Открытый стандарт беспроводной сети ONE-NET и аппаратные решения на его основе

(часть 1)

Константин Верхулевский, Юрий Шаропин (г. Томск)

Преимущества беспроводных технологий приводят к появлению и развитию стандартов, способствующих их использованию для решения различных задач. В статье рассказывается о новом, открытом стандарте беспроводной сети One-Net, предназначенном для автоматизации и управления и ставшем прямым конкурентом ZigBee и KNX RF, который успел привлечь к себе внимание таких фирм, как Analog Devices, Texas Instruments, Silicon Labs и Semtech. Рассматривается спецификация стандарта One-Net для бюджетных устройств.

Введение

Бурный рост микропроцессорных технологий, постоянное снижение стоимости беспроводных решений и повышение их эксплуатационных параметров позволяют отказаться от проводных сетей в системах контроля, диагностики и обмена информацией. Беспроводные сети отличаются более гибкой архитектурой, требуют меньших затрат при установке и обслуживании. Важным аспектом при этом является стандартизация протокола передачи данных, что делает систему совместимой с изделиями других производителей.

В последнее время прилагаются значительные усилия для разработки беспроводных стандартов передачи данных, используемых в задачах автоматизации, дистанционного управления и мониторинга. Производителои пытаются решить проблемы масштабируемости и интеграции разнородных устройств с помощью различных протоколов связи. Несмотря на это, разработчики систем зачастую вынуждены использовать устройства и решения, базирующиеся на отдельных микросхемах трансиверов (приёмопередатчиков) от различных производителей электронных компонентов, и идти на большие затраты при создании собственных протоколов взаимодействия и программных стеков для организации персональных беспроводных сетей.

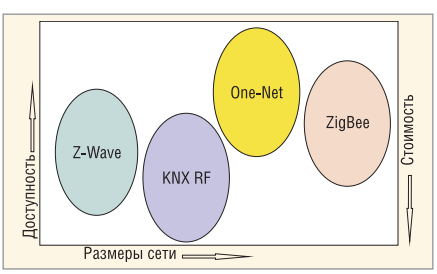

Рис. 1. Основные беспроводные стандарты для систем автоматизации и управления

Так, например, известный производитель радиомодулей компания Micrel до сих пор предоставляет потребителям собственный сетевой протокол, а компания Microchip использует запатентованный протокол MiWi для беспроводных персональных сетей (WPAN), основанный на той же спецификации IEEE 802.15.4, что и ZigBee. Применение закрытых и несвободных (проприетарных) протоколов оказывает негативное влияние на стоимость конечного изделия и сроки выхода готового продукта на рынок. Кроме того, сопряжение разнородного оборудования, управление которым осуществляется посредством закрытых протоколов, остаётся одной из наиболее серьёзных проблем. Основная причина медленного внедрения несвободных протоколов – необходимость платы за их использование в разработках. В большинстве случаев информация о самом протоколе, его спецификация, а также стек протоколов и примеры реализации узлов сети доступны на сайте альянса производителей, но только для ознакомления. Коммерческое же использование закрытых или несвободных стандартов подразумевает вступление в альянс производителей, что требует значительных затрат и неприемлемо для бюджетных решений.

В настоящее время существует несколько конкурирующих решений, претендующих на то, чтобы стать международными на рынке беспроводных устройств. Классификация основных беспроводных стандартов, используемых в задачах автоматизации и управления, представлена на рисунке 1.

Характеристики наиболее известных протоколов передачи данных, используемых в АСУ ТП, представлены в таблице 1. На сегодняшний день наиболее известными беспроводными протоколами передачи данных являются ZigBee, KNX RF и Z-Wave.

На рынке устройств диспетчеризации и управления зданием широко применяется международный стандарт KNX. На данный момент в мире существует более 100 предприятий – членов ассоциации и почти 7 тыс. групп сертифицированных продуктов KNX. Особенностью данной технологии является то, что каждый датчик или исполнительное устройство имеет свой контроллер, в который «зашита» прикладная программа этого устройства и таблица управляющих сигналов. Первоначально целью стандарта KNX являлась реализация всех приложений на уровне полевой шины. Однако в мае 2006 г. помимо использования традиционных проводных сетей стала применяться беспроводная передача данных (KNX RF), сертифицированная на соответствие требованиям Европейского (EN50090) и международного (ISO/IEC 14543) стандартов для автоматизации зданий. Недостатками данного стандарта являются низкая защищённость передаваемых данных и высокая стоимость аппаратной реализации протокола.

Датская компания Zensys не только разработала технологию Z-Wave, но и является главной движущей силой альянса Z-Wave, насчитывающего 125 чле-

нов, среди которых датский поставщик средств автоматизации жилых зданий компания Danfoss и швейцарский поставщик компьютерного периферийного оборудования компания Logitech. Z-Wave – это беспроводная технология, использующая частоту 908 МГц и продвигаемая в настоящее время на рынок в качестве более дешёвой альтернативы технологии ZigBee [1]. Технология Z-Wave предназначена для домашней автоматизации и обладает аналогичным принципом построения, но меньшей функциональностью. Встроенный протокол маршрутизации поддерживает работу в многоячейковых сетях. Очевидным недостатком Z-Wave является отсутствие масштабируемости, необходимой при увеличении числа поддерживаемых функций в домашних и промышленных сетях. Кроме того, стоимость использования протокола Z-Wave колеблется от 300 до 30 000 долл. США в зависимости от типа приобретаемой лицензии [2].

ZigBee – технология организации сетей, отличительной особенностью которых является невысокая скорость передачи данных и малая дальность действия. Спецификация ZigBee позволяет реализовывать беспроводное сетевое решение с низким энергопотреблением, обеспечивающее защиту информации и надёжность системы. Максимальная заявленная скорость передачи – 250 кбит/с. Реальная скорость передачи данных ниже, т.к., во-первых, время передачи заметно увеличивается при прохождении пакета через множество узлов сети, во-вторых, кроме полезной информации в радиопакете присутствуют и служебные данные. На физическом уровне применяется O-QPSK – квадратурная фазовая манипуляция со смещением для диапазона 2,4 ГГц (16 каналов, 250 кбит/с) и BPSK – двоичная фазовая манипуляция для диапазонов частот 915 МГц (10 каналов, 40 кбит/с) и 868 МГц (1 канал, 20 кбит/с).

Технология ZigBee поддерживается одноименным альянсом, учреждённым в 2002 г. с целью объединения усилий по разработке наиболее эффективных протоколов и обеспечения совместимости устройств различных производителей. Основными целями стандарта являются создание сетевого программного уровня безопасности и программного уровня приложений пользователя, обеспечение возможности взаимодействия сетей и согласование методик тестирования, а также международное продвижение торговой марки ZigBee. В альянс входит более 150 ведущих мировых производителей.

Протоколы двух нижних уровней ZigBee – PHY и MAC – регламентируются стандартом IEEE 802.15.4. Протоколы более высоких уровней закреплены документами альянса ZigBee. В настоящее время продолжается работа по созданию профилей устройств, т.е. формальному описанию свойств конкретных элементов сети, выполняющих одинаковые функции, например измерителей температуры. Использование профилей устройств позволяет обеспечить совместимость продукции разных производителей. До недавнего времени информация о спецификации стандарта была закрытой. Но в конце 2006 г. описание стандарта ZigBee было выложено в открытый доступ, и теперь ознакомиться с ним (после заполнения соответствующей заявки) могут все желающие.

Существует мнение, что использовать ZigBee следует только для того, чтобы обеспечить совместимость с ZigBee-устройствами сторонних фирм. Однако критики ZigBee утверждают [3], что именно совместимость является одной из слабых сторон этого стандарта. В ZigBee так много различных параметров, возможностей реализации и уровней криптографической защиты, что, по их словам, беспроблемное выполнение единой задачи модулями разных производителей в одной сети маловероятно. Так, например, изменения в версии стандарта, выпущенного в 2006 г., настолько серьёзны по сравнению с версией 1.0 (2004 г.), что без применения специальных мер устройства, построенные на базе различных спецификаций, не совместимы. Основной причиной несовместимости версий стало изменение системы адресации устройств.

Кроме того, спецификацией ZigBee-2007, выложенной на интернет-странице альянса, можно бесплатно пользоваться только для изучения и макетирования. Коммерческое применение ZigBee возможно только для членов альянса, вступить в который можно после уплаты минимального взноса в размере 3,5 тыс. долл. США за 1 год пребывания в альянсе, при этом сертификация каждого продукта потребует еще 1 тыс. долл. США [4].

Сертификация для ZigBee требует вложения денег и затрат времени, в первую очередь, на тестирование устройства, затем на покупку диапазона MAC-адресов и т.п. Большинство раз-

Таблица 1. Сравнение основных протоколов передачи данных

Сеть	One-Net		ZigBee			Z-Wave		KNX RF
Преимущества	Доступность, низкое энергопотребление, конфигурируемые схемы построения, высокая надёжность		Размеры сети, использование менее загруженных диапазонов частот			Низкое энергопотребление, простота использования		Простота использования
Частоты, ГГц	0,868	0,915	0,868	0,915	2,4	0,868	0,908	0,868
Максимальная скорость передачи данных, Кбит/с	38,4…230,4		20	40	250	9,6		16,384
Расстояние между узлами в помещении (вне помещения), м	100 (500)		30 (100)			40 (60)		30 (100)
Многоканальность	Да		Да			Отсутствует		Отсутствует
Количество поставщиков ИС	Много		Много			Один		Много
Размер сети (количество узлов)	2^{12} с возможностью объединения		65 536 (16-битные адреса), 2^{64} (64-битные адреса)			2^{32} (возможно объединение сетей посредством шлюзов)		*
Метод шифрования данных	XTEA-32, XTEA-8		AES-128			Отсутствует		Отсутствует
Среда разработки	Свободная		Зависит от поставщика кристалла			От компании Zensys (5…10 тыс. долл. США)		*
Лицензия на стек протоколов	Свободная		«Зашита» в кристалл поставщиком			Платная		Платная
Размер кода требуемой памяти программ	16K		48-128K			32K		*
Топология сети	«P2P», «звезда», «многоячейковая сеть»		«Точка-точка», «звезда», «дерево» «многоячейковая сеть»			«Многоячейковая сеть»		«P2P»

**Данные отсутствуют*

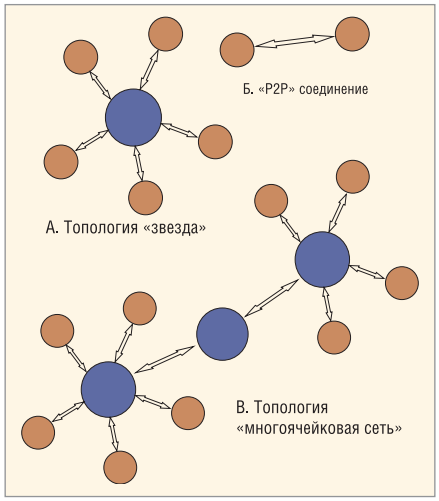

Рис. 2. Топологии сетей, поддерживаемые стандартом One-Net

работчиков имеют бюджетные ограничения и предпочитают отказаться от логотипа и сэкономить на сертификации [5].

Поэтому неудивительным оказалось появление нового, свободно распространяемого стандарта беспроводной связи One-Net, основанного на соглашении об открытом программном коде. Данный стандарт был анонсирован 14 ноября 2006 г. как альтернатива существующим закрытым и несвободным стандартам.

Стандарт One-Net

Открытый и свободный стандарт сети One-Net позиционируется как стандарт для производителей маломощных беспроводных устройств. В настоящее время членами сообщества разработчиков данного стандарта являются следующие компании: Analog Devices, Integration Associates, Micrel Semiconductor, Renesas Technology, RF Monolithics, Silicon Labs, Texas Instruments, Freescale Semiconductors, Semtech Corporation и Threshold Corporation. Последняя компания является разработчиком стандарта. Остальные компании, вступив в партнёрство, предоставили свои проекты узлов сети One-Net: схемы приёмопередатчиков, исходные коды и руководства по применению.

Новый стандарт оптимизирован для использования в системах управления и контроля жилых помещений и небольших предприятий, поэтому главным его преимуществом является доступность и низкая стоимость решений. При разработке беспроводных устройств с использованием данного протокола не требуется вступать в альянс производителей и платить за это, поскольку стек протоколов распространяется совершенно свободно в соответствии с упрощённой лицензией BSD.

Протокол One-Net основан на известной модели взаимодействия открытых систем (OSI) и предназначен для проектирования беспроводных средств, отличающихся высокой степенью защищённости данных и малым энергопотреблением. Участвующие в продвижении стандарта One-Net компании объединились для разработки свободно распространяемой спецификации на основании совместного накопленного опыта, чтобы как можно большее количество потребителей могло воспользоваться преимуществами беспроводной связи.

Сообщество разработчиков стандарта One-Net опубликовало на интернет-странице www.One-Net.info подробное описание протоколов сетевого и физического уровней, примеры исходного кода для микроконтроллеров, схемы и спецификации, необходимые для начала работы, топологию печатных плат и примеры применения. Данные материалы распространяются совершенно свободно. Логотип One-Net могут получить устройства, протестированные на соответствие требованиям стандарта.

Топологии сетей One-Net

Одним из ключевых преимуществ беспроводной системы является мобильность и гибкость её узлов. Устройства, реализованные на основе стандарта One-Net, способны работать не только в простых соединениях «точка-точка» и «звезда», но также и в сложных сетях с многоячейковой топологией, поддерживающих ретрансляцию и поиск наиболее эффективного маршрута для передачи данных. Как известно, многоячейковые сети менее восприимчивы к сторонним вмешательствам, условиям окружающей среды и обеспечивают более высокое качество обслуживания (QoS).

Рассмотрим подробнее применяемые топологии сетей согласно спецификации стандарта ONE-NET [6]. На рисунке 2 представлены различные варианты топологии сетей One-Net. Соединения типа «звезда» подходят для самых простых приложений, обладают минимальной стоимостью, максимально низким энергопотреблением и позволяют использовать стратегию стандартного множественного доступа. В каждой сети с топологией «звезда» имеется один координатор (мастер) сети, который задаёт адрес и любые другие параметры сети для каждого вновь добавленного узла.

При организации одноранговой или пиринговой (peer-to-peer) сети координатор назначает всем устройствам сети равные права. При этом каждый элемент сети является как клиентом, так и сервером. Поэтому оконечные устройства могут общаться непосредственно друг с другом, даже если координатор удалён из сети. Принимающему элементу не требуется знать, что он является частью P2P-соединения, настроенного координатором. Он просто реагирует на запросы устройства, которое к нему обращается, поэтому принимающий модуль может быть частью многих P2P-соединений. Каждое устройство сети One-Net может поддерживать от 4 до 15 одноранговых соединений.

При многоячейковой топологии в случае возникновения препятствия на пути сигнала от одного узла к другому (железобетонная или металлическая преграда и т.п.) выбирается альтернативный маршрут передачи данных, в результате чего сеть самовосстанавливается. Увеличение концентрации сетевых узлов повышает защищённость и надёжность системы.

Для организации многоячейковой сети One-Net используются ретрансляторы. Ретрансляторы представляют собой оконечные устройства, обнаруживающие так называемые «мультихоповые» пакеты данных и повторяющие их для увеличения дальности передачи сообщений. Поскольку ретрансляторы должны следить за наличием в сети мультихоповых пакетов, они постоянно находятся в активном режиме и для обеспечения бесперебойного функ-

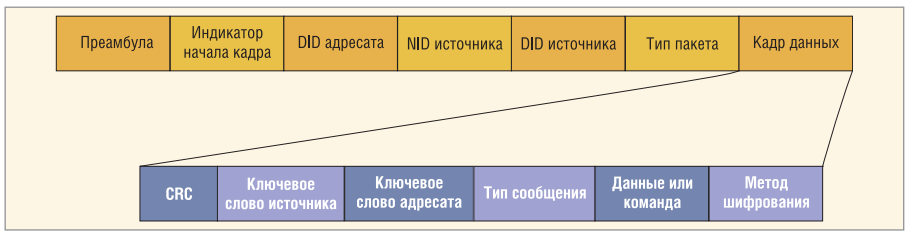

Рис. 3. Структура пакета данных в сетях One-Net

ционирования должны работать от сети электропитания. Мультихоповый пакет данных в сетях One-Net имеет собственный идентификационный номер, поэтому его нельзя спутать с обычным пакетом. Таким образом, ретрансляторы могут передавать пакеты без дополнительных пауз, появляющихся при передаче без ретрансляторов [6].

Мультихоповый пакет содержит поле длиной в три бита, в котором задаётся оставшееся число ретрансляций сигнала. Благодаря этому время передачи остаётся постоянным и предотвращается «блуждание» пакета по сети. Другие три бита отвечают за максимальное количество прыжков (хопов). Эти данные необходимы для получателя, чтобы он знал, сколько было ретрансляций. При обнаружении и приёме ретранслятором мультихопового пакета количество оставшихся прыжков уменьшается, и если значение больше нуля, то происходит ретрансляция пакета.

Для доступа к каналу используется хорошо отработанный в сети Ethernet механизм множественного доступа к среде с контролем несущей и предотвращением коллизий (CSMA), основанный на определении состояния канала связи перед началом передачи, что позволяет существенно сократить конфликты, вызванные передачей данных одновременно несколькими устройствами.

Попытка передачи данных всегда начинается с «прослушивания» эфира. Если канал занят (несущая обнаружена), попытка передачи данных возобновляется через 5 мс. Передача сообщения производится после обнаружения свободного канала. При возникновении конфликта данные считаются утерянными и повторная передача происходит через интервал времени от 2 до 10 мс в зависимости от приоритета сообщения. После восьми неудачных попыток принимается решение о том, что данные передать не удалось. Каждое передающее устройство освобождает канал после передачи одного пакета данных, чтобы другие устройства имели возможность участвовать в работе сети.

Адресация в сетях One-Net

Адрес устройств в сетях One-Net занимает 48 бит, 36 из которых соответствуют сетевому адресу (Network ID, NID), а остальные 12 определяют адрес устройства в сети (Device ID, DID) [6]. Сетевой адрес NID представляет собой уникальное 36-битное число, которое присваивается беспроводному модулю при изготовлении. Если в дальнейшем данный модуль будет выполнять функции координатора, то все элементы сети, находящиеся под его управлением, получат его уникальный идентификационный номер. Уникальный DID назначается координатором сети.

Структура пакета данных

Структура пакета данных в сетях One-Net изображена на рисунке 3. Длина пакета данных является переменной величиной и может принимать значения от 120 до 472 бит в зависимости от типа пакета. Всего применяется 30 различных типов пакетов. Каждый пакет данных содержит заголовок, состоящий из преамбулы, индикатора начала кадра (SOF), DID-адресата информации, типа пакета (PID), NID и DID отправителя. За заголовком следует кадр данных. В мультихоповый пакет добавляются 6 бит, определяющих разрешённое количество ретрансляций.

Все данные отправляются старшим значимым разрядом вперёд. До передачи каждый бит данных проходит четыре стадии преобразования:

- исходные данные;
- исходные данные с присоединённым CRC (для выявления ошибок в кадре);
- зашифрованные данные (для повышения конфиденциальности данных);
- кодированные данные (для улучшения синхронизации и выравнивания потребления мощности, а также повышения достоверности данных благодаря вводимой избыточности).

При формировании самого кадра данных также используются строго определённые правила. Для выявления ошибок в кадре данных используется CRC. Приём кадра данных подтверждается квитанцией ACK. Приём считается правильным в случае отсутствия ошибок в кадре данных. Если квитанция получена с ошибками, передача кадра данных производится повторно.

Поле ключевого слова отправителя сообщений принимает произвольное значение, которое изменяется в каждом пакете данных. Это повышает степень защищённости передаваемых сообщений. Отправитель посылает в запросе к получателю случайное число и проверяет, корректное ли значение содержится в его ответе. Далее полученное значение встраивается отправителем в передаваемый пакет данных. В случае получения приёмником пакета

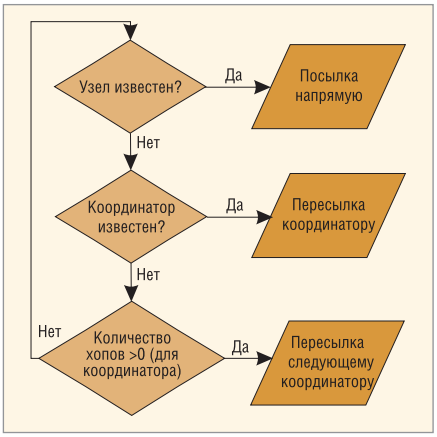

Рис. 4. Упрощённый алгоритм работы сети One-Net

с ошибочным ключом данные считаются повреждёнными и приёмником выдаётся соответствующая квитанция.

Поле ключевого слова приёмника сообщений содержит информацию, выдаваемую по требованию передатчика.

Тип сообщения может принимать три значения: данные (0000), команда управления при отправке одиночного пакета (0001) или команда при отправке блока пакетов (0010). Следующее поле содержит непосредственно данные или управляющую команду. Данные помимо одиночных пакетов могут передаваться блоками (максимум 150 байт) или потоком [7].

Последнее поле из двух бит определяет метод шифрования данных. В настоящее время используется алгоритм XTEA-XX, где XX – число циклов шифрования. При покадровой и поблочной передаче используется метод XTEA-32, при потоковой передаче данных – XTEA-8.

Алгоритм работы сети One-Net

Подключение нового устройства к сети One-Net осуществляется следующим образом. После подсоединения к сети каждый вновь добавленный узел начинает сканировать доступные частотные каналы (не менее 1 с на каждой частоте). Координатор сети по меньшей мере три раза в секунду отправляет специальный широковещательный сигнал, сигнализирующий о возможности подключения. После обнаружения данного сигнала новое устройство передаёт координатору сигнал состояния, содержащий подтверждение подключения к сети и свои параметры. Дальнейшая работа сети осуществляется согласно алгоритму, представленному на рисунке 4.

Продолжение следует