УДК 519-7

А. И. Колыбельников

Московский физико-технический институт (государственный университет)
Микротест

Обзор технологий беспроводных сетей

Рассматриваются современные технологии беспроводных сетей, их безопасность и перспективы применения в области организации защищенной связи.

Ключевые слова: беспроводные технологии, протоколы, информационная безопасность, шифрование.

1. Введение

На сегодняшний день большое развитие в области передачи данных получили беспроводные сети — сети радиосвязи. Это объясняется удобством их использования, дешевизной и приемлемой пропускной способностью. Исходя из текущей динамики развития, можно сделать вывод о том, что по количеству и распространенности беспроводные сети в скором времени превзойдут проводные сети.

Эта динамика непосредственным образом влияет на требования к защите информации в беспроводных сетях. В данной работе подробно рассматривается текущее состояние ряда протоколов беспроводной связи, дается оценка перспективам их применения и предлагаются варианты перспективных направлений исследований по обеспечению защиты информации в беспроводных сетях.

2. Технологии беспроводных сетей

Данная статья посвящена обзору основных современных технологий беспроводных сетей, причем особое внимание уделено вопросам обеспечения их безопасности, так как проблема надежной защиты информации служит одним из главных сдерживающих факторов развития беспроводных сетей и систем на их основе.

Радиосети (беспроводные сети) обеспечивают обмен данными между локальными компьютерными сетями, когда использование традиционных кабельных технологий затруднено или нецелесообразно (дорого). Примером эффективного использования беспроводной технологии радиодоступа является обеспечение связи между сегментами локальных сетей при нехватке финансовых средств, отсутствии разрешения на проведение кабельных работ или отказе телефонной станции в аренде выделенного канала. В закрытых помещениях прокладка кабеля может оказаться невозможной из-за неразборного пола или при запрете монтажных работ.

Основой любой беспроводной сети служит ее протокол. Как правило, протокол регламентирует топологию сети, маршрутизацию, адресацию, порядок доступа узлов сети к каналу передачи данных, формат передаваемых пакетов, набор управляющих команд для узлов сети и систему защиты информации. Поэтому в данной работе особое внимание уделено краткому описанию протоколов.

3. Описание протоколов

Все многообразие протоколов беспроводной передачи данных можно классифицировать несколькими различными путями, выбрав в качестве основного один из параметров, например топологию сети, скорость работы или алгоритмы безопасности. Наиболее распространенный метод классификации в технической литературе исходит из максимального радиуса действия беспроводной сети. Ниже приведена классификация рассматриваемых протоколов по порядку уменьшению радиуса.

WWAN (Wireless Wide area network) – в основном это сети сотовой связи, их радиус действия составляет десятки километров. К этим сетям относятся следующие протоколы: GSM, CDMAone, iDEN, PDC, GPRS и UMTS.

WMAN (Wireless Metropolitan Area Networks – это беспроводные сети масштаба города. Радиус действия таких сетей несколько километров. Примером протокола этой сети служит WiMAX.

Wireless LAN (Wireless Local Area Network; WLAN) – это беспроводная локальная вычислительная сеть. Радиус действия этого класса сетей — несколько сотен метров. К ним относятся следующие протоколы: UWB, ZigBee, Wi-Fi.

WPAN применяются для связи различных устройств, включая компьютеры, бытовые приборы и оргтехнику, средства связи и т. д. Радиус действия WPAN составляет от нескольких метров до нескольких десятков метров. WPAN используется как для объединения отдельных устройств между собой, так и для связи их с сетями более высокого уровня. Примером таких сетей могут служить протоколы RuBee, X10, Insteon, Bluetooth, Z-Wave, ANT, RFID.

Ниже кратко описывается каждый из рассматриваемых протоколов. Эти протоколы выбраны для анализа вследствие их широкого распространения в современных беспроводных сетях связи. Такой выбор позволяет дать обзор текущего состояния информационной безопасности в сетях беспроводной связи вне зависимости от решаемых беспроводными сетями задач.

4. Модель OSI

Помимо радиуса действия сетей роль протоколов важна при определении уровней в модели OSI. Эталонная модель OSI, иногда называемая стеком OSI, предусматривает 7–уровневую сетевую иерархию, разработанную Международной организацией по стандартам (International Standardization Organization — ISO). Ниже представлено разделение уровней и решаемые на этих уровнях задачи.

1	Физический	Собственно кабель или физический носитель
2	Канальный	Передача и прием пакетов, определение аппаратных адресов
3	Сетевой	Маршрутизация и ведение учета
4	Транспортный	Обеспечение корректной сквозной пересылки данных
5	Сеансовый	Аутентификация и проверка полномочий
6	Представления данных	Интерпретация и сжатие данных
7	Прикладной	Предоставление услуг на уровне конечного пользователя: почта, регистрация и т.д.

Следует отметить, что многие из рассмотренных ниже протоколов были разработаны IEEE. Группа протоколов IEEE 802.X содержит описание сетевых спецификаций и дает стандарты, рекомендации и информационные документы для сетей и телекоммуникаций.

Рекомендации IEEE связаны главным образом с двумя нижними уровнями модели OSI — физическим и канальным. Эти рекомендации делят канальный уровень на два подуровня: нижний — MAC (управление доступом к среде) и верхний — LLC (управление логическим каналом).

4.1. Bluetooth

Протокол передачи информации по беспроводному каналу связи Bluetooth был разработан группой компаний Ericsson, IBM, Intel, Toshiba и Nokia. Группа разработки была создана в начале 1998 года. 20 мая 1998 года произошло официальное представление специальной рабочей группы (SIG — Special Interest Group), призванной обеспечить беспрепятственное внедрение технологии, получившей название Bluetooth.

Bluetooth обеспечивает обмен информацией между такими устройствами, как карманные и обычные персональные компьютеры, мобильные телефоны, ноутбуки, принтеры, цифровые фотоаппараты, мышки, клавиатуры, джойстики, наушники, гарнитуры на надёжной, недорогой, повсеместно доступной радиочастоте для ближней связи. Связь этих устройств может осуществляться в радиусе от 10 до 100 метров друг от друга даже в разных помещениях.

4.2. UWB

Протокол UWB был разработан альянсом компаний WiMedia, а в 2007 году этот протокол был утвержден в качестве международного стандарта ISO/IEC 26907.

WiMedia UWB является стандартом широкополосной беспроводной связи на коротких расстояниях. Протокол затрагивает аспекты взаимодействия между устройствами на физическом уровне (PHY) и подуровне доступа к среде (MAC). Максимальная скорость передачи данных между устройствами WiMedia UWB составляет 480 Мбит/с (как и у проводного USB), устройства работают в диапазоне частот от 3,1 до 10,6 ГГц. Протокол UWB конкурирует с протоколом Bluetooth.

4.3. ZigBee

Протокол ZigBee — это стандарт для недорогих, маломощных беспроводных сетей с ячеистой топологией. Низкая стоимость позволяет широко применять данную технологию для беспроводного контроля и наблюдения, а благодаря малой мощности сенсоры сети способны работать долгое время, используя автономные источники питания.

Протокол был разработан альянсом компаний ZigBee. Этот альянс служит органом, определяющим для ZigBee стандарты высоких уровней; он также публикует профили приложений, что позволяет производителям исходных комплектующих выпускать совместимые продукты.

Нижние уровни для данного стандарта разработаны IEEE и определяются стандартами IEEE 802.15.4-2006.

4.4. Insteon

Протокол INSTEON разработан для управления беспроводными устройствами, предназначенными для «умного дома». В протоколе предусмотрена обратная совместимость с более старым протоколом X10. Скорость передачи сигнала управления по новому стандарту гораздо выше, предусматриваются встроенные средства обнаружения ошибок и повторной передачи сигнала, а для передачи используется гибридный канал — радиосвязь и сеть электропитания. Однако в отличие от X10 спецификации INSTEON защищены патентами и используются только его разработчиками — компанией Smarthome Technology.

4.5. Z-Wave

Ячеистая сеть Z-Wave с функциями самоорганизации и самовосстановления в сочетании с гибкими инсталляционными процедурами представляет собой простое в использовании сетевое решение. Протокол Z-Wave и чип высокой степени интеграции обеспечивает невысокую стоимость без компромисса в отношении надежности или универсальности.

Реализуется совместимость приложений и устройств Z-Wave, выпущенных разными производителями.

Z-Wave поддерживает полный спектр устройств, включая устройства, питающиеся от сети переменного тока, от батарей, устройства с фиксированным расположением и перемещаемые устройства, а также устройства, выполняющие роль мостов с другими протоколами.

В технологии Z-Wave узлы делятся на три типа: контроллеры (Controllers), маршрутизирующие исполнительные механизмы (Routing Slaves) и исполнительные механизмы (Slaves). В реальной сети все типы устройств могут работать в любой комбинации.

4.6. ANT

Протокол передачи данных ANT был разработан компанией Dynastream Innovations.

Данный протокол прежде всего рассчитан на компактные устройства с автономным питанием (трансиверы, использующие этот протокол, отличаются исключительно малым током потребления) для передачи относительно коротких пакетов данных. Протокол предусматривает организацию открытых и частных беспроводных сетей, в том числе сложного типа с динамической конфигурацией. Он создан на основе технологии PAN (Personal Area Network) и поддерживает слои 1–4 стека OSI (Open Systems Interconnection network model). Типичное применение такого протокола — беспроводные датчики.

Несущая частота по протоколу ANT — 2,4 ГГц, количество частотных каналов при этом равно 125 (шаг 1 МГц в диапазоне 2400...2524 МГц). Скорость передачи данных по радиоканалу (включая протокол) может составлять до 1 Мбит/с.

4.7. RuBEE

RuBee (IEEE P1902.1) — протокол двухсторонней беспроводной связи в местной региональной сети с использованием длинноволнового диапазона (LW) и пакетов данных не более 128 байт. Протокол RUBee подобен протоколам серии IEEE 802, также известным как Wi-Fi (IEEE 802.11), WPAN (IEEE 802.15.4) и Bluetooth (IEEE 802.15.1). RuBee networked, работает по принципу точка-точка и является развитием стандартов RFID. RuBee предусматривает работу на низкочастотной несущей (131 кГц), позволяя использовать узлы сети с малым потреблением энергии.

4.8. RFID

RFID Radio Frequency IDentification. Радиочастотная идентификация появилась более тридцати лет назад. В 1973 году Марио Кардулло и его соавторы опубликовали патент US 3713148, описывающий первый пассивный транспондер RFID (радиометку). Развитие и широкое внедрение радиочастотной идентификации долго сдерживалось отсутствием стандартизации. Но в 90-х годах прошлого века Международная Организация Стандартизации (ISO) приняла ряд стандартов в области RFID (серия стандартов ISO 18000-6).

4.9. X10

X10 — это международный открытый индустриальный стандарт, применяемый для связи электронных устройств в системах домашней автоматизации. Стандарт X10 определяет методы и протокол передачи сигналов управления электронными модулями, к которым подключены бытовые приборы, с использованием обычной электропроводки или беспроводных каналов.

Стандарт X10 разработан в 1975 году компанией Pico Electronics (Шотландия) для управления домашними электроприборами. Считается, что это первый стандарт для домашней автоматизации.

4.10. WI-FI

Wi-Fi создан в 1991 году NCR Corporation/AT&T (впоследствии — Lucent Technologies и Agere Systems) в Нидерландах. *Wireless Fidelity* — «беспроводная точность» — торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11.

Обычно схема Wi-Fi сети содержит не менее одной точки доступа (так называемый режим infrastructure) и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка, когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0.1 Мбит/с каждые 100 мс. Поэтому 0.1 Мбит/с — это 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.

4.11. PDC

PDC (Personal Digital Cellular) — стандарт сотовой связи поколения 2G. Разработан ассоциацией ARIB (Association of Radio Industries and Business) в апреле 2001 года. Используется исключительно на территории Японии. В настоящее время количество абонентов сотовой связи, работающих на данном стандарте, сократилось до 10 миллионов человек. Притом, что в период максимальной распространенности этого стандарта количество абонентов достигало 80 миллионов человек. PDC использует частотные каналы по 25 кГц с модуляцией pi/4-DQPSK с тремя временными слотами, обеспечивающими передачу со скоростью 11.2 кбит/с или 6 временными слотами со скоростью передачи 5.6 кбит/с.

PDC использует два диапазона частот — 800 МГц и 1,5 ГГц.

4.12. IDEN

IDEN (Integrated Digital Enhanced Networks) – технология для сетей транкинговой и сотовой связи, разработана компанией MOTOROLA в 1994 году. В основе технологии iDEN архитектура GSM, при передаче используют частотные каналы по 25 кГц, при этом для передачи данных используется часть канала шириной 20 кГц, остальное преназначено для защиты канала. Протокол получил широкое распространение во всем мире. Диапазон частот — 821–825 МГц.

4.13. CDMAOne

Стандарт CDMAOne разработан в 1995 году как технологический стандарт группы ANSI. CDMAOne основан на использовании CDMA (множественного доступа с кодовым разделением).

Система CDMA IS-95 фирмы Qualcomm рассчитана на работу в диапазоне частот 800 МГц, выделенном для сотовых систем стандартов AMPS, N-AMPS и D-AMPS. (Стандарты TIA IS-19, IS-20; IS-54; IS-55, IS-56, IS-88, IS-89, IS-90, (S-553).

Последующее развитие технологии CDMA происходит в рамках технологии CDMA2000. При построении системы мобильной связи на основе технологии CDMA2000 1X первая фаза обеспечивает передачу данных со скоростью до 153 кбит/с, что позволяет предоставлять услуги голосовой связи, передачу коротких сообщений, работу с электронной почтой, Интернетом, базами данных, передачу данных и неподвижных изображений.

4.14. 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.

Название «WiMAX» было предложено WiMAX Forum — организацией, основанной в июне 2001 года для продвижения и развития технологии WiMAX. Форум описывает WiMAX как «основанную на стандарте технологию, предоставляющую высокоскоростной беспроводной доступ к сети, альтернативный выделенным линиям и DSL» Максимальная скорость — до 1 Гбит/с.

4.15. GSM

GSM (от названия группы Groupe Special Mobile, позже переименован в Global System for Mobile Communications) (русск. СПС-900) — глобальный цифровой стандарт для мобильной сотовой связи с разделением частотного канала по принципу TDMA и средней степенью безопасности. Разработан под эгидой Европейского института стандартизации электросвязи (ETSI) в конце 1980-х годов.

Коммерческое использование стандарта началось в середине 1991 г., а к 1993 г. было организовано 36 сетей GSM в 22 странах. В дополнение к европейским государствам стандарт GSM выбрали многие страны Южной Африки, Ближнего и Дальнего Востока, а также Австралия. К началу 1994 г. число абонентов GSM достигло 1.3 миллиона. Термин GSM является сокращением от Global System for Mobile telecommunications — глобальная система мобильных телекоммуникаций.

GSM относится к сетям второго поколения (2 Generation), хотя на 2010 год условно находится в фазе 2,75G благодаря многочисленным расширениям (1G — аналоговая сотовая связь, 2G — цифровая сотовая связь, 3G — широкополосная цифровая сотовая связь, коммутируемая многоцелевыми компьютерными сетями, включая Интернет).

Сотовые телефоны выпускаются для 4 диапазонов частот: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц.

4.16. GPRS

GPRS (General Packet Radio Service — пакетная радиосвязь общего пользования) — надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю сети сотовой связи производить обмен данными с другими устройствами в сети GSM и с внешними сетями, включая Интернет.

Передача данных разделяется по направлениям «вниз» (downlink, DL) — от сети к абоненту и «вверх» (uplink, UL) — от абонента к сети. Мобильные терминалы разделяются на классы по количеству одновременно используемых таймслотов для передачи и приёма данных. По данным за июнь 2006 г., телефоны поддерживают до 4-х таймслотов одновременно для приёма по линии «вниз» (то есть могут принимать 85 кбит/с по кодовой схеме CS-4) и до 2-х – для передачи по линии «вверх» (class 10 или 4+2).

4.17. UMTS

UMTS (Universal Mobile Telecommunications System — Универсальная Мобильная Телекоммуникационная Система) — технология сотовой связи разработана Европейским Институтом Стандартов Телекоммуникаций (ETSI) для внедрения 3G в Европе. В качестве способа передачи данных через воздушное пространство используется технология W-CDMA, стандартизованная в соответствии с проектом 3GPP в качестве ответа европейских учёных и производителей на требование IMT-2000, опубликованное Международным союзом электросвязи как набор минимальных критериев для сети сотовой связи третьего поколения.

Согласно спецификациям стандарта, UMTS использует спектры частот: 1885–2025 МГц для передачи данных в режиме «от мобильного терминала к базовой станции» и 2110–2200 МГц для передачи данных в режиме «от станции к терминалу». В США по причине занятости спектра частот в диапазоне 1900 МГц сетями GSM выделены диапазоны 1710–1755 МГц и 2110–2155 МГц соответственно. Кроме того, операторы некоторых стран (например, американский AT&T Mobility) дополнительно эксплуатируют полосы частот 850 и 1900 МГц. Правительство Финляндии на законодательном уровне поддерживает развитие сети стандарта UMTS900, покрывающей труднодоступные районы страны и использующей диапазон 900 МГц (в данном проекте участвуют такие компании, как Nokia и Elisa).

5. Топологии

Все перечисленные беспроводные сети работают в одном или нескольких вариантах топологии. На рис.1 приведены топологии беспроводных сетей различных конфигураций.

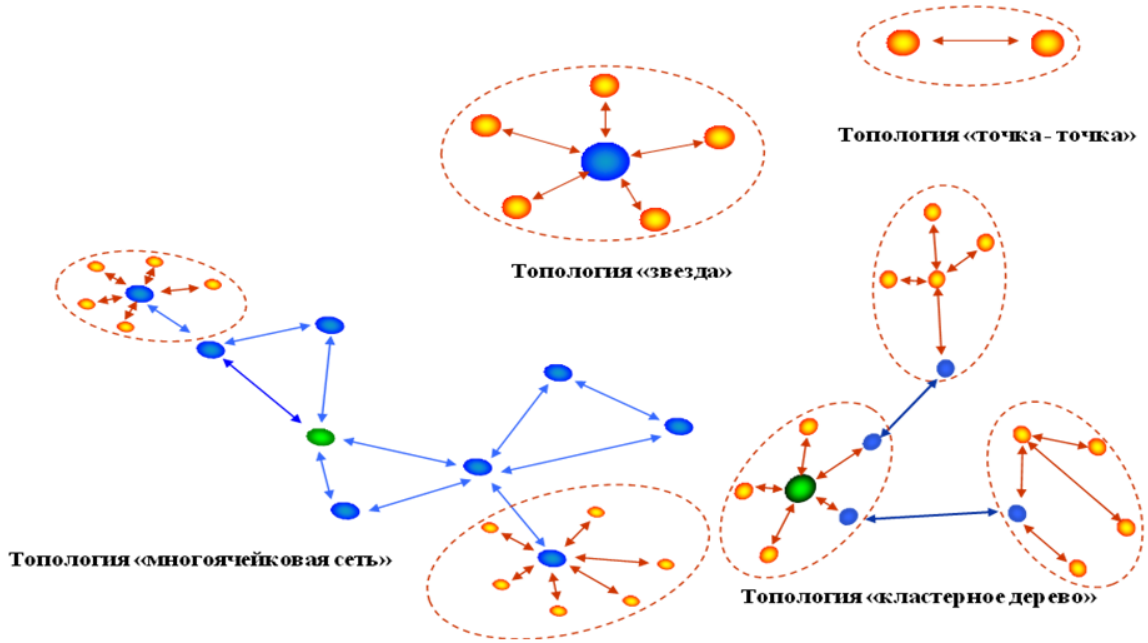

Рис. 1. Топологии беспроводных сетей

5.1. Топология точка-точка

Самый простой вариант организации сети из двух устройств. Как правило, узлы этой сети являются равноправными, то есть сеть одноранговая.

Эта топология характерна для Bluetooth, ANT, RFID, RuBee, PDC, WI-FI, Insteon, UWB, ZigBee и прочих.

5.2. Топология «Звезда»

Эта топология служит основой организации всех современных сетей связи и вычислительных сетей. Данную топологию используют протоколы WI-FI, Insteon, ZigBee, UWB, IDEN, CDMAOne, WIMAX, GSM, GPRS, UTMS.

5.3. Топология «многоячейковая сеть»

Многоячейковая сеть — базовая полносвязная топология компьютерных сетей и сетей связи, в которой каждая рабочая станция сети соединяется со всеми другими рабочими

станциями этой же сети. Характеризуется высокой отказоустойчивостью, сложностью настройки и избыточным расходом кабеля в проводных сетях. Каждый узел имеет несколько возможных путей соединения с другими узлами, за счет этого такая топология очень устойчива. Так как исчезновение одного из каналов не приводит к потере соединения между двумя компьютерами. Эта топология допускает соединение большого количества узлов и характерна, как правило, для крупных сетей, она строится из полносвязной путем удаления некоторых возможных связей.

Топология применима для сетей с использованием протоколов UWB, WI-FI, Insteon, ZigBee, UWB, IDEN, CDMAOne, WIMAX, GSM, GPRS, UTMS.

5.4. Топология «кластерное дерево»

Топология «Кластерное дерево» образуется в основном в виде комбинаций вышеназванных топологий вычислительных сетей. Основание дерева вычислительной сети располагается в точке (корень), в которой собираются коммуникационные линии информации (ветви дерева).

Вычислительные сети с древовидной структурой строятся там, где невозможно непосредственное применение базовых сетевых структур в чистом виде.

6. Методы разделения доступа к радиоканалу

В этом разделе описаны основные методы разделения доступа к радиоканалу. Использование этих методов доступа в современных протоколах передачи информации по беспроводным каналам связи вызвано необходимостью передавать большие объемы информации за короткий промежуток времени, поддерживать связь с несколькими абонентами в узких диапазонах частот.

В современных протоколах передачи данных предусматривается три основных метода разделения доступа устройств связи к радиоканалу — CDMA, FDMA, TDMA. Также существует ряд их модификаций.

6.1. CDMA

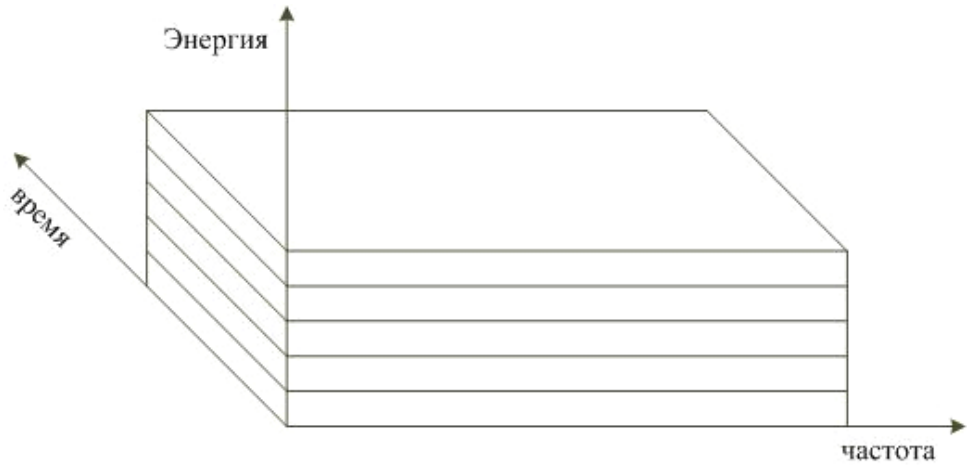

Рис. 2. Разделение канала в CDMA

Code Division Multiple Access (CDMA) — это другой метод доступа к каналу, который используется в мобильной телефонии третьего поколения (3G). CDMA является расширением нескольких технологий доступа, использующим уникальную схему кодирования, позволяющую нескольким пользователям одновременно общаться по одному физическому каналу. Таким образом, каждой группе пользователей предоставляется уникальный общий

код, причем не может быть, чтобы в одном и том же канале работали несколько пользователей с разными кодами, и общаться и понимать друг друга может единственная группа пользователей, имеющих один и тот же код.

Основная особенность этой технологии в том, что она позволила увеличить количество сигналов для заданной частотной полосы. Первоначальный стандарт CDMA, известный также как IS-95 или cdmaOne, до сих пор используется в сетях мобильной телефонии 2G. CDMA обеспечивает более высокую по сравнению с другими методами доступа скорость передачи данных.

Чтобы продемонстрировать различия в работе трех методов разделения доступа к каналу, допустим, что в одной комнате находится две группы абонентов. Используя FDMA, члены каждой группы располагают различными частотными полосами голосовой связи, т.е. осуществляется разделение по частоте. В системе TDMA каждой группе отводится для разговора свой временной интервал, т.е. осуществляется разделение по времени. И, наконец, CDMA предоставляет обеим группам возможность общаться на разных языках на одинаковых частотах в одно и то же время, т.е. реализуется разделение по коду.

6.2. CSMA

Carrier Sense Multiple Access (CSMA) — вероятностный сетевой протокол канального (MAC) уровня. Узел, желающий передать пакет данных, выполняет процедуру оценки чистоты канала, то есть в течение заранее заданного времени определяет уровень шума в передающей среде. Если передающая среда оценивается как чистая, узел может передать пакет данных. В противном случае, если выполняется другая передача, узел «отстраняется», то есть, прежде чем опять предпринять процедуру отправки пакета, узел ждёт определённое время.

На практике более распространена модификация этой технологии — CSMA/CD, предусматривающая контроль коллизий. Существует также технология CSMA/CA, в которой предпринимаются меры по исключению коллизий. На рис. 3 представлен один кадр для метода доступа устройств в сеть CSMA.

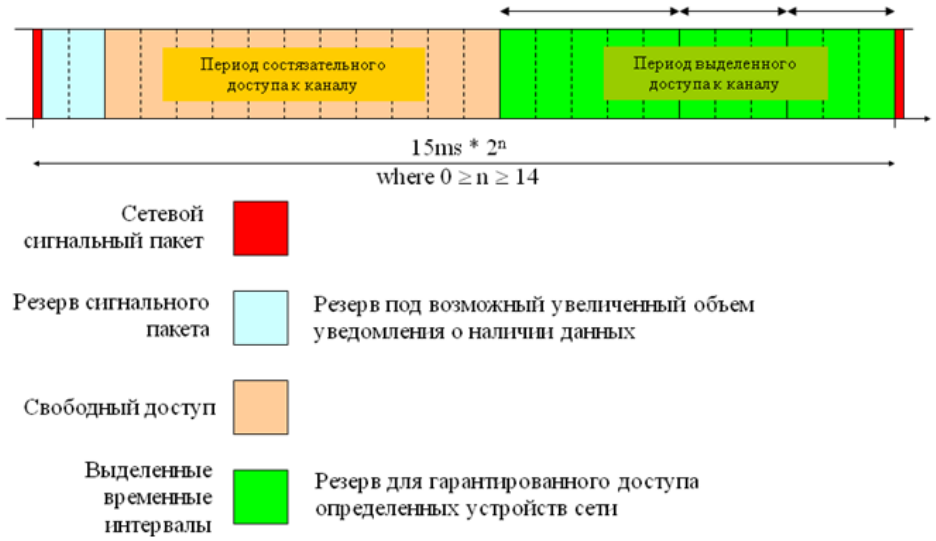

Рис. 3. Система синхронизации и обеспечения множественного доступа к каналу CSMA

6.3. TDMA

TDMA Time Division Multiple Access — множественный доступ с разделением по времени — способ использования радиочастот, когда в одном частотном интервале находится

несколько абонентов, причем для передачи разным абонентам отведены разные временные интервалы (слоты). Это приложение метода временного мультиплесирования (TDM — Time Division Multiplexing) к радиосвязи.

Таким образом, TDMA предоставляет каждому пользователю полный доступ к частотному интервалу в течение короткого промежутка времени (в GSM один частотный интервал делится на 8 временных слотов). В настоящее время TDMA является доминирующей технологией для мобильных сотовых сетей и используется в стандартах GSM, TDMA (ANSI-136), PDC.

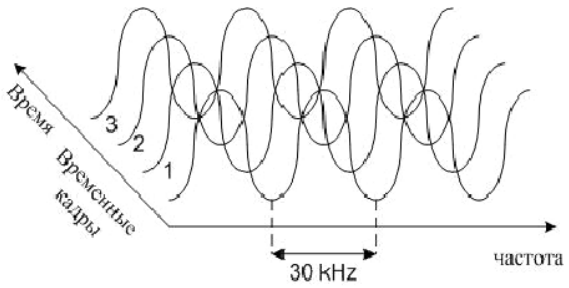

Рис. 4. Распределение каналов в TDMA

FDMA Frequency Division Multiple Access — множественный доступ с разделением каналов по частоте — способ использования радиочастот, когда в одном частотном диапазоне находится только один абонент, а разные абоненты в пределах соты используют разные частоты. Является приложением частотного мультиплексирования (FDM) в радиосвязи. Пока начальный запрос не закончен, канал для других сеансов связи закрыт. При полном дуплексном режиме (Full-Duplex) по методу FDMA требуется два канала — один для передачи, а другой для приема. FDMA использовался в аналоговой связи первого поколения (1G): этот принцип реализован в стандартах AMPS, N-AMPS, NMT, ETACS (американский стандарт).

На рис. 5 проводится сравнение методов разделения канала TDMA и FDMA. Можно заметить зависимость появления сигналов в канале от времени и частоты для каждого из методов разделения. В случае TDMA основной служит ось времени, в случае FDMA — ось частоты.

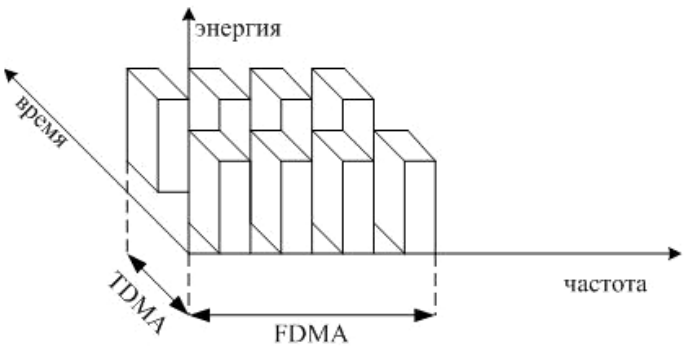

Рис. 5. Сравнение методов разделения радиоканала

6.4. OFDM

OFDM (Orthogonal frequency-division multiplexing) — ортогональное частотное разделение каналов с мультиплексированием) является цифровой схемой модуляции, которая ис-

пользует большое количество близко расположенных ортогональных поднесущих. Каждая поднесущая модулируется по обычной схеме модуляции (например, квадратурная амплитудная модуляция) на низкой символьной скорости, сохраняя общую скорость передачи данных, как и у обычных схем модуляции одной несущей в той же полосе пропускания. На практике сигналы OFDM получаются путем использования БПФ (быстрое преобразование Фурье).

Все приведенные методы разделения доступа к каналу применяются в беспроводных сетях с множественным доступом. При этом сети могут иметь разную топологию.

6.5. Безопасность беспроводных сетей

Безопасность беспроводных сетей зависит от использования ряда технологий: шифрования, цифровой подписи, паролей, смены ключей и прочего. То, как используются эти технологии сильно влияет на уровень защищенности сети. Иногда, методика использования ранее перечисленных технологий такова, что они никак не влияют на уровень защищенности сети. Эти вопросы детально рассматриваются ниже.

6.6. Шифрование

Ниже перечислены алгоритмы шифрования, применяемые в каждой из технологий, в перечне указана технология, стандарт шифрования и его режим.

- Bluetooth – E0 – ECB;
- UWB – AES – CBC;
- ZigBee – AES – CBC;
- Insteon – Rolling code system – поточное;
- Z-Wave – 3DES только в 100 серии – ECB;
- ANT – нет;
- RuBee - AES;
- RFID – Crypto1, DES – асиметричный;
- X10 – нет;
- WI-FI – RC4, AES – CBC;
- PDC – A5 – поточное;
- IDEN – A5 – поточное;
- CDMA – CMEA – ECB;
- WIMAX – 3DES, AES – ECB;
- GSM – A5 (COMP-128) – поточное;
- GPRS – GEA1, GEA2 – поточное;
- UMTS – A5 (COMP-128) KASUMI MILENAGE – поточное.

Стандарт шифрования E0. В стандарте Bluetooth применяется поточный шифр E0, построенный на базе трех линейных генераторов сдвига. Общая схема шифрования и генерации общего ключа приведена на рис 6. Эта схема применяется в Bluetooth в режимах обеспечения безопасности 2 и 3. Данные режимы безопасности применяются в протоколе Bluetooth v2.0 + EDR.

В протоколе Bluetooth v2.0 + EDR (и более ранних версий, работающих в режимах безопасности 2 и 3) два устанавливающих соединение устройства одновременно получают одинаковый сеансовый ключ в случае, если пользователь установил для них одинаковый PIN. Ввод PIN-кода и установка сеансового ключа схематически представлены на рис. 6. Следует отметить, что если PIN-код короче 16 байтов, то для генерации сеансового ключа как дополнение к значению текущего PIN-кода используется BD_ADDR.

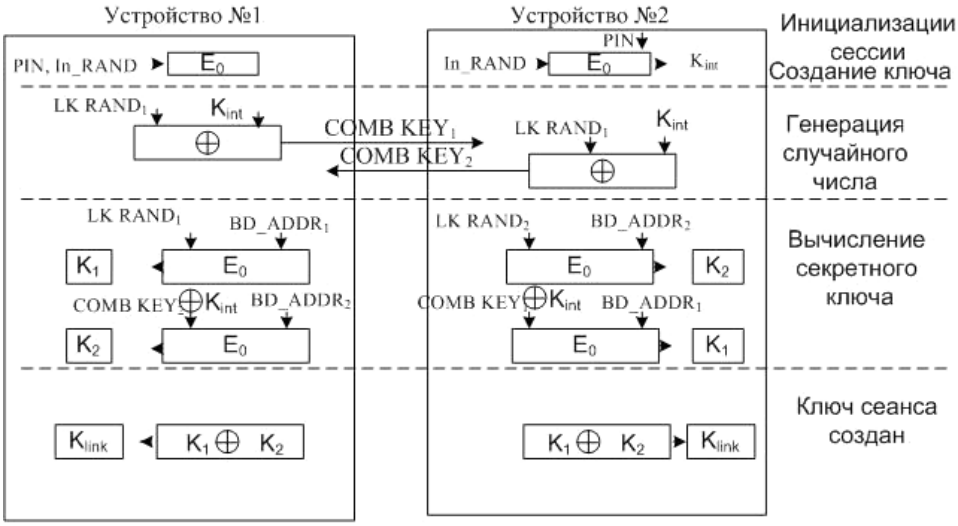

Рис. 6. Схема соединения двух устройств Bluetooth для генерации общего ключа

Основой процедуры шифрования в протоколе Bluetooth служит алгоритм потокового шифрования E0. Ключ потока суммируется по схеме XOR с битами открытого текста и передается на принимающее устройство. Ключ потока генерируется посредством криптографического алгоритма на базе линейного рекуррентного регистра (ЛРР). Функция шифрования получает следующие входные данные: главный идентификатор (BD_ADDR), 128-битное случайное число (EN_RAND), номер слота и ключ шифрования, который также инициализирует ЛРР, если шифрование включено. Номер слота, используемый в потоковом шифре, меняется с каждым пакетом, меняя тем самым инициализацию ядра шифра, другие же переменные при этом не меняются.

Ключ шифрования KC генерируется из текущего сеансового ключа и может иметь длину от 8 до 128 бит. Установление размера ключа происходит в ходе установления сеанса шифрования между устройствами. Начальный размер ключа вносится в устройство производителем, и размер его не всегда максимален.

Следует отметить, что алгоритм E0 не сертифицирован FIPS как национальный стандарт.

Имеется теоретическая оценка стойкости данного алгоритма. При атаке со знанием открытого текста требуется 238 переборов, в то время как при атаке грубой силы необходимо перебрать 2128 возможных ключей.

Шифр Диффи–Хеллмана на эллиптических кривых. В режиме обеспечения безопасности 4 по протоколу Bluetooth v2.1 + EDR используется пара ключей безопасного простого сопряжения (Secure Simple Pairing — SSP). Эта пара ключей представляет собой ключи алгоритма асиметричного шифрования Диффи–Хеллмана на эллиптических кривых. Взаимодействие двух абонентов с использованием ключей SSP показано на рис. 8.

Данный алгоритм надежен: реализуемых на практике эффективных атак на сам алгоритм в данный момент не существует. Но имеется вероятность того, что атака окажется успешной при программной и аппаратной реализации алгоритма.

6.7. Стандарт шифрования AES

Данный стандарт шифрования наиболее широко применяется для защиты беспроводных каналов передачи информации. Он используется в протоколах UWB, ZigBee, RuBee, WI-FI и WIMAX. В связи с широким распространением данного алгоритма его описание в данной работе не приводится. Если ключи генерируются на каждый сеанс надежной системой распределения секрета, эффективных атак на данный алгоритм нет.

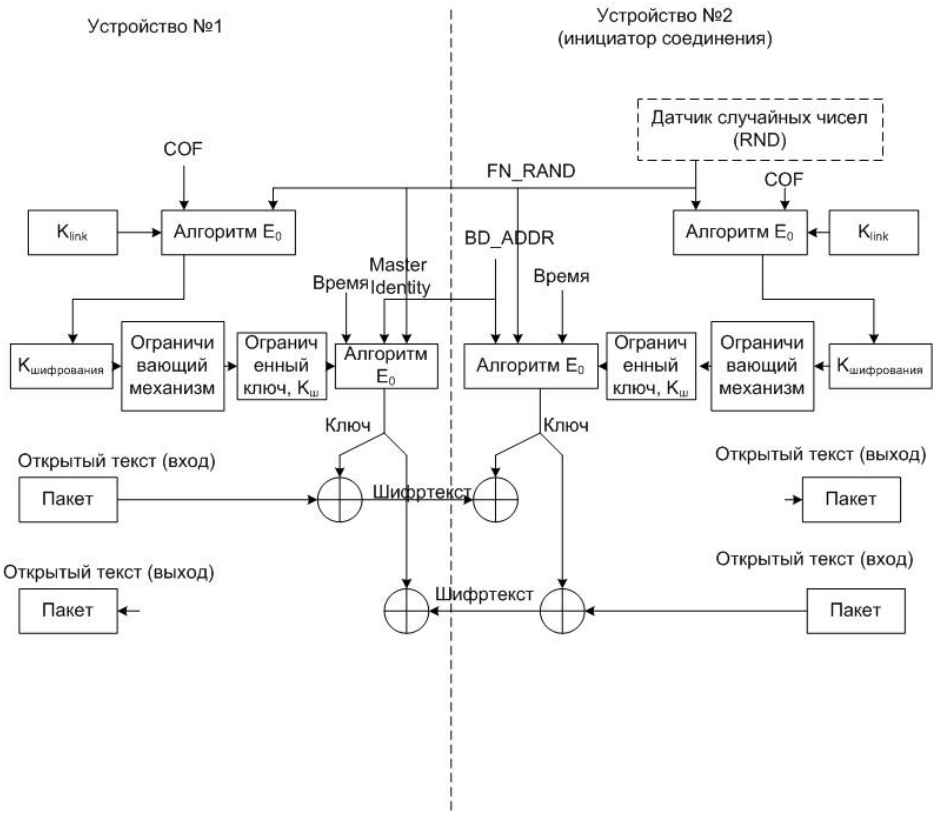

Рис. 7. Порядок установления защищенного соединения

Шифр CMEA. Безопасность связи обеспечивается также применением процедур аутентификации и шифрования сообщений. В CDMA для генерации 128 бит ключа в сотовой связи используется стандартный алгоритм аутентификации и шифрования речи CAVE (Cellular Authentication Voice Encryption). Ключ называется SSD (Shared Secret Date — «общие секретные данные»). Эти данные генерируются на основе A-ключа, который хранится в мобильной станции, из полученного от сети псевдослучайного числа. Общие секретные данные (SSD) генерирует алгоритм CAVE. Они разделяются на две части: SSD-A (64 бита), предназначенную для выработки цифровой подписи (authentication signature), и SSD-B (64 бита), предназначенную для генерации ключей, используемых для шифрования речи и передачи сигнала сообщения. SSD может использоваться поставщиками услуг для местной аутентификации при роуминге. Новые общие секретные данные (SSD) могут генерироваться при перемещении мобильной станции к чужой сети или ее возвращении к домашней сети.

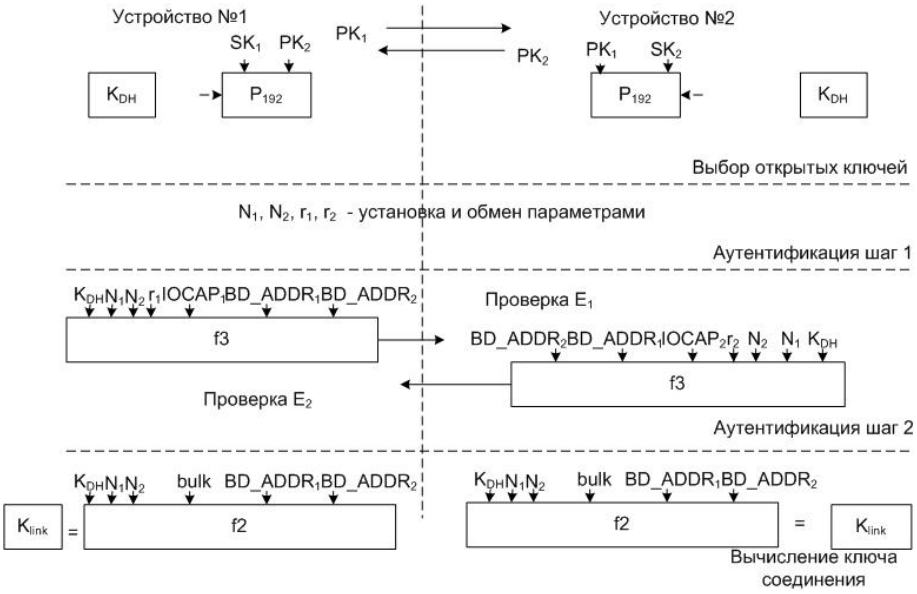

Рис. 8. Взаимодействие абонентов при помощи ключей SSP

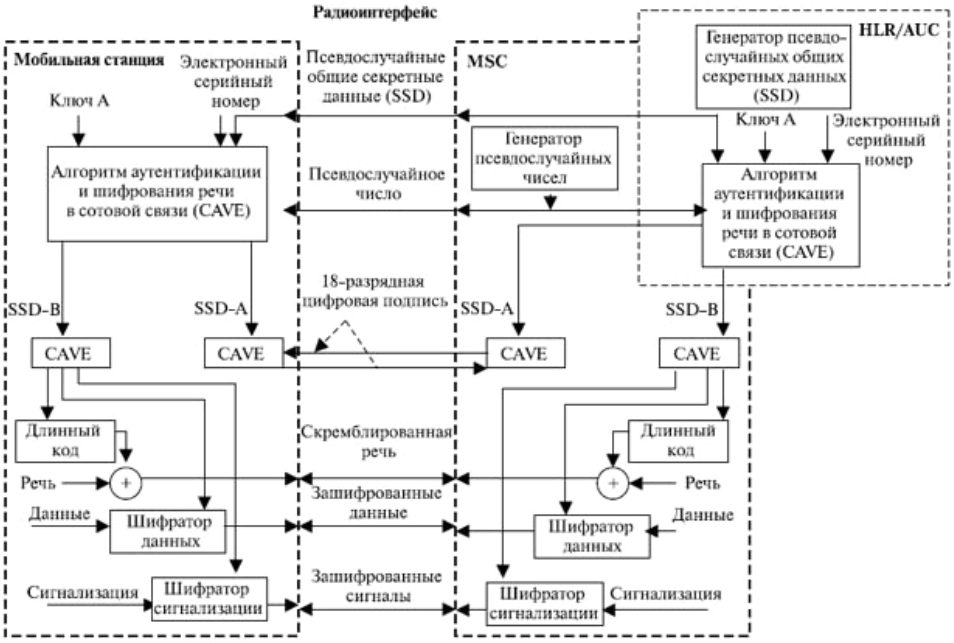

Рис. 9. Процедура шифрования в CDMA с использованием шифра CMEA

6.8. Алгоритм Rolling code system

Этот шифр, называемый также KeeLoq, использует линейный рекуррентный регистр сдвига. Длина основного регистра 32 бита, длина дополнительного регистра 5 бит. Шифрование производится побитным суммированием с ключом. Для данного алгоритма существуют эффективные атаки. Например, чтобы получить систему линейных уравнений, позволяющую восстановить начальное заполнение линейного регистра, достаточно путем прослушивания ключевой последовательности перехватить ее 216 символов.

6.9. Алгоритм Crypto 1

Данный алгоритм использует комбинацию линейных и нелинейных рекуррентных регистров. Длина ключа — 48 бит.

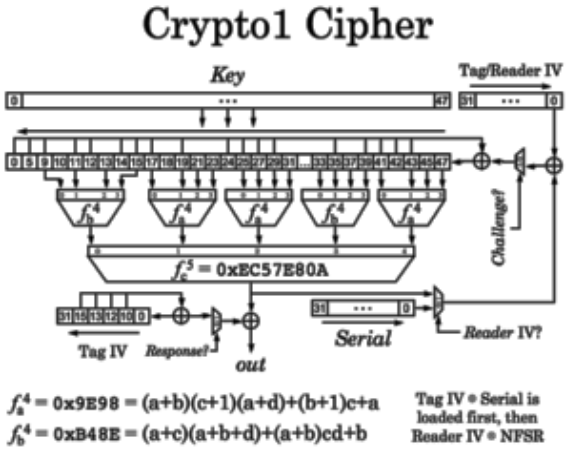

Рис. 10. Алгоритм Crypto 1

В настоящий момент предлагаемые методы криптоанализа Crypto 1 позволяют восстанавливать весь ключ при перехвате его 12 бит.

Алгоритм шифрования A5. Поток данных (передаваемый на DCCH и TCH) шифруется побитно (потоковым шифром), то есть поток данных, получаемых по радиоканалу от пользователя, и поток битов ключа, сгенерированный алгоритмом A5, суммируются. Ключ шифрования — Kc.

Для многоканальных конфигураций (например, SCSD) используются различные ключи для разных каналов. Для канала n посредством алгоритма A5 по ключу Kc вычисляется ключ Kcn, причем вычисление производится следующим образом.

Пусть BN обозначает двоичный код временного интервала n (длиной от 0 до 7) из 64 бит. Бит i ключа Kcn — Kcn(i) вычисляется по формуле $Kcn(i)xor(BN \ll 32(i))$ (где xor — побитовое суммирование, $\ll 32$ обозначает 32-битный циклический сдвиг). Количество сложений определяется из условия, что lsb клоча Kc складывается посредством операции xor с lsb смещенного BN.

Расшифрование производится аналогичным способом.

При шифровании с помощью алгоритма A5 каждые 4.615 мс вырабатывается последовательность из 114 шифрующих/расшифрующих битов ключа (далее блок), побитно суммируемых с битами открытого текста. Полученный посредством алгоритма A5 первый бит ключа шифрования добавляется к e0, второй — к e1 и так далее.

Для каждого канала расшифрование выполняется на стороне MS; BLOCK1 содержит 114 битов ключа шифрования и используется для шифрования и расшифрования блока BLOCK2. Поэтому алгоритм A5 должен каждые 4.615 мс выдавать два блока.

Синхронизация обеспечивается введением в A5 переменной времени COUNT, получаемой из номера кадра TDMA. Таким образом, каждый 114-битный блок, производимый алгоритмом A5, зависит только от номера кадра TDMA и ключа шифрования Kc.

COUNT содержит 22 бита, соединенных путем конкатенации параметров T1, T3 и T3. Это входные параметры алгоритма A5. Состав переменной COUNT указан на рис. 11.

Двоичное представление графа. Бит 22 – старший бит (MSB), бит 1 — младший бит (LSB) графа. T1, T3 и T2 представлены в двоичной системе. (Для определения T1, T3 и T2 см. GSM 05,02.)

Алгоритм A5 имеет два входных параметра (COUNT и Kc) и выходные параметры (BLOCK1и BLOCK2), причем используются следующие форматы:

Длина ключа Kc — 64 бита;

Длина COUNT — 22 бита;

Длина BLOCK1 — 114 битов;

Длина BLOCK2 — 114 битов.

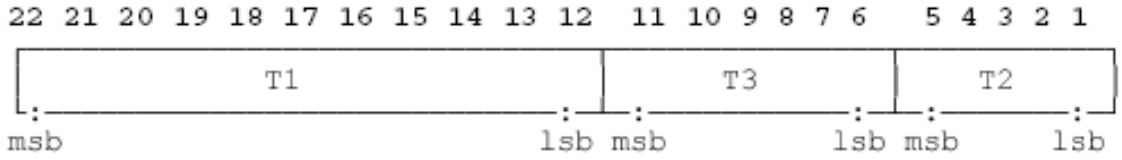

Рис. 11. Переменная COUNT

Алгоритм A5 должен выдавать блоки BLOCK1 и BLOCK2 быстрее, чем вырабатывается один кадр TDMA, то есть за 4.615 мс.

Примечание: Если фактическая длина ключа меньше 64 битов, то шифрование выполняется старшими битами ключа Kc, остальные устанавливаются в 0.

Стойкость данного шифра составляет 220, что на практике соответствует скорости взлома 3–5 минут.

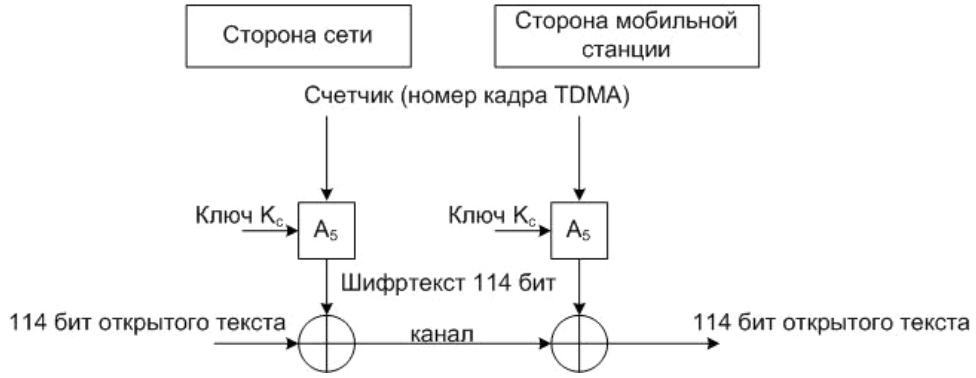

Рис. 12. Расшифрование на стороне мобильной станции

6.10. Шифрование в iDEN

Процедура установления защищенного соединения по протоколу iDEN идентична аналогичной процедуре в протоколе GSM, но информация об используемых криптоалгоритмах в открытых источниках отсутствует.

7. Аутентификация

В приводимой ниже таблице представлены обобщенные данные по использованию процедур аутентификации в рассматриваемых протоколах. В качестве наиболее значимых параметров были определены следующие.

1) Аутентификация устройств — процедура аутентификации устройств служит основным средством определения периметра беспроводной сети и легальности подключаемых узлов.

2) Аутентификация процессов — процедура, позволяющая подтвердить, что на узле сети используется доверенный (легальный) исходный код.

3) Аутентификация пакетов — процедура, позволяющая определить автора передаваемого пакета данных. Эта процедура необходима для защиты от атаки «человек-посередине».

4) Аутентификация пользователей — процедура аутентификации.

Название технологии	Аутентификация устройств	Аутентификация процессов	Аутентификация пакетов	Аутентификация пользователей
Bluetooth	По PIN	нет	нет	нет
UWB	По MAC и SSID	нет	нет	нет
ZigBee	По MAC и SSID	нет	MIC-64	нет
Insteon	XOR	нет	есть	нет
Z-Wave	По MAC и SSID	нет		
ANT	По ключу	нет	нет	нет
RuBee	По ключу AES	нет		
RFID	Crypto1	нет	нет	нет
X10	XOR	нет	есть	нет
WI-FI	CCMP	нет	TKIP	TKIP
PDC	A3	нет	A3	PIN
IDEN	По ключу	нет	По ключу	PIN
CDMAOne	CAVE	есть	есть	PIN
WIMAX	AES	EAP-TLS, PEAP	AES	Parol
GSM	A3	-		PIN
GPRS	A3/A8	-	A3/A8	PIN
UMTS	IMSI	AKA	MAC-I(F9)	USIM

Аутентификация в Bluetooth. Аутентификация в протоколе Bluetooth построена по схеме запрос-отзыв (стратегия идентификации пользователя путём проверки правильности его реакции на непредсказуемый запрос системы). Эта схема предполагает, что запрашиваемое устройство знает секретный сеансовый ключ. В протоколе Bluetooth используется алгоритм аутентификации E1, построенный по данной схеме. Алгоритм E1 приведен на рис. 13.

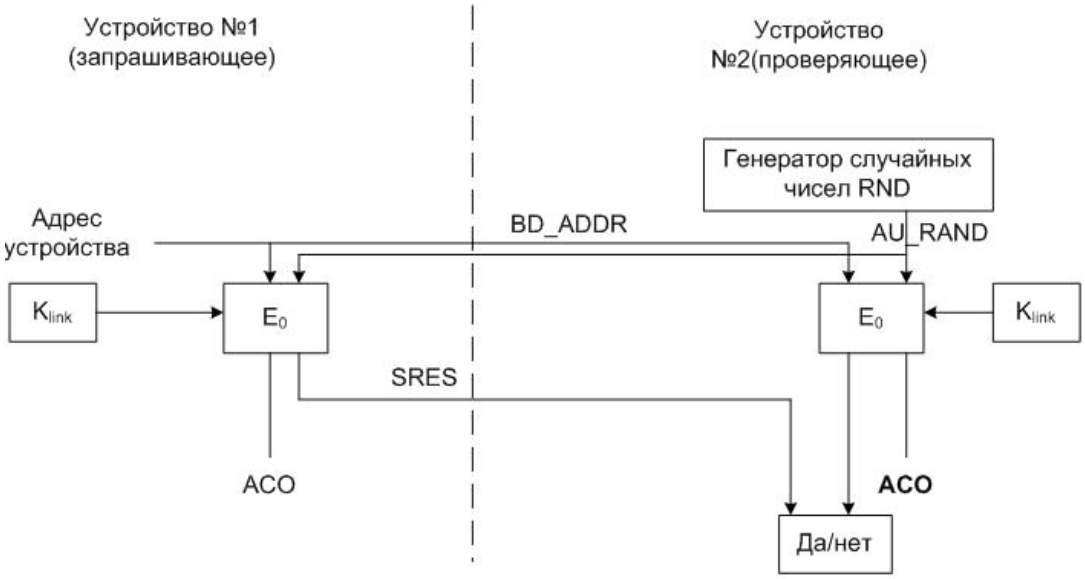

Рис. 13. Алгоритм аутентификации E1

Схема аутентификации с использованием алгоритма E1(*SAFER+*)

Проверяемая сторона передает проверяющей 128-битное случайное число AU_RAND. Проверяющая сторона вычисляет ответ для проверяемой, используя алгоритм E1, свой уникальный 48-битный адрес устройства BD_ADDR, сеансовый ключ и выход генератора случайных чисел AU_RAND. Для аутентификации используются только 32 старших разряда, получаемых после шифрования E1; оставшиеся 96 бит от 128-битного выхода шифра носят название Authenticated Ciphering Offset (ACO) и используются позже для генерации

ключа шифрования Bluetooth.

Проверяемая сторона возвращает 32 старших бита как вычисленный ответ SRES. Проверяющая сторона самостоятельно вычисляет значение SRES и сравнивает его с полученным значением.

Если полученные 32 бита сходятся с вычисленными, то аутентификация проходит, если не сходится – аутентификации не происходит.

7.1. Аутентификация в ANT

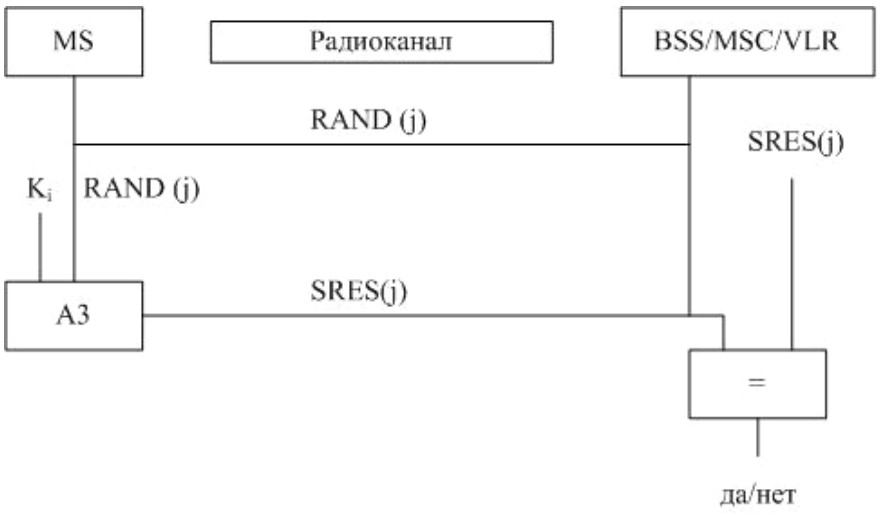

Рис. 14. Процедура аутентификации в протоколе ANT

В приведенной схеме MS обозначает мобильную станцию связи, BSS/MSC/VLR — узлы сети связи.

Алгоритм A3. Посредством алгоритма A3 вычисляется время ожидания ответа SRES по числу RAND от генератора случайных чисел, присылаемому по сети. При этом используется секретный ключ аутентификации Ki. На стороне MS алгоритм A3 содержится в модуле идентификации пользователей (Subscriber Identity Module).

На стороне сети эти действия реализованы в HLR или в AuC. Два входных параметра (RAND и Ki) и выходной параметр (SRES) алгоритма A3 имеют следующий формат:

длина Ki — 128 бит;

длина RAND — 128 бит;

длина SRES — 32 бита.

Время работы алгоритма A3 превышает 500 мс.

7.2. Аутентификация в PDC

Подсистема аутентификации в протоколе PDC реализует следующую процедуру обмена информацией между сетью и абонентом (MS).

Сеть связи высылает абоненту MS случайное число RAND.

Абонент MS вычисляет подпись для RAND под названием SRES, используя алгоритм A3 и секретный индивидуальный ключ аутентификации абонента Ki.

Абонент посылает в сеть подпись SRES.

Сеть проверяет SRES.

Вся процедура отображена на рис. 15.

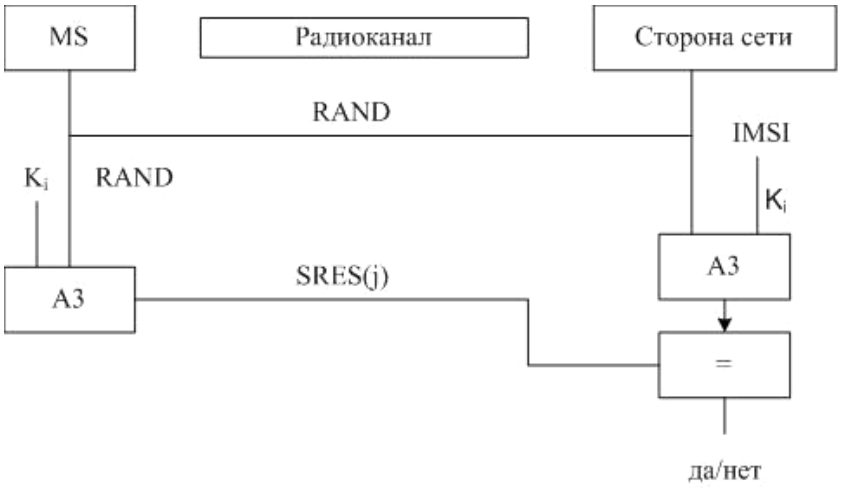

Рис. 15. Аутентификация устройств в протоколе PDC

7.3. Аутентификация в IDEN

Процесс аутентификации происходит между абонентом MS и системой iDEN и позволяет аутентифицировать абонента MS и назначить ему права доступа к сервисам. При этом используется цифровая подпись.

Во время первоначальной регистрации абонента в сети ему в соответствие ставится IMEI и алгоритм аутентификации Ki. Базовая станция HLR использует алгоритм подписи абонента MS для генерации 32 подписей из 32 случайных чисел. После генерации эти числа заносятся в таблицу VLR.

Для аутентификации абонент посылает в VLR свой ID. ID включает в себе следующее.

Международный мобильный идентификатор оборудования IMEI (получаемый при первичной регистрации).

Международный мобильный идентификатор абонента IMSI (получаемый в процессе регистрации).

Временный мобильный идентификатор абонента TMSI (получаемый при звонках в роуминге).

IP адрес для передачи данных по сети.

VLR посылает одно из случайных чисел абоненту. Абонент запускает генератор подписи, вычисляет подпись и пересылает ее в VLR. Там она сравнивается со значениями таблицы и по результатам сравнения назначаются права доступа или дается отказ в них.

Эти действия иллюстрирует приведенный ниже рисунок.

При первом включении телефона абонент MS проходит регистрацию в системе. В процессе регистрации абонент

- посылает свой IMEI в сеть iDEN FNE;
- получает IMSI, изданный DAP/MSC;
- получает остальные параметры сети.

Эти параметры позволяют получить доступ к основному каналу управления сети.

После получения абонентом ID системы IMEI больше в качестве идентификатора доступа не используется до тех пор, пока в мобильном телефоне не будут удалены все параметры сети.

Канал радиосвязи содержит специальную информацию согласно протоколам RLP и Mobis.

Информация об абоненте MS включает

- международный мобильный идентификатор абонента IMSI;
- аутентификатор Ki;
- временный мобильный идентификатор абонента TMSI.

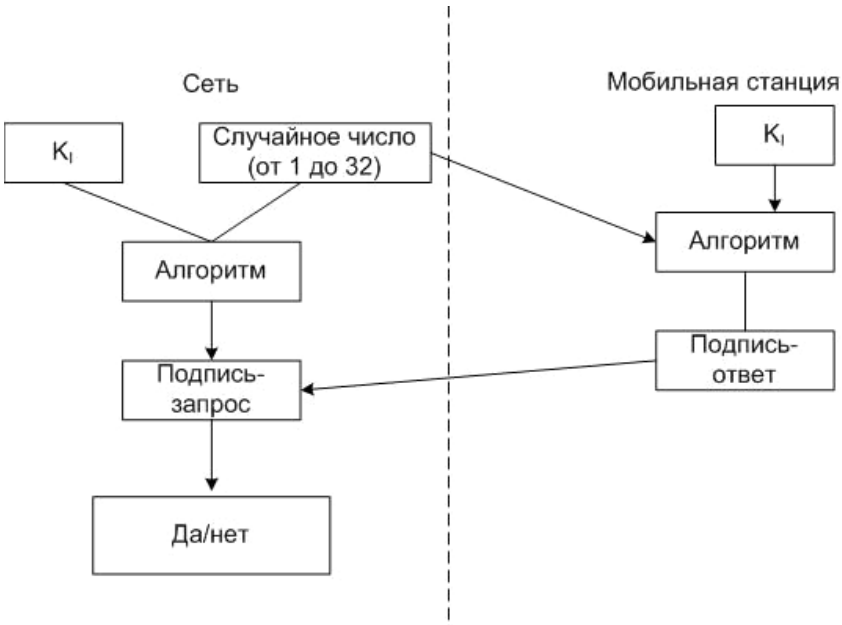

Рис. 16. Процесс аутентификации абонента

Уникальный идентификатор IMSI «домашняя сеть», выдает абоненту MS при инициализации.

Ключ аутентификации Ki служит для идентификации абонента MS путем подписания случайных чисел цифровой подписью.

Случайное число — это часть таблицы, которая используется для аутентификации MS.

Цифровые подписи — это часть таблицы, которая используется для аутентификации MS.

TMSI — это временный идентификатор абонента в роуминговых сетях, который используется для аутентификации абонента MS пока он активен в данной сети. Этот параметр ограничивает рассылку различных пакетов сильнее, чем при использовании идентификатора IMSI. IMSI присваивается абоненту как только он появляется в «домашней сети».

7.4. CCMP

В алгоритме CCMP для проверки подлинности и целостности данных используется метод CBC-MAC.

Стандарт AES, используемый в CCMP, предусматривает работу со 128-битным ключом и 128-битным блоком. С любым блочным алгоритмом шифрования можно использовать общий режим CMM. Алгоритм CCM предусматривает два параметра (M и L), причем в CCMP используются следующие их значения:

1) M = 8 (вследствие того, что поле MIC [1] – 8-октетное [2]).
2) L = 2 (указывает на то, что длина поля составляет 2 октета, чего достаточно для хранения пакетов MPDU всех возможных длин по стандарту IEEE 802.11).

Стандарт для алгоритма CMM требует использования новых временных ключей для каждой новой сессии. Кроме того, CMM требует уникального значения Nonce для каждого

кадра, защищённого конкретным выбранным временным ключом. CCMP использует для этого 48-разрядный номер пакета (PN). Повторное использование PN-номера с тем же временным ключом обнуляет все гарантии безопасности.

7.5. CAVE

Функция перемешивания, использующаяся в протоколах аутентификации запрос-ответ и для генерации ключей.

Для аутентификации абонента в CDMA-сети используется вспомогательный ключ SSD_A генерируемый алгоритмом CAVE с учетом параметров A-key, ESN и RANDSSD. Управляющее сетью устройство генерирует и рассылает открыто по эфиру случайное число RAND*, а мобильные устройства используют его как входные данные для алгоритма CAVE. Они генерируют 18-битную аутентификационную цифровую подпись (AUTH_SIGNATURE) и посылает ее на базовую станцию. В центре коммутации (Mobile services Switching Center – MSC) она сверяется с подписью, генерируемой самим MSC, для проверки легитимности абонента. Число RAND* может быть либо одинаковым для всех пользователей, либо генерироваться каждый раз заново.

Мобильное устройство и сеть ведут 6-битные счетчики вызовов, что обеспечивает возможность выявления работающих двойников: Для этого достаточно лишь контролировать соответствие значений счетчиков на телефоне и в MSC.

Секретный ключ A-key является перепрограммируемым, а в случае его изменения информация на мобильном телефоне и в HLR/AC должна быть синхронизирована. A-key может перепрограммироваться несколькими способами: на заводе, дилером в точке продаж, абонентом через интерфейс телефона, а также с помощью OTASP (Over The Air Service Provisionig). Служба OTASP использует 512-битный алгоритм согласования ключей Диффи-Хеллмана, гарантирующий достаточную безопасность. OTASP предоставляет легкий способ смены ключа A-key мобильного телефона на случай появления в сети двойника мобильного телефона. Изменение ключа A-key автоматически влечет за собой отключение услуг двойнику мобильного телефона и повторное включение услуг легитимному абоненту.

7.6. Пароли и ключи

Название технологии	Установка пароля	Смена пароля и ключа	Черные/белые листы	Контроль качества
Bluetooth	да	да	да	нет
UWB	да	да	да	нет
ZigBee	да	да	да	нет
Insteon	да	да	нет	нет
Z-Wave	да	да	нет	нет
ANT	нет	нет	нет	нет
RuBee	да	да	нет	нет
RFID	нет	нет	нет	нет
X10	нет	нет	нет	нет
WI-FI	да	да	нет	нет
PDC	да		нет	нет
IDEN	да	да	нет	нет
CDMAOne	да	да	да	нет
WIMAX	да	да	да	нет
GSM	да	да	нет	нет
GPRS	да	да	да	нет
UMTS	да	да	нет	нет

Управление ключами в PDC. Ключ назначается абоненту при первом включении абонента в домашней сети. Ключ меняется с каждым сеансом путем шифрования случайного

числа RAND/ SRES ключом Ki при помощи алгоритма A3. Процедура смены ключа сеанса представлена на рис. 17.

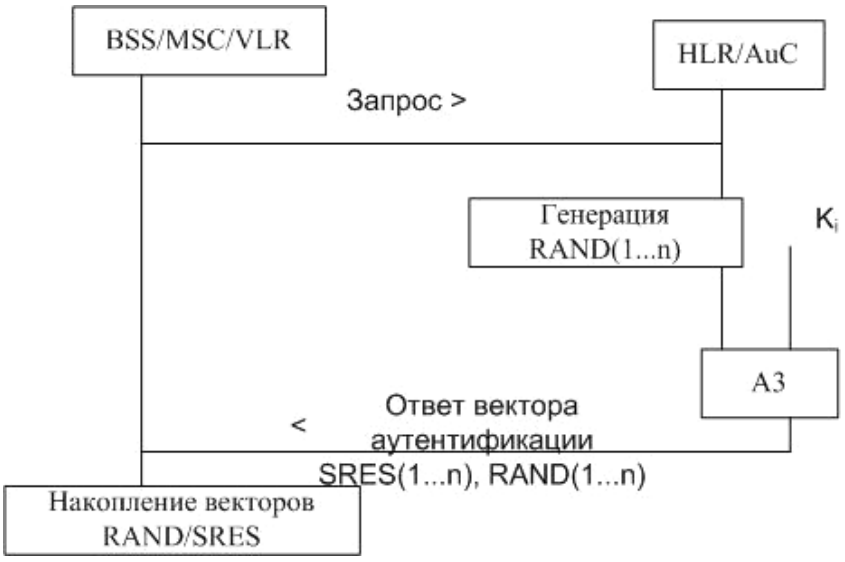

Рис. 17. Процедура смены ключа сеанса связи в протоколе PDC

В данной схеме BSS/MSC/VLR — это стационарные станции сети связи, которые управляют сетью. HLR/AuC — подвижные станции сети PDC, на которых осуществляется генерация случайных чисел RAND, хранение ключа Ki и генерация векторов аутентификации SRES.

Алгоритм управления ключами — A8 (GSM/GPRS). Использование алгоритма A8 зависит от решения оператора GSM и согласно меморандуму GSM/MoU производится по запросу.

На стороне MS алгоритм A8 содержится в SIM-карте.

На стороне сети A8 располагается совместно с A3.

Два входных параметра (RAND и Ki) и выходной параметр (Kc) алгоритма A8 должны иметь следующие форматы:

длина Ki — 128 бит;

длина RAND — 128 бит;

длина Kc — 64 бита.

Так как в соответствии с требованиями GSM/MoU максимальная длина ключа шифрования зафиксирована, A8 должен давать ключ требуемой длины и при необходимости расширять его до 64-битного слова, в котором младшие значащие биты равны нулю.

8. Уязвимости и риски

8.1. Уязвимости

Ниже представлены основные уязвимости для беспроводных протоколов

1) Ключи устройства используются повторно и скомпрометированы.

2) Ключи при обмене перехватываются.

3) Слабое управление PIN-кодами.

4) Ключ для шифрования повторяется после 23,3 часа его применения (в Bluetooth).

5) Ненадежное хранение ключей.

6) Повтор попыток аутентификации.

7) Стойкость процедуры запрос-ответ генератора псевдослучайных чисел неизвестна.

8) Ключ изменяемой длины.

9) Главный ключ открытый.

10) Нет аутентификации пользователей.

11) Используется слабый алгоритм шифрования **E0**.

12) Конфиденциальность может быть нарушена, если адрес Bluetooth устройства (BD_ADDR) захватывается и связан с конкретным пользователем.

13) Аутентификация устройства построена на очень простом и слабо защищенном принципе раскрытия секрета процедуры «запрос-ответ».

14) Защита канала точка-точка не выполняется.

15) Очень ограниченная степень безопасности.

16) Устройства уязвимы для атак во время процесса обнаружения и подключения.

8.2. Риски

Риск прослушивания. Самый существенный риск связан с пассивным прослушиванием канала третьей стороной. Существует несколько методов организации прослушивания:

1) Подслушивание абонента при громком разговоре.

2) Прослушивание при помощи закладок в помещении.

3) Перехват беспроводного соединения.

4) Перехват информации на узлах сети.

5) Перехват информации при передаче между узлами сети.

Риск кражи записей информации. Данный риск характерен для автоответчиков и телефонов с функцией диктофона. Суть данного риска заключается в возможности воровства записанной информации с носителей. В роли носителей выступают автоответчики телефонов, память диктофонов, совмещенных с телефонами, память узлов сенсорных сетей и т.д.

Анализ передаваемого потока управления. Для злоумышленника может представлять интерес любая информация о действиях пользователя:

- Время и дата разговоров и сеансов передачи данных.
- Вызываемые абоненты.
- Местоположение абонентов.
- Номера и IP адреса абонентов.
- История сеансов связи.
- Телефонная книга и перечень адресов.
- Определение местоположения.

Этот риск характерен для любого пользователя передающего устройства, находящегося в сети с промежуточными устройствами. Например, для пользователей сотовых телефонов.

Прочие риски

Загрузка кода. Существующие беспроводные устройства слабо защищены от загрузки программного кода и его исполнения на узлах сети. Этот код может работать в интересах третьей стороны и наносить ущерб системе передачи информации, передаваемой информации и пользователям системы.

Восстановление удаленных сообщений. Особенности электронной памяти, используемой в современных беспроводных устройствах, таковы, что она может долго сохранять в себе ранее удаленную информацию. Это связано также с алгоритмами удаления. Как правило, разработчики программного обеспечения ограничиваются стиранием ссылок на записанную информацию или заголовков, не затирая саму информацию.

Кражи. Одним из самых существенных рисков для узлов беспроводных сетей является риск кражи самих узлов. Это связано как с ценностью самих узлов, так и с отсутствием возможности контролировать распространение и перепродажу краденых узлов беспроводных сетей.

8.3. Атаки на беспроводные сети

Для беспроводных сетей характерны следующие виды атак:

1) Отказ в обслуживании (DoS).

2) Пассивное прослушивание (eavesdropping).

3) Атака «человек-посередине» (man-in-the-middle attacks).

4) Модификация сообщений (message modification).

5) Захват ресурса (resource misappropriation).

9. Модель угроз

Для всех представленных беспроводных технологий характерны угрозы нарушения целостности, конфиденциальности и доступности информации.

При этом вне зависимости от топологии и протокола связи пути реализации этих угроз таковы:

1) Перехват ключа шифрования при обмене между устройствами.

2) Использование старых (неизменяемых или скомпрометированных) ключей шифрования.

3) Ненадежное хранение ключей шифрования — в случае вирусной атаки или несанкционированного доступа к узлу сети можно получить ключ шифрования.

4) В ряде технологий отсутствуют или сильно урезаны процедуры аутентификации устройств, процессов, пакетов и пользователей.

5) Используются небезопасные протоколы установления соединений.

6) Стойкости используемых алгоритмов шифрования, как правило, недостаточно.

При этом следует учитывать, что в роли криптоаналитика может выступать как узел, не находящийся в сети, так и узел, являющийся ее частью.

10. Модель криптоаналитика

Для сенсорных сетей всех типов характерна модель криптоаналитика, представленная в [11, 13]. Возможности криптоаналитика таковы:

1) Перехват сообщений и их взлом.

2) Модификации блоков данных, как в канале, так и на узлах сети.

3) Подделки авторства передаваемых блоков.

4) Повторная передача устаревших блоков данных.

5) Отказ передавать далее принятые блоки данных.

В первом случае криптоаналитик представлен «надежным, но любопытным узлом»: он принимает и передает все принятые пакеты. Но при этом копирует их и пытается взломать. Вероятность взлома в данном случае сильно зависит от местоположения узла в сети. Чем ближе он находится к источникам данных до осуществления сетевого кодирования другими узлами, тем проще криптоаналитику получить исходное сообщение или его часть.

Модели прослушивающего криптоаналитика, приводимые в современной литературе, сводятся, как правило, к задаче восстановления исходного текста из перехватываемых сообщений из одного или нескольких (подмножества) каналов. В работах [16–18] представлено обоснование условий использования теоретически стойких систем шифрования в системах с линейным кодированием и несколькими источниками информации.

Также применима схема криптоаналитика, когда предусмотрено знание им всех передаваемых открытых текстов. В данном случае для защиты системы передачи данных используется линейное кодирование [19] с подбором коэффициентов сети.

11. Выводы

Беспроводные сети получили широкое распространение в повседневной жизни, и динамика процесса распространения такова, что количество беспроводных сетей будет только возрастать. Ценность информации передаваемой по беспроводным сетям растет вместе с количеством информации и сетей.

Используемые криптографические алгоритмы и протоколы не обеспечивают необходимого уровня защиты передаваемой, хранимой и обрабатываемой информации. Причины этого заключатся в недостаточной криптографической стойкости алгоритмов шифрования к атакам, в том числе к атаке «грубой силы»; в отсутствие надежных протоколов смены и генерации ключей; в отсутствие или слабости протоколов аутентификации узлов и передаваемых информационных пакетов.

Из всех рассмотренных протоколов только протоколы Z-wave, UWB. ZigBee, Wi-Fi, Wimax обладают шифрами, в достаточной мере устойчивыми к взлому, способными противостоять атакам «грубой силы» — 3DES, AES. Все остальные протоколы располагают алгоритмами шифрования со стойкостью к взлому не более чем 238, что приблизительно равно 1011,44. Такого уровня стойкости абсолютно недостаточно. Так, вычислительная система на базе процессора Core 2Quad Q6600 выполняет до 17,6 миллиардов операций в секунду, то есть около 1010 вычислений. Для перебора всех ключей таких алгоритмов понадобится не более 15–20 минут. Для перебора ключей DES с длиной ключей 56 бит понадобится около 42 дней.

1) Для современных беспроводных систем связи необходим шифр со стойкостью к взлому не менее 292 вариантов ключей.

2) Необходима надежная схема смены симметричных ключей.

3) Необходима возможность вести широковещательную рассылку на симметричных алгоритмах.

4) Алгоритм шифрования должен максимально использовать свойства сети, топологий, устройств для обеспечения безопасности.

При этом несомненным плюсом рассмотренных протоколов следует считать возможность создания и использования криптографических протоколов на верхних уровнях протоколов передачи данных.

При создании безопасных беспроводных систем передачи данных следует уделить особое внимание возможности использования особенностей случайного и детерминированного сетевого кодирования для защиты от существующих угроз. В работах [10–14] предлагается ряд алгоритмов шифрования и кодирования в ранговых метриках, используя которые можно обеспечить приемлемый уровень безопасности от рассмотренных угроз.

В работе [1] рассмотрена система аутентификации с нулевым разглашением секрета. Эта система представляет интерес в качестве системы аутентификации узлов беспроводной сети.

Литература

1. *De Koning Gans Gerhard, Hoepman J.-H., Garcia F.D.* A practical attack on the MIFRARE Classic // 8th Smart Card Research and Advanced application Workshop (CARDIS 2008), LNCS, Springer.
2. *Courtois Nicolas T., Karsten Nohl, Sean O'Neil.* Algebraic attack on the Crypto-1 Stream cipher in MIFRARE classic and Oyster cards. Cryptology ePrint Archive.
3. *Garcia Flavio D., de Koning Gans Gerhard, Muijrers Ruben, van Rossum Peter, Verdult Roel, Schreur Ronny Wichers, Jacobs Bart.* Dismantling MIFRARE Classic // 13th European symposium on research in computer security (ESORISC 2008), LNCS, Springer.
4. *Garcia Flavio D., van Rossum Peter, Verdult Roel, Schreur Ronny Wichers.* Wirelessly pickopocketing a mifrare classic card // 30th IEEE Symposium on security an privacy (S&P 2009), IEEE.
5. *Eisenbarth Thomas, Kasper Timo, Moradi Amir, Paar Christof, Salmasizadeh Mahammad, Shalmani Mohammad T. Manzuri.* Physical cryptanalysis of KeeLogCode Hopping applications. Ruhr university of Bochum, Germany/ Retired 2009-03-22.
6. *Novotny Martin, Kasper Timo.* Cryptanalysis of keeLoq with COPOCOBANA, SHARCS 2009 Conferece.
7. *Scarfone Karen, Padgette John.* Guide to Bluetooth security // NIST special publication sep. 2008.
8. ISO/IEC 26907 Information technology — Telecommunications and information exchange between systems — High-rate ultra-wideband PHY and MAC standard.
9. IEEE 802.15.4 IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks — Specific requirements.
10. *Buttyı'an L., Czap L., Vajda I.* Securing coding based distributed storage in wireless sensor networks // Proceedings of the IEEE Workshop on Wireless and Sensor Network Security (WSNS), Atlanta, USA, 2008.
11. *Lima L., Vilela J., Oliveira P., Barros J., Filiz I., Guo X., Morton J., Sturmfels B., Mungan M., Ramasco J.* [*et al.*] Network Coding Security Attacks and Countermeasures. 2008.

12. *Jaggi S., Langberg M., Katti S., Ho T., Katabi D., Mɾ'edard M.* Resilient network coding in the presence of byzantine adversaries // Proceedings of the Conference of the IEEE Computer and Communications Societies (INFOCOM), Anchorage, Alaska, USA, 2007. P. 616–624.

13. *Buttyɾ'an Levente, ɾ'o Czap Lɾ'aszl, Vajda Istvɾ'an.* Pollution Attack Defense for Coding Based Sensor Storage Proceedings of the Conference of the IEEE Computer and Communications Societies (INFOCOM), Anchorage, Alaska, USA, 2010.

14. *Dong J., Curtmola R., Nita-Rotaru C.* Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks, in WiSec '09 // Proceedings of the second ACM conference on Wireless network security. New York, NY, USA: ACM, 2009. – P. 111–122.

15. *Courtois N.* Efficient zero-knowledge authentication based on a linear algebra problem minrank // Proceedings of ASIACRYPT, 2001. – P. 402–421.

16. *Cai N., Yeung R.* Secure network coding // Proceedings of the IEEE International Symposium on Information Theory. Lausanne, Switzerland. 2002.

17. *Cai N., Yeung R.* Network error correction // Proceedings of the IEEE International Symposium on Information Theory, Yokohama, Japan, July. 2003.

18. *Cai N., Yeung R. W.* A Security Condition for Multi-Source Linear Network Coding // IEEE International Symposium on Information Theory (ISIT). Nice, France. 2007.

19. *Lima L., Vilela J. P., Barros J., Medard M.* 2008. An Information-Theoretic Cryptanalysis of Network Coding — is protecting the code enough? // International Symposium on Information Theory and its Applications, ISITA2008. Auckland, New Zealand.

Поступила в редакцию 24.07.2011.