Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК

Дульский

Дмитрий, Васильевич

Анализ и характеристики методов доступа сетевых Wi-Fi устройств

АВТОРЕФЕРАТ
на соискание степени магистра наук

по специальности 1-458101 Системы, сети и устройства телекоммуникаций

Научный руководитель

(Королев А.И.)

Минск, 2015

ВВЕДЕНИЕ

Во всем мире стремительно растет потребность в беспроводных соединениях, особенно в сфере бизнеса и IT технологий. Пользователи с беспроводным доступом к информации всегда и везде могут работать гораздо более производительно и эффективно, чем их коллеги, привязанные к проводным телефонным и компьютерным сетям, так как существует привязанность к определенной инфраструктуре коммуникаций.

На современном этапе развития сетевых технологий, технология беспроводных сетей Wi-Fi является наиболее удобной в условиях требующих мобильность, простоту установки и использования. Wi-Fi (от англ. wireless fidelity - беспроводная связь) - стандарт широкополосной беспроводной связи семейства 802.11 разработанный в 1997г. Как правило, технология Wi-Fi используется для организации беспроводных локальных компьютерных сетей, а также создания так называемых горячих точек высокоскоростного доступа в Интернет.

Беспроводные сети обладают, по сравнению с традиционными проводными сетями, немалыми преимуществами, главным из которых, конечно же. является:

1. Простота развёртывания;
2. Гибкость архитектуры сети, когда обеспечивается возможность динамического изменения топологии сети при подключении, передвижении и отключении мобильных пользователей без значительных потерь времени:
3. Быстрота проектирования и реализации, что критично при жестких требованиях к времени построения сети;
4. Так же. беспроводная сеть не нуждается в прокладке кабелей (часто требующей дробления стен).

Характеристика работы и краткое содержание работы

Основные сведения о Wi-Fi сетях

В данной работе был произведен анализ и характеристики методов доступа сетевых Wi-Fi устройств.

Самыми популярными стандартами являются, 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, поговорим о них подробней.

802.11a – стандарт сетей Wi-Fi. Использует частотный диапазон 5 ГГц U-NII (англ.).

Несмотря на то, что эта версия используется не так часто из-за стандартизации IEEE 802.11b и внедрения 802.11g, она также претерпела изменения в плане частоты и модуляции. OFDM позволяет передавать данные параллельно на множественных подчастотах. Это позволяет повысить устойчивость к помехам и поскольку отправляется более одного потока данных, реализуется высокая пропускная способность.

IEEE 802.11a может развивать скорость вплоть до 54 Мб/с в идеальных условиях. В менее идеальных условиях (или при чистом сигнале) устройства могут вести связь со скоростью 48 Мб/с, 36 Мб/с, 24 Мб/с, 18 Мб/с, 12 Мб/с и 6 Мб/с.

Стандарт IEEE 802.11a несовместим с 802.11b 802.11g.

802.11b

Работа над стандартом IEEE 802.11b (др. назв. — IEEE 802.11 High rate, высокая пропускная способность) была закончена в 1999 году, и именно с ним связано название Wi-Fi (Wireless Fidelity, беспроводная точность). Работа стандарта основана на методе прямого расширения спектра (DSSS) с использованием восьмиразрядных последовательностей Уолша. При этом каждый бит данных кодируется с помощью последовательности дополнительных кодов (CCK). Это позволяет достичь скорости передачи данных 11 Мбит/с. Как и базовый стандарт, IEEE 802.11b работает с частотой 2,4 ГГц, используя не более трех неперекрывающихся каналов. Радиус действия сети при этом составляет около 300 м. Этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

802.11g

Стандарт IEEE 802.11g унаследовал самые лучшие свойства стандартов IEEE 802.11a и IEEE 802.11b и обладает многими собственными полезными качествами. Целью создания данного стандарта было достижение скорости передачи данных 54 Мбит/с. Как и IEEE 802.11b, стандарт IEEE 802.11g разработан для работы в частотном диапазоне 2,4 ГГц. IEEE 802.11g предписывает обязательные и возможные скорости передачи данных:

- обязательные – 1, 2, 5.5, 6, 11, 12, 24 Мбит/с;
- возможные – 33, 36, 48 и 54 Мбит/с.

Для достижения таких показателей используется кодирование с помощью последовательности дополнительных кодов (CCK), метод ортогонального частотного мультиплексирования (OFDM), метод гибридного кодирования (CCK-OFDM) и метод двоичного пакетного сверточного кодирования (PBCC). Стоит отметить, что одной и той же скорости можно достичь разными методами, однако обязательные скорости передачи данных достигаются только с помощью методов CCK и OFDM, а возможные скорости – с помощью методов CCK-OFDM и PBCC.

Даже сейчас в 2014, году стандарт 802.11g очень часто используется примеров много, один из них, ТСД(терминал сбора данных) используется в торговых и складских сетях, для подсчет товара.

802.11n

Этот стандарт был утверждён 11 сентября 2009

Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с брутто или около 20 Мбит/с нетто), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с брутто, применяя передачу данных сразу по четырём антеннам. По одной антенне – до 150 Мбит/с.

Устройства 802.11n работают в диапазонах 2,4-2,5 или 5,0 ГГц.

Кроме того, устройства 802.11n могут работать в трёх режимах:

- наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a;
- смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n;
- «чистом» режиме – 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n).

Черновую версию стандарта 802.11n (DRAFT 2.0) поддерживают многие современные сетевые устройства. Итоговая версия стандарта (DRAFT 11.0), которая была принята 11 сентября 2009 года, обеспечивает скорость до 300 Мбит/с, Многоканальный вход/выход, известный как MIMO, и большее покрытие.

802.11ac – стандарт беспроводных локальных сетей, работающий в диапазоне частот 5 ГГц. Обратно совместим с IEEE 802.11n.

Стандарт позволяет существенно расширить пропускную способность сети, начиная от 433 Мбит/с(устройства с 433 Мбит/с на канал уже были доступны летом 2014 г.) и до 6.77 Гбит/с при 8x MU-MIMO-антеннах. Это наиболее существенное нововведение относительно IEEE 802.11n. Кроме

того, ожидается снижение энергопотребления(Дж/бит), что, в свою очередь, продлит время автономной работы мобильных устройств.

20 января 2011 года была принята первая черновая редакция версии 0.1. 1 февраля 2013 года принята черновая редакция версии 5.0 (завершено на 95 %). 4 апреля 2013 года обновлена черновая редакция версии 5.0 (завершено на 96 %).

На апрель 2013 года некоторыми производителями (Quantenna, Broadcom, Buffalo, D-Link, Cisco) уже представлены чипы, поддерживающие работу по стандарту IEEE 802.11ac Draft 0.1, а также выпущены на рынок устройства, поддерживающие черновой вариант данного стандарта.

Принятие финальной версии спецификации 802.11ac состоялось в январе 2014 года.

Комплекс технических средств Wi-Fi сетей: классификация и краткая характеристика

К техническим средствам Wi-Fi сетей мы можем отнести:

1. Сетевые адаптеры;
2. Точка доступа (AP);
3. Репитер (ретранслятор);
4. Коммутатор;
5. Роутер;
6. Котроллер;
7. Антенна.

Топология и методы организации режимов передачи данных от несанкционированного доступа Wi-Fi сетей

Классификация и принцип построения топологии Wi-Fi сетей

Топология (структура) сети есть геометрическая проекция сети на плоскость. Топология сети определяет места расположения оконечных устройств (PDA, ПК, принтеров) и коммутационного (распределительного) оборудования сети (точек радиодоступа, маршрутизаторов и мостов) на обслуживаемой территории, а также их взаимосвязь друг с другом на основе соответствующих беспроводных каналов связи, а в случае необходимости и на основе проводных каналов связи.

Стандартом IEEE802.11 на сегодняшний день определены три основных типа топологий или принципов (вариантов) построения Wi-Fi сетей, а именно:

1. IBSS (Independent Basic Service Sets) – независимая базовая зона обслуживания, или Ad-Hoc - независимая конфигурация;

2. BSS (Basic Service Sets) – базовая зона обслуживания или «Инфраструктура»;

3. EBSS (Extended Basic Service Sets) – расширенная базовая зона обслуживания или «Расширенная Инфраструктура»;

Общая сущность основных топологий Wi-Fi сетей:

1. Топология (режим ПД) Wi-Fi сети Ad-Hoc или «Независимая конфигурация» (IBSSs) которую часто называют «Точка-Точка» имеет самую простую схему построения и настройку сети;

2. Топология (режим ПД) Wi-Fi сети типа «Инфраструктурная конфигурация» или BSS (базовая зона обслуживания) или «Инфраструктура»**;**

3. Топология Wi-Fi сети типа (Расширенная инфраструктурная конфигурация), или (Расширенная инфраструктура);

4. Топология Wi-Fi сети типа «Кольцо»;

5. Топология Wi-Fi сети типа «Звезда»;

6. Топология Wi-Fi сети типа «Шина»;

7. Топология (режим ПД) Wi-Fi сети типа «Точка-Точка» или «Мост»;

8. Топология (режим ПД) Wi-Fi сети типа «Точка - много Точек»

9. Топология (режим ПД) Wi-Fi сети типа «Удалённый абонент» («Режим клиента»);

10. Wi-Fi сети с топологией (режимами ПД) типа WDS и WDS with AP.

Методы организации режимов передачи данных в Wi-Fi сетях

Методы передачи данных в Wi-Fi сетях:

1. Звезда - это топология с явно выделенным центром, к которому подключаются все другие абоненты. Весь обмен информацией идет исключительно через центральный компьютер, на который таким способом ложится очень большая нагрузка, потому ничем другим, кроме сети, оно заниматься не может;

2. Шина самой своей структурой допускает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов. При таком соединении компьютеры могут передавать только по очереди, потому что линия связи единственная. В противном случае переданная информация будет искажаться в результате наложения (конфликту, коллизии). Таким образом, в шине реализуется режим полудуплексного (half duplex) обмена (в обоих направлениях, но по очереди, а не одновременно);

3. Кольцо – это топология, в которой каждый компьютер соединен линиями связи только с двумя другими: от одного он только получает информацию, а другому только передает. На каждой линии связи, как и в случае звезды, работает только один передатчик и один приемник. Это позволяет отказаться от применения внешних терминаторов.

Методы организации защиты данных от несанкционированного доступа в Wi-Fi сетей

Для защиты сетей стандарта IEEE 802.11 предусмотрен комплекс мер безопасности передачи данных.

На раннем этапе использования Wi-Fi сетей таковым являлся пароль Server Set ID (SSID) для доступа в локальную сеть. Однако данная технология не обеспечивает надежную защиту.

Главной защитой долгое время было использование цифровых ключей шифрования потоков данных с помощью функции Wired Equivalent Privacy (WEP). Ключи являются обыкновенными паролями длиной от 5 до 13 символов кода ASCII.

Однако взломать такую защиту можно соответствующими утилитами из Интернета, например Airsnot, WEPcrack и др. Слабое место такой защиты - это вектор инициализации, так как используется 24 бита и формируется около 16 миллионов комбинаций, после использования которых ключ начинает повторяться, поэтому хакеру необходимо найти эти повторы (для этого потребуется менее часа времени) и за секунды взломать остальную часть ключа. После этого он может входить в сеть как обычный зарегистрированный пользователь.

Так как стандарт WEP не обеспечивает надежной защиты данных для проводных и беспроводных сетей, то в 2001 г. был внедрен новый стандарт EEEE 802.11X, который использует вариант динамических 128-разрядных ключей шифрования, т. е. периодически изменяющихся во времени. Таким образом, пользователи сети работают сеансами, по завершении которых им присылается новый ключ. Например, Windows XP поддерживает данный стандарт, и по умолчанию время одного сеанса равно 30 минутам. IEEE 802.11X – это новый стандарт, который оказался ключевым для развития индустрии беспроводных сетей в целом.

В конце 2003 г. был внедрен стандарт Wi-Fi Protected Access (WPA), который совмещает преимущества динамического обновления ключей стандарта IEEE 802.11X с кодированием протокола интеграции временного ключа TKIP.

Стандарт TKIP использует автоматически подобранные 128-битные ключи, которые создаются непредсказуемым способом, и общее число вариации которых достигает 500 миллиардов. Сложная иерархическая система алгоритма подбора ключей и динамическая их замена через 10 Кбайт (10 тыс. передаваемых пакетов) делают систему максимально защищенной.

Беспроводная сеть считается защищенной, если в ней функционируют три основные составляющие системы безопасности: аутентификация пользователя, конфиденциальность и целостность передачи данных. Для получения достаточного уровня безопасности необходимо воспользоваться рядом правил при организации и настройке частной Wi-Fi-сети, а именно:

- шифровать данные путем использования различных алгоритмов и систем. Максимальный уровень безопасности обеспечит применение VPN;
- использовать протокол стандарта 802.11X;
- запретить доступ к настройкам точки доступа с помощью беспроводного подключения;
- управлять доступом клиентов по MAC-адресам;
- запретить трансляцию в эфир идентификатора SSID;
- располагать антенны как можно дальше от окон, внешних стен здания, а также ограничивать мощность радиоизлучения:
- использовать максимально длинные ключи;
- изменять статические ключи и пароли;
- использовать метод WEP-аутентификации «Shared Key», так как клиенту для входа в сеть необходимо будет знать WEP-ключ;
- пользоваться сложным паролем для доступа к настройкам точки доступа;
- по возможности не использовать в беспроводных сетях протокол TCP/IP для организации папок, файлов и принтеров общего доступа. Организация разделяемых ресурсов NetBEUI в данном случае безопаснее;
- не разрешать гостевой доступ к ресурсам общего доступа и использовать длинные сложные пароли;
- не использовать в беспроводной сети DHCP. Вручную распределить статические IP-адреса между - легитимными клиентами безопаснее;
- на всех ПК внутри беспроводной сети установить файерволлы. устанавливать точку доступа вне брэндмауэра. использовать минимум протоколов внутри WLAN (например только HTTP и SMTP);
- регулярно исследовать уязвимость сети с помощью специализированных сканеров безопасности (например NetStumbler);
- использовать специализированные сетевые операционные системы, такие, как Windows NT, Windows 2003, Windows XP.

Классификация методов доступа сетевых устройств Wi-Fi сетей

В настоящее время известно большое число ММД которые продолжают разрабатываться и совершенствоваться. Важнейшим требованием, предъявляемым к разрабатываемым ММД является, обеспечение равноправного доступа абонентских устройств (радиостанций) к общей среде ПИ (р/каналу)

В соответствии со стандартом IEEE 802.11 ММД реализуются протоколами двух нижних связных уровней модели OSI, а именно:

a. PL (Physical Layer) – физического уровня, состоящего из двух подуровней, а именно:

- PMD (Physical Medium Dependent) - подуровень, зависящий от типа среды ПИ;
- PLCP (Physical Layer Convergence Procedure) - подуровень процедур (функций) определения состояний физического уровня;

b. CL (Chanel Layer) - канального уровня, состоящего из двух подуровней, а именно:

- MAC (Media Access Control) - подуровень управления доступом к среде ПИ;
- LLC (Logical Link Control) - подуровень управления логическим соединением.

Основную роль в реализации метода доступа к среде ПИ или к РК играет подуровень MAC.

Методы доступа к среде передачи данных, которые используются в локальных беспроводных сетях Wireless LAN (WLAN), – это методы множественного доступа с контролем несущей и предупреждением коллизий или столкновений (CSMA/CA – Carrier Sense Multiple Access/Collision Avoidance).

Метод (механизм) ММД CSMA/CA предусматривает использование и реализацию двух способов коллективного доступа абонентских и других устройств Wi-Fi сетей к среде ПИ (р/каналу) или двух способов прослушивания канала, а именно:

1. DCF (Distributed Coordination Function) – функция распределённой координации, или распределённый режим доступа к среде ПИ или р/каналу;
2. PCF (Point Coordination Function) – функция централизованной координации, или централизованный режим доступа.

Кроме вышеназванных ММД, стандартом IEEE 802.11 разрешено к использования в Wi-Fi сетях дополнительно ещё два метода (механизма) коллективного доступа к среде ПИ, а именно:

3. EDCF (Enhanced DCF) – расширенная функция распределённой координации, или расширенный распределённый метод (механизм) доступа;

4. HCF (Hybrid Coordination Function) – гибридная функция координации

Разработка методики организации и настройки режимов передачи данных Wi-Fi сетей с топологиями BSS(инфраструктуры) и EBSS(расширенная инфраструктура)

Разработка методики организации и настройки режимов передачи данных Wi-Fi сетей с топологиями BSS(инфраструктуры)

Проектирование сети рекомендуется выполнять по следующей методике:

1. Начинать проектирование сети надо с выезда на место эксплуатации сети и выполнить все те пункты, которые отмечались ранее, например: уточнить места расположения оконечных устройств и их количество, определить количество перегородок и их тип, количество шкафов в комнате и/или комнатах офиса, предварительно определить место расположения точки Р/доступа и предварительно проработать вопросы организации безопасности сети.

2. Выбирать тип стандарта IEEE802.11 проектируемой сети в соответствии с данными ТЗ и особенно с объемом допустимого финансирования организуемой сети.

3. Если в ТЗ не указана топология (структура) сети (Звезда, Кольцо, Шина и т.д.), то целесообразно выбрать топологию «Звезда», обеспечивающая меньшую сложность проектирования и реализации.

4. Выбрать фирму производителя беспроводного сетевого оборудования, а далее приступить к выбору типа конкретного сетевого оборудования.

Разработка методики организации и настройки режимов передачи данных Wi-Fi сетей с топологиями EBSS(расширенная инфраструктура)

Так для расширенных WLAN (беспроводных локальных сетей) необходимо учесть (учитывать) следующие факторы:

1. Расчетная производительность сети в пересчете на одного абонента;

2. Тип передаваемой информации, обозначаемые иногда в литературе терминами «Потоковые и пульсирующие типы приложений»;

3. Конкуренция за среду ПИ и допустимая задержка ПИ.

Сущность этих факторов состоит в следующем:

a. расчетная производительность каждого абонента уменьшается с вводом в базовую зону обслуживания - BSS (Basic Service Sets) каждого нового абонента;

b. тип передаваемой информации влияет на объемы передачи информации;

c. конкуренция за среду ПИ зависит как от метода доступа, так и от количества точек Р/доступа и абонентских станций. С увеличением количества абонентских станций и при малом количестве точек Р/доступа в сети увеличивается задержки ПИ, а при увеличении количества точек Р/доступа увеличивается стоимость сети. Эффективными методами выхода из этих ситуаций является: фрагментирование ПД и использование квитанций (фреймом) RTS/CTS.

Разработка методики организации и настройки режимов защиты данных от несанкционированного доступа

Выбор и обоснование политики безопасности Wi-Fi сети.

Обеспечение безопасности Wi-Fi является важнейшей задачей. Эта задача частично решается на этапе проектирования путём разработки, так называемой, политики безопасности сети в рамках законов конституции различных стран.

Во-первых, необходимо очень внимательно проанализировать требования, предъявляемые к безопасности, проектируемой сети и предварительно определить методы, обеспечивающие требуемый уровень защиты сети. Например, должны обязательно предусмотрены механизмы шифрования: для небольших — WEP, WPA, а для больших, т.е расширенных, и внешних сетей - WPA2.

Во-вторых, предварительно определить методы аутентификации абонентских станций, которые будут предложены к реализации в сети, например, можно порекомендовать к использованию в сети методы взаимной аутентификации типа LEAP или EAP-TLS.

В-третьих, предварительно определить тип программного обеспечения, поддерживающего аутентификацию, или в ОС, или в прикладных программах абонентских станций, маршрутизаторах, коммутаторах и т.д.

В-четвёртых, разработанная политика безопасности сети обязательно должна быть доведена до каждого сотрудника офиса.

Общая методика тестирования безопасности сети

Прежде чем приступить к тестированию сети на предмет аттестации её безопасности необходимо:

1. Проверить наличие и ознакомиться с политикой безопасности

тестируемой беспроводные сети;

2. Проверить установку в точках р/доступа и сетевых беспроводных адаптеров ГТК и ноутбуков соответствующих механизмов (алгоритмов) аутентификации и шифрования данных. Очень важно, чтобы все точки р/доступа и сетевые адаптеры или программные обеспечения соответствующих политике безопасности сети;

3. Убедиться, что физические порты консолей точек р/доступа, беспроводных маршрутизаторов и коммутаторов недоступны для посторонних (чужих) лиц.

Общие рекомендации по организации эксплуатации проектируемой Wi-Fi сети

По умолчанию сетевые беспроводное оборудование не использует никаких дополнительных механизмов защиты и является абсолютно открытым. Поэтому после создания сети необходимо в первую очередь выполнять процедуры, которые позволят максимально защищать сеть.

К таким процедурам защиты сети можно отнести следующие:

- отключение трансляции SSiD;
- создание списка MAC-адресов;
- выбор уровня шифрования;
- снижение мощности передатчиков;
- экранирование помещений с помощью покраски стен краской с примесью металлов и оклеивание окон помещений пленкой со встроенными металлическими нитями.

ЗАКЛЮЧЕНИЕ

Мобильный Интернет и мобильные локальные сети открывают корпоративным и домашним пользователям новые сферы применения карманных ПК, ноутбуков. Одновременно с этим появляется спрос на беспроводное соединение Wi-Fi и расширяется его ассортимент. Wi-Fi также подходит для людей, которым по долгу необходимо перемещаться по помещению, к примеру, на складе или в магазине. В этом случае для учета (отгрузки, приема и т. п.) товаров используются носимые терминалы, которые постоянно соединены с корпоративной сетью по протоколу Wi-Fi, и все изменения сразу отражаются в центральной базе данных. WLAN применим и в организации временных сетей, когда долго и нерентабельно прокладывать провода, а потом их демонтировать.

Еще один вариант использования – в исторических постройках, где прокладка проводов невозможна или запрещена. Иногда не хочется портить внешний вид помещения проводами или коробами для их прокладки. Кроме того, Wi-Fi-протокол подходит и для бытового применения, где тем более неудобно прогладывать провода.

Wi-Fi технологии становятся все более совершенными и качество их соединения и безопасность стремительно приближается к возможностям обычного, широко используемого, проводного соединения.