Коняхін Г. Ф. к. т. н. проф. каф. ЕКТСУ

Шахов А. С. асистент каф. ЕКТСУ

СРАВНИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ

Радиодоступ к локальным и подвижным абонентам может быть реализован на основе:

1. Систем сотовой связи.

2. Системы DECT.

3. Систем транкинговой связи.

4. Беспроводных локальных сетей.

Применение систем сотовой связи в качестве систем передачи информации следует считать экономически неэффективным. Системы DECT являются низкоскоростными или имеют небольшой радиус зоны обслуживания. Также неэффективными являются системы транкинговой связи, т.к. обладают большой избыточностью при обслуживании стационарных абонентов.

Беспроводные локальные сети могут строиться на основе стандартов семейства IEEE 802.11-802.16

Сравнительные технические характеристики СШП устройств и других систем с малым радиусом действия приведены в таблице 1 [7].

Стандарт 802.15.1 (Bluetooth) обеспечивает скорость передачи информации в канале 720 кбит/с., при этом обеспечивается существенно меньшее энергопотребление, чем у устройств стандарта 802.11 [7]. Технология стандарта Bluetooth позволяет объединять в пикосети до восьми устройств, обеспечивать реализацию беспроводного ввода, организации каналов связи для различных устройств и временн ых локальных сетей. Спецификация стандарта описывает пакетный способ передачи информации с временным мультиплексированием. Для радиообмена используется диапазон частот 2400 – 2483,5 МГц.

В радиотракте предусмотрен метод расширения спектра посредством частотных скачков и двухуровневая частотная модуляция [11].

Технология Bluetooth имеет недостатки, связанные с реализованным в ней механизмом защиты от несанкционированного доступа. В процессе сопряжения два Bluetooth-устройства формируют защищенный 128-битный ключ, который затем хранится в их памяти и используется каждый раз при пересылке данных между двумя устройствами. В качестве первого шага идентификации для установления связи пользователю необходимо ввести в оба устройства одинаковый четырехсимвольный PIN-код. Затем из него сложными математическими процедурами извлекается ключ.

Примером возможности взлома является искусственно инициированный ключ сопряжения. Bluetooth-устройство хакера вмешивается в контакт, выдавая себя за другое.

При этом на устройство жертвы посылалось сообщение о том, что ключ забыт [12]. Старый ключ аннулировался, а устройства начинали процедуру сопряжения вновь, что позволяло хакеру перехватить полноценный пароль и использовать его впоследствии в своих целях.

Кроме того, нельзя исключать возможность возникновения радиопомех, поскольку диапазон 2,4 ГГц, в котором работают средства Bluetooth, используется и беспроводными ЛВС стандарта 802.11.

Стандарт IEEE 802.15.4 (ZigBee) используется для решения спектра задач достаточно низкой скорости передачи и разрабатывался исходя их требований создания систем с изменяющейся сетевой структурой, малой стоимости и малого энергопотребления входящего в сеть оборудования. Он предусматривает работу в трех диапазонах частот: один канал 896,0 – 868,6 МГц (для Европы), 10 каналов в диапазоне 902 – 928 МГц, и 16 каналов в диапазоне 2400 – 2483,5 МГц. Для предотвращения несанкционированного доступа к передаваемым данным может применяться шифрование (криптозащита). Применение криптозащиты требует значительной вычислительной мощности от микроконтроллерного блока, как на приемной, так и на передающей стороне.

Структура стандарта IEEE 802.11 для беспроводных локальных компьютерных сетей предполагает наличие в своем составе точек доступа к проводной сети общего пользования и большого количества абонентских

станций, между которыми обеспечивается беспроводная связь и связь через точки доступа с абонентами проводной сети. Стандарт 802.11 предусматривает две длины ключей — 40 бит и 104 бита.

При длине ключа в 104 бита декодирование данных прямым перебором становится довольно утомительным занятием даже при работе новейшей вычислительной техники. На первый взгляд, реализованный в WEP (Wired Equivalent Privacy – безопасность, эквивалентная проводной) механизм криптозащиты должен быть устойчив ко взлому. Но отправитель и получатель должны обладать секретным ключом, используемым вместе с вектором инициализации для кодирования и декодирования информации. А в стандарте 802.11b не оговорен механизм обмена ключей между сторонами. В результате, при интенсивном обмене данными, реальна ситуация повторного использования значений векторов инициализации с одним и тем же секретным ключом. Особенность реализованного алгоритма криптозащиты приводит к тому, что, имея два сетевых пакета, зашифрованных одним кодирующим ключом, можно не только расшифровать данные, но и вычислить секретный ключ. Это позволяет не только декодировать всю перехваченную информацию, но и имитировать активность одной из сторон. Тонкость работы с алгоритмом кодирования, реализованном в WEP, в том, что нельзя допускать повторного использования кодирующих ключей. И этот момент был упущен при разработке стандарта [1].

Стандарт 802.16 разработан для описания радиоинтерфейса, основанного на общем протоколе (MAC) доступа к общему каналу. Стандартом предусматривается диапазон частот 2 – 11 ГГц и 10 – 66 ГГц. В диапазоне частот 10 – 66 ГГц радиосвязь между абонентами возможна лишь в условиях прямой видимости. В диапазоне 2 – 11 ГГц допускается возможность решения задач радиосвязи в условиях многолучевого распространения и при отсутствии прямой видимости.

В соответствии со стандартом IEEE 802.16, для предотвращения несанкционированного доступа к беспроводным службам и защиты пользовательских данных в Nateks-Multilink 3 осуществляется шифрование трафика в пределах всей беспроводной сети. Базовые станции передают данные о ключах (DES/3DES) на абонентские комплексы с помощью протокола обмена ключами безопасности (Privacy Key Management, PKM).

Этот протокол используется базовой станцией для предоставления условного доступа к сети и во время синхронизации информации о ключах с абонентской стороной. Авторизация абонентских комплексов осуществляется на базе сертификата X.509. В системе предусмотрена защита паролем (до 16 различных символов) доступа к интерфейсу GUI-управления. Таким образом, обеспечивается защита служб управления, конфигурирования и обновления паролей и программного обеспечения системы. В Nateks-Multilink 3 встроены дополнительные средства защиты, которые запрещают неопознанной удаленной станции посылать данные на порт Ethernet другой удаленной станции Nateks-Multilink 3. В результате уменьшается вероятность утечки данных с подключенного сегмента локальной сети.

Требования к скорости передачи информации, ее защищенности, стоимости и потребляемой мощности в современных устройствах передачи данных, а также загруженность радиочастотного спектра требуют создания новых технологий, обеспечивающих более экономичное применение радиочастотного ресурса и высокую помехозащищенность. Использование таких беспроводных технологий, как Bluetooth, ZigBee или протоколы семейства 802.11и 802.16, имеет ряд ограничений. Главный недостаток этих протоколов заключается в их сравнительно небольшой полосе пропускания и алгоритмах защиты информации.

Таблица 1. Сравнительные технические характеристики СШП устройств и других систем

Тип устройства	Скорость передачи данных	Радиус зоны обслуживания, м	Диапазон частот, ГГц	Уровень мощности	Тип модуляции
СШП	До 500 Мбит/с	15	1-11	-30…40 дБм/МГц	PPM/ другой тип
Bluetooth	722 кбит/с	15	ISM 2, 4	Класс 1: 20дБм Класс 2: 4дБм Класс 3: 0 дБм	GMSK
ZigBee	20 кбит/с 40 кбит/с 250кбит/с	>20 >20 >20	0,868-0,8686 0,902-0,928 2,4-2,4835		
802.11a, WLAN	До 54 Мбит/с	50	5	От 200 мВт до 1 Вт	60-QAM, 16-QAM, BPSK, OFDM
802.11b, WLAN	До 11 Мбит/с	100	ISM 2, 4	От 100 мВт до 2 Вт	CCK (8 Complex Chip Spreading)
802.11g, WLAN	До 54 Мбит/с	100	ISM 2, 4	От 100 мВт до 2 Вт	64-QAM, 16-QAM, BPSK, OFDM