МЕСТО UWB ТЕХНОЛОГИЙ В СТАНДАРТАХ БЕСПРОВОДНОЙ ТЕХНОЛОГИИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Андреевская Т.М., Чекункова Т.О.
Москва, МИЭМ НИУ ВШЭ

В работе рассмотрен ряд стандартов беспроводных систем связи, позволяющих оценить основные характеристики и параметры различных технологий организации локальных и персональных сетей связи.

Location UWB technology in wireless technology standard transmission.
Andreevskaya T.M., Chekunkova T.O.
In this paper a number of standarts of the wireless communication systems, allowing to estimate the basic characteristics and parameters of various technologies of the organization of local and personal communication networks is considered.

Беспроводные технологии передачи информации – одно из наиболее быстро прогрессирующих направлений телекоммуникационного рынка. Они вытесняют региональные и локальные беспроводные сети. Эти технологии добрались и до персональных сетей с минимальным радиусом действия.

Основным классификационным признаком является размер территории, которую покрывает сеть. К локальным сетям относят сети, абоненты которой сосредоточены в радиусе от нескольких метров до 1-2-х километров. Чаще всего такая коммуникационная сеть принадлежит одной организации. Благодаря малым расстояниям имеется возможность использовать хорошие линии связи, в том числе и беспроводные, которые позволяют достигать высоких скоростей (до 100 Мбит/с) и отличаются большим разнообразием услуг, в том числе и работой в on-line. Широко развиваются UWB (сверхширокополосные – СШП) технологии передачи информации с новыми методами модуляции и обработки цифровых сигналов. Широкая полоса частот на одной несущей в гигагерцовом диапазоне позволяет использовать множественный доступ с большим числом каналов.

Также как и для других сетевых технологий, для локальных систем разработаны международные стандарты. Стандарты создаются для соблюдения производителями общепринятых правил построения оборудования. Каждая технология только тогда приобретает соответствующий статус, когда она закрепляется в соответствующем стандарте.

На рис.1 показана диаграмма в координатах дальность – скорость, на которой видно семейство стандартов IEEE 802.15, которое образует беспроводную сеть WPAN (Wireless Personal Area Network - Беспроводные персональные сети) и работает в различных стандартах, в том числе с рассматриваемым в данной работе стандартом IEEE 802.15.4a/b.

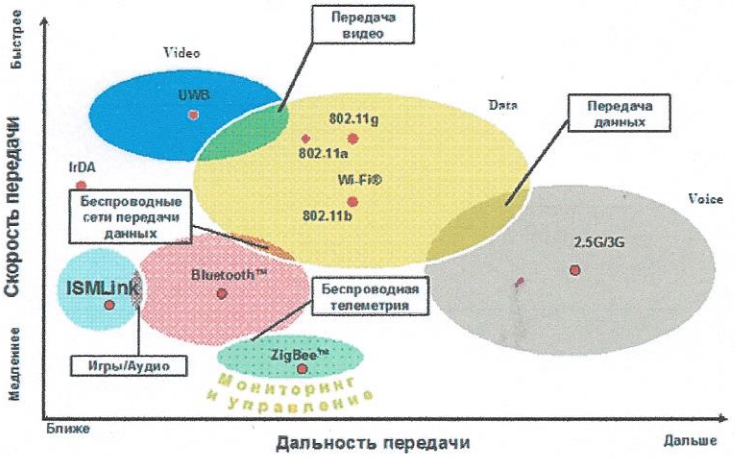


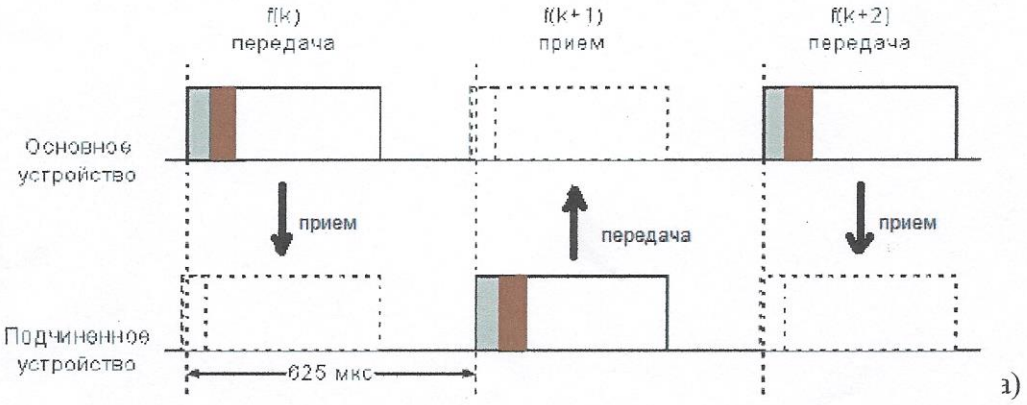
Рис.1.

IEEE 802 — группа стандартов семейства IEEE, касающихся локальных вычислительных сетей (LAN) и сетей мегаполисов (MAN). Службы и протоколы, указанные в IEEE.802 находятся на двух нижних уровнях (Канальный уровень и Физический) семиуровневой сетевой модели OSI. Фактически, IEEE 802 разделяет канальный уровень OSI на два подуровня — Media Access Control (MAC - управление доступом к среде) и Logical Link Control (LLC - подуровень управления логической связью).

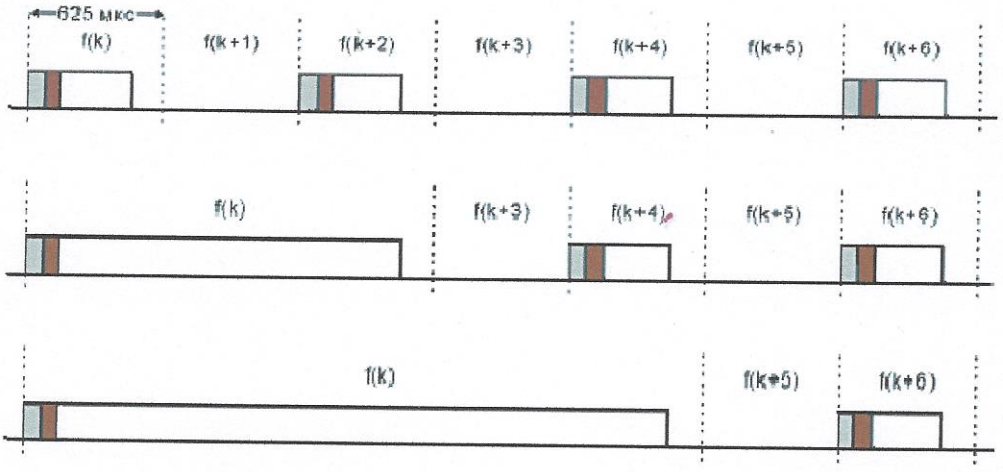
Рассмотрение начнем со стандарта для беспроводной сети Bluetooth, т.к. технология UWB возникла как одно из возможных направлений его развития.

Стандарт Bluetooth использует радиочастоты в диапазоне 2400…2483,5 МГц. Этот диапазон называется ISM (Industrial, Scientific, Medicine – промышленный, научный и медицинский), он используется во многих странах для безлицензионного доступа. В технологии Bluetooth весь диапазон разбит на 78 каналов шириной 1 МГц каждый.

В стандарте Bluetooth предусмотрена дуплексная передача на основе разделения времени (Time Division Duplexing - TDD). Основное устройство передает пакеты в нечетные временные сегменты, а подчиненное устройство – в четные. Рис.2,а иллюстрируют принцип действия системы при дуплексной передаче с временным разделением каналов, а рис.2,б– передачу пакетов различной длины [1]. Пакеты в зависимости от длины могут занимать до пяти временных сегментов. При этом частота канала не меняется до окончания передачи пакета.



а)



б)

Рис.2 (а,б).

Рассмотрим далее стандарты, которые регулируют технологию UWB. Стандарт *IEEE 802.15.3*, предназначен для беспроводных частных сетей типа WPAN, и является прямым наследником Bluetooth (частота 2,4 ГГц). Использование полосы 2,4 ГГц и технологии модуляции OQPSH (Offset Quadrature Phase Shift Keying, квадратурная манипуляция фазовым сдвигом со смещением) позволяют достигать скорости передачи данных до 55 Мбит/с на расстоянии до 100 метров, одновременно работать в такой сети могут до 245 пользователей. При возникновении помех со стороны других бытовых устройств или иных сетей, сети на основе IEEE 802.15.3 будут автоматически переключать каналы. Также поддерживаются скорости передачи данных - 11, 22, 33 и 44 Мбит/с. Шифрование данных в сетях IEEE 802.15.3 может осуществляться по стандарту AES 128. К достоинствам можно отнести низкое энергопотребление и низкую стоимость.

Стандарт *IEEE 802.15.3a* используется для организации персональных высокоскоростных сверхширокополосных сетей (High-Speed Ultra Wide Band PAN). Он используется в основном в Северной Америке и Японии, в дальнейшем предполагается глобальное использование во всем мире. Основной частотный диапазон 3.1-10.6 ГГц. Используемые виды модуляци: широкополосные радиоимпульсы и многочастотная OFDM. Предусматривается возможность множественного доступа с обнаружением несущей и предотвращением коллизий CSMA-CA. Пользовательская скорость передачи данных более 100 Мбит/с. Обеспечивает передачу данных и видеосигналов абонентам с низкой подвижностью, беспроводной USB. Высокая скорость достигается путем увеличения спектральной ширины канала при переходе в область сверхширокополосной связи (СШП, UWB).

По принятым в комитете IEEE 802 правилам, для того чтобы утвердить стандарт, за предложенный вариант должны проголосовать не менее 75% членов рабочей группы. Однако, несмотря на численный перевес сторонников MB-OFDM, им не удалось на прошедших голосованиях набрать заветные 75% голосов от общего числа компаний, работающих над стандартом IEEE 802.15.3a. Причин тут несколько, возможно, одна из основных кроется в особенностях многополосной организации работы систем с MB-OFDM, суть которой заключается в том, что весь разрешенный

диапазон делится на полосы шириной 528 МГц. В стандартном режиме предусмотрено три полосы, в расширенном –семь, например так, как показано на рис.3.

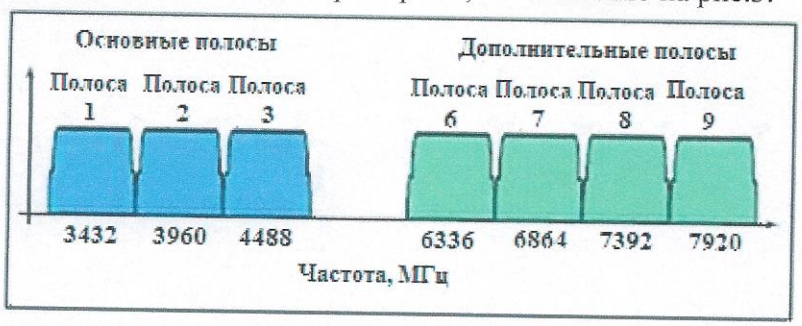


Рис.3.

Каждая полоса, в свою очередь, разбивается на полосы со 128 поднесущими частотами с шагом 4,125 МГц. Из них используется 122: 100 для модуляции данных, 12 поднесущих – пилотные и еще 10 – защитные. Каждая поднесущая модулируется посредством QPSK. Один OFDM-символ содержит 100 или 200 кодированных бит (100 в случае, когда одинаково модулируются две поднесущие, симметричные относительно центральной). Период следования символов – 312,5 нс. Многополосность системы означает, что последующий символ может передаваться в иной частотной полосе по жестко организованной определенной схеме для каждого логического канала (предполагается четыре таких канала). Последовательность перехода с одной полосы на другую называют частотно-временным кодом.

Преимущество MB-OFDM заключается в уменьшении необходимого количества временных защитных интервалов. При последовательном сигнале защитные интервалы добавляются между каждыми символами, а при многочастотном – между группами OFDM-символов.

Отметим основные особенности сигналов OFDM:

– мультиплексирование несущих колебаний (называемых поднесущими) осуществляется модулированными информационными символами по выбранному закону (QPSK, 16QAM, 64QAM,OQAM). Поднесущие ортогональны, или, по крайней мере, квазиортогональны;

– каждый OFDM-символ имеет защитный временной интервал для исключения межсимвольной интерференции. Этот защитный интервал выбирается с учетом импульсной характеристики линии связи (физической среды распространения радиосигнала); при модуляции вида OQAM защитный интервал не обязателен;

– использование операции дискретного обратного преобразования Фурье как в приемнике, так и в передатчике, упрощает реализацию приемо-передающего устройства с OFDM [6] .

Стандарт IEEE 802.15.4a/b (UltraWideband) предназначен для систем, работающих на принципе передачи множества закодированных импульсов негармонической формы очень малой мощности (~0,05 мВт) и малой длительности в широком диапазоне частот (от 3,1 до 10,6 ГГц). Передача данных на расстояниях до 5 метров осуществляется со скоростью от 400 до 500 Мбит/с. Тип используемой модуляции: OFDM, QPSK. U(2

При помощи UWB-технологии можно создавать специальные сети, в которых несколько сверхширокополосных устройств смогут поддерживать связь между любыми узлами. Короткие сигналы UWB сравнительно устойчивы к многолучевому распространению. Высокоскоростные UWB-устройства хорошо подходят для работы с

6. Андреевская Т.М., Чекункова Т.О. Применение технологии многочастотной модуляции типа OFDM в сверхширокополосных системах связи // В кн.: Инновации на основе информационных и коммуникационных технологий: материалы международной научно-технической конференции / Отв. ред.: И.А. Иванов; под общ.ред.: С.У. Увайсов. М.: МИЭМ НИУ ВШЭ, 2012. С. 313-315.

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ШИФРОВАНИЯ И ИХ ПРИМЕНЕНИЕ В АЛГОРИТМАХ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ

Антонов Д. С., Балакин А. Р.
Тольятти, ПВГУС.

Данная статья описывает понятия криптографии, информационной безопасности и электронно-цифровой подписи, методы шифрования информации и способы их реализации на практике. Так же в статье наглядно рассматривается частный случай реализации электронно-цифровой подписи на основе дискретного логарифмирования в частности при помощи эллиптических кривых.

Analysis of modern encryption systems and their use in the algorithm of the digital signature. Antonov D. Balakin A.

This paper describes the concepts of cryptography, data security and digital signatures, encryption of information and ways to implement them in practice. Also in the article clearly considered a special case of the implementation of digital signatures based on the discrete logarithm problem in particular by means of elliptic curves.

Информация в наше время является крайне ценным ресурсом. Именно поэтому её защита становится задачей первостепенной важности. Данную задачу призвана решить криптография - защита информации путем ее преобразования, исключающая ее прочтение посторонним лицом. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные.

Криптография - сознательное изменение знаков, системы или способа письма с целью затруднить или сделать невозможным его прочтение для нежелательного пользователя. По сути, криптография представляет собой совокупность двух процессов:

- Шифрование - процесс применения шифра к защищаемой информации, т.е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение с помощью определенных правил, содержащихся в шифре.
- Дешифрование - процесс, обратный шифрованию, т.е. преобразование шифрованного сообщения в защищаемую информацию с помощью определенных криптографических алгоритмов.[1]

Первые алгоритмы криптографии были симметричными, т.е. представляли собой системы с неким секретным ключом: существовало некое тайное знание (способ шифрования или ключ к нему), и тот, у кого был доступ к этому знанию, мог зашифровать и впоследствии расшифровать любое сообщение.

Среди таких систем есть очень стойкие (даже абсолютно стойкие): пока вы не узнаете или не подберете ключ, расшифровать сообщение невозможно. Однако надо