ICP) — обеспечивает голосовые звонки между Bluetooth-совместимыми устройствами.
- LAN Access Profile (LAP) — обеспечивает доступ Bluetooth-устройствам к вычислительным сетям LAN, WAN или Интернет посредством другого Bluetooth-устройства, которое имеет физическое подключение к этим сетям. Bluetooth-устройство использует PPP поверх RFCOMM для установки соединения. LAP также допускает создание ad-hoc Bluetooth-сетей.
- Personal Area Networking Profile (PAN) — позволяет использовать протокол Bluetooth Network Encapsulation в качестве транспорта через Bluetooth-соединение.
- Service Discovery Application Profile (SDAP) — используется для предоставления информации о профилях, которые использует устройство-сервер.
- SIM Access Profile (SAP, SIM) — позволяет получить доступ к SIM-карте телефона, что позволяет использовать одну SIM-карту для нескольких устройств.
- Video Distribution Profile (VDP) — позволяет передавать потоковое видео. Поддерживает H.263, стандарты MPEG-4 Visual Simple Profile, H.263 profiles 3, profile 8 поддерживаются опционально и не содержатся в спецификации.

Источники:

1. Bluetooth. https://ru.wikipedia.org
2. Стек Bluetooth. https://ru.wikipedia.org
3. Семёнов, Ю.А. Телекоммуникационные технологии. http://citforum.ru
4. Bluetooth в целом. http://www.rtcs.ru
5. Bluetooth - технология. http://www.gaw.ru

Беспроводные системы ПД

Лекция 08
Радиочастотная идентификация. RFID-метки

RFID (Radio Frequency IDentification, радиочастотная идентификация) — способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках.

Любая RFID-система состоит из считывающего устройства (считыватель, ридер или интеррогатор) и транспондера (RFID-метка или RFID-тег).

По дальности считывания RFID-системы можно подразделить на системы:
- ближней идентификации (считывание производится на расстоянии до 20 см);
- идентификации средней дальности (от 20 см до 5 м);
- дальней идентификации (от 5 м до 300 м)

Классификация RFID-меток

Способы систематизации RFID-меток и систем:
- По рабочей частоте
- По источнику питания
- По типу памяти
- По исполнению

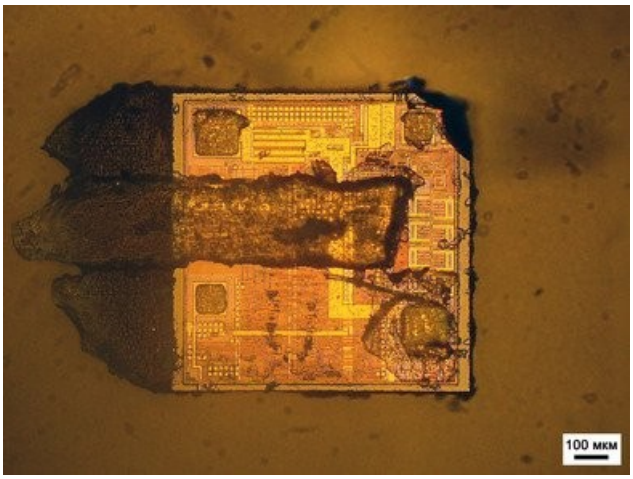
По типу источника питания RFID-метки делятся на:
- Пассивные
- Активные
- Полупассивные

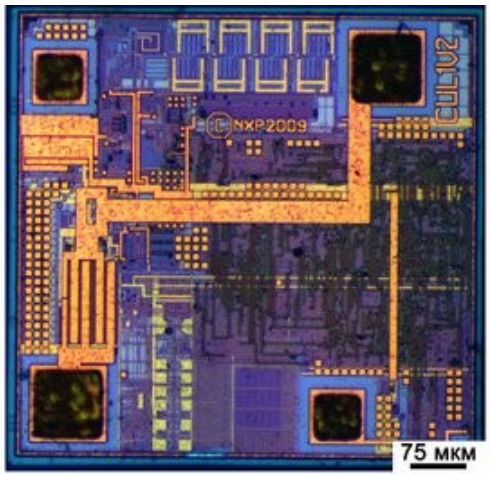
Пассивные RFID-метки

Пассивные RFID-метки не имеют встроенного источника энергии. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функционирования кремниевого КМОП-чипа, размещённого в метке, и передачи ответного сигнала.

Метки такого типа являются, самыми распространенными. Они применяются для создания стикеров для пометки товара в магазинах, для проездных БСК, для карт-ключей для прохода в здания.

Ниже крупнее показана микросхема.





В данном случае, это микрочип производства компании NXP (или по ее лицензии). Используется технология CUL1V2 — Circuit ULtralite 1 Version 2. Такие чипы выпускаются под торговой маркой MIFARE. Исходно MIFARE — это продукт компании Mikron (США). В 1998 она была куплена Philips, а в 2006 от Philips отделилась компания NXP Semiconductors. В зависимости от типа современные чипы MIFARE могут хранить до 8 кбайт памяти. Приведенный на фото чип содержит 192 байта памяти.

Размеры и форма антенны в разных RFID-метках могут отличаться. Именно от размера антенны зависят габариты RFID-меток.

Производством чипов для RFID занимаются различные компании. Помимо NXP это Hitachi, Alien Technology, SmartCode, Symbol Technologies. Существуют, и очень популярны из-за низкой стоимости, микрочипы китайского производства.

Современные технологии производства меток направлены на удешевление их производства. Например, техпроцесс FSA (Alien Tech.) позволяет производить свыше 2 миллионов чипов в час

Пассивные метки УВЧ и СВЧ диапазонов (860–960 МГц и 2,4–2,5 ГГц) передают сигнал методом модуляции отражённого сигнала несущей частоты (Backscattering Modulation — модуляция обратного рассеяния). Антенна считывателя излучает сигнал несущей частоты и принимает отражённый от метки модулированный сигнал. Пассивные метки ВЧ диапазона (13 МГц) передают сигнал методом модуляции нагрузки сигнала несущей частоты (Load Modulation — нагрузочная модуляция). Каждая метка имеет идентификационный номер. Пассивные метки могут содержать перезаписываемую энергонезависимую память EEPROM-типа. Дальность действия меток составляет 1–200 см (ВЧ-метки) и 1–10 метров (УВЧ и СВЧ-метки).

Наиболее массово производятся метки-наклейки на бумажной или пластиковой основе в рулонах, с которых метки отделяются вручную или с помощью аппликатора и наклеиваются на заданный объект.

Конструктивно метки представляют из себя электронный чип, закрепленный с помощью специального клея на контактных площадках металлизированной антенны. Форма антенны рассчитывается специально для удовлетворения оптимальных параметров согласования по радиосигналу с чипом метки и может принимать довольно разнообразные формы, хотя фактически большинство из них является «редуцированными» диполями, т. е., диполями по характеристикам излучения, но меньшими размерам, чем половина длины волны, что в этом диапазоне около 17 см. Антенны разных конфигураций имеют отличия в диаграммах направленности, энергоэффективности и «устойчивости» резонансной настройки антенны при ее размещении на разных объектах.

В среднем действует правило – чем меньше максимальный линейный размер метки, тем меньше ее «чувствительность» и дистанция регистрации, хотя между конкретными моделями меток сравнимого размера есть отличия.

Активные RFID-метки

Активные RFID-метки обладают собственным источником питания и не зависят от энергии считывателя, вследствие чего они читаются на дальнем расстоянии (до 300 м), имеют большие размеры, больший объем памяти и могут быть оснащены дополнительной электроникой. Однако, такие метки наиболее дороги, а у батарей ограничено время работы.

Практически все активные метки построены на основе однокристальных микроконтроллеров с встроенным или внешним радиочастотным приемопередатчиком с синтезатором частоты. Микроконтроллер может иметь дополнительные цифровые и аналоговые порты ввода-вывода (подключение датчиков, линий управления, кнопок), и часы реального времени.

Также активные метки конструктивно содержат антенну (на печатной плате метки или внешнюю, подсоединяемую через разъем), небольшое число согласующих элементов для соединения антенны с чипом, кварцевые генераторы радиочастотного синтезатора и часов реального времени, заменяемую или одноразовую батарею питания (обычный срок службы 1–5 лет, зависит от способа работы и емкости батареи).

В активных метках могут быть реализованы, в зависимости от назначения, разные способы и протоколы обмена со считывателями или другими метками, что определяется «прошитым» в микроконтроллер метки ПО. Для многих современных активных меток в качестве протокола радиоинтерфейса используется стандарт IEEE 802.15.4 (физический уровень низкоскоростных WPAN).

Активные метки в большинстве случаев более надёжны и обеспечивают самую высокую точность считывания на максимальном расстоянии. Активные метки, обладая собственным источником питания, также могут генерировать выходной сигнал большего уровня, чем пассивные, позволяя применять их в более агрессивных

для радиочастотного сигнала средах: воде (включая людей и животных, которые в основном состоят из воды), металлах (корабельные контейнеры, автомобили), для больших расстояний на воздухе. Большинство активных меток позволяет передать сигнал на расстояния в сотни метров при жизни батареи питания до 10 лет. Некоторые RFID-метки имеют встроенные сенсоры, например, для мониторинга температуры скоропортящихся товаров. Другие типы сенсоров в совокупности с активными метками могут применяться для измерения влажности, регистрации толчков/вибрации, света, радиации, температуры и газов в атмосфере (например, этилена).

Полупассивные RFID-метки

Полупассивные RFID-метки, также называемые полуактивными или «BAP» — Battery Assisted Passive, очень похожи на пассивные метки, но оснащены батареей, которая обеспечивает чип энергопитанием.
Постоянное питание чипа таких меток может несколько улучшать ее характеристики по дальности регистрации, но чаще дополнительное питание используется для встроенных датчиков (температуры, ускорения, влажности и т. п.). Батарея используется для питания датчиков и накопления данных при нахождении метки вне поля считывателя, с последующим их считыванием при входе в зону регистрации.

По типу используемой памяти RFID-метки делятся на:

- RO (Read Only) — данные записываются только один раз, сразу при изготовлении. Такие метки пригодны только для идентификации. Никакую новую информацию в них записать нельзя, и их практически невозможно подделать.
- WORM (Write Once Read Many) — кроме уникального идентификатора такие метки содержат блок однократно записываемой памяти, которую в дальнейшем можно многократно читать.
- RW (Read and Write) — такие метки содержат идентификатор и блок памяти для чтения/записи информации. Данные в них могут быть перезаписаны многократно.

По рабочей частоте

- Метки диапазона НЧ (LF — 125–134 кГц). Пассивные системы данного диапазона имеют низкие цены, и в связи с физическими характеристиками, используются для подкожных меток при чипировании животных, людей и рыб. Однако, в связи с длиной волны, существуют проблемы со считыванием на большие расстояния, а также проблемы, связанные с появлением коллизий при считывании.
- Метки диапазона ВЧ (HF — 13,56 МГц). Системы 13 МГц дешевы, не имеют экологических и лицензионных проблем, хорошо стандартизованы, имеют широкую линейку решений. Применяются в платежных системах, логистике, идентификации личности. Для частоты 13,56 МГц разработан стандарт ISO 14443 (виды A/B). Используются стандартизованные алгоритмы шифрования. Для существовавших в данном диапазоне частот стандартов были

найдены серьёзные проблемы в безопасности: например, совершенно отсутствовала криптография у дешёвых чипов карты Mifare Ultralight, позднее была взломана считавшаяся более надёжной карта Mifare Classic. Как и для диапазона LF, в системах, построенных в HF-диапазоне, существуют проблемы со считыванием на большие расстояния, считывание в условиях высокой влажности, наличия металла, а также проблемы, связанные с появлением коллизий при считывании.

- Метки диапазона УВЧ (UHF — 860–960 МГц). Метки данного диапазона обладают наибольшей дальностью регистрации, во многих стандартах данного диапазона присутствуют антиколлизионные механизмы. Ориентированные изначально для нужд складской и производственной логистики, метки диапазона UHF не имели уникального идентификатора. Предполагалось, что идентификатором для метки будет служить EPC-номер (Electronic Product Code) товара, который каждый производитель будет заносить в метку самостоятельно при производстве. Однако скоро стало ясно, что помимо функции носителя EPC-номера товара хорошо бы возложить на метку ещё и функцию контроля подлинности. То есть возникло требование, противоречащее самому себе: одновременно обеспечить уникальность метки и позволить производителю записывать произвольный EPC-номер. В 2008 году компания NXP выпустила два новых чипа SL3S1202 и SL3FCS1002 в стандарте EPC Gen 2.0. В них поле памяти TID (Tag ID), в которое при производстве обычно пишется код типа метки (и он в рамках одного артикула не отличается от метки к метке), разбито на две части. Первые 32 бита отведены под код производителя метки и её марку, а вторые 32 бита — под уникальный номер самого чипа. Поле TID — неизменяемое, и, таким образом, каждая метка является уникальной. Новые чипы имеют все преимущества меток стандарта Gen 2.0. Каждый банк памяти может быть защищен от чтения или записи паролем, EPC-номер может быть записан производителем товара в момент маркировки. В UHF RFID-системах по сравнению с LF и HF ниже стоимость меток, при этом выше стоимость прочего оборудования. В настоящее время частотный диапазон УВЧ открыт для свободного использования в Российской Федерации в так называемом «европейском» диапазоне — 863–868 МГц.

Стандарты RFID

Международные стандарты RFID, как составной части технологии автоматической идентификации, разрабатываются и принимаются международной организацией ISO совместно с IEC.

Организации-разработчики стандартов

- **EPCglobal** (совместное предприятие GS1 и GS1 US) работает по международным стандартам в области использования RFID, с целью создать возможность идентификации любого объекта в цепи поставок товаров компаний во всем мире.

- **AIM Global** — международная торговая ассоциация, представляющая поставщиков автоматической идентификации и мобильных технологий. Ассоциация активно поддерживает развитие AIM стандартов за счёт собственного технического комитета и группы экспертов RFID, а также через участие в промышленных, национальных (ANSI) и международных (ISO) группах разработок.
- **Ассоциация UNISCAN/GS1 Russia.**
- **GRIFS** (Global RFID Interoperability Forum for Standard) — проект по созданию Форума совместимости Стандартов RFID координируется GS1 совместно с ETSI. Проект финансируется Европейским сообществом. Начал свою деятельность в январе 2008 года.

Стандарт EPC Gen2

EPC Gen2 — сокращение от «EPCglobal Generation 2».

Electronic Product Code (EPC, Электронный код продукта) — торговая марка организации EPCglobal для набора совместимых технологий по бесконтактной маркировке товаров, в основном для целей логистики розничной торговли.

Технология предусматривает присвоение каждому товару уникального идентификатора по «принципу номерного знака». Физический уровень обмена данными основан на ISO/IEC 18000-63.

Стандарт EPC Gen2 (ISO/IEC 18000-63(C)) был разработан в 2004 и принят в 2006 как общепринятый протокол обмена между считывателями и метками УВЧ диапазона. На сегодня он является наиболее распространённым стандартом технологии RFID в УВЧ диапазоне.

Память меток стандарта Gen2 разделена на 4 банка, адресуемых соответствующими командами радиоинтерфейса:

1. Reserved Memory (00) используется для хранения:
- KILL-пароля (32 бита). При его ненулевом значении с помощью KILL-команды метка «убивается» навсегда и без возможности восстановления ее работы;
- ACCESS-пароля (32 бита). При его установке доступ к метке возможен только при знании этого пароля.
2. EPC (01, Electronic Product Code). Уникальный идентификатор метки, по которому метки отличаются друг от друга при их нахождении. Наиболее распространенная длина идентификатора 96 бит, хотя есть метки с 240 бит EPC (можно использовать меньше). «С завода» банк не защищен от записи и может быть перезаписан, а часто и должен быть перезаписан, т. к. метки могут быть с «пустым» EPC или у всех меток с одинаковым значением.
3. TID (10, Transponder ID). Идентифицирует производителя и модель чипа метки выделенным уникальным кодом. Также здесь может находиться дополнительный уникальный идентификатор каждой отдельной метки (Serialized TID), который может использоваться как средство защиты метки от подделки. EPC меток может быть продублирован, но банк TID защищается от

перезаписи при производстве метки и при наличии Serialized TID совместно с идентификатором производителя и чипа гарантировано уникален.

4. User Memory (11) – не обязательный, может отсутствовать. Используется для хранения любой информации. Если есть, то обычный размер от 32 до 512 бит. Есть модели и с большим объемом, но у них часты проблемы совместимости со считывателями.

Содержание банков EPC, User Memory и по отдельности областей KILL и ACCESS может быть защищено от изменения значения, временно или навсегда.

Особенности

- **ID.** Метки Gen 2 выпускаются как с записанным производителем номером, так и без него. Записанный производителем товара номер можно заблокировать так же, как и изначально встроенный.
- **Антиколлизионный механизм меток.** Современные метки стандарта Gen 2 используют эффективный антиколлизионный механизм, основанный на развитой технологии «слотов» — многосессионном управлении состоянием меток во время «инвентаризации» — считывании меток в зоне регистрации. Данный механизм позволяет увеличить скорость считывания-инвентаризации меток до 1500 меток/сек (запись — до 16 меток/сек) при использовании промышленных портальных считывателей. Считыватель и метки в начале запроса генерируют число q в диапазоне от 0 до 2 в степени n. Если число q считывателя и одной из меток совпало, то они производят обмен информацией. Если же количество отозвавшихся меток не равно единице, то считыватель производит новый запрос, при котором число q генерируется заново. В случае, если часто возникает ситуация, в которой не произошёл обмен информации с меткой (то есть если меток слишком много или слишком мало по сравнению с диапазоном, в котором лежит число q), считыватель корректирует степень двойки n, изменяя границы диапазона. Данный алгоритм работает гораздо быстрее алгоритма, используемого в Gen1, так как в первом случае считыватель побитно перебирает до 64-х бит, а во втором работает теория вероятности и имеется механизм регулировки.
- **Антиколлизионный механизм считывателей.** Gen 2 метки позволяют эффективно использовать в перекрывающихся и близких зонах несколько считывателей одновременно (Multiple Reader Mode) за счёт разнесения друг от друга частотных каналов считывателей.
- **Цена.** Метки Gen2 в настоящее время уже существенно дешевле меток предыдущего поколения, что также делает их использование предпочтительным, а оборудование (считыватели) первого поколения в большинстве случаев требуют для работы с новыми стандартами лишь перепрограммирования встроенной программы (перепрошивки).
- **Пароли.** Метки Gen2 обладают возможностью установки 32х-битного access-пароля. Кроме того, для каждой метки возможна установка «kill»-пароля, после введения которого метка навсегда прекращает обмен информацией со считывателями.

Считыватели RFID EPC Gen2:

Стационарный считыватель:

Стационарные считыватели самые производительные и обеспечивают максимальные скорости и дальности регистрации, что достигается за счет использования высокопроизводительных цифровых сигнальных процессоров, выделяющих слабый сигнал ответа метки на фоне несущей радиочастоты, шумов и помех.
У стационарных считывателей могут быть разные интерфейсы — RS232/485, USB, Wiegand, но «пром-стандартным» является UTP Ethernet.

У стационарных считывателей обычно от 2 до 8 разъемов для подключения антенн через встроенный коммутатор, т. е., одновременно работает только одна антенна. Переключение между антеннами происходит автоматически и довольно быстро, но настройками можно выбирать, какие антенны задействованы и индивидуально настраивать радиочастотные мощности для каждого выхода.
Также обычно все стационарные считыватели имеют специальный разъем с 4–8 цифровыми линиями для управления внешними устройствами — включением сигнальных ламп, открытием дверей, шлагбаумов, получения внешних сигналов — датчиков появления объектов, открытия дверей, и т. п.

Для программной интеграции считывателей в информационную систему или для связи с управляющим компьютером всеми производителями предоставляются SDK и API, а также готовое тестовое ПО, позволяющее проверить работу считывателя и подобрать настройки.
Последнее время все основные производители уже используют стандарт низкоуровневого протокола обмена со считывателем LLRP (Low Level Reader Protocol, стандарт ISO/IEC 24791-5), хотя все считыватели, к сожалению, имеют еще много индивидуальных особенностей, которые необходимо учитывать для достижения максимальной производительности и качества регистрации меток.

Портальные зоны регистрации

Портальные (воротные) зоны регистрации окружают антеннами, подключенными к стационарному считывателю, зону перемещения объектов с метками с боковых сторон и/или сверху. Например, регистрация меток товаров на провозимой паллете, меток персонала, проходящего через зону контроля, меток товаров, двигающихся по транспортерной ленте, меток книг, проносимых пользователями на выходе из библиотеки. Типичные размеры портальной зоны — до 3 метров в ширину и высоту.

В качестве антенн стандартно использование направленных антенн с круговой поляризацией, что необходимо для обеспечения регистрации меток в разных ориентациях. Возможно использование антенн с линейной поляризацией, что дает выигрыш по дистанции регистрации, но для этого нужна уверенность в постоянной

ориентации всех меток в зоне контроля, например, что все они всегда закреплены длинной стороной горизонтально.
Типичные одноэлементные патч-антенны имеют усиление около 8 дБ и характеристику направленности излучения по уровню 0,5 около ± 60º.

Потолочный считыватель:

В случаях, когда поток перемещения меток через зону регистрации небольшой и установка портального считывателя по бокам от прохода не желательна, возможно расположение антенн сверху. Бывают интегрированные потолочные считыватели, содержащие все в одном корпусе, включая считыватель и антенну.

Стационарные зоны считывания меток транспорта

Оптимальное расположение меток на автотранспорте — на лобовом стекле или на «торпеде» под ним, хотя также метки встраиваются в номерные знаки.
Регистрирующие антенны располагаются с направлением излучения вертикально вниз над центром полосы проезда, если предполагается двустороннее движение по полосе, либо под углом в сторону приближения автомобилей, что улучшает качество регистрации (но в другом направлении метки могут вообще не регистрироваться — тогда необходимо использовать пару антенн, «смотрящих» в разные стороны).

RFID-тоннель

При необходимости регистрации большого числа меток в небольшой зоне с линейными размерами менее метра оправдано использование тоннелей или боксов, содержащих антенны, окружающие зону регистрации с возможно большего числа сторон и направлений, и внешние экранирующие элементы, предотвращающие «паразитные» регистрации меток снаружи.

Еще одной эффективной областью применения RFID-тоннелей или боксов является регистрация меток на «сложных» объектах, содержащих воду, электролиты или большое число «вкраплений» металлов (например, при одновременной регистрации 200 меток на бирках ювелирных изделий в групповых упаковках).

В таких условиях считывание меток эффективно только в «ближней» зоне на расстоянии не больше 20–25 см от антенны. При этом для считывания более эффективно использование специальных «ближнепольных» петлевых антенн, а не патч-антенн.

Мобильные RFID-считыватели (терминалы)

В отличие от мобильных считывателей LF и HF (включая смартфоны с NFC), у которых дистанция регистрации меток составляет несколько сантиметров, мобильные Gen2 считыватели бывают с дистанцией регистрации до нескольких метров.
Возможна быстрая регистрация всех меток полки или вешалки с товарами, проходя мимо нее. Хотя скорость регистрации меток мобильными считывателями меньше, чем стационарными, обычно не более 10 уникальных меток в секунду.
Кроме RFID-считывателя в мобильных терминалах обычно есть сканер штрих кода, Wi-Fi, Bluetooth, и могут быть GPS/ГЛОНАС и GSM/3G модули.
Большая часть мобильных терминалов работает на Windows Mobile/CE, но появляются модели и на Android.
Мобильные терминалы обычно обладают хорошим классом защиты, позволяющим их использовать в производственных и уличных условиях.

Настольные считыватели

	Современные модели подключаются и питаются по USB и рассчитаны на считывание и запись небольшого числа меток с небольшого расстояния. Важны как сопутствующие считыватели для начальной привязки и нумерации меток, но могут выполнять и важную роль, например, на рабочем месте библиотекаря для быстрого оформления выдачи или приема сразу стопки книг с RFID-метками (и этот же считыватель используется для быстрой идентификации читателя по его пластиковой карте с меткой EPC Gen2).

Источники:

1. RFID. https://ru.wikipedia.org
2. Взгляд изнутри: RFID и другие метки. https://habrahabr.ru
3. RFID-технология. http://www.idexpert.ru

Беспроводные системы ПД

Лекция 09
Технология NFC

Near field communication (NFC) — технология беспроводной высокочастотной связи малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров. Анонсирована в 2004, когда Nokia, Philips (NXP Semiconductor) и Sony объявили о создании форума NFC с целью разработки и стандартизации интерфейса взаимодействия различных устройств, основанного на касании.

Центральная частота NFC равна 13,56 МГц. Скорость передачи данных достигает 424 кбит/с на расстоянии примерно 10 см. В отличие от существующих технологий бесконтактной связи на данном диапазоне частот, которые позволяют передавать информацию только от активного устройства пассивному, NFC обеспечивает обмен между двумя активными (равноправными) устройствами. Таким образом, NFC можно использовать для доступа к устройствам RFID.

NFC является расширением стандарта бесконтактных смарт-карт (ISO 14443) и соответственно обратно совместима с широко используемым стандартом смарт-карт на основе ISO/IEC 14443 A (например, Mifare) и ISO/IEC 14443 B, а также JIS X 6319-4 (FeliCa). Для обмена между двумя устройствами разработан новый протокол ECMA-340 и ISO/IEC 18092. Устройство NFC может поддерживать связь и с существующими смарт-картами, и со считывателями стандарта ISO 14443, и с другими устройствами NFC, и, таким образом, — совместимо с существующей инфраструктурой бесконтактных карт, уже использующейся в общественном транспорте и платежных системах. NFC нацелена прежде всего на использование в цифровых мобильных устройствах.

Для обеспечения совместимости между мобильным телефоном и картами RFID различных производителей необходимо выполнить тестирование цифрового протокола и провести измерение параметров РЧ-сигнала: временных характеристик, частоты несущей, амплитуды сигнала слушателя, а также амплитуды и чувствительности приемника в активном режиме.

Принцип работы

В основе NFC лежит индуктивная связь. Частота работы — 13,56 МГц, скорость передачи — 106 кбит/с (возможны 212 кбит/с и 424 кбит/с). Для передачи данных NFC использует два различных вида кодирования. Если активное устройство передает данные со скоростью 106 кбод, тогда используется модифицированный код Миллера со 100% АМн (ASK). Во всех других случаях используется манчестерское кодирование с коэффициентом АМн 10%.

Коэффициент АМн — основная характеристика амплитудной модуляции — отношение разности между максимальным и минимальным значениями амплитуд модулированного сигнала к сумме этих значений, выраженное в процентах $m = (A_{max} - A_{min})/(A_{max} + A_{min})$.

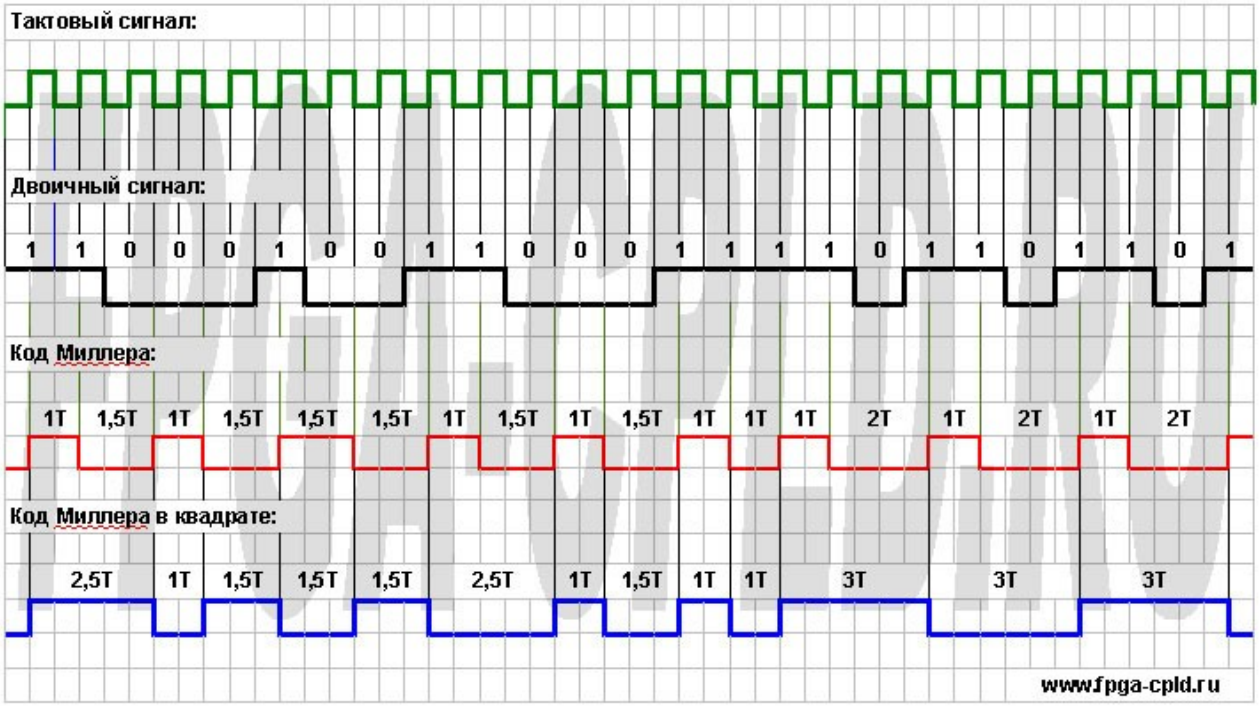
Код Миллера — Модифицированная Частотная Модуляция (МЧМ).

Данный код относится к классу трехканальных кодов, так как в нем используются три различных интервала для передачи бита относительно исходного сигнала — 1 (одинарный), 1,5 (полуторный) и 2 (двойной) .

При этом используется следующий алгоритм кодирования:

- 1 передается изменением полярности в середине тактового периода;
- при передаче последовательно двух нулей полярность меняется в конце тактового интервала;
- в комбинации 0 и следующая за ним 1 — полярность остается неизменной.

ДИАГРАММА СИГНАЛОВ КОДИРОВАНИЯ
ПО КОДУ МИЛЛЕРА и КОДУ МИЛЛЕРА В КВАДРАТЕ:



Основная особенность кода Миллера — использование импульсов одной и той же длительности для передачи различных символов. Импульсы тактовой длительности T передают и 0, и 1, а импульс 1,5T — символы 01 и 10. По этой причине могут возникать сбои в канале синхронизации, что ведет к появлению ошибок. Защита от таких сбоев основана на привязке синхроимпульсов к комбинации символов 101 — единственной, для которой выделен импульс 2T.

Недостатком кода Миллера является присутствие постоянной составляющей, при этом достаточно велик и низкочастотный компонент.

Отмеченный недостаток кода Миллера удалось преодолеть в модифицированном коде, названном Миллер в квадрате. В коде Миллера постоянная составляющая появляется при передаче четного числа единиц между двумя нулями. Модификация данного кода исправляет данный недостаток. В подобных комбинациях попросту вычеркивается последний перепад полярностей.

Сильной стороной кода Миллера и его модификации является высокая эффективность, хорошая способность к самосинхронизации. Однако надо учитывать, что за время, когда передается один символ исходной последовательности, надо принять решение — 0 это или 1, что приводит к снижению помехозащищенности, а следовательно для избежания этого надо расширять, как минимум вдвое, полосу частот.

При передаче информации пассивному устройству используется амплитудная манипуляция ASK. При обмене с активным устройством оба устройства равноправны. Каждое устройство имеет собственный источник питания, поэтому сигнал несущей отключается сразу после окончания передачи.

За счет индуктивной связи между опрашивающим и прослушивающим устройствами пассивное устройство влияет на активное. Изменение импеданса прослушивающего устройства вызывает изменение амплитуды или фазы напряжения на антенне опрашивающего устройства, которое он обнаруживает.

Электрический импеданс (комплексное сопротивление, полное сопротивление) — это комплексное сопротивление двухполюсника для гармонического сигнала. Импеданс — это аналог понятия сопротивления для постоянного тока в приложении к синусоидальному току.

Этот механизм называется модуляцией нагрузки. Она выполняется в режиме прослушивания с применением вспомогательной несущей 848 кГц. В зависимости от стандарта применяется амплитудная (ASK для 14443 A) или фазовая манипуляция (BPSK для 14443 B). Еще один пассивный режим, совместимый с FeliCa, осуществляется без вспомогательной поднесущей с манипуляцией АМн (ASK) на частоте 13,56 МГц.

Режимы работы

В NFC определено три основных режима работы:

- Пассивный (эмуляция смарт-карты). Пассивное устройство ведет себя как бесконтактная карта одного из существующих стандартов.
- Передача между равноправными устройствами. Производится обмен между двумя устройствами. При этом за счет собственного источника питания у прослушивающего устройства можно использовать NFC даже при выключенном питании опрашивающего устройства.
- Активный режим (чтение или запись).

В каждом режиме может применяться один из трех способов передачи: NFC-A (14443 A), NFC-B (14443 B), NFC-F (JIS X 6319-4). Для распознавания способа передачи инициирующее устройство посылает запрос.

Стандарт	Тип устройства	Кодирование	Модуляция	Скорость ПД, кб/с	Несущая, МГц
NFC-A	Опрашивающее	Модиф. код Миллера	ASK 100%	106	13,56
	Прослушивающее	Манчестер	ASK	106	13,56±848 кГц
NFC-B	Опрашивающее	NRZ-L	ASK 10%	106	13,56
	Прослушивающее	NRZ-L	BPSK	106	13,56±848 кГц

NFC-F	Опрашивающее	Манчестер	ASK 10%	212/424	13,56
	Прослушивающее	Манчестер	ASK	212/424	13,56 (без поднесущей)

В пассивном режиме используются метки NFC — пассивные устройства, предназначенные для обмена с активными NFC-устройствами. Как и метки RFID, метки NFC применяются для хранения небольшого количества данных. Всего определено 4 типа меток.

Тип	**1**	**2**	**3**	**4**
Стандарт	14443 A	14443 B	JIS 6319-4	14443 A/B
Совместимый продукт	Innovision Topaz	NXP Mifare	Sony FeliCa	NXP DESFire, SmartMX-JCOP, др.
Скорость ПД, кб/с	106	106	212, 424	106, 212, 424
Объем памяти	96 б, расширение до 2 кб	48 б, расширение до 2 кб	До 1 Мб	До 32 кб
Защита от коллизий	Нет	Есть	Есть	Есть

Использование

Сам по себе интерфейс NFC не дает никаких реальных практических сценариев использования или решений. В отличие, например, от Bluetooth, профили которого четко описывают, как передать файл, как подключить гарнитуру или обеспечить сетевой доступ, NFC является только базой, а непосредственные сценарии работы обеспечиваются дополнительным программным обеспечением, которое работает через него. С одной стороны, это открывает широкие возможности для разработчиков, а с другой — является для них же проблемой при обеспечении взаимодействия разных приложений и устройств.

Для устранения неопределенности Форум NFC предлагает стандартизировать протоколы для определенных сценариев (в частности NDEF — для хранения коротких сообщений на метках; SNEP — Simple NDEF Exchange Protocol — для обмена информацией между устройствами), однако практическое определение совместимости конкретных устройств обычно затруднено отсутствием детальной информации от производителя и средств диагностики. Еще одним помощником выступает здесь компания Google, которая предложила в последних версиях Android собственную разработку Android Beam. Она позволяет обмениваться некоторыми типами информации между совместимыми устройствами.

Источники:

1. Near Field Communication. https://ru.wikipedia.org
2. Технология NFC в смартфонах и ее практическое использование. http://www.ixbt.com
3. Технология NFC — связь на близком расстоянии. http://www.russianelectronics.ru

Беспроводные системы ПД

Лекция 10
Семейство протоколов ИК передачи данных
Infra red Data Assotiation

InfraRed Data Association — IrDA — ИК-порт — группа стандартов, описывающая протоколы физического и логического уровня передачи данных с использованием инфракрасного диапазона световых волн в качестве среды передачи. Является разновидностью оптической линии связи ближнего радиуса действия.

В 1993 году на общепромышленном совещании, организованном компанией Hewlett-Packard был сформирован консорциум всех ведущих компаний, названный *Ассоциацией инфракрасной передачи данных*. В июне 1994 года была объявлена первая одноименная версия стандарта, включающая физический и программный протоколы — IrDA 1.0.

Протокол IrDA позволяет соединяться с периферийным оборудованием без кабеля при помощи ИК-излучения в диапазоне 850–900 нм с "пиком" на длине волны 880 нм. Порт IrDA позволяет устанавливать связь на коротком расстоянии до 1 метра в режиме точка-точка. Интерфейс имеет малую можность потребления. Для создания такого оборудования и его использования сертификация не требуется.

IrDA широко использовался в 1990–2000 годах: мобильные телефоны, ноутбуки, КПК. Реже — принтеры и цифровые фотоаппараты. Очень редко ИК-порт ставился на стационарные ПК — обычно в виде платы расширения. В данное время практически вытеснена радиоинтерфейсами, например Bluetooth.

Основные причины отказа от IrDA:

- Усложнение сборки корпусов устройств, в которых монтировалось ИК-прозрачное окно.
- Ограниченная дальность действия и требования прямой видимости пары приёмник-передатчик.
- Относительно низкая скорость передачи данных первых реализаций стандарта. В последующих ревизиях стандарта этот недостаток исправили, однако широкого распространения скоростные варианты IrDA получить уже не успели.

Реализация и архитектура

Аппаратная реализация, как правило, представляет собой пару из излучателя, в виде ИК светодиода, и приёмника, в виде фотодиода расположенных на каждой из сторон линии связи. Наличие и передатчика и приёмника на каждой из сторон является необходимым для использования протоколов двусторонней передачи данных.

В ряде случаев, например при использовании в пультах дистанционного управления бытовой техникой, одна из сторон может быть оснащена только передатчиком, а другая только приёмником. Иногда устройства оснащают несколькими приёмниками,

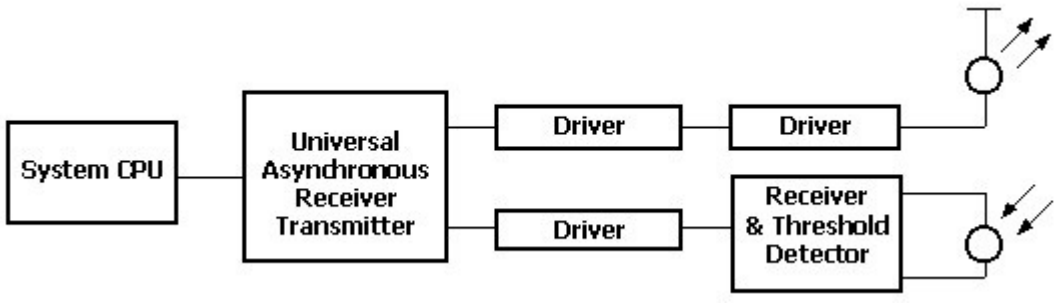
что позволяет одновременно поддерживать связь с несколькими устройствами. Использование при этом одного передатчика возможно благодаря тому, что протоколы логического уровня требуют лишь незначительного обратного трафика для обеспечения гарантированной доставки данных. Наличие нескольких передатчиков встречается гораздо реже.

Большинство оптических сенсоров, используемых в фото и видео камерах, имеет диапазон чувствительности гораздо шире видимой части спектра. Благодаря этому работающий ИК передатчик можно увидеть на экране или фотоснимке в виде яркого пятна.

В общем виде схема организации IrDA-канала выглядит примерно так, как показано на рис:

Канал ПД состоит из двух основных элементов: микросхемы, обеспечивающей модуляцию и демодуляцию поступающего двоичного сигнала согласно определенного алгоритма, и ИК приемно-передающего модуля.

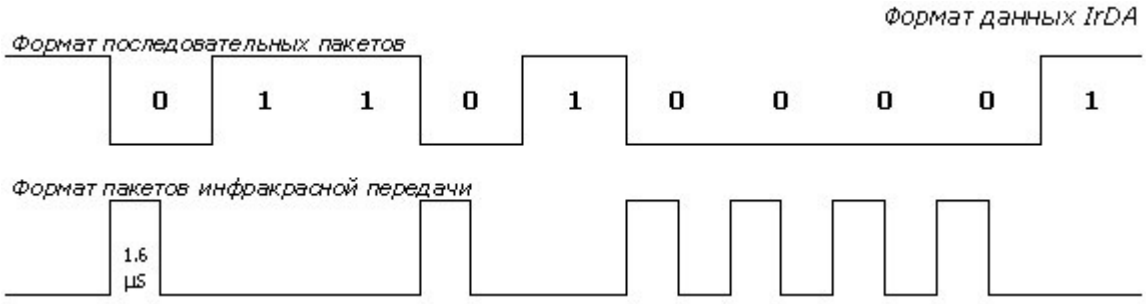
Сам порт IrDA основан на архитектуре коммуникационного COM-порта ПК, который использует универсальный асинхронный приемо-передатчик UART (Universal Asynchronous Receiver Transmitter) и работает со скоростью передачи данных 2400–115200 bps.



Связь в IrDA полудуплексная, т. к. передаваемый ИК-луч неизбежно засвечивает соседний усилитель приемника. Воздушный промежуток между устройствами позволяет принять ИК-энергию только от одного источника в данный момент.

Передающая часть

Байт, который требуется передать, посылается в блок UART из CPU командой записи ввода-вывода. UART добавляет старт-стоп биты и передает символ последовательно, начиная с младшего значения бита. Стандарт IrDA требует, чтобы все последовательные биты кодировались таким образом: логический "0" передается одиночным ИК-импульсом длиной от 1,6 мс до 3/16 периода передачи битовой ячейки, а логическая "1" передается как отсутствие ИК-импульса. Минимальная мощность потребления гарантируется при фиксированной длине импульса 1,6 мс.



По окончании кодирования битов необходимо возбудить один или несколько ИК-светодиодов током соответствующего уровня, чтобы выработать ИК-импульс требуемой интенсивности. ИК-светодиод должен иметь длину волны 880 нм. Радиальная чувствительность приемника и длины связи диктуются, исходя из требований самой спецификации IrDA.

Приемная часть

Переданные ИК-импульсы поступают на PIN-диод, преобразующий импульсы света в токовые импульсы, которые усиливаются, фильтруются и сравниваются с пороговым уровнем для преобразования в логические уровни. ИК-импульс в активном состоянии генерирует "0", при отсутствии света генерируется логическая "1". Протокол IrDA требует, чтобы приемник точно улавливал ИК-импульсы мощностью от 4 мВт/см^2 до 500 мВт/см^2 в угловом диапазоне ±15°.

PIN-диод — разновидность диода, в котором между областями электронной (n) и дырочной (p) проводимости находится собственный (нелегированный — intrinsic) полупроводник (i-область). Характерные качества pin-диода проявляются при работе в режиме сильной инжекции, когда i-область заполняется носителями заряда из сильнолегированных n+ и p+ областей, к которым прикладывается прямое смещение напряжения. pin-диод функционально можно сравнить с ведром воды с отверстием сбоку: как только ведро наполняется до уровня отверстия, оно начинает протекать. Точно так же и диод начинает пропускать ток, как только заполнится носителями заряда i-область.

Помехи

Для ИК-излучения существует два источника интерференции (помех), основным из которых является солнечный свет. Однако, в солнечном свете преобладает постоянная составляющая, а правильно спроектированные приемники должны компенсировать большие постоянные токи через PIN-диод. Другой источник помех — флуоресцентные лампы общего освещения. Хорошо спроектированные приемники должны иметь полосовой фильтр для снижения влияния таких источников помех. Вероятность ошибок связи будет зависеть от правильного выбора мощности

передатчика и чувствительности приемника. В IrDA выбраны значения, гарантирующие, что описанные выше помехи не будут влиять на качество связи.

Семейство протоколов IrDA

IrPHY (Infrared Physical Layer Specification) *— обязательный протокол самого низкого уровня среди спецификаций IrDA. Соответствует физическому уровню сетевой модели OSI.*

Основные характеристики спецификации IrPHY:

- Дальность: ≤ 1 м.
- Мин. отклонение от оси приёмника/передатчика: 15°.
- Скорость ПД: от 2.4 кбит/с до 16 Мбит/с.
- Модуляция: немодулированный сигнал, без несущей.
- Волновой диапазон: от 850–900 нанометров.
- Режим передачи данных: полудуплексный.

Спецификация этого протокола устанавливает стандарты для Ir-трансиверов, методов модуляции и схемы кодирования/декодирования, а также ряд физических параметров. Для стандарта IrDA (115,2 kbps) схема кодирования аналогична используемой в традиционной UART: бит старта ("0") и стоп-бит ("1") добавляются перед и после каждого байта соответственно. Но вместо схемы NZR (Non-Return to Zero) используется кодировка, подобная RZ (Return to Zero), т. е. двоичный "0" кодируется единичным импульсом, а "1" — его отсутствием. Кадры отделяются друг от друга байтами Escape-последовательности, содержащимися в теле самого кадра. Для определения ошибок используется 16bit циклическая контрольная сумма. В стандарте IrDA 1.1 для протокола обмена 1,152 Mbps и 4 Mbps старт-бит и стоп-бит не применяются.

Кадры, получаемые от более высокоуровневого протокола IrLAP, вкладываются в поле данных кадров SIR, согласно используемому методу кодирования. Стандарт не содержит обязательных вариантов реализации этой процедуры и допускает варьирование алгоритмов в зависимости от возможностей конкретного оборудования.

Спецификация не определяет максимальных допустимых значений для таких параметров как дальность или отклонение от оси, тем не менее, типичное расположение устройств для организации соединения подразумевает расстояние от 5 до 50 сантиметров на одной оси. Устройства с односторонней связью (например пульт ДУ и телевизор), как правило, поддерживают дальность не менее 10 метров.

Скорости передачи данных делятся на несколько поддиапазонов — SIR, MIR, FIR, VFIR, UFIR каждый из которых характеризуется не только разными скоростями но и использованием различных кодовых схем.

SIR — Serial Infrared использует те же скорости ПД, что и RS-232: 9,6; 19,2; 38,4; 57,6; 115,2 кбит/с. Скорости выбраны специально для простоты реализации COM-IrDA адаптеров.

Как правило наименьшая доступная скорость для устройств составляет именно 9,6 кбит/с. Именно она используется для передачи сигналов поиска, оповещения и сопряжения.

MIR — Medium Infrared — поддерживает скорости ПД 0,576 и 1,152 Мбит/с.

MIR не является официальным термином IrDA, однако то, что схема кодирования, используемая для этих скоростей, отлична как от SIR так и от FIR, делает этот термин довольно удобным и распространённым.

FIR — Fast Infrared — устаревший термин спецификации IrDA, ранее использовавшийся для обозначения устройств, поддерживающих скорость передачи данных от 9600 бит/с до 4 Мбит/с, что включает в себя и SIR и MIR. В наше время, как правило, термин FIR используется для обозначения скорости 4 Мбит/с. Некоторые источники используют термин FIR для обозначения всех скоростей, превышающих SIR.

VFIR — Very Fast Infrared — термин использующийся для обозначения поддержки скоростей передачи вплоть до 16 Мбит/с. На данный момент, 16 Мбит/с это самая высокая скорость передачи данных по IrDA, поддерживаемая серийными устройствами.

UFIR — Ultra Fast Infrared — в состоянии разработки, теоретически поддержка скорости вплоть до 100 Мбит/с.

IrLAP (Infrared Link Access Protocol) — обязательный протокол второго уровня, располагается поверх IrPHY, соответствует канальному уровню сетевой модели OSI.

IrLAP отвечает за:

- Контроль доступа.
- Поиск расположенных вблизи устройств.
- Установление и поддержку двунаправленного соединения.
- Распределение первичной и вторичной ролей среди устройств.

ИК технология поддерживает только однонаправленную передачу информации, поэтому, в следствие полудуплексной природы SIR, IrLAP использует архитектуру с одним главным (первичным) и множественными подчиненными (вторичными) устройствами. Схема обращения устройств представляет собой обычный протокол обмена данными, где есть фазы запросов (Request) и ответов (Response). Первичное устройство отвечает за организацию соединения, обработку ошибок, и посланные им кадры называются управляющими (Command Frames), а кадры вторичных устройств именуются ответными (Response Frames). Обмен информацией идет только с первичным устройством, которое всегда выступает инициатором соединения, однако его роль может играть любое из устройств, поддерживающих необходимые для этого функции. Опционально может быть включен протокол транспортного уровня,

позволяющий осуществлять контроль передачи между приложениями в случае одновременной работы нескольких приложений на одной физической линии.

Устройства, соответствующие стандарту IrDA, перед началом передачи должны в первую очередь попытаться выявить нет ли в ближайшей окрестности активности в ИК-диапазоне, т. е. установить не ведется ли какая-либо передача в пределах его досягаемости. Если такая активность обнаружена, то программе, выдающей запрос, посылается соответствующее сообщение, а сам блок откладывает передачу. Поскольку оба соединяющихся устройства могут быть компьютерами, то любое из них может быть ведущим. Выбор зависит от того, какое устройство первым проявит инициативу.

Каждое устройство имеет 32-битный адрес, вырабатываемый случайным образом при установлении соединения. Каждому кадру в пределах соединения ведущее устройство при старте присваивает 7-битный адрес соединения. Для возможных, но нежелательных случаев, когда два устройства имеют одинаковый адрес, предусмотрен такой механизм, когда ведущее устройство дает команду всем подчиненным устройствам изменить их адреса. В процессе установления связи два устройства "договариваются" о максимальной скорости, с которой они оба могут работать. Все первичные передачи, выполняемые до фазы переговоров, по умолчанию ведутся на скорости 9,6 kbps.

Максимальный квант передачи может быть равен 100, 200 или 500 мс. Он представляет собой максимальное время, в течение которого устройство передает данные до того, как перейдет к прослушиванию подтверждения приема и зависит от скорости передачи, емкости буфера в принимающем устройстве. Минимальная длительность передачи определяется неспособностью передающего устройства перейти к приему данных сразу после выдачи последнего бита, поскольку усилитель PIN-диода в передающем устройстве входит в состояние насыщения от собственной передачи. Время восстановления приемника — переменная величина, составляющая 0,001–10 мс. Этот параметр для данного устройства должен быть заранее известен и учитывается в фазе переговоров об установлении соединения. Процедуры расширенного восстановления включают в себя функцию сброса, которая прерывает связь, но потом восстанавливает активное состояние с параметрами соединения по умолчанию.

Стандартом предусмотрено два основных состояния:

- NRM (Normal Response Mode) — это состояние соединения с распределенными ролями первичного и вторичных устройств.
- NDM (Normal Disconnect Mode) — предусматривает функции детектирования доступных устройств, сбор информации о них, разрешение адресных конфликтов, а также позволяет передавать данные широковещательно, без установления соединения.

В протоколе IrLAP используется три типа кадров по аналогии с HDLC. Поле данных присутствует только у первого и последнего вида кадров, оно не ограничено по длине, но число бит в нем должно быть кратно 8. Ненумерованные (U-кадры) используются для установления связи: операции соединения и разъединения, информирования об ошибках и передачи данных, если нет необходимости в нумерации

последовательностей. Информационные (I-кадры) используются для передачи информации и предназначены для передачи данных. Их командное поле содержит номер кадра в последовательности, помогающей принимающему устройству отслеживать нарушения очередности. Нумерация организована так, что служит одновременно средством подтверждения приема: S- и I-кадры могут нести номер пакета, который ожидается на входе устройства-отправителя. Счетчик позволяет идентифицировать только 8 кадров, таким образом, номер следующего ожидаемого приемником пакета может высылаться не с каждым кадром, а только по получении нескольких промежуточных пакетов. Величина, определяющая их количество, называется размером окна. Четвертый бит контрольного поля у кадра, сгенерированного первичным устройством, означает запрос данных, а в ответном кадре он играет роль конечного бита, сигнализирующего о завершении передачи. Супервизорные (S-кадры) используются для функций handshaking (процедура договора устройств о параметрах синхронизации).

Договариваясь о соединении, устройства обмениваются информацией о скорости, максимальной и минимальной длительности цикла, максимальной величине кадра, размере окна, количестве дополнительных флагов BOF (Beginning Of Frame) и пороговом времени разрыва соединения (промежуток, в течение которого не было принято ни одного корректного кадра). *Под максимальным циклом (maximum turn-around time) подразумевается отрезок времени, по истечении которого устройство должно установить в своем кадре конечный бит, а под минимальным — длительность паузы, начиная с момента отсылки последнего байта последнего кадра, запрошенного передающим устройством, чтобы подготовиться к приему данных.* BOF выполняет роль задержки перед посылкой очередного кадра устройствам с большей задержкой. Предусмотрена команда смены ролей XCHG, позволяющая передавать право называться первичным устройством, как эстафету. Для проверки правильности передачи кадра к нему в конце дописывается полеконтрольной суммы FCS (Frame Check Sequence).

Протокол IrLAP устанавливает правила доступа к ИК-среде, процедуры открытия канала, согласование абонентов сети, обмена информацией и т.д. Хотя IrLAP и обязательный уровень IrDA, но не все его особенности являются таковыми. Любая станция, не принимающая в данный момент времени участия в обмене, перед тем как начать передачу, должна прослушивать канал не менее 500 мс, чтобы убедиться в отсутствии трафика. С другой стороны, станция, участвующая в обмене, должна вести передачу не более 500 мс. Доступ к среде передачи регулируется посредством специального бита PF (Poll/Final), который устанавливается в теле кадра. IrLAP допускает передачи без установления предварительного соединения. По своей природе такая передача является широковещательной и не требует получения подтверждения станции получателя. Процедура открытия канала в этом случае предусматривает обмен идентификационной информацией (ID). Инициатор широковещательного обмена передает ID предопределенное количество раз и прослушивает канал в интервалах между ссылками (слот, Slot). Станция-получатель случайным образом выбирает слот и посылает в ответ свой ID. При обнаружении коллизии процедура повторяется и применяется для согласования операционных параметров станций (скорость посылки бит, максимальная длина пакета). При установлении соединения обмен данными, объем которых не должен превышать 64

байта, осуществляется со скоростью 9,6 kbps. После того, как соединение установлено, скорость обмена и величина пакета данных могут быть по "договоренности" увеличены до максимальных. Кроме пакетов с пользовательскими данными, в обмене участвуют специальные, служащие для управления потоком, коррекции ошибок и передачи маркера. Связь может осуществляться в режиме "1:1" или "1:n". В процессе обмена одна станция является первичной, а остальные — вторичными. Помимо описанных процедур существуют и другие: разрешение конфликтов адресов, изменение роли станции "первичная-вторичная" и т.д.

IrLMP — Infrared Link Management Protocol — обязательный протокол третьего уровня. Соответствует сетевому уровню сетевой модели OSI.

Каждое устройство IrDA содержит таблицу сервисов и протоколов, доступных в настоящий момент. Эта информация может запрашиваться у других устройств. Мультиплексор администратора соединений и его схема управления позволяют нескольким приложениям обмениваться данными по одному физическому соединению.

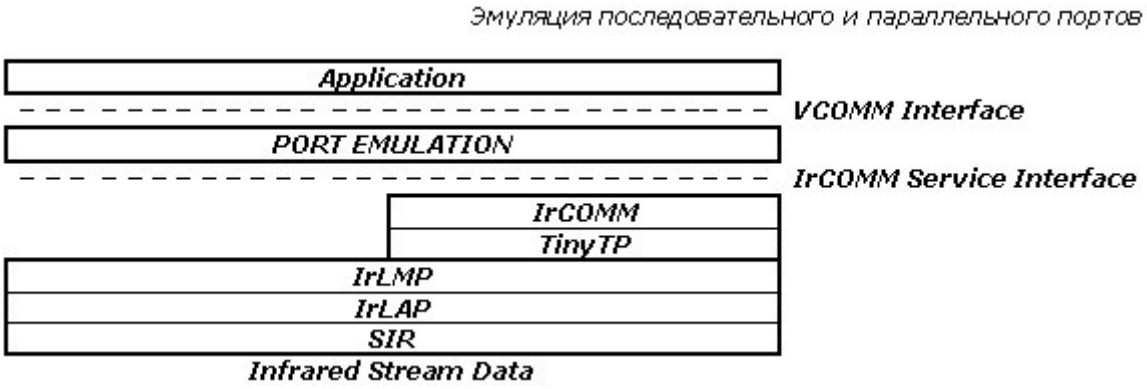
Состоит из двух подуровней:

1. LM-MUX (Link Management Multiplexer) — выполняет мультиплексирование каналов поверх одного соединения, устанавливаемого протоколом IrLAP. С этой целью в Ir-станции определяется множество точек доступа канала — LSAP (Link Service Access Point) — каждая с уникальным идентификатором. Таким образом каждое из LSAP-соединений определяет логически различные информационные потоки. Протокол LM-MUX обеспечивает передачу данных между точками доступа как внутри одной, так и между другими станциями. Он может работать в одном из двух режимах: эксклюзивном (активизируется только одно соединение LSAP и все ресурсы отдаются одному приложению) и мультиплексивном (несколько соединений LSAP могут разделять один канал IrLAP). В этом случае управление потоком должно быть обеспечено протоколами верхнего уровня или непосредственно приложением. Каждое виртуальное соединение представлено своей LSAP, таким образом, связь происходит на уровне двух LSAP (LSAP Connection). Также предусмотрено три варианта доступа: с установлением предварительного соединения, без установления предварительного соединения (Connectionless) и режим сбора информации о возможностях, сервисах и приложениях удаленного устройства (XID_Discovery).
2. LM-IAS (Link Management Information Access Service) — управляет информационной базой так, что станции могут запросить, какие службы предоставляются. Эта информация хранится как ряд объектов, с каждым из которых связан набор атрибутов.

Прочие протоколы

Tiny TP (Tiny Transport Protocol) — протокол, основанный на базе IrLMP. Позволяет передавать большие массивы данных и управлять потоком данных, расставляя приоритеты каждому логическому каналу.

IrCOMM (Infrared Communications Protocol) — протокол, который позволяет использовать ИК-соединение в качестве последовательного или параллельного порта, основанного на четырех типах сервиса: 3-Wire Raw, 3-Wire, 9-Wire и Centronics. Первый работает только через одно эксклюзивное соединение и используется, когда необходимо передавать исключительно данные. Второй эмулирует параллельную передачу по трем каналам (Signal Common, TD, RD), используя возможности TinyTP, Девятипроводный предназначен для эмуляции последовательных портов и обрабатывает, помимо трех вышеупомянутых, еще шесть сигналов (RTS, CTS, DSR, DTR, CD, RI). Centronics — это виртуальный параллельный интерфейс на базе TinyTP).



IrOBEX (Infrared Object Exchange) — протокол, основанный на базе Tiny TP. Обеспечивает возможность обмена произвольными объектами данных: контактами, событиями календаря и даже исполняемыми приложениями.

IrLAN (Infrared Local Area Network) — протокол, позволяющий подключиться к LAN-сети через IrDA-соединение одним из трёх способов: как точка доступа, одноранговая связь peer-to-peer, или в качестве хоста.

Источники:

1. Infrared Data Association. https://ru.wikipedia.org
2. Инфракрасный протокол связи — IrDA / М. Лень. http://www.ixbt.com
3. Реализация инфракрасной связи. https://msdn.microsoft.com
4. IrDA. http://www.gaw.ru

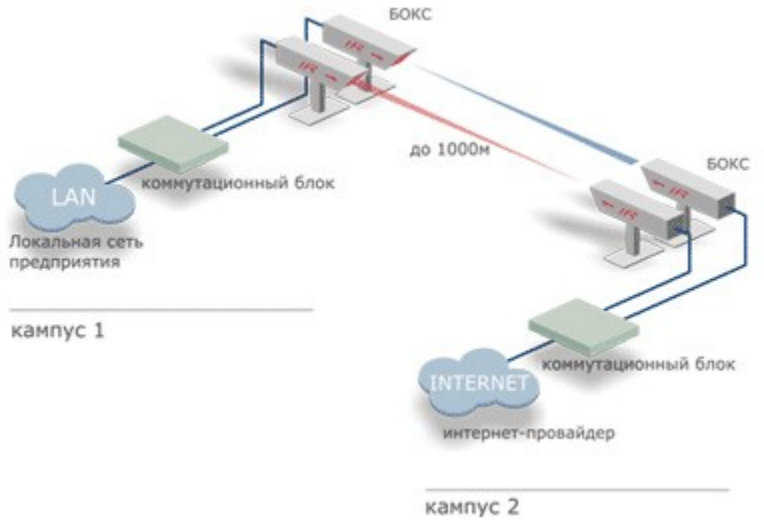
Беспроводные системы ПД

Лекция 11
Атмосферная оптическая линия связи

Атмосферная оптическая линия связи (АОЛС) — Free Space Optics (FSO) — Wireless Optics (WO) — вид оптической связи, использующий электромагнитные волны оптического (как правило ИК) диапазона, передаваемые через атмосферу. Английский термин также включает в себя передачу данных через вакуум.

Назначение оптических сетей – соединить беспроводным способом две точки в сеть и передавать данные на высокой скорости между ними. Существует множество вариантов использования АОЛС:

- создание локальной сети доступа к Интернету;
- построение «последней мили» в сетях широкополосного доступа;
- телефония — соединение телефонных станций;
- соединение центров обработки данных для передачи информации;
- соединение серверов с автоматически управляемыми производственными комплексами на предприятиях;
- соединение серверов видеонаблюдения с конечной видеоаппаратурой (в т.ч. HDTV);
- соединение БС в сетях мобильной связи и т. д.



<u>Принцип работы АОЛС</u>

В основе АОЛС лежит передача ИК излучения через атмосферу — информация передается модулированным излучением в ИК части спектра. Благодаря такой оптической системе данные (текстовые файлы, музыка, видео и аудио) передаются посредством лазерной связи, без кабелей. В отличие от других беспроводных технологий, АОЛС использует те частоты, на которые не требуется разрешение (~400 ТГц).

Данные поступают в приемопередающий модуль, где происходит кодирование информации, фокусировка оптической системой в узкий лазерный луч и непосредственно передача. На другой части линии связи стоит принимающая оптическая система, которая фокусирует оптический сигнал на высокочувствительный фотодиод и преобразовывает его в электрический сигнал. Чем выше частота, тем больше объем передаваемой информации.
Длина волны в большинстве реализованных систем варьируется в пределах 700–950 нм или 1550 нм, в зависимости от применяемого лазерного диода.

Ключевой принцип АОЛС основан на компромиссе: чем большую продолжительность простоев вследствие неблагоприятных погодных условий (туманов) допускает заказчик, тем протяженнее будет канал связи.

Преимущества АОЛС:

- использование частот, не требующих лицензирования;
- оптические системы не чувствительны к электромагнитному шуму;
- системы не создают помех для радиооборудования (поэтому для их построения не нужно разрешений и согласований с уже установленным оборудованием);
- не создают помех друг для друга (благодаря чему их можно использовать в густонаселенных районах, устанавливая оборудование в непосредственной близости друг от друга);
- простота монтажа, небольшие габариты оборудования (единственный важный момент в том, что крепиться оборудование должно к неподвижным, прочным опорам – многоэтажки, сварные стальные конструкции и т.п. Просто поднять антенну повыше и прикрепить передатчик не получится);
- высокая скорость передачи данных;
- сохранение инвестиций в сеть при переезде (оборудование снимается и монтируется в новом месте);
- нет необходимости в инфраструктуре (сеть можно развернуть там, где нет возможности проведения кабельных сетей);
- высокий уровень безопасности передачи информации (подключиться к сети и воровать трафик практически невозможно, поскольку согнал передается при помощи лазера, а не отправляется в радиоэфир).

Недостатки АОЛС:

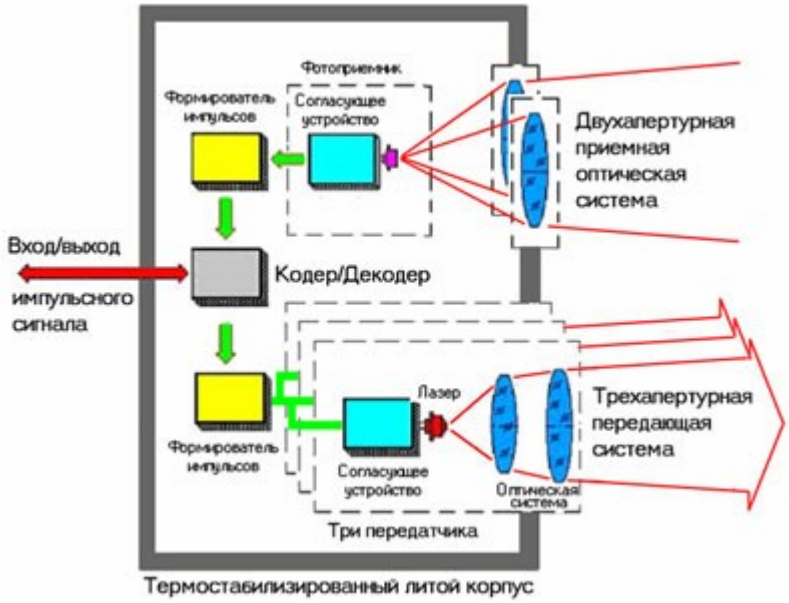
- зависимость от погодных условий (тумана, снегопадов, но зато даже сильный ливень не уменьшает качество сигнала);
- строгий лимит по расстоянию между передатчиком и приемником;
- дороговизна оборудования;
- для качественной работы сети нужно прочное крепление оборудования, поскольку смещение (ветер, механические нагрузки и проч.) передатчика или приемника ухудшает связь;
- недостаточная осведомленность пользователей о данной технологии, из-за чего отрасль развивается недостаточно быстро.

Пример оборудования АОЛС

Для примера рассмотрим АОЛС-оборудование Artolink серии M1 (патент РФ 2155450) производства ГУП Государственного Рязанского приборного завода. Оборудование предназначено для беспроводной полнодуплексной передачи цифровых данных между двумя точками с активным оборудованием. В настоящее время данная серия включает в себя модели, обеспечиваюощие сопряжение с наиболее популярными в России протоколами ПД — E1, Ethernet и Fast Ethernet.

Изделия серии M1 применяются при организации телекоммуникационных сетей интегрированного обслуживания, ЛВС, обеспечении доступа в Интернет, соединении БС сотовой связи, АТС и в других случаях, когда нужно высокоскоростное и экономичное решение для передачи информации между пространственно разнесенными объектами (часто разделенными естественными и искусственными преградами — реками, мостами, эстакадами, автотрассами и т. д.).

Все изделия серии состоят из двух идентичных терминалов. Каждый терминал включает в себя приемо-передающий модуль (ППМ), обеспечивающий передачу и прием оптических сигналов в атмосферном канале и устройство внешнего интерфейса (УВИ), служащее для обеспечения питания ППМ и стыка с внешним контрольным оборудованием. Блоки каждого поста соединяются между собой кабелем внутреннего интерфейса (КВИ) длиной до 100 м.



Резервное радиооборудование

Апертура в оптике — характеристика оптического прибора, описывающая его способность собирать свет и противостоять дифракционному размытию деталей изображения. В зависимости от типа оптической системы эта характеристика может быть линейным или угловым размером. Как правило, среди деталей оптического прибора специально выделяют так называемую апертурную диафрагму, которая сильнее всего ограничивает диаметры световых пучков, проходящих через оптический инструмент. Часто роль такой апертурной диафрагмы выполняет оправа или края одного из оптических элементов (линзы, зеркала, призмы).

Беспроводный оптический канал связи (БОКС) образуется входящим в состав каждого ППМ оптическим стыком, состоящим из передатчика и приемника.

Оптический передатчик включает в себя 3 синфазных лазерных излучателя работающих на длине волны 800+50 нм и обеспечивающих суммарную импульсную мощность излучения 120–135 мВт.

Приемная часть ППМ состоит из двух приемных объективов общей площадью 70 см2, оптической схемы, обеспечивающей некогерентное суммирование световых сигналов, их пространственную и частотную фильтрацию и фотоприемного устройства на основе быстродействующего PIN-фотодиода или лавинного фотодиода (ЛФД, avalanche photodiode, APD). АЧХ фотоприемного устройства оптимизирована в каждой модели под необходимую скорость передачи и тип линейного кодирования данных. В состав приемной части входит также датчик пространственного положения оптической оси, который позволяет контролировать точность наведения ППМ друг на

друга. Для его работы, оптическая схема использует небольшую часть (около 4%) суммарного принятого оптического излучения.

Система пространственной стабилизации (СПС, autotracking) автоматически поддерживает направление оптической связи, что позволяет устанавливать ППМ на нестабильных основаниях (например, деревянные крыши или вышки сотовой связи).

В зависимости от типа внешнего стыка, ППМ содержат в своем составе необходимый интерфейс с соответствующей программой управления. Он обеспечивает прием и передачу сигналов распространяющихся по электрическим линиям, их перекодировку под требования оптического канала и, при необходимости, мультиплексирование потоков. Все интерфейсы являются не настраиваемыми, не программируемыми и прозрачными. Длина соединительных сигнальных кабелей может достигать 100 м для потоков Ethernet и Fast Ethernet и 150 м для потоков E1.

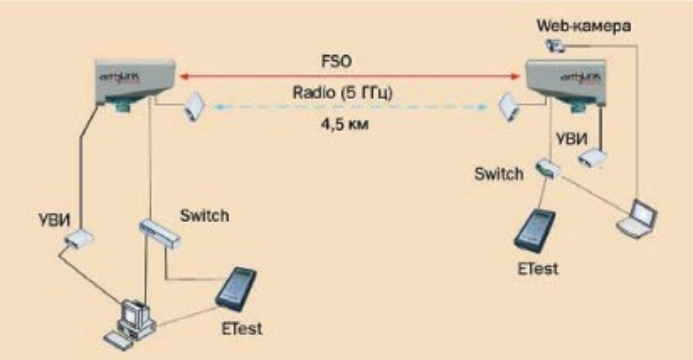
В состав ППМ входит мультипроцессорный вычислительный модуль, работающий под управлением специально разработанной ОС. Она позволяет в реальном масштабе времени обрабатывать асинхронные и параллельно протекающие процессы.

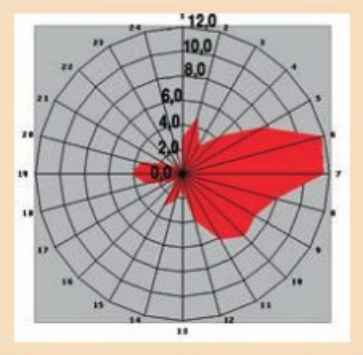
Во всех моделях серии M1 данный модуль обеспечивает следующие функции и сервис:

- Контроль рабочих режимов узлов ППМ, включая температуру.
- Стабилизацию параметров изделия во всем диапазоне изменений условий внешней среды.
- Мягкий запуск аппаратуры при отрицательных температурах эксплуатации.
- Переключение режимов работы ППМ: автоматическое поддержание направления связи, центрирование СПС.
- Индикация состояния ППМ и направления связи на встроенном 24 разрядной контрольной панели.
- Формирование последовательного потока информации в стандарте RS-232 для обеспечения функций удаленного мониторинга и управления.

Для обеспечения удобства и простоты установки атмосферной оптической линии связи каждый пост снабжен опорно-поворотным устройством. Оно обеспечивает жесткое закрепление ППМ на горизонтальной опорной поверхности, грубую и точную угловые юстировки. Для первоначальной визуальной наводки в состав ППМ входят диоптрийные прицелы. Внешне, различные изделия серии отличаются только типом соединителей сигнальных портов.

Существуют результаты испытаний, показывающие, что такое оборудование обеспечивает доступность канала порядка 98,67% без учета резервного канала связи.





Месяц	Доля времени работы линии по резервному каналу, %	Доступность канала связи без учета резерва, %	Доступность канала связи с учетом резерва, %	Расчетная доступность с "холодным" резервом, %
Май	0,676	99,324	99,9925	99,850
Июнь	1,421	98,579	99,9842	99,684
Июль	0,652	99,348	99,9928	99,855
Август	0,062	99,938	99,9993	99,986
Сентябрь	2,375	97,625	99,9736	99,472
Октябрь	2,290	97,710	99,9746	99,491
Средние значения за 6 мес.	1,327	98,673	99,9853	99,705

Источники:

1. FSO (технология). https://ru.wikipedia.org
2. Беспроводная оптика АОЛС / FSO – еще одно решение для преодоления «последней мили». http://rubroad.ru
3. FSO технология. http://www.moctkom.ru
4. 4,5 километра FSO-соединения с операторской надежностью. Практические результаты / С. Кузнецов, Б. Огнев, С. Поляков // Технологии и средства связи. №6. 2008. http://www.moctkom.ru
5. Атмосферная оптика FSO / М. Милых. http://nag.ru

Беспроводные системы ПД

Лекция 12
Технология Li-Fi

Li-Fi (Light Fidelity) — это двунаправленная, высокоскоростная беспроводная коммуникационная технология, использующая видимый свет в качестве канала связи. Термин был придуман Харальдом Хаасом, который является одним из основоположников технологии. Li-Fi принадлежит к технологиям VLC — Visible light communications. В июне 2011 года д-р Харальд Хаас продемонстрировал, что светодиодная лампа, оснащенная модулятором для кодирования сигнала, может передавать на компьютер HD-видеоизображение.

Связь по видимому свету работает путём переключения подачи напряжения на светодиоды на очень высокой частоте, незаметной для человеческого глаза. Световые волны не могут проникать через стены, поэтому радиус действия Li-Fi невелик, с другой стороны Li-Fi лучше защищен от взлома, чем обычный беспроводной канал связи. Также нет надобности в прямой видимости для передачи сигнала — свет, отраженный от стен может достигать пропускной способности в 70 Мбит/сек.

Первой доступной потребителю Li-Fi системой является PureLiFi, представленная в 2014 году на Mobile World Congress в Барселоне.

Bg-Fi — Li-Fi система, состоящая из приложения для мобильного устройства, и простого устройства, как например, IoT устройства, с датчиком цвета, микроконтроллером и встроенным программным обеспечением. Свет от дисплея мобильного устройства отправляется на датчик цвета, который преобразует свет в цифровую информацию. Светоизлучающие диоды позволяют синхронизироваться с мобильным устройством.

Li-Fi использует протоколы, аналогичные 802.11.

Стандарт IEEE 802.15.7 (2012) определяет физический уровень (PHY) и уровень управления доступом к среде (MAC).

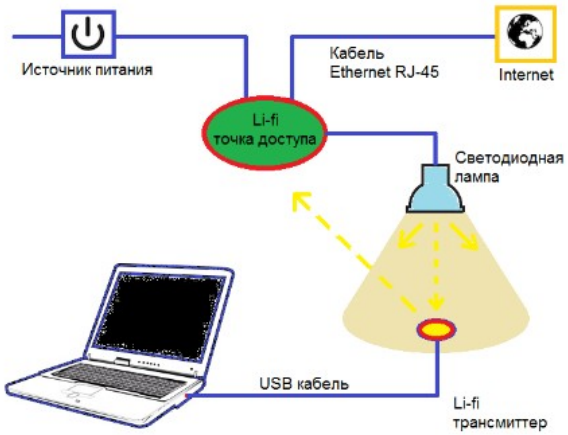
Стандарт определяет три физических (PHY) уровня с разными пропускными способностями:

- PHY I был создан для наружного применения и работает на скоростях 11,67–267,6 кбит/сек.
- PHY II позволяет достигать скоростей ПД 1,25–96 Мбит/сек.
- PHY III предназначен для множественных источников с определённым методом модуляции: Color Shift Keyring (CSK) — «Манипуляция смещением длины волны». PHY III может достигать скорости 12–96 Мбит/сек.

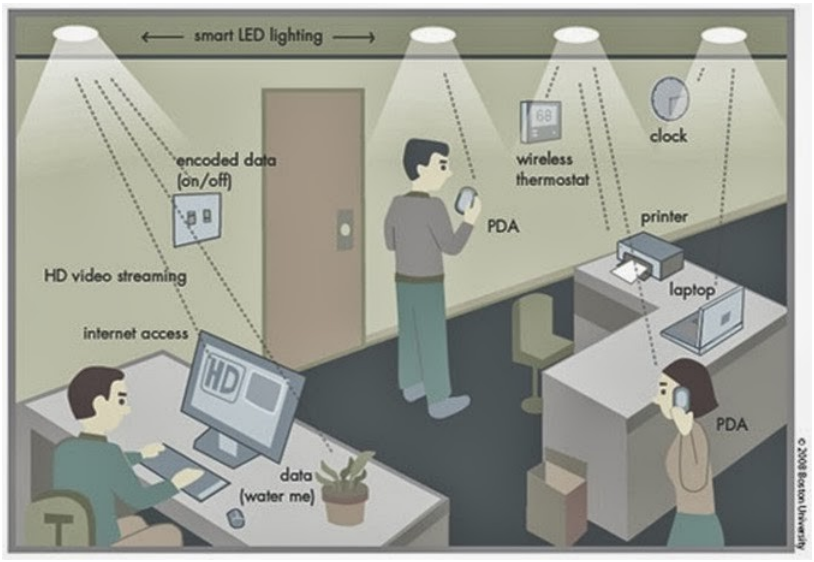
Теоретически, с помощью микросветодиодной лампы, можно достигать скорости передачи данных 3,5 Гб/с через каждый из трех цветов — красный, зеленый и синий. Сложив спектральные каналы, можно передавать данные с общей скоростью 10 Гб/с.

Сброс сигнала у использующихся светодиодов и фотодиодов происходит достаточно быстро для того, чтобы не выдерживать паузу для его надёжного затухания.

Для передачи данных обратно Li-Fi требует использования других технологий ПД, таких как PLC (Power Line Communication) или высокоскоростные варианты IrDA — VFIR или UFIR.



Пример использования Li-Fi



Источники:

1. Li-Fi. https://ru.wikipedia.org
2. Киричек Р.В., Нгуен Д.К., Герасимова Е.М. Сравнительный обзор технологии Li-Fi и перспектива практического использования для Интернета Вещей // Информационные технологии и телекоммуникации. — 2015. — № 4 (12). — С. 77–86.