УДК 66.067

ОСОБЕННОСТИ ПОСТРОЕНИЯ СЕТЕЙ WI-FI

© 2018 П. И. Русанов, А. Г. Юрочкин

Воронежский институт высоких технологий (г. Воронеж, Россия)
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (г. Воронеж, Россия)

В статье раскрываются особенности построения сетей Wi-Fi. Современные технологии открывают человеку массу возможностей, упрощающих решение текущих житейских задач. На сегодняшний день, одной из самых быстроразвивающихся, востребованных и перспективных технологий на рынке IT является беспроводная сеть. С помощью беспроводных сетей появилась достижимость объединения абонентских устройств в группы для конверсии информацией. Главным преимуществом данного метода является то, что все происходит без использования проводов и позволяет участникам группы свободно перемещаться, оставаясь онлайн.

Ключевые слова: беспроводные сети Wi-Fi, доступ к ресурсам сети, технологии беспроводных сетей.

В нынешнем, быстро процветающем мире IT мобильность и независимость становится важнейшим ультиматумом, применяемым к актуальным устройствам и на данный момент фактически не осталось электронных устройств, не объединенных между собой или всемирной сетью Интернет.

За короткий период времени беспроводные нанотехнологии обрели огромную известность и всеобщее применение. И сейчас, мало кого можно ошеломить, установив у себя дома точку доступа. Построив беспроводную локальную сеть, можно освободиться от проводов, разведенных по всем комнатам квартиры и мониторить всемирную паутину с планшета, где только душе угодно, а не докуда посчастливилось дотащить провод. Разумеется, нанотехнология Wi-Fi может применяться в офисах, поликлиниках, магазинах для подключения инициативных работников (владеющих ноутбуками или смартфонами), которым нужно передвигаться по офисам и иметь доступ к интернету. Огромную популярность получили так называемые HotSpot'bi – точки доступа со свободным выходом в интернет, размещенного в публичных местах, такие как парки, аэропорты или кафе. К соцсетям коннектится все, от известных нам смартфонов и цифровых часов до ядерных носителей и космических шаттлов. Можно связать в общую сеть любое устройство в Вашем офисе или квартире, если это будет иметь хоть малейший смысл. Хотите увидеть, чем занимается Ваш домашний питомец в Ваше отсутствие? – Пожалуйста. Хотите включить кухонную мультиварку, чтобы она приготовила обед в Ваше отсутствие или подогрела его к Вашему возвращению домой. – Тоже легко. Все зависит не только от Вашей фантазии, но и от ваших денежных ресурсов.

Целью работы является знакомство с сетями Wi-Fi, позволяющими давать клиентам доступ к ресурсам сетей.

В 1988 году Институтом инженеров по электронике и радиоэлектронике (IEEE) был создан стандарт беспроводной связи 802.11. Вышел он в свет, примерно, через десять лет. И в 1997 году этот стандарт был, в конечном итоге принят и одобрен. Он предполагал скорость передачи данных 1-2 Мбит/с, что для начала 1990-х совсем даже неплохо. Но ко времени одобрения этого стандарта, выделяемая им скорость, уже не соответствовала запросам пользователей.

Из-за этого работники института начали модернизировать стандарт 802.11 и в итоге, к концу 1999 года обществу были показаны, два новых варианта: 802.11b (работающий на частоте 2.4 ГГц со скоростью до 11 Мбит/с) и 802.11a (работающий на частоте 5ГГц и предоставляющий скорость 54 Мбит/с). В том же году была основана самостоятельная организация WECA – Wireless Ethernet Compatibility Alliance (Ассоциация

Русанов Петр Игоревич – ВИВТ-АНОО ВО, студент, vwb5@mail.ru.
Юрочкин Анатолий Геннадьевич – РАНХиГС при Президенте Российской Федерации, д. т. н., профессор,yuroch89udnncalexf@yanfex.ru.

по совместимости беспроводных сетевых устройств), которая потом была переименована в Wi-Fi Alliance. В эту организацию входят большие фирмы по созданию сетевого оборудования. Первостепенной задачей является залог совместимости оборудования для беспроводных компьютерных сетей от разных производителей и их сертификация.

Оборудование, которое отвечает запросам стандарта 802.11 в терминологии WECA, обозначается как Wi-Fi (Wireless Fidelity переводится как беспроводная точность, покорность или надежность, в общем, сходство утвержденному стандарту). Вот откуда пошло такое сокращение, которое мы видим на коробках из точек доступа или потребитель беспроводных адаптеров, а так же на знаках «Wi-Fi zone», висящих в местах, где дается возможность работы с WLAN. В 2000 году была создана группа Task Group G, которой доверили построить беспроводной стандарт, использующий частоту 2.4 ГГц и содержащий высокую скорость передачи данных. Так, через год и шесть месяцев родился на свет стандарт 802.11g, который как и 802.11a, снабжает скорость в 54 Мбит/с, но в отличие от последнего он еще и обратно сочетаем со стандартом 802.11b. Это содействовало плавному переходу от одного стандарта к другому, то есть вносило шанс работать новому оборудованию, со старым.

Технологии беспроводных сетей.

Наиболее простой регламент работы сети, когда в ней не применяется точка доступа. Так же, оборудования располагающие у себя на борту Wi-Fi адаптеры, могут легко основать свою беспроводную сеть и работать в ней. Это весьма практично, когда нужно на короткий интервал времени, основать сеть для обмена сведениями, но нет ресурсов соединить оборудования с помощью точки доступа. Такие сети называются общими беспроводными сетями (или Ad-Hoc сетью), так как каждый абонент имеет право пользоваться такой сетью.

Дальнейший регламент деятельности беспроводной сети – Инфраструктура. На этом месте применяется беспроводная точка доступа (Wireless Access Point). Собственно она создает сеть, к которой могут подключаться остальные абоненты. AP, с каким-либо интервалом времени, посылает в эфир Beacon пакеты (широковещательный идентификатор сети). Он нужен для выявления беспроводной сети. Абонентские установки, сканируя сеть, обнаруживают данные пакеты, в которых находится информация о WLAN, расположенная рядом, и определяют, что это за сеть и стоит ли к ней подключаться.

Затем идет распределенная беспроводная система (Wireless Distribution System). Она разрешает точкам доступа устанавливать соединение не только с беспроводными абонентами, но и друг с другом. То есть можно будет объединять два отрезка сети по радио каналу, например, если между ними нет вероятности провести провод. Такого рода порядок называется беспроводным мостом.

Защита беспроводных сетей.

Весь трафик в WLAN передается по беспроводному каналу на конкретной частоте. Это не только дает возможность абонентам быть мобильными, но и создает некую угрозу засекреченности данных. В отличие от обыкновенной проводной сети, правонарушителю не нужно будет копать землю или открывать электрощитки, чтобы найти провод и присоединится к нему. Все передается по радио каналу. Можно просто, сидеть у себя в машине, ловить весь трафик, который передается по воздуху. Следовательно, сейчас мы посмотрим способы защиты беспроводной сети от нежелательных посетителей.

Первый способ защиты это WEP (Wired Equivalent Privacy). Он применялся на ранних этапах развития беспроводных сетей. Для обеспечения хотя бы минимального уровня безопасности необходимы два компонента: аутентификация и шифрование данных.

Аутентификация может быть двух видов:

- с открытым ключом – можно считать, что тут никакой аутентификации нет;

- с совместным ключом – в этом случае для доступа к сети клиенту необходимо знать общий ключ секретности.

Шифрование в протоколе WEP осуществляется при помощи 40-битного (5 символов ASCII) или 104-битного (13 символов ASCII) ключа. Используется алгоритм шифрования RC4 на поточном ключе, в котором были найдены уязвимости, поэтому он не считается надежным. При шифровании к статической составляющей ключа добавляется вектор инициализации, служащий для рандомизации оставшейся части ключа. Его длина 24 бита, вот и получается 64 или 128-битное шифрование, которое мы привыкли видеть. Но дело в том, что эти векторы после определенного промежутка времени начнут повторяться, так как количество их комбинаций не

так уж и велико. И, насобирав необходимое количество IV (Initialization Vector), можно уже будет подобрать статическую часть ключа. Вот и выходит, что WEP не может обеспечить должный уровень безопасности беспроводной сети.

В 2001 году была внедрена такая технология защиты, как 802.1x. Она может применяться как в проводных, так и беспроводных сетях. 802.1x обеспечивает аутентификацию удаленных клиентов и выдает им временные ключи для шифрования данных. Алгоритм шифрования остался прежним – RC4, но частая смена ключей уменьшает вероятность взлома. Кстати, эта технология требует наличия RADIUS-сервера (Remote Access Dial-In User Server) который будет определять, можно ли клиенту подключаться к сети и какими правами на использование сети он обладает. Вот как раз необходимость этого RADIUS-сервера и сделала эту технологию защиты не очень удобной для домашнего использования. Поэтому она больше применяется в различных организациях и серьезных учреждениях.

После того, как стало понятно, что WEP не может должным образом защитить беспроводную сеть, начались разработки нового стандарта 802.11i. Но, пока его тестировали, решено было выпустить в свет промежуточный стандарт WPA (Wi-Fi Protected Access, введен в работу с конца 2003 года). В нем так же, как и в 802.1x реализована работа динамической смены ключа, плюс к этому новый протокол шифрования TKIP (Temporal Key Integrity Protocol), однако алгоритм остался прежним – RC4. Вдобавок был реализован протокол проверки целостности пакетов MIC (Message Integrity Check). Он следит за тем, чтобы в сеть не вставлялись пакеты от третьих лиц. WPA предусматривает два варианта аутентификации: WPA-Enterprise с аутентификацией на RADIUS-сервере, и WPA-PSK с предустановленным ключом. Второй вариант предпочтительнее для домашних сетей. Для подключения к сети и шифрования данных, клиенту необходимо знать ключ длиной от 8-ми до 63-х символов ASCII. Мы видим, что WPA намного усложняет жизнь взломщикам и пробраться в нашу сеть теперь не так легко. В 2004 году был окончательно реализован стандарт 802.11i, который стали еще называть как WPA2. Он сочетает в себе все возможности WPA, только теперь в качестве основного шифра используется стойкий блочный шифр AES.

К основным технологиям защиты беспроводных сетей можно еще добавить такую возможность защиты сети, как скрытие SSID (Service Set Identifier идентификатор сети, то есть ее имя). Если клиент не будет знать имя сети, он не сможет к ней подключиться. Но узнать SSID не так уже и сложно при помощи активного сканирования. Некоторые точки доступа предоставляют такую возможность, как фильтрация клиентов по MAC адресу. Значит ты не сможешь подключиться к сети, если твой MAC не находится в «белом списке», или наоборот – находится в «черном списке». Говоря иными словами, пользователь не сможет подключиться к сети, если его MAC не находится в «белом списке», или наоборот – находится в «черном списке».

Узнать MAC клиента, которому разрешено работать с сетью, можно простым прослушиванием эфира. А сменить MAC своей карточки, на используемый – это не самая сложная задача. Так что, эти два способа защиты сетей следует использовать только в качестве дополнения к основному. Настраивая беспроводную сеть, не забывайте первым делом поменять стандартный пароль на вход к настройкам точки доступа. А еще лучше выключить возможность заходить в настройки по беспроводному соединению.

В сентябре 2009 года был официально утвержден стандарт 802.11n, который, обеспечивает пропускную способность в 300Мбит/с. Прирост производительности обеспечивается за счет системы MIMO (Multiple input, Multiple output). В ее основе лежит использование нескольких передатчиков и приемников со своими антеннами. В принципе стандарт 802.11n может обеспечить скорость передачи данных до 600 Мбит/с, применяя передачу по четырем антеннам сразу. В январе 2014 года, утвердили новый стандарт 802.11ac, который обеспечивает скорость передачи данных до 6.77 Гбит/с, для устройств, с 8 антеннами и стандарт 802.11ad с дополнительным диапазоном 60ГГц, скорость передачи данных до 7 Гбит/с.

Ассоциация Wi-Fi Aliance, в конце 2009 года, внедрила новую структуру беспроводного соединения для Wi-Fi оборудования, которая называется Wi-Fi Direct. Она заменила устаревший вариант Ad-Hoc со всеми его недостатками. То есть пропускная способность стала ограничена, только возможностями самого беспроводного адаптера, появилась поддержка WPA2, а так же возможность подключать устройства с исполь-

зованием упрощенной технологии WPS, которая оперирует PIN-кодами для авторизации устройств.

Следующим шагом в развитии беспроводных технологий стала WiMAX – телекоммуникационная технология, задачей которой является предоставление беспроводной связи на больших расстояниях. По сути это будет альтернативой выделенным линиям и ADSL, только вместо кабелей будут радиоволны. Эта технология напоминает структуру сотовой связи, ведь в ней тоже будут свои вышки покрывающие определенное пространство. Только надо понимать, что в основе данной технологии лежит стандарт 802.16 (так же его называют как Wireless MAN). То есть это другая технология и с Wi-Fi она несовместима. Используются разные частоты, схемы модуляции и методы доступа.

На сегодняшний день, существует четыре поколения мобильной связи. Если провести экскурс, то можно увидеть, что новое поколение мобильной связи появлялось примерно каждые 10 лет. Первое поколение 1G(NMT) появилось в 1981 году, второе 2G(GSM) в 1992 году, третье 3G(WCDMA/FOMA) в 2001 году, четвертое 4G(3GPP, LTE) в 2010 году. Внедрение международного стандарта 5G должно появиться к 2020 году. Получается, что в будущем к сети будет подключено еще больше устройств, большинство из которых будут работать всегда онлайн.

Пропускная способность сети 5G будет выше 10 Гбит/с.

Поддержка одновременного подключения до 100 миллионов устройств на квадратный километр.

Современные технологии открывают перед человеком массу возможностей, упрощающих решение текущих житейских задач. С помощью беспроводных сетей появилась достижимость объединения абонентских устройств в группы для конверсии информацией.

В будущем беспроводные сети будут играть все большую роль в нашей жизни. Главное, чтобы, когда они достигнут пика своего развития и массовости применения, не наступила глобальная мировая интерференция.

ЛИТЕРАТУРА

1. Головинов С. О. Цифровая обработка сигналов / С. О. Головинов, С. Г. Мирончено, Е. В. Щепилов, А. П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 4. – С. 064-065.

2. Головинов С. О. Разработка имитатора тракта передачи данных спутникового диапазона / С. О. Головинов, И. Я. Львович, А. П. Преображенский // Вестник Воронежского государственного технического университета. – 2009. – Т. 5. – № 4. – С. 214-217.

3. Казаков Е. Н. Разработка и программная реализации алгоритма оценки уровня сигнала в сети Wi-Fi / Е. Н. Казаков // Моделирование, оптимизация и информационные технологии. – 2016. – № 1 (12). – С. 13.

4. Львович И. Я. Расчет характеристик металлодиэлектрических антенн / И. Я. Львович, А. П. Преображенский // Вестник Воронежского государственного технического университета. – 2005. – Т. 1. – № 11. – С. 26-29.

5. Львович И. Я. Моделирование электромагнитных полей, рассеянных объектом в ближней зоне беспроводных сенсорных сетей / И. Я. Львович, А. П. Преображенский, О. Н. Чопоров, Г. А. Тамбовцев // Акустооптические и радиолокационные методы измерений и обработки информации Материалы 10-й Международной научно-технической конференции. Российское НТОРЭС им. А. С. Попова. – 2017. – С. 36-39.

6. Львович И. Я. Минимизация вторичного поля рассеяния от объектов сложной формы / И. Я. Львович, О. Н. Чопоров, А. П. Преображенский, Е. А. Москалёва // Информация и безопасность. – 2017. – Т. 20. – № 1-1 (4). – С. 117-120.

7. Львович Я. Е. Исследование метода трассировки лучей при проектировании беспроводных систем связи / Я. Е. Львович, И. Я. Львович, А. П. Преображенский, С. О. Головинов // Информационные технологии. – 2011. – № 8. – С. 40-42.

8. Преображенский А. П. Методы прогнозирования характеристик рассеяния электромагнитных волн / А. П. Преображенский // Моделирование, оптимизация и информационные технологии. – 2014. – № 1 (4). – С. 3.

9. Преображенский А. П. Прогнозирование радиолокационных характеристик идеально проводящей полости в диапазоне длин волн / А. П. Преображенский // Телекоммуникации. – 2005. – № 12. – С. 29-31.

10. Преображенский А. П. Моделирование характеристик рассеяния объектов, в состав которых входят кромки / А. П. Пре-

ображенский // Моделирование, оптимизация и информационные технологии. – 2016. – № 2 (13). – С. 7.

11. Преображенский А. П. Моделирование рассеяния электромагнитных волн на несимметричном объекте / А. П. Преображенский, О. Н. Чопоров, К. В. Кайдакова // В мире научных открытий. – 2015. – № 8.1 (68). – С. 526-531.

12. Scherbatyh S. S. The development of radiation models for wireless communication networks / S. S. Scherbatyh, O. N. Choporov, A. P. Preobrazhensky // Modern informatization problems in the technological and telecommunication systems analysis and synthesis Proceedings of the XXIII-th International Open Science Conference. Editor in Chief O. Ja. Kravets, 2018. – С. 272-276.

13. Чопоров О. Н. Анализ затухания радиоволн беспроводной связи внутри зданий на основе сравнения теоретических и экспериментальных данных / О. Н. Чопоров, А. П. Преображенский, А. А. Хромых // Информация и безопасность. – 2013. – Т. 16. – № 4. – С. 584-587.

FEATURES OF CONSTRUCTION OF WIRELESS NETWORKS WI-FI

© 2018 P. I. Rusanov, A. G. Yurochkin

Voronezh Institute of High Technologies (Voronezh, Russia)
Russian Academy of national economy and public administration under the President of the Russian Federation (Voronezh, Russia)

Modern technology gives our generation a lot of opportunities to simplify solving current everyday problems. Today, one of the fastest growing, in-demand technologies on the market IT is a wireless network. With the help of wireless networks appeared reachability enterprises subscriber devices in the group for conversion information. The main advantage of this method is that everything happens wirelessly and allows team members to move freely, while remaining online.

Key words: wireless network, Wi-Fi, access to network resources, wireless networking technologies.