ZigBee: взгляд вглубь

В предыдущем номере журнала мы начали рассказ о новом перспективном и набирающем все большую популярность беспроводном стандарте связи ZigBee. В материале были подробно освещены самые интересные с точки зрения разработчиков электронных систем особенности и технические характеристики этого, пожалуй, самого экономичного с точки зрения энергопотребления беспроводного стандарта. Сегодняшний материал является продолжением начатой темы и более подробно познакомит читателей с самой основой ZigBee — стандартом IEEE 802.15.4, регламентирующим самый нижний физический уровень передачи данных (PHY) и уровень управления доступом к беспроводной среде (MAC).

Александр Скуснов, к. т. н.

info@cec-mc.ru

Для начала кратко напомним об основных особенностях и назначении ZigBee. Этот беспроводной стандарт предназначен для организации низкоскоростных беспроводных персональных сетей, так называемых LR-WPAN (low-rate wireless personal area network). Основное применение — разнообразные датчики, промышленное и медицинское оборудование, «умные» дома и т. п. На фоне своих конкурентов ZigBee выделяет, прежде всего, ориентация на следующие важнейшие моменты: простая инсталляция, высокая надежность передачи данных, сверхнизкая стоимость беспроводного решения и особый упор на экономичное потребление. Краткие характеристики стандарта приведены в таблице 1.

Таблица 1. Характеристики стандарта ZigBee

Параметр	Характеристики
Скорость передачи данных	20–250 кбит/с
Дальность связи	до 100 м
Системные ресурсы	4–32 кбайт
Время работы от батареи	до нескольких лет
Адресация	16 или 64 разряда
Поддерживаемые топологии сети	звезда, «каждый с каждым»

Предполагается, что читатели уже знакомы с основами ZigBee: организация сети, виды устройств и т. д. Если же нет, то рекомендуем предварительно почитать материал, опубликованный в журнале «Компоненты и технологии», № 3'2005.

Итак, начнем. Как известно, любой популярный стандарт обычно имеет в своей основе другой, часто сокрытый от глаз постороннего наблюдателя. Например, в случае с Bluetooth это IEEE 802.15.1. Здесь мы наблюдаем аналогичную ситуацию. «Фундамент» ZigBee составляет спецификация IEEE 802.15.4. Именно она отвечает за реализацию всех основных функций — от физической передачи данных и объединения в сеть до шифрования данных современными криптографическими алгоритмами.

Для того чтобы понять, что же представляет собой ZigBee, как такая беспроводная сеть функционирует, как «дышит», что на самом деле передается по воздуху помимо данных, как организуется доступ устройств к сети и прочие тонкости, нам как раз и поможет IEEE 802.15.4.

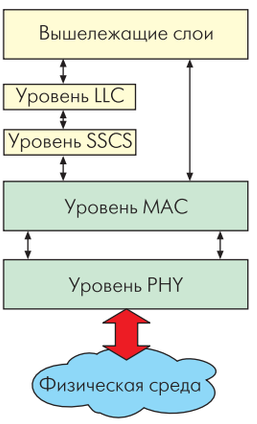

Рис. 1. Архитектура устройств LR-WPAN сети

Архитектура IEEE 802.15.4

Архитектура LR-WPAN сети, в общем, стандартна и очень схожа с классическими компьютерными сетями. LR-WPAN состоит из набора «кирпичиков», слоев или уровней, соединенных между собой логическими связями. Каждый слой отвечает за выполнение набора каких-то конкретных функций, а также предоставляет сервисы для вышестоящих уровней. Структура слоев IEEE 802.15.4 соответствует стандартной общепринятой модели OSI (Open Systems Interconnection).

Основным используемым методом доступа к физической среде, предлагаемым стандартом, является случайный доступ с контролем несущей и предотвращением конфликтов — CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance). Здесь также реализованы и такие дополнительные функции, как детектирование энергии (ED — Energy detection) и индикатор качества соединения (LQI — Link quality indication). Для передачи могут использоваться 16 каналов в диапазоне 2450 МГц, 10 каналов в диапазоне 915 МГц и 1 канал на частоте 868 МГц.

Стандарт IEEE 802.15.4 реализует два важнейших уровня сети — физический уровень передачи данных (PHY — Physical Layer), описывающий низкоуровневый механизм управления радиочастотным приемопередатчиком, и уровень управления доступом к беспроводной среде (MAC — Medium Access Control), отвечающий за доступ к физическим каналам всех типов обращений вышестоящих уровней (рис. 1).

Уровень LLC (Logical Link Control) отвечает за управление логическим соединением — это верхний подуровень канального уровня, который позаимствован из IEEE 802.2. Уровень SSCS (Service Specific Convergence Sublayer) — промежуточный сервис, обеспечивающий доступ LLC к уровню MAC. К вышележащим слоям также относятся сетевой уровень, обеспечивающий конфигурацию сети, управление и маршрутизацию данных, а также уровень пользовательских приложений, реализующий доступ к основным функциям устройства. Регламентирование работы этих слоев находится вне спецификации IEEE 802.15.4 и ложится на плечи разработчиков конкретных устройств стандарта ZigBee.

Одной из отличительных особенностей сети IEEE 802.15.4 является поддержка так называемой «суперфреймовой» структуры. Формат суперфрейма определяется координатором сети. Напомним, координатор — это главное сетевое устройство, которое управляет передачей всех потоков данных. Суперфрейм начинается с передачи специального фрейма — «сетевого маркера» (Network Beacon), который посылает сам координатор (рис. 2). «Маркер» предназначен, в первую очередь, для синхронизации и управления работой всех активных в сети устройств. После отправки «маркера» координатор самоотстраняется от управления сетью, предоставляя устройствам самостоятельно «разбираться», кто главнее.

Для этого в суперфрейме предназначен специальный отрезок времени — период конкурентного доступа устройств к радиоканалу (Contention Access Period), который разбит на фиксированные временные участки — так называемые временные слоты (time slots). В то же время для приложений, критичных к скорости и темпу передачи данных, после участка конкурентного доступа могут идти дополнительные временные слоты (Contention Free Period), в течение которых они гарантированно смогут отправить или получить срочную информацию.

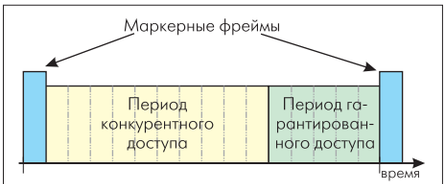

Рис. 2. Структура суперфрейма

В отличие от рабочего цикла, приведенного на рис. 2, который предполагает непрерывную передачу суперфреймов, возможен и более экономичный режим работы, при котором после периода гарантированного доступа следует период «неактивности», и никакие данные в сети не передаются до появления очередного «маркера».

Использование в конкретной сети суперфреймовой структуры и, в частности, «маркерных» фреймов не является обязательным — обмен данными может осуществляться и обычными способами. Другое дело, что часто такое применение дает определенную выгоду (об этом будет рассказано ниже).

В спецификации IEEE 802.15.4 разрешены только три формата обмена данными. Возможность использования того или иного из них определяется топологией сети и поддержкой маркерных фреймов. Например, в топологии «звезда» возможны только два первых вида транзакций. Но давайте рассмотрим их подробнее.

1. Устройство передает данные координатору сети.

В этом случае, вне зависимости от того, используются в сети «маркеры» или нет, обмен происходит в целом одинаково. Если «маркерные фреймы» используются, то устройство сначала ожидает его, обнаружив — синхронизируется и в подходящий момент передает свой фрейм данных.

В случае с сетью без маркеров все еще проще. Устройство просто передает фрейм данных в произвольный момент времени. В обоих случаях координатор сообщает об успешном завершении транзакции опциональным фреймом-уведомлением (Acknowledgment).

2. Устройство получает данные от координатора сети.

В сети, поддерживающей «маркерные» фреймы, этот формат обмена реализуется следующим образом. Когда координатору необходимо передать данные в устройство, он сообщает во время передачи сетевого маркера о том, что готовится передача сообщения. В свою очередь, устройство просматривает сетевой «маркер» и при обнаружении метки о готовности сообщения передает MAC-команду запроса данных. Координатор сообщает об успешном получении запроса данных и передает (опционально) фрейм подтверждения, после чего посылает и сами данные. Транзакция заканчивается фреймом с подтверждением получения пакета данных от устройства.

В сети без «маркерных» фреймов обмен происходит по другому сценарию. Устройство-получатель в произвольный момент передает MAC-команду запроса данных. Координатор в ответ посылает подтверждение получения запроса и, если данные готовы, передает их. Если данные еще не готовы, координатор посылает фрейм данных нулевой длины, сообщая об их отсутствии. Устройство подтверждает получение данных фреймом уведомления.

3. Данные передаются между двумя устройствами (peer-to-peer), минуя координатор.

При таком виде транзакций устройство может обмениваться данными с любыми аналогичными модулями в пределах досягаемости. Для того чтобы делать это эффективно, устройства, которые хотят обмениваться информацией, должны либо постоянно находиться в режиме «приема», либо каким-то образом синхронизироваться с остальными. Причем в последнем случае должен применяться некий особый механизм синхронизации, не описываемый стандартом, который разработчики ZigBee-совместимых устройств будут изобретать самостоятельно.

Простой анализ рассмотренных выше форматов обмена данными приводит к логичному выводу: в целом скорость передачи данных в сети без использования сетевых «маркеров» должна быть выше — в первую очередь потому, что не требуется ожидать передачи координатором сети этого самого «маркера». С другой стороны, очевидно, например, что при запросе данных из координатора применение маркерных фреймов позволит избежать «пустых» циклов запроса данных. Чтобы понять, какой способ организации беспроводной сети все-таки лучше, давайте подробнее рассмотрим виды передаваемых в сети фреймов, включая и «маркерный».

Фреймовая структура

Фреймовая структура, используемая в IEEE 802.15.4, была разработана для максимального упрощения и одновременно повышения надежности передачи в условиях зашумленного радиоэфира. Каждый вышестоящий протокольный уровень добавляет к структуре собственные специфические метки и разделы. В рассматриваемой нами сегодня сети определены четыре фреймовые структуры:

- маркерный фрейм, передаваемый координатором сети;
- фрейм данных для всех видов передачи информации;
- фрейм уведомления (подтверждения), используемый для подтверждения успешного получения какого-то фрейма;
- фрейм MAC-команды, предназначенный для управления всеми передачами данных.

Каждый фрейм проходит две степени формирования, за которые отвечают уровни MAC и PHY. На MAC-уровне формируется содержание фрейма, PHY-уровень отвечает за синхронизацию. Рассмотрим структуру самого объемного фрейма — «маркерного» (рис. 3).

Для начала определимся с полями, формируемыми на MAC-уровне, что позволит получить наглядное представление о задачах, которые здесь решаются. Сначала идут поля заголовка (MHR — MAC header):

- Поле «frame control» содержит информацию о типе фрейма (маркерный, данные, подтверждение, MAC-команда), о битах, отвечающих за наличие включенной криптографической защиты, о подготовленных для передачи данных, о принадлежности фрейма (для внутренней или для внешней соседней сети), о типе адресации в сети (16 или 64 разрядов).
- Поле «sequence number» — уникальный 8-разрядный номер фрейма, который используется для дополнительной идентификации пакетов в сети. Например, получив пакет с данными, устройство должно

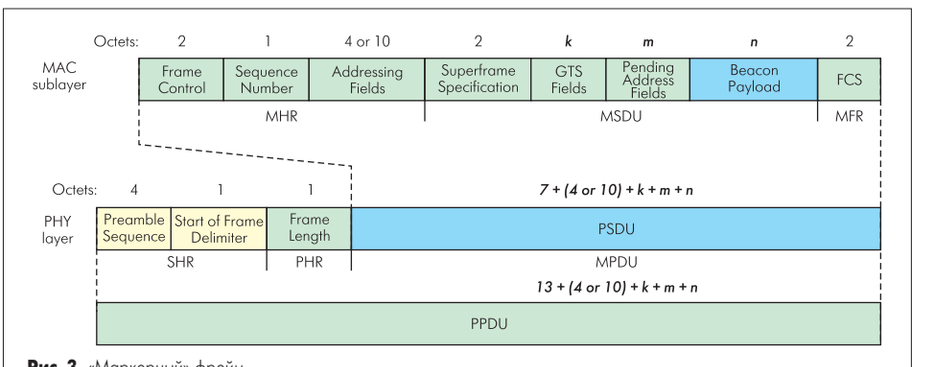

Рис. 3. «Маркерный» фрейм

послать фрейм подтверждения с точно таким же идентификационным номером.

- Поле «addressing fields» определяет 4- и 10-байтовый адрес устройства, отправившего данный фрейм. Первые два байта поля — это 16-разрядный уникальный идентификатор самой сети, причем адрес 0xFFFF обозначает широковещательный запрос, который воспримут как запрос своей сети все устройства, «слушающие» данный канал. Оставшиеся 2 или 8 байт — это адрес самого устройства: 16-разрядный — короткий адрес, 64-разрядный — длинный адрес.

Следом идут поля, отвечающие за данные (MSDU — MAC service data unit):

- Поле «superframe» specification оговаривает различные параметры суперфрейма: интервал передачи «маркера», разрешено ли в данный момент присоединение новых устройств к сети, кто передает сетевой «маркер» (координатор сети или кто-то другой) и т. д.
- Поле «GTS fields» активирует режим предоставления гарантированных временных слотов устройствам, чувствительным ко времени передачи данных, позволяет выбрать до семи адресов таких устройств с указанием, сколько временных слотов требуется каждому из них, а также выбрать номер устройства, которое будет опрошено в данном «маркерном» интервале. Здесь же устанавливается направление передачи данных — только от устройства или только к устройству.
- Поле «pending address fields» описывает количество, а также список коротких и длинных адресов устройств, для которых координатор сети готов передать данные. Число таких адресов ограничено семью, 16-разрядные адреса должны идти по списку первыми.
- Поле «beacon payload» представляет собой последовательность, предназначенную для передачи в «маркерном» фрейме данных вышележащего слоя. Это поле присутствует здесь опционально. При получении произвольным устройством «маркерного» фрейма с непустым полем beacon payload сначала происходит передача этих данных на вышележащий уровень, а только потом обработка полей superframe specification и pending address. Если поле beacon payload пустое, то обработка полей superframe specification и pending address начинается сразу.

В конце части фрейма, формируемой на MAC-уровне, идет окончание фрейма (MFR — MAC footer), здесь содержатся 16 проверочных разрядов FCS (frame check sequence), представляющих собой обычную CRC (cyclic redundancy check) сумму основных полей.

Вышеперечисленные модули MHR, MSDU и MFR формируют так называемый модуль протокола данных MAC (MPDU — MAC protocol data unit). MPDU затем проходит обработку на PHY-уровне, где он превращается в модуль сервиса данных физического уровня (PSDU — PHY service data unit), к которому добавляются в начале еще две компоненты: блок SHR, который используется для синхронизации принимающего устройства с передающим, и блок PHR, содержащий информацию о длине фрейма.

Рассмотрим подробнее их содержимое:

- Поле «Preamble Sequence» — это «преамбула» для синхронизации устройств, состоящая из 32 двоичных нулей и используемая передатчиком как идентификатор начала пакета.
- Поле «start-offrame delimiter» (SFD) — это 8 разрядов (содержащих число 0xA7), которые означают окончание полей «преамбулы» и начало пакета данных.
- Поле «frame length» — это 7-разрядное число, содержащее информацию о длине пакета PSDU.

Сформированный таким образом пакет называется физическим пакетом данных (PPDU — PHY data packet) и напрямую транслируется в физическую среду.

Теперь кратко рассмотрим остальные виды фреймов. Они имеют более простую структуру, чем «маркерный», причем отличия наблюдаются только на MAC-уровне, физический уровень не затрагивается. Часть полей, присущих «маркерному» фрейму, у остальных видов либо отсутствует, либо заменяется на другие. Ниже приведены их краткие отличия.

Фрейм данных отличает от «маркерного», в первую очередь, содержимое блока MSDU. В нем находится только одно поле — Data payload, в котором располагаются данные, затребованные вышестоящим слоем для передачи через MAC-уровень.

Фрейм «подтверждения» — самый простой по структуре. Он содержит всего два поля в заголовке MHR: frame control с идентификатором типа фрейма «подтверждение» и sequence number с номером фрейма, получение которого подтверждается. После чего сразу идет окончание фрейма MFR.

Фрейм MAC-команды, как и фрейм данных, отличается только содержимым блока MSDU. Здесь присутствуют два новых поля: тип команды (Command type) и сама команда.

Сама по себе фреймовая структура, используемая в IEEE 802.15.4, не очень сложна. К сожалению, она не дает представления обо всех возможностях устройств при работе в сети, а только регламентирует виды и формат передающихся сообщений. Наибольшей наглядностью в этом отношении обладают команды, предназначенные для передачи во фрейме MAC-команды.

Команды сети ZigBee

Обзор разрешенных для передачи в сети команд (в количестве девяти) позволит составить представление как о возможностях самой сети ZigBee, так и о функционирующих в ней устройствах. Итак, перечислим их:

- «Association request» — запрос на присоединение к существующей сети. Данный запрос устройство посылает координатору, когда хочет подключиться к сети. В запрос включается информация о характеристиках устройства — способно ли оно выполнять функции координатора сети, тип устройства (полнофункциональное устройство или устройство с ограниченными возможностями), способ питания (от обычной сети или иной), отключает ли устройство радиоприем, когда находится в «спящем» режиме, поддерживается ли криптозащита, 16- или 64-разрядный адрес хочет иметь устройство. Запрос на подсоединение могут посылать только те устройства, которые к данной сети еще не подключались.
- «Association response» — ответ координатора сети устройству, запросившему присоединение к сети. При этом координатор может: подключить это устройство к сети с присвоением адреса, сообщить, что свободных мест нет, или отказать в доступе без объяснения причин.
- «Disassociation notification» — команда отключения от сети. Может посылаться координатором, при этом он сообщает адрес устройства, которое из сети исключается. Команда также может посылаться и любым устройством в сети, при этом оно сообщает координатору свой адрес.
- «Data request» — команда, которую посылает устройство при запросе данных от координатора.
- «PAN ID conflict notification» — команда, которую посылает устройство координатору сети, когда оно обнаруживает конфликт идентификаторов сети.
- «Orphan notification» — команда, которую посылает включенное в сеть устройство при потере синхронизации с координатором.
- «Beacon request» — команда, которую посылает устройство для выявления в пределах дальности своей работы всех координаторов сетей.
- «Coordinator realignment» — команда ресинхронизации сети, которую посылает координатор либо в ответ на команду потери синхронизации (Orphan notification), либо если какие-то атрибуты сети претерпели изменения. В первом случае команда отправляется конкретному устройству, испытывающему проблемы с синхронизацией, во втором случае отправляется широковещательная команда всем доступным устройствам.
- «GTS request» — команда, которая предназначена для управления гарантированными временными слотами, предоставляемыми некоторым устройствам для передачи данных в пределах маркерного фрейма. GTS request позволяет устройствам как запрашивать выделение таких слотов, так и освобождать уже выделенные. Гарантированные слоты предоставляются только устройствам с короткими адресами, в запросе указывается число требуемых или высвобождаемых слотов времени, направление передачи данных (только прием или только передача относительно запрашивающего устройства) и 1 разряд — собственно просьба (выделить или освободить указанные временные слоты).

При рассмотрении действующих в сети ZigBee команд обращает на себя внимание следующий факт. Устройства с ограниченными возможностями могут не поддерживать подавляющее большинство из них. Причем, что характерно, в спецификации про эти команды говорится по-разному. Некоторые являются «необязательными», другие могут присутствовать «опционально». В чем конкретно разница между этими двумя случаями — непонятно, скорее всего, это одно и то же.

Надежность

Вернемся к возможностям IEEE 802.15.4. Как вы помните, одной из заявленных характеристик беспроводных сетей, строящихся на базе этого стандарта, является высокая надежность передачи данных. Какие механизмы применяются для этого на уровнях PHY и MAC, нам и предстоит сейчас разобраться.

В данной LR-WPAN применяются различные механизмы для обеспечения надежности и достоверности передаваемой информации. Эти методы включают в себя использование механизма передачи CSMA-CA, фреймы подтверждения получения и верификации данных. Рассмотрим их подробнее.

В IEEE 802.15.4 используется два типа доступа к каналам передачи, зависящие от конфигурации сети. В сетях, где «маркерные» фреймы не используются (Nonbeacon-enabled networks) и доступ к каналу происходит случайным образом, задействуется механизм, называемый «unslotted CSMA-CA channel access mechanism». Каждый раз, когда устройству требуется передать фрейм данных или MAC-команду, оно должно сначала выждать некоторый промежуток времени (его длительность выбирается случайным образом). Если канал после этого окажется свободным (idle), устройство передает свои данные. Если же канал оказывается занятым (busy) после этой произвольной задержки, устройству следует подождать еще один случайный отрезок времени и потом опять попытаться получить доступ к каналу.

В сетях с «маркерными» фреймами используется механизм с фиксированными временными слотами ожидания передачи «slotted CSMA-CA», идущими сразу после «маркерного» фрейма. Каждый раз, когда устройство захочет передать данные в период конкурентного доступа к каналу, оно должно сначала определить границу ближайшего слота ожидания и отсчитать от него случайное число подобных слотов. Если канал окажется занят после этой паузы, устройству предстоит подождать следующее случайное число фиксированных временных слотов, перед тем как попытаться получить доступ к каналу снова. Если канал свободен, устройство может начать передачу сразу с границы ближайшего слота ожидания.

Случайный доступ с контролем несущей и предотвращением конфликтов (CSMA-CA) не используется в следующих случаях:

- При отправке фреймов подтверждения, которые отправляются тут же, без ожидания освобождения канала в течение случайных промежутков или слотов времени.
- При передаче «маркерного» фрейма. Его отправка происходит уже после того, как завершаются периоды конкурентного и гарантированного доступа устройств к каналу, все разрешенные транзакции закончены и радиоканал гарантированно свободен.
- При передаче данных в течение периода гарантированного доступа. Тут все понятно по определению. Гарантированные слоты доступа предоставляются в фиксированном объеме и конкретным устройствам. Никакого случайного доступа к каналу тут не предусмотрено, поэтому он и не применяется.

Вторым уровнем обеспечения надежной доставки данных, как мы уже говорили, являются фреймы подтверждения успешного приема и достоверности полученных данных или MAC-команды. Алгоритм работы прост — если принимающее устройство не смогло по каким-либо причинам получить данные, то ответное уведомление не посылается. Если инициатор отправки сообщения не получает в течение какого-то времени подтверждения доставки, он считает данную транзакцию неуспешной и снова пытается повторить передачу. Если подтверждение не приходит и после нескольких повторов, то инициатор может по своему выбору либо прекратить транзакцию, либо пытаться отсылать данные до бесконечности.

Последний «столп» обеспечения надежности — верификация данных, которая обеспечивается с помощью 16-разрядных контрольных сумм CRC. Контрольная сумма выполняется только над полями заголовка MAC header и содержимым, передаваемым из вышестоящих слоев через MAC-уровень.

Энергопотребление

Как неоднократно говорилось выше, одним из главных достоинств стандарта ZigBee является ориентация на малое энергопотребление беспроводных устройств. Не зря ведь в анонсах и рекламных проспектах одним из первых оговаривается именно этот немаловажный параметр. На деле, как обычно, все оказывается немного сложнее. Дело в том, что в основе ZigBee — стандарте IEEE 802.15.4 — о низком потреблении говорится совсем немного. Здесь, например, оговаривается следующий момент: данный стандарт разработан, в принципе, с возможностями применения в условиях ограниченного питания. Однако физическое применение стандарта требует дополнительных изысканий в этом направлении, а это уже выходит за рамки IEEE 802.15.4.

При всем этом разработчики дают общие указания о том, как уменьшить энергопотребление устройств, которым это действительно необходимо. В аппаратуре подобного типа, использующей в качестве элементов питания батареи или аккумуляторы, предлагается в обязательном порядке применение циклического режима работы. Большую часть времени такие устройства должны проводить в «спящем» режиме. Причем им следует периодически включать радиотракт и прослушивать эфир на случай готовящихся для передачи сообщений. Этот простой и в то же время гибкий механизм, прежде всего, позволит разработчикам программных приложений на высоком уровне соблюдать баланс между экономией электроэнергии и задержкой в передаче сообщений.

Понятно, что для устройств, имеющих источник постоянного питания, например, «от сети», применение циклического режима лишено всякого смысла. Решениям такого класса разработчики IEEE 802.15.4 рекомендуют постоянно оставаться на связи.

Безопасность

Еще одним наиважнейшим параметром, характеризующим любую сеть, а тем более беспроводную, является безопасность передаваемых данных и защита их от несанкционированного доступа. В привычных для нас локальных проводных сетях эта проблема на аппаратном уровне обычно не решается, безопасность передаваемых данных обеспечивается сервисами и службами более высокого программного уровня.

Точно так же могли поступить и создатели IEEE 802.15.4, однако они все же ввели в стандарт некоторый набор базовых функций, обеспечивающих начальный уровень безопасности на MAC-уровне. Базисными сервисами в этом направлении стали: поддержка списков контроля доступа ACL (access control list) и криптографическое шифрование передаваемых данных.

Способность выполнять простейшие действия по обеспечению безопасности не является обязательной, однако разработчики настоятельно рекомендуют использовать эти функции постоянно и во всех устройствах.

Механизм шифрования, задействованный в данном стандарте, основан на применении симметричного ключа, который поставляется «сверху». Это значит, что вышележащие слои должны уметь определять, когда используются режимы безопасности на MAC-уровне, и формировать все основные параметры (в том числе и ключи) для работы сервисов защиты. Задачи создания и управления симметричными ключами ложатся на плечи разработчиков конкретных беспроводных чипов.

Перечислим основные сервисы защиты, предусмотренные в IEEE 802.15.4:

- Управление доступом с помощью списков контроля доступа ACL. Если устройство поддерживает данный сервис, оно должно иметь в своем ACL-списке перечень всех устройств, от которых оно ожидает получения данных.
- Шифрование данных для защиты от несанкционированного доступа. Для обеспечения криптозащиты используются симметричные ключи. Данные могут шифроваться как с использованием ключа, общего для группы устройств, так и с помощью отдельных ключей для каждой пары устройств (при этом ключ хранится также в ACL-списке).
- Контроль целостности фрейма. Данный сервис использует специальный код целостности сообщения (MIC — Message Integrity Code) для защиты передаваемых данных от возможных изменений их устройствами, не «знающими» криптографического ключа. Код этот также может быть общим для группы устройств или личным для пар устройств.
- Sequential freshness — специальный сервис, предназначенный для обновления рассылаемых устройствам в сети симметричных ключей.

В зависимости от режима, в котором работает беспроводное устройство, и выбранного режима безопасности, MAC-уровень обеспечивает различные сервисы защиты. В режиме

с отключенной защитой (unsecured mode) они не задействованы вообще. В режиме ACL mode обеспечиваются совместными усилиями надлежащих над MAC-уровнем слоев и сервисом управления доступом с помощью списков ACL. В третьем режиме — режиме защиты (secured mode) — могут быть активированы любые из вышеописанных сервисов, в зависимости от выбранного стандарта криптования.

В таблице 2 приведены все поддерживаемые в IEEE 802.15.4 стандарты 32-, 64- и 128-разрядного шифрования с указанием поддерживаемых сервисов защиты. Все алгоритмы обеспечения безопасности соответствуют стандарту AES (Advanced Encryption Standard). AES — это спецификация шифрования электронных данных, в том числе финансовой, телекоммуникационной и правительственной информации, предложенная Национальным институтом стандартов и технологий США (National Institute of Standards and Technology). AES пришел на замену морально устаревшему DES — самому распространенному криптоалгоритму в мире и сейчас уже заложен, например, в последних спецификациях семейства беспроводных стандартов IEEE 802.11 (Wi-Fi).

Все чипы, соответствующие IEEE 802.15.4 и поддерживающие функции защиты данных, должны в обязательном порядке поддерживать стандарт AES-CCM-64. Поддержка всех остальных стандартов осуществляется опционально. Это, в свою очередь, означает, что разработчикам беспроводных устройств на базе ZigBee, а особенно комплексных решений, следует внимательно относиться к выбору элементной базы и заранее справляться о поддержке тех или иных модификаций AES.

Таблица 2. Поддерживаемые стандарты шифрования

Идентификатор	Стандарт	Управление доступом	Шифрование	Контроль целостности фрейма	Sequential freshness
0x00	Защита выключена				
0x01	AES-CTR	X	X		X
0x02	AES-CCM-128	X	X	X	X
0x03	AES-CCM-64*	X	X	X	X
0x04	AES-CCM-32	X	X	X	X
0x05	AES-CBC-MAC-128	X		X	
0x06	AES-CBC-MAC-64	X		X	
0x07	AES-CBC-MAC-32	X		X	

* Стандарт должен поддерживаться всеми беспроводными чипами с функциями защиты данных.

Заключение

Надеемся, что наш краткий экскурс в глубины IEEE 802.15.4 оказался достаточным для того, чтобы читатели смогли понять общие принципы и задачи, решаемые на двух основополагающих «китах» этого стандарта, — уровнях PHY и MAC. Спецификация 802.15.4 довольно сложна, поскольку синтезировала все последние достижения в области беспроводных технологий и средств передачи данных. То, что рассмотрено в данной статье — лишь самая верхушка огромного айсберга под аббревиатурой IEEE 802.15.4.

Что же касается практического воплощения, то, как легко заметить, рассмотренная нами спецификация предусматривает огромное количество нюансов и вариантов реализации тех или иных возможностей, обозначенных в тексте фразами «являются необязательными» или «присутствует опционально». Поддержка функций такого рода определяется целиком производителем, что, несомненно, приведет к выпуску довольно большой номенклатуры ZigBee-совместимых устройств, обладающих незаметными на первый взгляд отличиями. Именно эти отличия разработчики, внедряющие новые технологии в жизнь, должны прекрасно себе представлять и, только определившись с собственными требованиями к будущим беспроводным устройствам, приступать к выбору элементной базы.

В следующей статье, посвященной ZigBee, мы затронем вопросы, касающиеся конкретных беспроводных чипов, представленных флагманом рынка решений ZigBee — компанией Freescale Semiconductor. В этом материале на конкретных примерах будут рассмотрены как оригинальные классы выпущенных платформ, так и особенности реализации MAC-уровней. Кроме того, будет проведен анализ их возможностей и оценка целевого назначения, одним словом, все то, что позволит нам наглядно продемонстрировать практический потенциал этой беспроводной технологии.

Литература

1. Скуснов А. ZigBee: обзор технологии // Компоненты и технологии. 2005. № 3.
2. www.cec-mc.ru.
3. www.ZigBee.org.