Кашкаров А.П.

УПРАВЛЕНИЕ И НАСТРОЙКА Wi-Fi В СВОЕМ ДОМЕ

Андрей Петрович Кашкаров

Управление и настройка Wi-Fi в своем доме

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=11387595
Управление и настройка Wi-Fi в своем доме: ДМК Пресс; Москва; 2014
ISBN 978-5-97060-351-2

Аннотация

Несколько лет интерес разработчиков электронной аппаратуры и радиолюбителей связан с цифровыми программируемыми исполнительными устройствами, управление которых осуществляется посредством Интернета и сети Wi-Fi. К их достоинствам относят высокую точность, возможность размещения до двух десятков независимых цифровых датчиков на одном трехпроводном шлейфе длиной до 50 метров и управление несколькими десятками независимых каналов (исполнительных устройств). Целый дом можно сделать управляемым с помощью предложенных решений. В зависимости от изменений среды и воли владельца, дистанционно переданной управляющей команды включать или выключать какую-либо нагрузку (к примеру, освещение, нагреватель или вентилятор) теперь несложно. Для решения этой задачи в книге предложены способы коммутации нагрузки мощностью

до 5 кВт. Устройства, описанные в книге, предназначены для управления электрическими приборами через домашнюю или корпоративную Wi-Fi-сеть и могут быть использованы в проектах с общим названием «Интернет вещей» и «Умный дом». Примеры настройки электронных модулей даны не только для Windows, но и для приложения Android.

Для широкого круга заинтересованных читателей.

Содержание

1. Аспекты организации сети Wi-Fi 5
1.1. Особенности Wi-Fi 8
1.2. Преимущества и недостатки перед другими формами передачи данных на небольшие расстояния 10
1.2.1. Общеизвестные преимущества Wi-Fi 10
1.2.2. Недостатки 11
1.3. Защита от вторжения: разные варианты 13
Конец ознакомительного фрагмента. 16

Андрей Кашкаров
Управление и настройка Wi-Fi в своем доме

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

1. Аспекты организации сети Wi-Fi

Довольно распространенная сегодня аббревиатура Wi-Fi расшифровывается как торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity (перевод – «беспроводное качество» или «беспроводная точность»)) уже несколько лет высокими темпами развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Отчасти и поэтому любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и по-

лучить соответствующий сертификат и право нанесения логотипа Wi-Fi. По другой версии, термин «Wi-Fi» изначально был придуман как игра слов для привлечения внимания потребителя «намеком» на Hi-Fi (англ. High Fidelity – высокая точность). Несмотря на то что поначалу в некоторых пресс-релизах WECA фигурировало словосочетание «Wireless Fidelity» («беспроводная точность»), на данный момент от такой формулировки отказались, и термин «Wi-Fi» никак не расшифровывается.

История создания Wi-Fi такова. В 1991 году NCR Corporation/ AT&T (впоследствии – Lucent Technologies и Agere Systems) в Сига, Нидерланды, разработали новый продукт, предназначавшийся для систем кассового обслуживания, который был выведен на рынок под маркой WaveLAN и обеспечивал скорость передачи данных от 1 до 2 Мбит/с. Один из создателей Wi-Fi – Вик Хейз (Vic Hayes) – разработчик таких стандартов, как IEEE 802.11b, IEEE 802.11a и IEEE 802.11g, покинул компанию в 2003 году, и Agere Systems не смогла конкурировать на равных с другими, несмотря на то что продукция занимала нишу относительно бюджетных Wi-Fi-решений. 802.11abg all-in-one-чипсет Agere (кодовое имя: WARP) плохо продавался, и Agere Systems решила уйти с рынка Wi-Fi еще в конце 2004 года.

Широко известный сегодня стандарт IEEE 802.11n утвержден 11 сентября 2009 года. Его применение позволило повысить скорость передачи данных практически в четыре ра-

за, по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с [2]. С 2011 по 2013 год разрабатывался стандарт IEEE 802.11ac, окончательное принятие стандарта было запланировано на начало 2014 года. Скорость передачи данных при использовании 802.11ac может достигать нескольких Гбит/с. Большинство ведущих производителей оборудования уже анонсировали устройства, поддерживающие данный стандарт. Эволюция продолжалась, и в 2011 году Институт инженеров электротехники и электроники (IEEE) выпустил официальную версию стандарта IEEE 802.22. Системы и устройства, поддерживающие этот стандарт, позволят принимать данные на скорости до 22 Мбит/с в радиусе 100 км от ближайшего передатчика.

1.1. Особенности Wi-Fi

Блок-схема сети Wi-Fi содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), 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 – 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 приемник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi дает клиенту полную свободу при выборе критериев для соединения. Более подробно принцип работы описан в официальном тексте стандарта. Однако сей стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей.

По способу объединения точек доступа в единую систему

можно выделить:

• автономные точки доступа (называются также самостоятельные, децентрализованные, умные);

• точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные);

• бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

• со статическими настройками радиоканалов;

• с динамическими (адаптивными) настройками радиоканалов;

• со «слоистой» или многослойной структурой радиоканалов.

1.2. Преимущества и недостатки перед другими формами передачи данных на небольшие расстояния

1.2.1. Общеизвестные преимущества Wi-Fi

Беспроводной Интернет позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развертывания и/или расширения сети. Места, где нельзя проложить кабель, к примеру вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями. Также такое решение позволяет иметь доступ к сети мобильным устройствам. Для всех Wi-Fi-устройств гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi. Другим отличительным фактором использования Wi-Fi-устройств и сетей являются их доступность в бытовом плане, легкий монтаж и мобильность. Пользователь больше не привязан к одному месту и может пользоваться Интернетом в комфортной для вас обстановке. В пределах Wi-Fi-зоны в сеть Интернет могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д. Излучение от

Wi-Fi-устройств в момент передачи данных на порядок (в 10 раз) меньше, чем у сотового телефона. И тем не менее мы еще вернемся к вопросу безопасности применения Wi-Fi в этом разделе далее, поскольку с медицинской точки зрения известны несколько противоречий на сей счет.

1.2.2. Недостатки

Как ни странно, но недостатки Wi-Fi тоже имеют место быть.

В диапазоне 2,4 ГГц работает множество устройств, таких как устройства, поддерживающие Bluetooth, и др., и даже микроволновые печи, что ухудшает электромагнитную совместимость. Производителями оборудования указывается скорость на L1 (OSI), в результате чего создается иллюзия, что производитель оборудования завышает скорость, но на самом деле в Wi-Fi весьма высоки служебные «накладные расходы». Получается, что скорость передачи данных на L2 (OSI) в Wi-Fi-сети всегда ниже заявленной скорости на L1 (OSI). Реальная скорость зависит от доли служебного трафика, которая зависит уже от наличия между устройствами физических преград (мебель, стены), наличия помех от других беспроводных устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.

Частотный диапазон и эксплуатационные ограничения в различных странах не одинаковы. Во многих европейских

странах разрешены два дополнительных канала, которые запрещены в США; в Японии есть ещё один канал в верхней части диапазона, а другие страны, к примеру Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, к примеру Россия, Белоруссия и Италия, требуют регистрации всех сетей Wi-Fi, работающих вне помещений, или требуют регистрации Wi-Fi-оператора. О том, как можно заглушить Wi-Fi, тоже будет рассказано далее.

Внимание, важно!

Добавлю, что в России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации.

1.3. Защита от вторжения: разные варианты

Стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Новые устройства поддерживают более совершенные протоколы шифрования данных WPA и WPA2. Принятие стандарта IEEE 802.11i (WPA2) в июне 2004 года сделало возможным применение более безопасной схемы связи, которая доступна в новом оборудовании. Обе схемы требуют более стойкого пароля, чем те, которые обычно назначаются пользователями. Многие организации используют дополнительное шифрование (VPN) для защиты от вторжения.

Сегодня основным методом взлома WPA2 является подбор пароля, поэтому рекомендуется использовать сложные цифробуквенные пароли, для того чтобы максимально усложнить задачу подбора пароля. В режиме точка-точка (Ad-hoc) стандарт предписывает лишь реализовать скорость 11 Мбит/сек (802.11b). Шифрование WPA(2) недоступно, только «легковзламываемый» WEP.

Актуальные вопросы безопасности беспроводных сетей

Безопасности беспроводных сетей стоит уделять особое внимание. Ведь Wi-A! является беспроводной сетью с относительно большим радиусом действия. Соответственно, злоумышленник может перехватывать информацию или же атаковать пользовательскую сеть, находясь на относительно безопасном расстоянии. Существует множество различных способов защиты, и при условии правильной настройки можно быть уверенным в обеспечении необходимого уровня безопасности. Разберемся в них предметно.

WEP – это протокол шифрования, использующий довольно нестойкий алгоритм RC4 на статическом ключе. Существует 64-, 128-, 256– и 512-битное WEP-шифрование. Чем больше бит используется для хранения ключа, тем больше возможных комбинаций ключей, а соответственно, более высокая стойкость сети к взлому. Часть wep-ключа является статической (40 бит в случае 64-битного шифрования), а другая часть (24 бит) – динамическая (вектор инициализации), то есть меняющаяся в процессе работы сети. Основной уязвимостью протокола WEP является то, что векторы инициализации повторяются через некоторый промежуток времени, и взломщику потребуется лишь собрать эти повторы и вычислить по ним статическую часть ключа. Для повыше-

ния уровня безопасности можно дополнительно к wep-шифрованию использовать стандарт 802.1x или VPN.

WPA – более стойкий протокол шифрования, чем WEP, хотя используется тот же алгоритм RC4. Более высокий уровень безопасности достигается за счет использования протоколов TKIP и MIC.

TKIP (Temporal Key Integrity Protocol). Протокол динамических ключей сети, которые меняются довольно часто. При этом каждому устройству также присваивается ключ, который тоже меняется.

MIC (Message Integrity Check). Протокол проверки целостности пакетов. Защищает от перехвата пакетов и из перенаправления. Также возможно использование 802.1x и VPN, как и в случае с wep-протоколом.

Существует два вида WPA: WPA-PSK (Pre-shared key). Для генерации ключей сети и для входа в сеть используется ключевая фраза. Оптимальный вариант для домашней или небольшой офисной сети – WPA-802.1x. Вход в сеть осуществляется через сервер аутентификации. Оптимально для сети крупной компании.

Усовершенствование протокола WPA активно происходит все предыдущие годы. В отличие от WPA, используется более стойкий алгоритм шифрования AES. По аналогии с WPA, WPA2 также делится на два типа: WPA2-PSK и WPA2-802.1x.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.