"Реализация bluetooth-технологии и обеспечение безопасности взаимодействия bluetooth-устройств"

1.История создания и развития технологии Bluetooth

История развития технологии Bluetooth насчитывает уже около 7 лет.В 1994 году компания Ericsson(Швеция) начала заниматься решением задач,связаннных с организацией беспроводного соединения между сотовыми телефонами и аксессуарами к ним.В результате исследований была предложена идея маломощного и относительно дешевого радиоинтефейса,выступавшим альтернативой традиционным соединительным кабелям.

В начале 1998 Ericsson выступила инициатором создания группы разработчиков новой технологии.20 мая 1998 года Ericsson, Intel, Nokia, Toshiba объявили о создании специальной группы(Special Interest Group) для разработки и продвижения технологии на рынок телекоммуникаций и электроники.При этом любая компания, которая планирует разрабатывать устройства и программное обеспечение на основе спецификаций Bluetooth, может бесплатно войти в эту группу.

В результате, в последующие годы состав SIG непрерывно увеличивался, и сейчас в нее входят более 2000 компаний, включая такие гигантов компьютерного и телекоммуникационного рынка как 3Com, Compaq, Dell, Lucent Technologies, Microsoft, Motorola, Qualcomm, а также многие другие.В консорциум SIG вошли также компании из таких отраслей, как автомобильная промышленность, автоматизация производства, индустрия бытовой электроники и домашней техники и др.

2.Основные характеристики обмена данных по технологии Bluetooth

Технология беспроводной связи Bluetooth представляет собой недорогой радиоинтерфейс с низким энергопотреблением (мощность передатчика всего порядка 1 мВт) для организации персональных сетей (Personal Area Networking).Обеспечивает передачу в режиме реального времени цифровых данных и звуковых сигналов.Bluetooth реализует собой интерфейс беспроводного взаимодействия между электронными устройствами,используя для этого специальные небольшие приемопередатчики,либо интегрированные в само устройство,либо подключаемые к ним через свободный порт или интерфейсную карту компьютера,избавляя при этом пользователей устройств применять соединительные провода.

Изначально дальность действия радиоинтерфейса закладывалась равной 10 метрам.Такого расстояния хватает для взаиодействия устройств в пределах комнаты.Но в настоящее время спецификациями Bluetooth уже определена и вторая зона взаимодействия - около 100 м - для покрытия стандартного дома или офиса. При этом для Bluetooth нет необходимости в том, чтобы соединяемые устройства находились в зоне прямой видимости друг друга,как например этого требует инфракрасная связь.,и их могут разделять различные препятствия (стены, мебель и т. п.),не экранирующие высокочастотные радио-сигналы.К тому же приборы могут находиться в движении в пределах зоны покрытия устройства.

Для работы устройства Bluetooth используется нижний (2,45 ГГц) диапазон ISM (Industrial, Scientific, Medical), предназначенный для работы промышленных, научных и медицинских приборов. Особенностью данного диапазона является то, что почти во всех странах мира (включая Россию), он свободен от лицензирования, не требующего получение дополнительного разрешения.

Канал радиочастот обладает полной пропускной способностью около 1 Мбит/с, что обеспечивает создание асимметричного канала передачи данных на скоростях 723,3 кбит/с или полнодуплексного канала на скорости 433,9 кбит/с. Через Bluetooth-

соединение можно передавать до 3 дуплексных аудиоканалов по 64 кбит/с в каждом направлении. Разрабатывается также комбинированная передача данных и звука.
В организации обмена данными Bluetooth соответствует спецификации стандарта локальных сетей IEEE 802 и использует сигналы с расширением спектра путем скачкообразной перестройки частоты (FHSS) по псевдослучайному закону со скоростью 1600 переключений в секунду в полосе 2400-2483,5 МГц.
Технология FHSS делает спецификацию bluetooth независимой от выбора полосы радиочастотного взаимодействия.В диапазоне частот, выбранном для Bluetooth, функционирует огромное количество различных устройств:промышленных, медицинских, бытовых , включая микроволновые печи, автомобильные сигнализации и устройства для открывания дверей гаража, коммерческие системы передачи данных и беспроводные локальные сети в стандарте IEEE 802.11. Так как использование всех этих устройств разрешено на безлицензионной основе ,то выбор любой фиксированной частоты функционирования устройства Bluetooth неизбежно приводил бы к "частотному конфликту" с другими устройствами и невозможности работы из-за взаимных радиопомех. Использование технологии FHSS приводит тому, что поражение отдельных частот помехами будет приводить к потерям только небольших фрагментов данных, которые могут быть легко восстановлены путем применения помехозащищенного кодирования. Также,смена частот по псевдослучайному закону снижает влияние интерференционных замираний сигналов за счет переотражений от окружающих предметов, а также затрудняет перехват передаваемых данных злоумышленниками.
Большинство современных устройств,использующих технологию Bluetooth,защищено шифрованием передачи данных на уровне протокола.

3.Принципы взаимодействия между устройствами

Технология bluetooth подразумевает в себе многоточечный радиоканал,управляемый многоуровневым протоколом.
Топология локальной радиосети организована по принципу множественных пикосетей (PAN), взаимодействующих между собой по стандартному радиоканалу. При этом в пикосетях устройства Bluetooth взаимодействуют по принципу master-slave Статус " master предпочтительно должно иметь наиболее мощное устройство, устанавливающее соединения с несколькими другими,и которое и координирует посылку и прием данных в рамках образованной пикосети(основной протокол передачи данных предусматривает более независимое соединение между устройствами). Число активных (активно обменивающихся данными) slaves- устройств в пикосети может доходить до 7. Кроме активных может существовать и множество неактивных устройств, которые не могут обмениваться данными с активными устройствами, пока заняты все каналы, но, тем не менее, остаются синхронизированы с ним. Если в радиусе действия "ведущего" оказывается более 7 активных устройств, то формируется вторая пикосеть, управляемая первой, где роль master выполняет одно из slave устройств первой сети. Такое наращивание сети, в принципе, может идти до бесконечности. Множество пикосетей, способных взаимодействовать друг с другом, формируют распределенную сеть (scatternet). В рамках scatternet разные устройства могут не только быть одновременно master и slave для различных пикосетей, но и просто slave для разных сетей. Более того, в случае необходимости любой slave в пикосети всегда может стать master Естественно, старый master при этом станет одним из slave-устройств Таким образом, в scatternet могут объединяться любые количества устройств Bluetooth, а логические связи - образовываться и изменяться, как это требуется.
Благодаря использованию в Bluetooth-технологии метода скачкообразной перестройки частоты, пикосети могут взаимодействовать друг с другом с минимальным риском

взаимных помех. Единственным условием здесь является то, что различные пикосети, входящие в один scatternet, должны иметь разные каналы связи, то есть работать на различных частотах и иметь различный порядок смены каналов, определяемый в стандарте параметрами FHSS - последовательности скачков. Всего существующий вариант спецификации стандарта предусматривает 10 вариантов **hopping sequence**: 5 с циклом в 79 смен частот и 5 - с циклом в 23 смены.
Одним из важнейших свойств рассматриваемой мной технологии является то, что соединения в пикосетях осуществляются автоматически, как только различные устройства оказываются в пределах досягаемости.Это обстоятельства является большим плюсом в дальнейшей разработке устройств,испоьзующих bluetooth. Для реализации такого автоматизма, работа любых Bluetooth-устройств в незнакомом окружении начинается с режима поиска других устройств.Для этого посылается специальный запрос, ответ на который, однако, зависит не только от наличия в радиусе связи других активных Bluetooth-устройств, но и от режима их работы. На этом этапе возможно три основных режима:

1) **discoverable mode** -устройства в этом режиме всегда отвечают на полученные запросы;
2) 2)**limited discoverable mode** -устройства отвечают на запросы только ограниченное время или при соблюдении определенных условий;
3) **non-discoverable mode** -устройства не отвечают на новые запросы(с установкой определенных правил безопасности-при этом все обнаруженные устройства могут быть в non-connectable mode или в connectable mode. В первом случае найденное устройство не позволяет настроить параметры соединения, и, таким образом, обмен данными с ним невозможен. Во втором случае - связавшиеся Bluetooth-устройства устанавливают между собой соглашения о параметрах соединения (используемый диапазон частот, порядок их смены, размер страниц данных и т. п.).

По окончании процесса обнаружения новое Bluetooth-устройство получает набор адресов для идентификации. Каждое устройство Bluetooth имеет уникальный сетевой адрес(48 бит) и «имена» всех доступных устройств, после чего происходит определение услуг (service discovery), предоставляемых этими устройствами.
В качестве еще одной меры защиты в Bluetooth-устройствах предусмотрено кодирование передаваемых данных, а также выполнение процедуры авторизации устройств. При этом возможны три уровня защиты:

1) минимальная - данные кодируются общим ключом и могут приниматься любыми устройствами без ограничений;
2) защита на уровне устройств - непосредственно в чипе прописывается уровень доступа, в соответствии с которым устройство может получать определенные данные от других устройств;
3) защита на уровне сеанса связи - данные кодируются 64/128-битными случайными числами, хранящимися в каждой паре устройств, участвующих в конкретном сеансе связи.

Рассмотрим теперь алгоритмы и технологии шифрования данных,применяемые в беспроводных сетях Bluetooth.

4.Метод скачкообразной перестройки частоты(FHSS)
Метод скачкообразной перестройки частоты(Frequency Hoping Spread Spectrum) является
одной из компонент спецификации Bluetooth,являющийся основой для конкурентно способного сосуществования Bluetooth с другими спецификациями беспроводной связи.

При методе FH передача данных ведется обычными методами, как в традиционных узкополосных системах, но несущая частота сигнала периодически изменяется, что позволяет легко исправить ошибочно принятые на пораженной помехами частоте блоки, путем их повторной передачи на другой частотной позиции. Порядок следования частот должен быть одинаковым на передающей и приемной стороне. Это достигается одинаковой настройкой аппаратуры и передачей синхросигналов, определяющих моменты начала очередного цикла смены частот. Стандартом IEEE 802.11 предусмотрено использование 79 частотных позиций при времени передачи на каждой в течение 20 мс. Порядок смены частотных позиций определяется псевдослучайным кодом, что обеспечивает определенную защиту передачи от несанкционированного доступа к передаваемой информации.

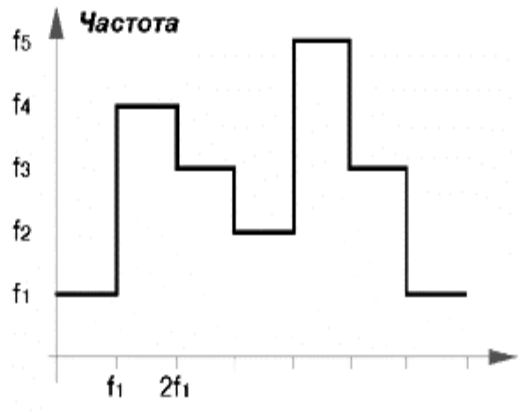


Рис1.Частотные скачки при формировании сигнала

На рис. 1 представлена частотно - временная матрица сигнала скачкообразной перестройки частоты, состоящая из 7 частотных позиций. После использования всех частот начинается их повторное использование в уникальном, установленном для данных передатчика и приемника порядке.

Количество вариантов смены частот легко определить, пользуясь следующими простыми правилами. Допустим, имеется набор из N частот для передачи. Тогда первая частота может быть выбрана N способами, для выбора второй остается (N-1) вариантов, для третьей - (N-2) и т.д.

Последняя, N-ая частота, выбирается единственным способом. Таким образом, количество комбинаций частот для передачи методом FH равно N!. Для рекомендованного стандартом количества частот N=79 количество вариантов выбора порядка их следования имеет значение 8.946*10^116. В общем случае, вероятность принять сигнал FH злоумышленником обратна этой величине, т.е. такое событие практически невозможно. Следовательно, при методе FH обеспечивается дополнительная защита передаваемой информации на уровне физического канала.

5. Технология криптования Wired Equivalent Privacy (WEP), использующая 64-битный ключ и алгоритм RC4,как средства защиты пакетной информации при взаимодействии Bluetooth-устройств

а.) Алгоритм WEP

Алгоритм WEP (Wired Equivalent Privacy) предусматривается стандартом IEEE 802.11 как средство обеспечения безопасности беспроводных сетей. В основе алгоритма - симметричный поточный шифр RC4, разработанный Роном Райвестом, одним из основателей компании RCA Data Securiy.

Достоинства алгоритма WEP:

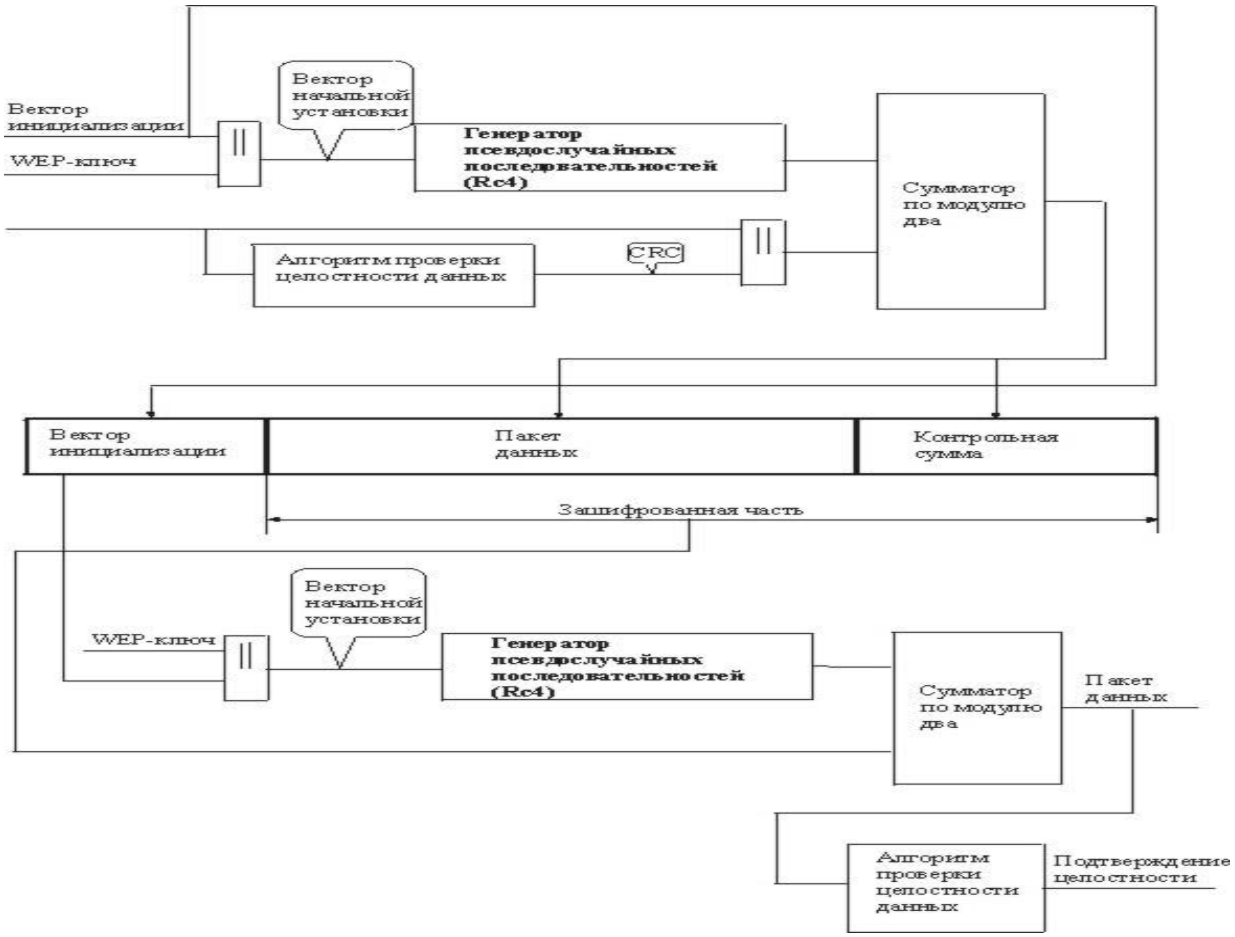
1.Возможность периодической смены ключа и частой смены вектора инициализации;

2.Самосинхронизация шифра по каждому сообщению, что снижает вероятность потери пакетов;

3.Эффективность алгоритма и возможность его реализации как программными, так и аппаратными средствами;

4.Статус дополнительной возможности, что позволяет пользователю самому решать вопрос об использовании этого алгоритма.

Сущность алгоритма WEP поясняется на рисунке.



Секретный 40-бит ключ вводится во все беспроводные устройства сети. При необходимости его может изменять администратор беспроводной сети.

При передаче пакета в аппаратуре формируется 24-разрядный вектор инициализации, который объединяется с секретным ключом в результате операции конкатенации, обозначенной на рисунке значком ||. Полученный 64-разрядный вектор начальной установки используется для приведения в исходное состояние генератора псевдослучайных последовательностей, начинающего формировать псевдослучайную последовательность двоичных символов, равную длине передаваемого пакета с 4-байт контрольной комбинацией циклического кода CRC (Cycliar Redundancy Check). Такая последовательность складывается поразрядно с символами передаваемого пакета и CRC. По радиоканалу передаются оригинальный для каждого пакета вектор инициализации и зашифрованный пакет данных с CRC.

На приемной стороне из пакета выделяется 4-разрядный вектор инициализации, из которого в результате конкатенации с тем же секретным ключом что и на передающей стороне, формируется вектор начальной установки генератора псевдослучайной

последовательности. Сформированная последовательность суммируется по модулю 2 с зашифрованной частью принятого пакета, в результате чего выделяются незашифрованные данные и CRC, используемая для контроля правильности приема пакета данных.

Проблемы в WEP - протоколе
Специалисты, изучающие проблему защиты информации, опубликовали подробный отчет о слабостях в методах кодирования, широко применяемых для засекречивания информации при передаче по беспроволочным сетям.

Корень проблемы – имеющиеся лазейки в обеспечении секретности, возникающие от недостатков в алгоритме присвоения кода, используемом в Wired Equivalent Privacy (WEP) - протоколе, являющимся частью сетевого радио-стандарта 802.11.

Уязвимости защиты при радиопередаче данных были широко описаны и прежде, но основное отличие недавно обнаруженного недостатка заключается в том, что его гораздо проще эксплуатировать. По сообщению EE-Times, пассивный перехват зашифрованного текста с дальнейшей обработкой его по методу, предложенному исследователями, позволил бы злоумышленнику с радио LAN-подключением подбирать защитные коды менее чем за 15 минут. Увеличение длины ключа, применяемого при кодировании, не дало бы пользы при отражении нападений, основанных на использовании фундаментальной ошибки, заключающейся в самой методологии используемой техники кодирования.
Промышленные группы, вовлеченные в продвижение беспроволочных технологий, уже заявили, что работа исследователей продемонстрировала, что защитные меры, применяемые по 802.11-стандарту, недостаточны,поэтому в bluetooth-сетях применяются дополнительные меры шифрования на физическом уровне.

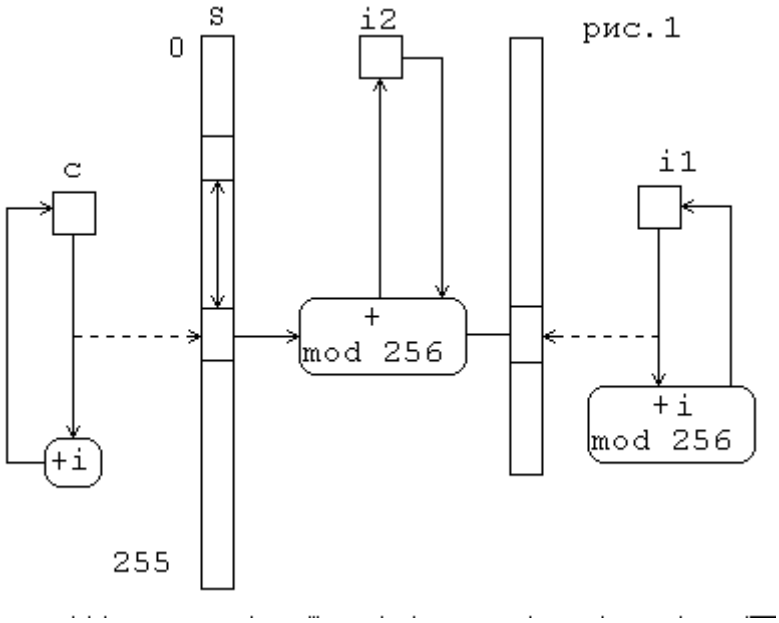
6.Алгоритм RC4

Алгоритм RC4 состоит из трех частей:

1. Создание ключа (иногда называют - расширение ключа).
2. Алгоритм шифрования.
3. Алгоритм расшифровки.

Создание ключа.

Ключ в RC4 представляет собой последовательность байтов произвольной длинны, по которой строится начальное состояни шифра ***S*** - перестановка всех 256 байтов. Алгоритм получения начального состояния изображен на рис.1.

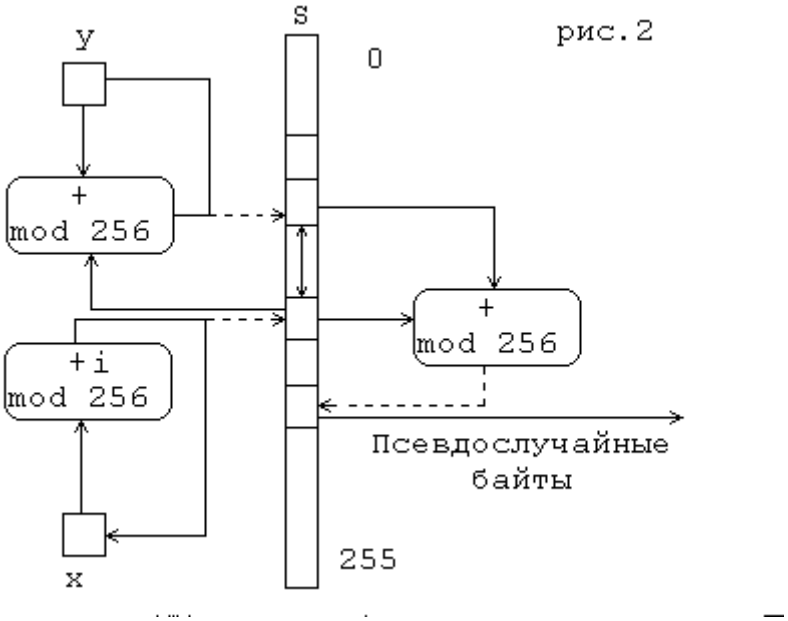


Первоначально ***S*** заполняется последовательными значениями от 0...255. Затем каждый очередной элемент ***S*** обменивается местами с элементом , номер которого определяется элементом ключа ***K***, самим элементом и суммой номеров элементов, с которыми происходил обмен на предыдущих итерациях.

Значения счетчиков ***i*** и с изначально равны 0. Сплошные стрелки означают передачу значений между элементами схемы (присваивание), двусторонние стрелки - обмен значениями, пунктирные стрелки - индексацию в массиве.

Алгоритм шифрования.

Собственно алгоритм псевдослечайных битов в RC4 схематически изображен на рис. 2.



Очередной элемент псевдослучайной перестановки ***S*** всех байтов обменивается с другим, номер которого равен сумме элементов, выбрнных на предыдущих шагах. В качестве очередного байта выдается значение третьего элемента ***S***, номер которого равен сумме первых двух. Значение счетчика *x* первоначально равно 0, но оно увеличивается на 1 уже перед первой выборкой ***S(x)***. Значение *y* первоначально равно 0.

Но затем высчитывается как элемент ключа по номеру ***x*** + предыдущее значение ***y*** и вся сумма по ***mod 256***.

Некоторые важные свойства алгоритма RC4.

- Преобразование очередного состояния генератора (S,x,y) обратимо, так что все возможные состояния повторяются с одинаковой частотой с некоторым периодом.
- Поскольку ***S*** содержит каждый байт ровно один раз, маловероятно, что одни байты будут выдаваться в качестве результата чаще, чем другие.

Заключение

Таким образом,рассмотрев технологию Bluetoothв аспекте безопасности передачи данных,можно отметить,что беспроводные сети,в частности на базе Bluetooth имеют достаточно прочную систему защиту от несанкционированного доступа. При правильном построении сети из bluetooth(куда могут входить PC,PDA,мобильные телефоны,принтеры и многое др.) наиболее вероятную угрозу безопасности представляет нарушение физической целостности, нехарактерное для проводных сетей. При этом следует иметь в виду, что в сетях Bluetooth(и в др стандарта IEEE802.11) без каких-либо ограничений могут применяться средства обеспечения безопасности, предоставляемые операционными системами и программно-аппаратными средствами мониторинга сетей.