**Эссе по курсу "Защита информации", кафедра радиотехники,
Московский физико-технический институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec.**

Безопасность соединения bluetooth-устройств.

Выполнил: Моргунов А.Е.
10.04.2005

Введение. Bluetooth- это технология беспроводной связи, рассчитанная на работу на малых расстояниях (10м, с использованием усилителей делают устройства с дальностью приема 100 м). С помощью этой технологии соединяются персональные офисные устройства, бытовая техника и т.д. с портативными устройствами, такими, как мобильные телефоны, электронные записные книжки, датчики сигнализации, телеметрии, носители информации и т.д.

Bluetooth- это возможность объединять в локальные сети любые устройства: от персонального компьютера до микроволновой печи. Технология обладает такими немаловажными параметрами, как низкая стоимость устройства связи, компактность, совместимость и простота встраивания в различные устройства.

К примеру, возможные сценарии использования Bluetooth:

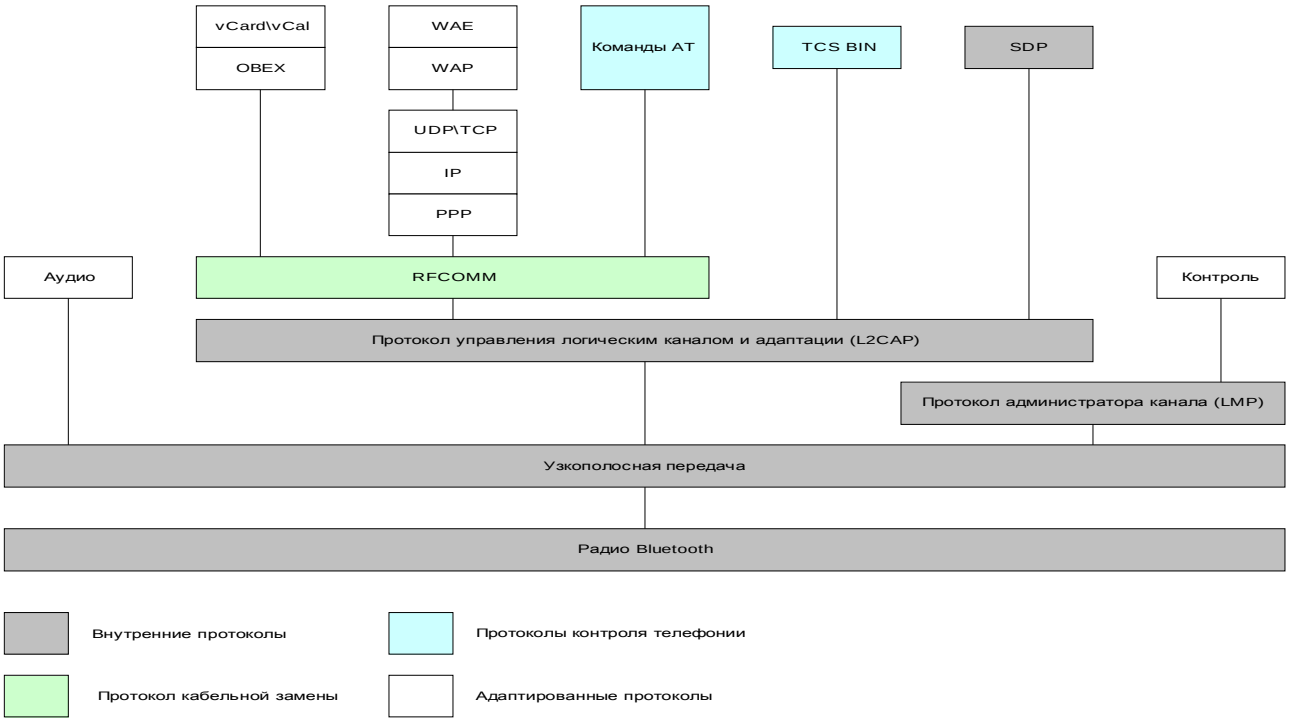
- Телефон «три в одном»
- Мост Internet
- Удалённый головной телефон
- Громкоговоритель портативного ПК
- Автоматическая синхронизация
- Беспроводной настольный компьютер

И этот список можно продолжить. В силу такого разнообразия возможностей использования технологии, сфера её применения постоянно расширяется.

Bluetooth появилась в 1998 году, когда группа компаний (Nokia, Ericsson, Intel, IBM, Toshiba) выступила с инициативой создания новой беспроводной технологии связи, для чего была создана специальная рабочая группа SIG (Special Interest Group), в которую в настоящее время входят чуть ли не все крупнейшие компании мира, занятые в сфере. Всего же SIG насчитывает более 3000 членов.

По многим прогнозам технология Bluetooth будет технологией «де-факто» для беспроводной связи, встраиваемой в портативные устройства.

Обзор технологии. Стандарты Bluetooth- это труд, размещённый более чем на 1500 страницах, содержащих внутреннюю спецификацию и спецификации профиля. Во внутренней спецификации рассматриваются детали уровней протокольной архитектуры Bluetooth. Спецификации профиля описывают модели поведения в различных приложениях.



AT- сигнальная последовательность
IP- протокол Интернета
OBEX- протокол объектного обмена
PPP- протокол двухточечного соединения
RFCOMM- протокол замещения кабеля
SDP- протокол обнаружения службы
TCP- протокол управления передачей
TCS BIN- протокол управления телефонией (бинарная)
UDP- протокол пользовательских датаграмм
vCal- виртуальный календарь
WAE- среда беспроводных приложений
WAP- протокол беспроводных приложений

Выше приведена архитектура протоколов Bluetooth. Внутренние протоколы образуют пятиуровневый стек и состоят из:

- Радио (детали радиоинтерфейса)
- Узкополосная передача (установление соединения в пределах пикосети (piconet), формат пакетов, адрессация)
- Протокол администратора канала связи (Link Manager Protocol- LMP). Отвечает за установление канала между устройствами, его администрирование, включая аутентификацию и шифрование.
- Протокол управления логическим каналом и адаптации (Logical Link Control and Adaption Protocol- L2CAP). Адаптирует протоколы высшего уровня к протоколу узкополосной передачи.
- Протокол обнаружения службы (Service Discovery Protocol- SDP). Для установления связи может запрашиваться информация об устройстве, о службах, о характеристиках служб.

Bluetooth использует полосу радиочастот 2.4-2.4835 ГГц в диапазоне ISM (Industrial, Scientific, Medical), не требующим лицензирования. Эта полоса делится на 79 каналов по 1 МГц шириной. В некоторых странах (Япония, Испания, Франция) часть этой полосы используют военные, так что число каналов в них меньше- 23. Для модуляции в устройствах Bluetooth выбрана гауссова частотная манипуляция, бинарная единица представляется положительным отклонением частоты от центральной, ноль- отрицательным. Минимальное отклонение- 115 кГц. Полоса радиочастот делится на каналы с той целью, чтобы:

- Обеспечить работу нескольких пикосетей.
- Обеспечить работу в диапазоне, в котором могут присутствовать сторонние сигналы, так как полоса свободна для использования.

Опишем схему преодоления обозначенных препятствий. Bluetooth-устройство использует каждый канал в течение 0.625 мс (смена канала происходит 1600 раз в секунду), причём смена канала происходит согласно псевдослучайной последовательности, одинаковой для всех устройств одной пикосети. Такая схема называется FH (Frequency Hopping). Устройства общаются между собой с использованием дуплекса с временным разделением (Time Division Duplex- TDD). Это схема, в которой в каждый момент времени данные передаются только в одну сторону, а направления передачи чередуются. Так как среду пикосети могут использовать до 8-ми устройств, то их корректная работа достигается использованием схемы TDMA (Time Division Multiple Access). Таким образом, общую схему работы Bluetooth- устройств можно обозначить, как FH-TDD-TDMA. Если в одной области будут работать разные пикосети, то, так как у каждой из них будут свои псевдослучайные последовательности, большую часть времени они будут работать в разных каналах, а когда случайно каналы совпадут, то это будет восприниматься, как банальная ошибка, внесённая на этапе транзакции.

В Bluetooth- спецификациях обозначены 3 схемы исправления ошибок:

- FEC(Forward Error Correction- помехоустойчивое кодирование) со скоростью кода 1/3.
- FEC со скоростью кода 2/3.
- ARQ (Automatic Repeat Request- автоматический запрос повторной передачи).

Между устройствами могут устанавливаться 2 вида соединения:

- Ориентированный на установление соединения синхронный канал (Syncronous Connection Oriented - SCO). Выделяется фиксированный канал двухточечному соединению. В основном этот тип соединения используется для передачи данных, требующих фиксированной скорости передачи в ущерб гарантированной доставке, таких как речь. Может поддерживаться до 3-х каналов SCO.
- Асинхронный канал без установления соединения (Asynchronous Connection Less- ACL). Канал ACL может быть только один. Вследствие различных помех в канале ACL большое количество пакетов передается повторно.

Для передачи аудио в спецификациях указаны 2 вида перевода сигнала в цифровой вид: PCM (Pulse Code Modulation- ИКМ- Импульсно Кодовая Модуляция) и CVSD (Continuous Variable Slope Delta- дельта- модуляция с непрерывной переменной огибающей). В отличие от PCM, считывающей в каждый момент полную информацию об амплитуде сигнала, CVSD говорит только об изменении сигнала, причём известно только увеличился или уменьшился сигнал. Приращение, используемое в CVSD, динамически подстраивается, путём специального сравнения смоделированного сигнала в разные моменты времени. А именно, если у нас n раз подряд приходила информация об увеличении амплитуды, то мы должны увеличить приращение на некоторую величину. Аналогично с уменьшением амплитуды.

Безопасность. Как и в любой другой технологии связи, в Bluetooth нужно подумать о безопасности соединения устройств. Всегда находятся люди, желающие получить несанкционированный доступ к устройству. Приведу несколько типов атак.

Bluejacking. Это атака на телефон со встроенной технологией Bluetooth, целью которой является анонимно оставить на нем свои карточки, обычно с целью флирта или шутки. Эта атака не включает в себя удаление или порчу данных.

Bluebugging. Цель этой атаки- получить доступ к командам телефона без оповещения о том владельца. Она позволяет злоумышленнику делать звонки с чужого

телефона, читать и отсылать сообщения, редактировать телефонную книгу, выходить в Интернет.

Bluesnarfing позволяет получить доступ к данным, хранящимся на телефоне (телефонная книга с ассоциированными картинками, календарь, IMEI(International Mobile Equipment Identity).

Для осуществления атаки злоумышленник должен находиться на расстоянии не большем десяти метров.

В спецификациях Bluetooth определены следующие инструменты организации безопасного канала между устройствами:

- Аутентификация
- Шифрование
- Управление с использованием ключей

Алгоритмы, осуществляющие кодирование и аутентификацию, используют следующие параметры:

- Адрес модуля (общеизвестный 48-битовый адрес устройства)
- Секретный ключ аутентификации (секретный 128-битовый ключ)
- Секретный частный ключ (4- 128 бит)
- Случайное число (128-битовое случайное число, сгенерированное в устройстве Bluetooth)

Секретные ключи, упомянутые выше, должны быть известны только устройству-обладателю и не должны разглашаться.

Аутентификация- это процедура, в результате которой становится известно, с каким устройством устанавливается связь, либо то, что устройство неизвестно, и к нему стоит относиться с осторожностью. Аутентификация в Bluetooth осуществляется следующим образом: устройство A генерирует случайное число и отсылает его устройству B. Затем устройство A, используя алгоритм шифрования E1 (см. рис. ниже), вычисляет 32-битовое проверочное число: на вход алгоритма поступают случайное число, отосланное устройству B, адрес устройства B и общий секретный ключ. Точно такие же вычисления проводит в свою очередь устройство B, получая число от A. Затем B отсылает это проверочное слово устройству A, которое в свою очередь сравнивает два проверочных числа (полученное от B и подсчитанное самостоятельно) и решает вопрос о надёжности этого устройства. Чтобы провести двухстороннюю аутентификацию, устройству B нужно провести действия, совершённые устройством A.

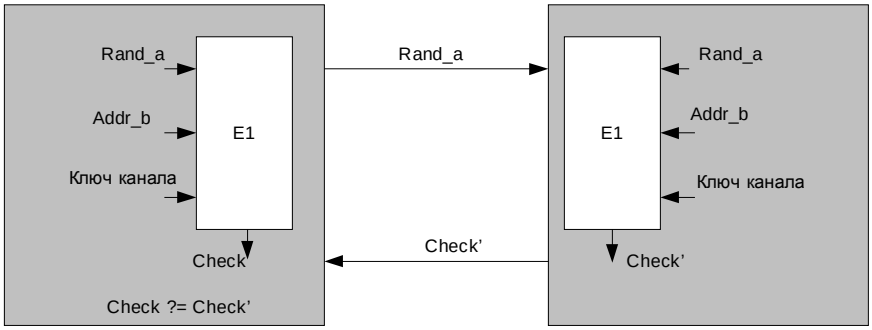


Рис. Аутентификация с запросом и ответом

Алгоритм аутентификации E1 основан на алгоритме шифрования SAFER+ (Secure And Fast Encryption Routine). На рисунке, приведённом ниже, изображена схема работы алгоритма E1. Блок A функционирует точно по алгоритму SAFER+, а A' немного отличается от A (входные данные первого раунда прибавляются ко входным данным третьего раунда). Сложение (плюс в квадрате) проводится побайтовое по модулю 256.

На выходе алгоритма получается 128 битовое число, но для аутентификации используются только 32 младших бита.

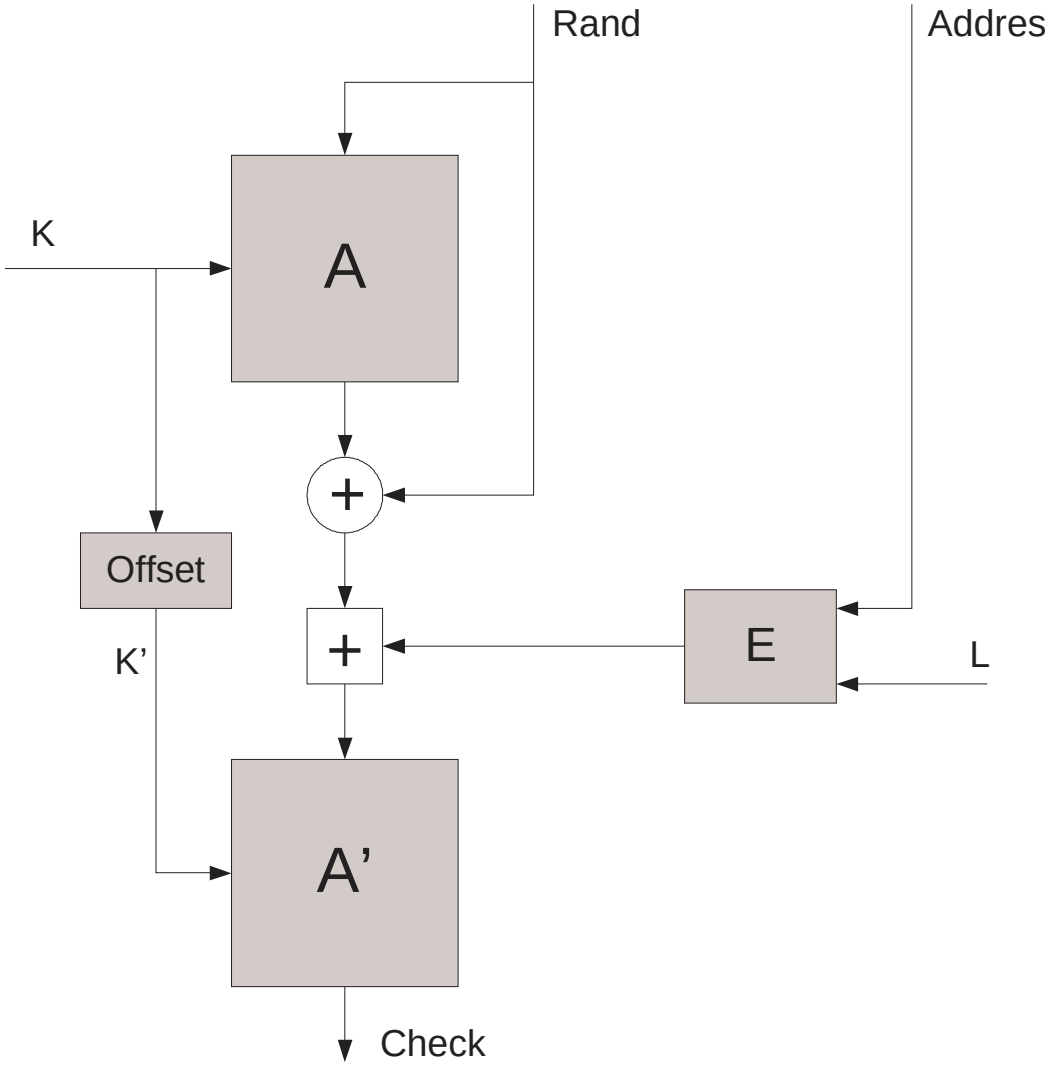


Рис. Алгоритм шифрования E1

Пользовательская информация может быть защищена путем шифрования полезной нагрузки передаваемого пакета. Код доступа и заголовок пакета никогда не шифруются. Шифрование данных происходит по алгоритму E0. Для шифрования каждого пакета генерируется новый ключ. Вначале генерируется ключ полезной нагрузки. Для этого устройство A генерирует псевдослучайное число, которое передается и B. Это число в сочетании с адресом ведущего устройства, текущим временем и общим секретным ключом дает ключ полезной нагрузки, который используется как входной параметр алгоритма E0. Алгоритм E0 (см. рис. ниже) реализуется на линейном регистре сдвига с обратной связью (linear feedback shift register- LFSR), который инициализируется как раз ключом полезной нагрузки. В результате на выходе генератора ключа потока получается непрерывный поток битов, который суммируется по модулю 2 с полезной нагрузкой как на этапе шифрования, так и на этапе расшифрования. Поскольку для каждого сеанса шифрования текущее время различно, то безопасность увеличивается ещё за счёт постоянного изменения ключа шифрования.

Рис. Поточное шифрование Bluetooth

Список литературы:

[1] www.bluetooth.org. Specification of the Bluetooth System, version 1.1.

[2] www.bluetooth.com/help/security.asp.

[3] Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В. *Основы криптографии: Учебное пособие, 2-е изд., испр. и доп.* — М.:Гелиос АРВ, 2002.

[4] www.ichip.ru/index.php?page=archive_special_articles&id=20

[5] Вильям Столлингс. Беспроводные линии связи и сети— Изд. Вильямс, 2003.