Виктор Денисенко

Беспроводные локальные сети

Часть 1

Существует много объектов автоматизации, где сложно обойтись без беспроводных сетей или где их применение явно желательно:

- датчики и исполнительные устройства на подвижных частях конвейеров, мельниц, лифтов, миксеров, тележек для перемещения грузов по цеху, на крыльях и лопастях самолетов, на подшипниках двигателей, на роботах, в передвижных лабораториях, датчики вибрации на контейнерах для перевозки грузов, а также датчики на теле человека и животных;
- объекты, в которых нежелательно сверлить стены или портить дизайн, например офисные здания, в которых устанавливаются пожарная и охранная сигнализация, датчики для систем обогрева и кондиционирования воздуха, датчики для мониторинга механических напряжений в конструкциях зданий, жилые помещения со статусом «умного дома», в которых развёрнуты системы управления бытовыми приборами, освещением, микроклиматом, контролем доступа и пр., а также музеи, памятники архитектуры и т.д.;
- системы, предполагающие эпизодическое программирование и диагностику ПЛК (прокладка постоянного кабеля из-за нерегулярного характера его использования здесь чаще всего просто невыгодна) или дистанционное считывание показаний счётчиков и самописцев;
- объекты с агрессивными средами, вибрацией, а также объекты, находящиеся под высоким напряжением или в местах, неудобных для прокладки кабеля;
- системы отслеживания траектории движения транспорта, охраны границ государства, мониторинга напряжённости автомобильного трафика в городах и условий на дорогах, мониторинга леса, моря, сельскохозяйственных угодий, мониторинга вредных для экологии выбросов и т.п.;
- любые объекты, для которых известно, что стоимость кабелей, кабельных каналов, опор или траншей, а также работ по монтажу и обслуживанию существенно превышает стоимость заменяющей беспроводной системы при условии отсутствия жёстких требований к надёжности доставки сообщений в реальном времени;
- объекты во взрывоопасных зонах [1].

В большинстве применений беспроводные сети позволяют достичь следующих преимуществ по сравнению с проводными [1]:

- существенно снизить стоимость установки датчиков;
- исключить необходимость профилактического обслуживания кабелей;
- исключить дорогостоящие узлы разветвлений кабеля;
- уменьшить трудозатраты, а также время на монтаж и обслуживание системы;
- снизить стоимость системы за счёт исключения кабелей;
- снизить требования к обучению персонала монтажной организации;
- ускорить отладку системы и поиск неисправностей;
- обеспечить удобную модернизацию системы.

Поскольку реконфигурация системы и её монтаж становятся гораздо более простыми, беспроводные сети можно использовать и в традиционных областях применения кабельных связей, когда стоимость кабеля и монтажа оказывается выше, чем установка беспроводной сети.

Беспроводные сети делятся на следующие классы:

- сотовые сети WWAN (Wireless Wide Area Network);
- беспроводные LAN (Wireless LAN — WLAN);
- беспроводные сети датчиков.

В промышленной автоматизации наибольшее распространение получили три типа беспроводных сетей: Bluetooth [2] на основе стандарта IEEE 802.15.1, ZigBee [3] на основе IEEE 802.15.4 [4] и Wi-Fi на основе IEEE 802.11 [5, 6]. Физические уровни модели OSI [1] для этих сетей основаны на соответствующих стандартах IEEE, а протоколы верхних уровней разработаны и поддерживаются организациями Bluetooth, ZigBee и Wi-Fi соответственно. Поэтому в названии сетей обычно указывают ссылки на стандарт. Все три сети используют нелицензируемый диапазон ISM (Industrial, Scientific, and Medical) 2,4 ГГц.

Проблемы беспроводных сетей и пути их решения

С точки зрения требований к промышленным сетям беспроводные сети уступают проводным по ряду характеристик.

- Время доставки сообщений: используемый механизм случайного доступа к каналу CSMA/CA не гарантирует доставку в заранее известное время [7], и эту проблему нельзя решить с помощью коммутаторов, как в проводных сетях.
- Помехозащищённость: беспроводные сети подвержены влиянию

электромагнитных помех значительно сильнее, чем проводные.

- Надёжность связи: при несвоевременной смене батарей питания, изменении расположения узлов сети или появлении объектов, вносящих затухание, отражение, преломление или рассеяние радиоволн, связь может исчезнуть.
- Ограниченная дальность связи без использования ретрансляторов (обычно не более 100 м внутри помещений).
- Резкое падение пропускной способности сети при увеличении количества одновременно работающих станций и коэффициента использования канала.
- Безопасность: возможность утечки информации, незащищённость от искусственно создаваемых помех, возможность незаметного управления технологическим процессом враждебными лицами.

Уникальным достоинством беспроводных сетей является отсутствие кабелей, что и определяет выбор областей их применения в системах промышленной автоматизации.

Рассмотрим физические причины возникновения перечисленных проблем и методы борьбы с ними. Основными причинами являются интерференция, дифракция, преломление, отражение, рассеяние (переизлучение) и снижение плотности мощности излучения при увеличении расстояния от источника, а также невозможность локализации радиоволн в ограниченном пространстве.

Зависимость плотности мощности излучения от расстояния

Известно, что плотность мощности радиоволны уменьшается по мере удаления от антенны вследствие расхождения пучка, рассеяния и поглощения волн препятствиями на пути их распространения. Плотность мощности P(d) волны на расстоянии d от источника приближённо описывается следующей зависимостью [7]:

$$P(d) \approx P_t (d_0/d)^{\gamma}, \qquad (1)$$

где d_0 — некоторая константа, определяемая экспериментально; параметр $\gamma = 2...6$ [7] зависит от конструкции антенны, диапазона частот, наличия препятствий на пути распространения электромагнитной волны. В условиях промышленного предприятия $\gamma = 2...3$ [7].

По указанным причинам каждый участник беспроводной сети имеет ограниченную зону уверенного приёма, которая представляется приближённо в форме сферы. Это приводит к необходимости планирования расположения беспроводных станций таким образом, чтобы зоны уверенного приёма непосредственно связывающихся станций перекрывались. Если станции расположены на расстоянии неуверенного приёма, то небольшие изменения окружающей обстановки могут привести к потере сообщений или снижению скорости передачи.

Ограниченность радиуса действия передатчиков привела к возникновению ячеистых сетей [8], в которых информация передаётся не через общий канал связи как в проводных сетях, а от узла к узлу, используя промежуточные узлы сети в качестве ретрансляторов и маршрутизаторов. При выходе из строя или удалении из сети некоторых узлов сеть автоматически находит новый маршрут, чтобы доставить данные адресату. Добавление к сети нового устройства также может происходить автоматически, то есть ячеистые сети обладают свойством самоорганизации.

Влияние интерференции волн

Электромагнитная волна передающей станции на пути следования испытывает интерференцию, дифракцию, отражение, преломление и рассеяние. Поэтому в точке приёма волна является суперпозицией множества волн, имеющих разные фазы и направления волнового вектора. Наложение волн приводит к интерференции, которая может быть конструктивной (когда сигнал в точке приёма усиливается) или деструктивной (когда сигнал ослабляется — эффект «замирания»). Деструктивная интерференция приводит к нескольким отрицательным следствиям. Во-первых, сигнал в точке приёма может оказаться ниже порога чувствительности приёмника, что приведёт к потере связи. Во-вторых, при движущемся источнике или приёмнике в точке приёма возможны многократные смены сильного и слабого сигнала, что может привести к потере нескольких битов информации или уменьшению скорости передачи за счёт повторных передач кадров с ошибкой. В-третьих, если разность времени задержки волн, прошедших разными путями, превысит длительность символа, соседние символы в сообщении могут накладываться друг на друга, вызывая эффект межсимвольной интерференции.

Источники помех

Существуют также другие причины искажений передаваемого сигнала: паразитное взаимовлияние соседних каналов, эффект Допплера, помехи от работающих двигателей, разряды статического электричества и др. Это может привести к потере пакета, повторной передаче и, как следствие, непредвиденной задержке в канале. Интенсивность потока ошибок зависит от мощности источников помех, типа модуляции и мощности передатчика, от частотного диапазона, других причин и обычно изменяется с течением времени.

Измерения, выполненные в работе [7], показали, что чипсет, соответствующий стандарту IEEE 803.11b, в индустриальном окружении даёт поток кратковременных ошибок, характеризующийся вероятностью $10^{-4}...10^{-2}$ при скорости передачи 2 Мбит/с и использовании квадратурной фазовой модуляции QPSK (Quadrature Phase-Shift Keying). Кроме того, в процессе измерений эпизодически возникали периоды продолжительностью до 1 мин, когда потери данных доходили до 10 и даже 80%. Аналогичные результаты наблюдались и в других экспериментах.

Следствием помех в канале может быть не только потеря данных или замедление скорости передачи, но и проблема пространственной непротиворечивости. Она заключается в следующем. Когда система использует широковещательный режим передачи без уведомления о получении, предполагается, что все приёмники должны получить одни и те же данные одновременно. Однако вследствие ошибок в канале некоторые потребители могут получить ошибочные данные. Такая ошибка особенно нежелательна, если широковещательный режим используется для обеспечения синхронной работы нескольких контроллеров в одном и том же технологическом процессе, поскольку она приведёт к рассинхронизации процесса.

Особенностью рассмотренного случая является то, что вероятность ошибки в системе резко возрастает по сравнению с вероятностью ошибки в одном канале p. Поскольку вероятность безошибочной передачи в системе является произведением вероятностей безошибочной передачи в каждом из каналов, то при количестве одинаковых каналов k вероятность отсутствия сбоев в системе будет равна $(1 - p)^k$. Например, в системе из 8 каналов при вероятности ошибки в канале $p = 0{,}1$ вероятность безошибочной передачи составит всего 43%.

Одним из примеров, где описанная ситуация может иметь место, является режим одновременного ввода несколькими устройствами сигналов датчиков. В проводных сетях для этого используют широковещательные команды, которые доходят до всех устройств одновременно (в сетях Modbus это команда с адресом 0). Если аналогичный режим использовать в беспроводной сети, то вероятность того, что все k датчиков введут отсчёты одновременно, будет также равна $(1 - p)^k$.

В сетях с передачей маркера помехи могут привести к потере маркера и отключению устройств с потерянным маркером на несколько периодов обращения маркера по логическому кольцу.

Широкополосная передача

Одним из методов устранения влияния интерференции волн и узкополосных помех является применение широкополосной модуляции. В беспроводных сетях используются два метода: широкополосная модуляция с прямым расширением спектра (Direct Sequence Spread Spectrum — DSSS) и с перескоком с одной несущей на другую (Frequency Hopping Spread Spectrum — FHSS).

Метод DSSS состоит в следующем. Если один бит информации представить прямоугольным импульсом, то эффективная ширина спектра импульса будет обратно пропорциональна его длительности. В методе DSSS один прямоугольный импульс заменяют последовательностью из 11 импульсов, которые в 11 раз короче исходного. При этом эффективная ширина спектра такой последовательности импульсов оказывается в 11 раз шире, чем у исходного одиночного импульса (бита), и для сетей Wi-Fi составляет 22 МГц. Поскольку энергия сигнала оказывается «размазанной» по всему спектру, то спектральная плотность мощности сигнала получается в 11 раз меньше, если её измерять в той же полосе частот, которую занимал первоначальный прямоугольный импульс. Практически мощность передатчика (около 1 мВт) для диапазона 2,4 ГГц выбирают таким образом, чтобы спектральная плотность полезного сигнала была сравнима или даже меньше спектральной плотности шума.

Для ещё большего уменьшения спектральной плотности мощности сигнала его спектральная характеристика должна быть близка к прямой линии, параллельной оси абсцисс, то есть сигнал должен быть подобен белому шуму. Для этого последовательность коротких импульсов не должна быть периодической, она должна быть шумоподобной (псевдослучайной), с малым временем автокорреляции. Процесс преобразования спектра сигнала к указанному виду называют процессом «обеления» («отбеливания») спектра. Кроме того, для облегчения обнаружения сигнала в приёмнике псевдослучайная последовательность, выбранная для кодирования, должна быть такой, чтобы её автокорреляционная функция имела только один ярко выраженный максимум. Такому требованию удовлетворяют, в частности, последовательности Баркера [9]. Последовательность (код) Баркера длиной 11 импульсов для кодирования логической единицы используется в сетях Wi-Fi и имеет вид 11100010010. Логический ноль кодируется инверсной последовательностью Баркера.

Для выделения полезного сигнала с такой малой мощностью на фоне шума в приёмнике должна храниться копия передаваемого сигнала (код Баркера). Это позволяет использовать очень эффективные методы оптимальной фильтрации [9]. Зная, что полезный сигнал представляет собой последовательность Баркера, в приёмнике строят оптимальный фильтр с импульсной характеристикой, которая представляет собой масштабную копию входного сигнала, расположенную зеркально по оси времени относительно входного сигнала и сдвинутую в сторону запаздывания на величину не менее длительности выделяемого импульса.

Ширина спектра сигнала в методе DSSS при скорости передачи 1 Мбит/с составляет 22 МГц, а ширина выделенного для Wi-Fi частотного диапазона — 83,5 МГц, то есть во всём диапазоне можно разместить только 3 неперекрывающихся канала. Однако стандарт делит весь диапазон на 11 перекрывающихся каналов, из которых только три (1-й, 6-й и 11-й) могут работать, не влияя друг на друга.

Достоинствами метода DSSS являются:

- высокая устойчивость к узкополосным помехам;
- возможность восстановления информации при потере во время передачи нескольких битов в коде Баркера.

Вторым методом широкополосной модуляции является FHSS — метод скачкообразного изменения несущей частоты. Он использует тот же диапазон 2,4 ГГц шириной 83,5 МГц, в котором выделяется 79 неперекрывающихся частотных полос по 1 МГц каждая. В процессе передачи частота несущей изменяется скачкообразно. Частота переходов с одной несущей на другую должна быть не менее 4 Гц в Wi-Fi и 1,6 кГц в сети Bluetooth. Для приёма такого сигнала приёмник и передатчик содержат таблицы, в которые занесена одна и та же последовательность смены каналов. При таком способе передачи узкополосные помехи приводят к потере только тех фрагментов сообщений, которые передаются на частоте помехи, то есть фактически только к увеличению времени передачи за счёт повторной передачи испорченных фрагментов.

Модификацией FHSS является адаптивный метод FHSS (Adaptive Frequency Hopping — AFH), в котором во время передачи обнаруживаются и запоминаются частоты, на которых передача выполнялась с ошибками контрольной суммы. Эти частоты исключаются из таблицы используемых частот.

Переход с одной частоты на другую уменьшает вероятность взаимного влияния при совместной работе нескольких передатчиков в сети, поскольку при 79 частотах вероятность совпадения частот двух работающих станций очень низка — порядка

$(1/79)^2 = 1{,}6\times10\times4$. Поэтому метод FHSS позволяет использовать большее количество одновременно работающих станций в сети. Практически на одной и той же территории могут работать до 15 передатчиков.

FHSS обеспечивает скорость передачи 1 и 2 Мбит/с. Используется частотная модуляция с двумя дискретными значениями частот f_1 и f_2, которые позволяют сделать четыре комбинации модулированных сигналов ($f_0 + f_1, f_0 - f_1, f_0 + f_2, f_0 - f_2$) и закодировать таким образом 4 бита информации.

На практике системы с FHSS способны работать при более высоком уровне шума, чем DSSS, благодаря тому, что они занимают более широкую полосу частот (83,5 МГц по сравнению с 22 МГц для DSSS), а вероятность того, что помеха будет занимать полосу 83,5 МГц, ниже, чем аналогичная вероятность для полосы 22 МГц. Однако интерференция, приводящая к замиранию сигнала, сильнее сказывается на FHSS, поскольку в DSSS замирания происходят только в узкой полосе частот, что приводит к выпадению нескольких битов из 11 передаваемых, а оставшихся битов достаточно для безошибочного распознавания закодированного значения 0 или 1.

Методы расширения спектра имеют следующие достоинства:

- высокая помехоустойчивость благодаря большой избыточности кода и возможности применения оптимальной фильтрации;
- возможность избежать влияния интерференции, поскольку она происходит только в части широкополосного диапазона (в методе DSSS она приводит только к потере нескольких битов, которые можно восстановить, а в методе FHSS — к потере отдельных фрагментов сообщений, которые восстанавливаются путём повторной передачи или теряются только один раз, до того как система исключит данную частоту из списка используемых по методу AFH);
- широкополосный сигнал сложнее перехватить, чем узкополосный (FHSS выглядит как шум, если в приёмнике не использована та же очерёдность смены частот, что и в передатчике);
- широкополосный передатчик может использовать один и тот же диапазон частот совместно с другими типами передатчиков с минимальным взаимовлиянием (в частности, он практически не вносит помех в узкополосные системы благодаря очень малой мощности);
- работа при спектральной плотности сигнала на уровне и ниже уровня шума позволяет исключить необходимость получения лицензии на использование таких передатчиков.

Методы модуляции несущей

Идея модуляции состоит в том, чтобы перенести спектр информационного сигнала в область высоких частот, в нашем случае — в диапазон 2,4 ГГц, что позволит передать его с помощью электромагнитной волны. Электромагнитные волны возбуждаются в антенне током синусоидальной формы $i = A\sin(\omega t + \varphi)$, который называется несущим колебанием, или просто *несущей*. По крайней мере один из параметров несущей A, ω, φ может зависеть от времени: $A = A(t)$, $\omega = \omega(t)$, $\varphi = \varphi(t)$. Форма этой зависимости соответствует форме сигнала, который нужно передать с помощью радиоканала. Процесс управления параметрами несущей называется *модуляцией*. Частным случаем модуляции является *манипуляция*, когда модулированные параметры изменяются скачкообразно между двумя их значениями. В зависимости от того, какой параметр становится зависимым от времени, модуляция называется амплитудной, *фазовой* или *частотной*. Возможны также комбинированные способы модуляции: амплитудно-фазовая, фазо-частотная и т.п.

Количество информации, которое может быть внесено в сигнал, можно увеличить, используя несколько одновременно изменяемых параметров. В цифровых системах передачи модулируемые параметры изменяются дискретно. Поэтому количество информации, приходящееся на *бодовый интервал*, можно увеличить, увеличивая количество дискретных уровней. Бодовым интервалом называют временной интервал, в течение которого параметры A, ω, φ остаются постоянными.

Поскольку $\sin(\omega t+\varphi)=\cos(\varphi)\sin(\omega t)+\sin(\varphi)\cos(\omega t)$, то есть изменение фазы можно представить с помощью изменений амплитуды синусоидальной и косинусоидальной компонент, параметры исходного синусоидального колебания можно представить на плоскости с помощью графика, представленного на рис. 1, у которого по оси абсцисс отложена амплитуда синусоидальной компоненты, то есть величина $\cos(\varphi)$ (её называют синфазной компонентой и обозначают на графике буквой I от слова In-phase), а по оси ординат — амплитуда косинусоидальной компоненты, то есть $\sin(\varphi)$ (её называют квадратурной компонентой и обозначают буквой Q от слова Quadrature). Полученный таким способом график называется сигнальным созвездием. Он совпадает с графиком, изображающим синусоидальное колебание на комплексной плоскости.

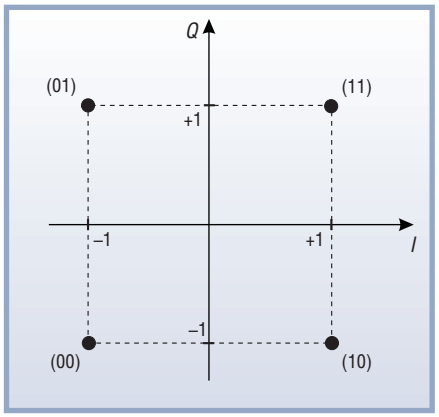

Рис. 1. Сигнальное созвездие для QPSK-модуляции

При амплитудной модуляции фаза не изменяется, поэтому все точки графика располагаются на оси абсцисс. При фазовой модуляции амплитуда постоянная, поэтому все точки графика лежат на окружности, радиус которой равен амплитуде колебания.

При двоичной фазовой модуляции (Binary Phase-Shift Keying — BPSK) фаза принимает только два дискретных значения — 0 и π, поэтому сигнальное созвездие состоит из двух точек, расположенных на оси абсцисс. Эта разновидность фазовой манипуляции является наиболее помехоустойчивой.

Модификацией этого метода является дифференциальная двоичная фазовая манипуляция (Differential BPSK — DBPSK). Здесь логическим значениям 0 или 1 соответствуют не абсолютные значения фазы, а изменение фазы относительно предыдущего её значения. Например, если

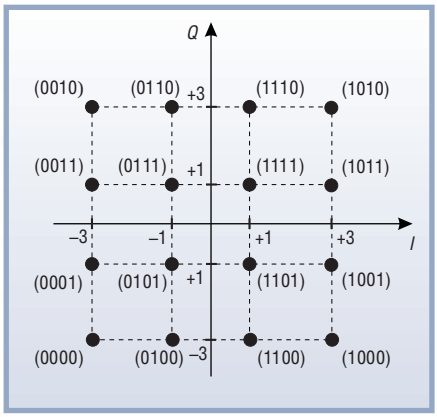

Рис. 2. Сигнальное созвездие для 16-QAM-модуляции

фаза сигнала была равна 0°, то для кодирования значения 1 её изменяют на 180°, а для кодирования логического 0 фазу оставляют прежней. Аналогичная идея используется в методе NRZI-кодирования, когда логической единице соответствует изменение уровня сигнала, а логическому нулю — отсутствие этого изменения.

Если cos(φ) принимает значения 0 или 1 и при этом sin(φ) принимает значения 1 и 0, то такая модуляция называется квадратурной фазовой манипуляцией QPSK (Quadrature Phase-Shift Keying) и позволяет получить 4 состояния передаваемого сигнала в пределах бодового интервала. Сигнальное созвездие QPSK показано на рис. 1.

Модификацией QPSK является DQPSK-модуляция (Differential QPSK), при которой аналогично DBPSK кодируется не величина фазы, а её изменение относительно предыдущего значения. Изменение фазы на 0° кодируется как 00, изменение на 90° кодируется как 01, на 180° — как 11, на 360° — как 10.

Помехоустойчивость метода модуляции можно оценить по расстоянию между точками сигнального созвездия; это расстояние характеризует амплитуду и фазу помехи, которая достаточна, чтобы был принят ошибочный сигнал. Поэтому при проектировании схем модуляции точки сигнального созвездия выбирают таким образом, чтобы расстояние от любой точки до её соседей было одинаковым для всех точек созвездия. При этом достигается одинаковая помехоустойчивость для любых передаваемых чисел.

Беспроводные сети используют также амплитудно-фазовую модуляцию 16-QAM (рис. 2) или 64-QAM. Здесь изменяется не только фаза, но и амплитуда колебания. Сигнал может принимать соответственно 16 и 64 бита информации на бодовый интервал, что увеличивает скорость передачи, но за счёт снижения помехоустойчивости.

Другие особенности беспроводных каналов

Ряд особенностей беспроводной передачи данных не позволяет использовать многие методы, характерные для проводных промышленных сетей.

Беспроводные трансиверы не могут передавать и принимать сигнал на одном и том же канале. Это связано с быстрым уменьшением плотности мощности излучения от расстояния (1). Сигнал собственного передатчика оказывается на порядки сильнее принимаемого сигнала и заглушает его. В отличие от этого в проводных каналах оба сигнала имеют примерно одинаковую мощность. Поэтому беспроводные трансиверы в принципе не могут прослушивать линию во время передачи, как это делается, например, в CAN или Ethernet. Описанное свойство делает невозможным применение методов доступа к сети, основанных на обнаружении коллизий.

Обнаружение несущей чужой станции даже при неработающем собственном передатчике также оказывается проблематичным (см. рис. 3 [7]). Здесь три окружности показывают границы приёма сигналов тремя станциями A, B и C. Предположим, что станция A передаёт сообщение станции B. В это время станция C прослушивает эфир и не слышит несущую, поскольку находится вне зоны действия станции A. Обнаружив отсутствие несущей, станция C начинает передачу одновременно со станцией A, что приводит к потере информации, поскольку станция B может принимать только один сигнал (проблема скрытого узла). Для решения этой проблемы можно использовать сигнал «занято», подаваемый станцией B. Однако наиболее общее решение проблемы предложено в стандарте IEEE 802.11. Оно заключается в том, что станция A начинает сеанс связи с обмена пакетами запроса на передачу RTS (Request To Send). Станция B может ответить

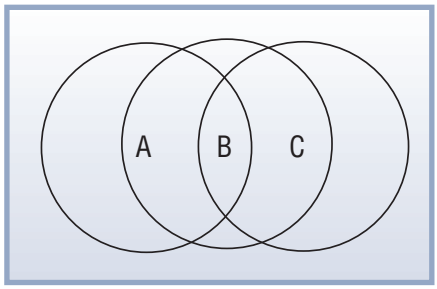

Рис. 3. Иллюстрация «проблемы скрытого узла»

пакетом CTS (Clear To Send — свободно). Только при получении этого сообщения станция A начинает передачу пакета данных. Любая другая станция, получившая пакет RTS или CTS, предназначенный не ей, будет оставаться в состоянии ожидания. Недостатком этого метода является то, что сигналы RTS/CTS существенно ухудшают скорость обмена между устройствами, поскольку размеры их пакетов сравнимы с размерами полезных данных.

Изложенное показывает, что беспроводные каналы не могут использовать метод доступа к каналу типа CSMA/CD [1]. Для них применяется метод CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) — множественный доступ с контролем несущей и *предотвращением* коллизий. От CSMA/CD он отличается тем, что коллизии в нём не обнаруживаются, в то время как в CSMA/CD коллизии обнаруживаются и принимаются меры для их разрешения. Поскольку в CSMA/CA коллизии не могут быть обнаружены, так как приёмник всегда заглушается сигналом своего передатчика, то принимаются специальные меры для снижения вероятности возникновения коллизий. В частности, используют сигналы резервирования канала связи, благодаря чему коллизии возникают между короткими сигналами резервирования, а не между длинными пакетами данных. Предотвращение коллизий выполняется благодаря тому, что станция, которая собирается начать передачу, информирует всех участников сети об этом, резервируя для себя определённое время, и только после того как все станции приняли этот сигнал, она начинает передавать. Используют также случайную задержку после освобождения канала (в методе CSMA/CD передача начинается сразу после освобождения

ЛУЧШИЕ СИСТЕМЫ ДЛЯ ХУДШИХ УСЛОВИЙ

IDAN™

HiDAN™

–40...+85°C

rtd®

- Широкий выбор процессорных плат и плат расширения
- Использование монтажной концепции PC/104
- Фрезерованный алюминиевый каркас для каждой платы
- Теплоотвод на стенки корпуса встроенными медными трубками
- Быстрая сборка и замена модулей
- Стандартные компьютерные разъёмы
- Диапазон рабочих температур от –40 до +85°C
- Виброгасящая платформа
- Размеры 130×152 мм в сечении

- Система конфигурируется пользователем на основе линейки продуктов фирмы RTD
- Используются разъёмы, выполненные в соответствии с MIL-C-38999
- Пользователь задает кабельную разводку внутри корпуса
- Экранированный водонепроницаемый корпус
- Все модули подсоединяются к каркасу процессорного модуля
- Фрезерованный алюминиевый каркас с защищёнными разъёмами
- Теплоотвод на стенки корпуса встроенными медными трубками
- Диапазон рабочих температур от –40 до +85°C
- Виброгасящая платформа
- Определяемые пользователем монтажные опции
- Размеры 130×160 мм в сечении

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР КОМПАНИИ IBASE В РОССИИ И СТРАНАХ СНГ **#417**

ProSoft®

МОСКВА	Тел.: (495) 234-0636 • Факс: (495) 234-0640 • E-mail: info@prosoft.ru • Web: www.prosoft.ru
С.-ПЕТЕРБУРГ	Тел.: (812) 448-0444 • Факс: (812) 448-0339 • E-mail: info@spb.prosoft.ru • Web: www.prosoft.ru
ЕКАТЕРИНБУРГ	Тел.: (343) 376-2820 • Факс: (343) 376-2830 • E-mail: info@prosoftsystems.ru • Web: www.prosoftsystems.ru
САМАРА	Тел.: (846) 277-9166 • Факс: (846) 277-9165 • E-mail: info@samara.prosoft.ru • Web: www.prosoft.ru
НОВОСИБИРСК	Тел.: (383) 202-0960; 335-7001/7002 • E-mail: info@nsk.prosoft.ru • Web: www.prosoft.ru
КИЕВ	Тел.: (+380-44) 206-2343/2478/2496 • Факс: (+380-44) 206-2343 • E-mail: info@prosoft-ua.com • Web: www.prosoft.ru
УФА	Тел.: (347) 2925-216; 2925-217 • Факс: (347) 2925-218 • E-mail: info@ufa.prosoft.ru • Web: www.prosoft.ru
КАЗАНЬ	Тел.: (843) 291-7555 • E-mail: kazan@prosoft.ru • Web: www.prosoft.ru
ОМСК	Тел.: (3812) 286-521 • E-mail: omsk@prosoft.ru • Web: www.prosoft.ru
ЧЕЛЯБИНСК	Тел.: (351) 239-9360 • E-mail: chelyabinsk@prosoft.ru • Web: www.prosoft.ru
КРАСНОДАР	Тел.: (861) 224-9513 • Факс: (861) 224-9513 • E-mail: krasnodar@prosoft.ru • Web: www.prosoft.ru

канала), чтобы уменьшить вероятность коллизии, поскольку очень вероятно, что многие станции ждут освобождения канала и могут начать передачу сразу и одновременно, как только он освободится.

Следующей проблемой является электропитание беспроводных сетей, поскольку беспроводные устройства (в основном это датчики) не должны подключаться куда-либо с помощью проводов. Поэтому очень актуальны проблема экономии энергии батарей, поиск простых способов их замены, исключение отказов по причине разряда, поиск альтернативных источников энергии. В литературе рассматриваются варианты передачи энергии питания электромагнитными волнами [10], трансформаторами с большим воздушным зазором (на расстояние до нескольких метров) [11], извлечение энергии сгорания топлива, применение солнечных батарей.

Методы уменьшения количества ошибок в канале

Изложенное ранее показывает, что ошибки в радиоканале появляются чаще, чем в экранированном кабеле, и обычно носят характер сбоев, в то время как в проводных системах, наоборот, ошибки чаще бывают катастрофическими, связанными с выходом из строя (отказом) канального оборудования. Тем не менее, после принятия всех описанных мер поток ошибок в радиоканале может быть снижен до необходимого уровня. Например, в авиации вероятность ошибок в беспроводных каналах составляет менее 10^{-19} [12]. Однако такие значения вероятности достигаются очень большими усилиями. Поэтому наиболее перспективной областью применения беспроводных сетей являются системы, в которых допускается некоторый процент ошибок. Вероятность ошибки может быть использована как компонента целевой функции при проектировании беспроводной системы.

В промышленных сетях часто используется режим широковещательной передачи, когда сообщение одновременно должны принять все участники сети. Его особенностью является отсутствие подтверждения о получении сообщения. В силу низкой вероятности безошибочной передачи по радиоканалу для реализации широковещательной передачи необходимо принять меры для увеличения вероятности доставки сообщений в беспроводном канале. Одним из возможных методов является кодирование широковещательного сообщения с большой избыточностью, при которой приёмник может восстановить утерянные во время передачи биты. Несмотря на снижение пропускной способности канала, такой метод может быть очень эффективен.

Для увеличения достоверности передачи используют метод ARQ (Automatic Repeat reQuest) — автоматический повтор в ответ на запрос [13]. Метод ARQ может использовать, например, следующие принципы [13]:

- передача дополнительно к сообщению корректирующего кода с большой избыточностью;
- отправление одновременно нескольких одинаковых пакетов (приёмник делает повторный запрос, только если ни один из пакетов не был принят без ошибок);
- использование нескольких антенн для повторной передачи сообщений.

Для увеличения достоверности передачи используют также *чередование*. Методы избыточного кодирования и коррекции ошибок обычно основаны на предположении о случайном характере воздействий, приводящих к появлению ошибок. Однако на практике ошибки могут быть коррелированы. Это может быть, например, в случае, когда период основной гармоники помехи равен длительности передачи нескольких битов. Чтобы сделать ошибки более похожими на некоррелированные, используют процедуру чередования — перестановку битов по определённому закону, одному и тому же в передатчике для выполнения чередования и в приёмнике для выполнения восстановления первоначального порядка следования битов. Одним из методов чередования является запись передаваемого фрейма в клеточки матрицы, например по три бита в строке, а затем считывание битов из матрицы не по строкам, а по столбцам.

Передача сообщений без подтверждения о получении

Существуют также другие методы увеличения достоверности передачи широковещательных сообщения без обратной связи от получателя: методы модуляции, устойчивые к интерференции радиоволн (Orthogonal Frequency-Division Multiplexing, или OFDM, — модуляция с применением нескольких несущих частот, которая использует большое число близко расположенных ортогональных поднесущих); передача одного и того же пакета несколько раз подряд; оптимизация пространственного размещения станций и применение дополнительной инфраструктуры (ретрансляторов и узлов доступа).

Системы связи с обратной связью получают от принимающей станции повторный запрос в случае, если сообщение было принято с ошибками. Такой способ используется, когда предъявляются высокие требования к достоверности передачи, например при передаче сигналов об аварии. Однако количество повторных запросов имеет естественный предел, который определяется предельным временем, по истечении которого передаваемая информация устаревает и поэтому становится бесполезной.

Используют также гибридный ARQ-метод HARQ (Hybrid Automatic Repeat reQuest), в котором сочетаются повторная передача, тайм-ауты и избыточные корректирующие коды. Если приёмник передающей станции не получил подтверждения от принимающей станции, то по истечении тайм-аута выполняется автоматическая повторная передача. Дополнительно используется избыточное кодирование, которое позволяет восстановить потерянные при передаче биты.

Приёмник может также использовать несколько принятых ошибочных пакетов для того, чтобы путём голосования выбрать из них биты, которые имеют наибольшую вероятностью того, что они правильные.

Поскольку уровень помех в беспроводном канале намного выше, чем в проводном, большинство систем используют в начале фрейма преамбулу увеличенной длительности по сравнению с проводными системами, что увеличивает долю «накладных расходов». Например, физический уровень стандарта IEEE 802.11 (Wi-Fi) с режимом DSSS использует преамбулу длиной 128 мкс, которая передаётся в каждом пакете и занимает значительную его часть.

Использование пространственного разнесения антенн

Вследствие замираний радиоволн напряжённость поля в точке приёма будет различной для разных положений приёмной антенны. Если два приёмника *r* и *s*, расположенные на одинаковом расстоянии от передатчика, находятся близко друг к другу, то вероятность того, что они оба находятся в зоне замирания, выше, чем когда они разнесены на большое расстояние, точнее, на расстояние, при котором эффекты, связанные с замираниями, становятся некоррелированными. Это свойство может найти несколько вариантов использования.

Один из вариантов состоит в применении нескольких антенн для одного приёмника. Расстояние между антеннами выбирают таким образом, чтобы при замирании в зоне расположения одной антенны в зоне другой был хороший приём. Приёмник должен быть способен отличить хороший сигнал от плохого и выбрать лучший.

Аналогичный вариант с несколькими антеннами может быть использован для передатчика. В методе передачи с обратной связью передающие антенны перебираются по очереди, пока от приёмника не придёт сигнал о том, что сообщение принято. Если применение нескольких антенн невозможно, вместо дополнительных антенн можно использовать другие станции в качестве ретрансляторов.

Вопросы безопасности

Проблемы безопасности разделяются на задачу аутентификации (установление подлинности личности), которая выполняется обычно с помощью идентификации имени пользователя и пароля, задачу разграничения прав доступа к системе и задачу защиты информации с помощью методов шифрования.

Механизмы шифрования [14] основаны на алгоритмах, которые преобразуют сигналы, несущие информацию, в шумоподобные (псевдослучайные) сигналы. Используются два вида шифров: поточный (групповой) и блочный шифр.

Шифры обоих типов генерируют ключевой поток, который определяется значением секретного ключа.

Ключевой поток смешивается с кодируемыми данными по схеме «исключающее ИЛИ», в результате чего получается закодированный текст.

В методах шифрования имеется много нюансов, подробности см. в [14].

Bluetooth

В настоящее время существуют три широко распространённых стандарта на беспроводные сети: Bluetooth (IEEE 802.15.1), ZigBee (IEEE 802.15.4) и Wi-Fi (IEEE 802.11). Оборудование для этих сетей не требует получения лицензии (что во многих случаях принципиально важно), хотя необходима регистрация [15].

Технология Bluetooth [2, 16] (www.bluetooth.com) была разработана на базе стандарта IEEE 802.15.1 специально для замены кабеля при соединении различных устройств офисной и бытовой техники с использованием частотного ISM-диапазона 2,4 ГГц. Спецификация Bluetooth поддерживается организацией SIG (Bluetooth Special Interest Group), образованной в 1998 году и объединяющей более 1900 членов. В системах автоматизации Bluetooth удобна для записи программ в ПЛК, дистанционного считывания показателей с накопителей информации. Она организована в виде пикосетей (piconet), в которых одно ведущее устройство осуществляет взаимодействие не более чем с семью ведомыми. Ведомые устройства могут взаимодействовать друг с другом только через ведущее. Каждое устройство может быть членом четырёх пикосетей одновременно, но главным может быть только в одной из них. Такое устройство выполняет роль моста между пикосетями. Несколько взаимодействующих пикосетей образуют так называемую scatternet (разбросанную сеть).

Трафик в сети организован с временным разделением каналов и дуплексной передачей. Временное разделение осуществляется интервалами (временными слотами) длиной в 625 мкс. Ведущие устройства могут начинать передачу только в течение интервалов с нечётными номерами, ведомые — отвечать в течение чётных интервалов. В течение каждого интервала можно передать 366 битов.

В Bluetooth используется широкополосная модуляция типа FHSS. Переход с одной частоты на другую выполняется по случайному закону, который устанавливается для каждого соединения индивидуально. Это повышает степень защиты информации. Несущая частота изменяется 1600 раз в секунду. Скорость передачи равна 433,9 кбит/с.

Если пикосети расположены близко одна от другой, то они могут влиять друг на друга, поскольку между ними нет никакой синхронизации. Чтобы уменьшить вероятность взаимовлияния, используется адаптивный метод скачкообразного изменения частоты AFH.

На канальном уровне используются два типа пакетов данных: ACL (Asynchronous ConnectionLess — асинхронный без прямого соединения каналов) и SCO (Synchronous Connection-Oriented — синхронный с прямым соединением). ACL-пакеты используются совместно с проверкой контрольной суммы (CRC). Если контрольные суммы приёмника и передатчика не совпадают, запрашивается повторная передача пакета. Используются шесть разных ACL-пакетов, охватывающих разное количество временных слотов. ACL-пакеты используются в том случае, когда целостность данных важнее скорости их доставки.

Пакеты SCO поддерживают трафик реального времени путём резервирования временных слотов. Повторная передача здесь не допускается, хотя имеется «расширенный» вариант SCO, в котором допускается ограниченное количество повторных передач. Существует три типа SCO-пакетов одинаковой длины (HV3, HV2, HV1) по 366 мкс, которые позволяют передавать данные со скоростью 64 кбит/с.

Каждое устройство стандарта Bluetooth имеет 48-битовый адрес.

Большинство устройств Bluetooth имеют мощность передатчика 1 мВт, однако разрешён следующий ряд мощностей, делящий все эти устройства на три класса:

- класс 1 — до 100 мВт (максимальная дальность на открытом пространстве до 100 м);
- класс 2 — до 2,5 мВт (максимальная дальность на открытом пространстве до 15 м);
- класс 3 — до 1 мВт (максимальная дальность на открытом пространстве до 5 м).

Можно назвать следующие достоинства технологии Bluetooth: малые размеры оборудования, простота использования, безопасность передачи информации (благодаря аутентификации и кодированию), хорошая поддержка со стороны соответствующих стандартов. К недостаткам можно отнести относительно большое потребление энергии и невозможность построения сетей сложной конфигурации. Эти особенности связаны с тем, что Bluetooth решает проблему замены кабелей для устройств, подключаемых к компьютеру, а не проблему создания беспроводной LAN.

ZigBee и IEEE 802.15.4

Стандарт IEEE 802.15.4 [4] является самым новым в серии беспроводных (принят в октябре 2003 года). На его основе ZigBee Alliance (www.zigbee.org) разработал спецификацию протоколов сетевого и прикладного уровня, которые анонсировал в декабре 2004 года под названием ZigBee [3]. ZigBee Alliance включает в себя более 180 фирм, работающих совместно над продвижением стандартов, стека протоколов и прикладных профилей для потребительского и промышленного сектора экономики. Прикладные профили ориентированы, в частности, на автоматизацию зданий, промышленный мониторинг, вентиляцию и кондиционирование, работу с датчиками. Спецификация ZigBee описывает построение сети, вопросы безопасности, прикладное программное обеспечение.

Основными областями применения ZigBee/IEEE 802.15.4 являются передача информации от движущихся и вращающихся частей механизмов (конвейеров, роботов), промышленные системы управления и мониторинга, беспроводные сети датчиков, отслеживание маршрутов движения и местоположения имущества и инвентаря, «интеллектуальное» сельское хозяйство, системы охраны.

В отличие от других беспроводных технологий, где ставится задача обеспечить высокую скорость передачи, большую дальность или высокое качество обслуживания, ZigBee/IEEE 802.15.4 создавался изначально по критериям малой дальности действия, низкой цены, малой потребляе-

СЕРВЕРНЫЕ СИСТЕМЫ *IntellecT* – БЕЗОПАСНЫЙ ДОСТУП К ЦЕННЫМ ДАННЫМ

#236

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР В РОССИИ И СТРАНАХ СНГ

МОСКВА Т/ф: (495) 234-0636 / 234-0640 ● info@prosoft.ru ● www.prosoft.ru
С.-ПЕТЕРБУРГ Т/ф: (812) 448-0444 / 448-0339 ● info@spb.prosoft.ru ● www.prosoft.ru
ЕКАТЕРИНБУРГ Т/ф: (343) 376-2820 / 376-2830 ● info@prosoftsystems.ru ● www.prosoftsystems.ru
САМАРА Т/ф: (846) 277-9166 / 277-9165 ● info@samara.prosoft.ru ● www.prosoft.ru
НОВОСИБИРСК Т/ф: (383) 202-0960; 335-7001; 335-7002 ● info@nsk.prosoft.ru ● www.prosoft.ru
КИЕВ Т/ф: (+380-44) 206-2343; 206-2478; 206-2496 / 206-2343 ● info@prosoft-ua.com ● www.prosoft.ru
УФА Т/ф: (347) 292-5216; 292-5217/ 292-5218 ● info@ufa.prosoft.ru ● www.prosoft.ru
КАЗАНЬ Т/ф: (843) 291-7555/ 570-43-15 ● kazan@prosoft.ru ● www.prosoft.ru
ОМСК Тел: (3812) 286-521 ● omsk@prosoft.ru ● www.prosoft.ru
ЧЕЛЯБИНСК Тел: (351) 239-9360 ● chelyabinsk@prosoft.ru ● www.prosoft.ru
КРАСНОДАР Т/ф: (861) 224-9513 / 224-9513 ● krasnodar@prosoft.ru ● www.prosoft.ru

PROSOFT®

мой мощности, небольшой скорости передачи и малых габаритов. Эти свойства идеально соответствуют требованиям к большинству промышленных датчиков. Поэтому ZigBee часто отождествляют с промышленными беспроводными сенсорными сетями WSN (Wireless Sensor Network) [17–22]. Устройства ZigBee используются в применениях, где технология Bluetooth оказывается слишком дорогой и не требуется высокая скорость передачи.

ZigBee, как и Bluetooth, использует нелицензируемый [15] диапазон 2,4 ГГц. Стандарт предусматривает также использование частот 868 МГц в Европе и 915 МГц в США. Максимальная скорость передачи составляет 250 кбит/с в диапазоне 2,4 ГГц. Диапазон 2,4 ГГц разделён на 11–26 каналов шириной по 5 МГц каждый.

Несмотря на то что вся идеология стандарта IEEE 802.15.4 построена в предположении, что типовая связь будет осуществляться на расстоянии около 10 м, стандарт не устанавливает требований к мощности передатчика. Этот параметр регулируется нормативными документами в области радиосвязи, специфическими для каждого государства. Наибольшее распространение на рынке имеют передатчики с мощностью 1 мВт, которые обеспечивают связь на расстоянии до 10 м в помещении, а также передатчики с мощностью 10 мВт, увеличивающие это расстояние до 80 м в помещении и до 1 км в условиях прямой видимости. Дальность связи можно увеличить применением антенн специальной конструкции.

Модель OSI сети ZigBee представлена в табл. 1. Она включает в себя физический уровень (PHY), канальный уровень, состоящий из подуровня доступа к среде передачи MAC и LLC (смысл обозначений см. в описании Ethernet), которые определяются стандартом IEEE 802.15.4, а также сетевой уровень NWK (NetWorK) и уровень приложений APL, состоящий из подуровня поддержки приложений (APplication Support sub-layer — APS), подуровня объектов устройств ZigBee (ZigBee Device Object — ZDO) и объектов Application Objects, определяемых изготовителем ZigBee-устройств.

Подуровень MAC управляет доступом к радиоканалу, используя метод

Таблица 1

Уровни модели OSI сети ZigBee/IEEE 802.15.4

Номер уровня	Модель OSI	Сеть	Функции
7	Прикладной	APL (APS, ZDO и Application Objects) ZigBee	Передача сообщений, обнаружение устройств, определение роли устройств
6	Уровень представления	—	—
5	Сеансовый	—	—
4	Транспортный	—	—
3	Сетевой	NWK ZigBee	Безопасность, маршрутизация
2	Канальный (передачи данных)	LLC IEEE 802.15.4	CSMA/CA, передача маячков, синхронизация
		SSCS IEEE 802.15.4	
		MAC IEEE 802.15.4	
1	Физический	PHY IEEE 802.15.4	Радиоканал 2,4 ГГц

CSMA/CA. Он также отвечает за передачу *маячковых фреймов* (см. следующий подраздел), синхронизацию и обеспечение надёжных методов передачи информации. Подуровень SSCS (Service Specific Convergence Sublayer — подуровень сближения специфических сервисов) выполняет роль интерфейса между подуровнями LLC и MAC. Подуровень LLC выполняет связь сетевого уровня с уровнем MAC.

Уровень NWK использует методы, обеспечивающие:

- регистрацию в сети нового устройства и исключение его из сети;
- безопасность при передаче фреймов;
- указание маршрута фрейма к месту назначения;
- прокладку маршрутов между устройствами в сети;
- обнаружение в сети ближайших соседей;
- запоминание необходимой информации о соседних узлах.

В ZigBee имеются три типа устройств:

- координатор формирует топологию сети и может устанавливать мосты с другими сетями (в каждой ZigBee-сети имеется только один координатор);
- маршрутизатор работает как промежуточное звено, передавая в нужном направлении данные от других устройств;
- конечное устройство передаёт данные координатору или маршрутизатору и не может связываться с аналогичными ему устройствами.

Уровень NWK отвечает за организацию новой сети, когда это нужно, и назначение адресов новым устройствам, подключаемым к сети.

Подуровень APS уровня приложений обеспечивает:

- обслуживание таблиц для связывания устройств сети на основе информации о необходимости и возможности связывания;
- передачу сообщений между связанными устройствами;
- определение группового адреса устройств, удаление и фильтрацию сообщений с групповыми адресами;
- отображение 64-битового адреса в 16-битовый;
- фрагментацию, перекомпоновку и транспортировку данных.

Подуровень ZDO обеспечивает:

- определение роли устройств в сети (координатор, маршрутизатор или оконечное устройство);
- инициирование или ответ на запрос соединения;
- защиту информации;
- обнаружение устройств в сети и определение того, какой сервис они предоставляют.

Топология Zigbee-сети поддерживается уровнем NWK и может иметь форму звезды, дерева или ячеистой сети. В топологии типа звезды сеть контролируется координатором. Координатор отвечает за инициализацию и обслуживание сетевых устройств и всех конечных устройств, непосредственно взаимодействующих с координатором. В ячеистой и древовидной структуре сети координатор отвечает за организацию сети и выбор некоторых ключевых параметров, но сеть может быть расширена с помощью ZigBee-маршрутизаторов. В сети с древовидной топологией маршрутизаторы перемещают данные и управляющие сообщения по сети, используя иерархическую

стратегию маршрутизации. Древовидные сети могут использовать маячковую стратегию маршрутизации (см. следующий подраздел).

Ячеистая сеть должна обеспечить полную одноранговую коммуникацию устройств, то есть в ячеистой сети нет устройств разных рангов (координаторов, маршрутизаторов и т.п.), все устройства равноправны.

Физический и канальный уровни

Физический уровень модели OSI обеспечивает интерфейс между стеком протоколов и средой передачи информации (эфиром). Физический (PHY) и канальный (MAC) уровни модели OSI (табл. 1) определены в стандарте IEEE 802.15.4. Они имеют следующие основные характеристики:

- скорость передачи — 250 кбит/с;
- короткий 16-битовый адрес или расширенный адрес длиной 64 бита;
- выделение интервала времени для передачи информации каждым узлом;
- метод доступа к каналу типа CSMA/CA;
- протокол обмена с уведомлением о получении;
- малое потребление мощности;
- контроль уровня энергии;
- наличие индикатора качества связи;
- 16 каналов в диапазоне 2,45 ГГц.

Частоты 868 и 902 МГц, предусмотренные стандартом, в России не применяются и поэтому в дальнейшем не упоминаются.

Стандарт IEEE 802.15.4 использует модуляцию типа OQPSK (Offset Quadrature Phase-Shift Keying) — смещённая квадратурная фазовая манипуляция.

Основным назначением физического уровня является приём и передача данных через радиоканал. Здесь также измеряется мощность радиосигнала, оценивается качество связи и чистота канала, осуществляется выбор канала.

Подуровень MAC управляет маячком, доступом к каналу, выделяет гарантированные слоты времени, проверяет достоверность передачи фреймов, передаёт фрейм подтверждения о получении, выполняет часть работы по обеспечению защиты информации.

Стандарт допускает опциональное использование суперфреймовой структуры сообщений (рис. 4). Формат суперфрейма определяется сетевым координатором. Суперфрейм с двух сторон ограничивается маячками, делится на 16 равных по длине слотов и посылается сетевым координатором. Маячок помещается на место первого слота каждого суперфрейма. Координатор может отключить режим сообщений с маячками. Маячки используются для синхронизации присоединённых устройств, для идентификации сети и для описания структуры суперфрейма. Любые устройства, желающие начать процесс коммуникации в промежуток времени между двумя маячками, должны использовать *слотовый* механизм доступа CSMA/CA. Передача сообщений должна быть закончена до прихода следующего маячка.

IEEE 802.15.4 устанавливает два механизма доступа к каналу CSMA/CA в зависимости от типа конфигурации сети. В сети без маячков используется обычный (бесслотовый) механизм доступа CSMA/CA. Каждый раз, когда устройство собирается

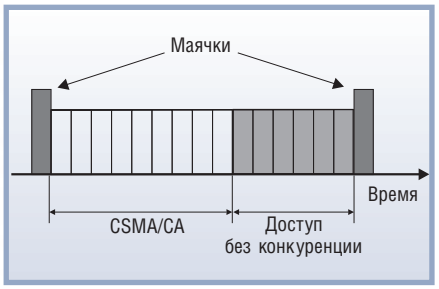

Рис. 4. Структура суперфрейма с гарантированными временными слотами

начать передачу, оно должно выдержать *паузу случайной величины* после того, как канал освободится. Случайная задержка нужна, так как очень вероятно, что многие устройства сети ждут освобождения канала и поэтому после его освобождения могут начать передачу одновременно. Если канал занят, то устройство может предпринять ещё одну попытку после повторной случайной задержки. Фреймы подтверждения о получении посылаются сразу, без использования описанного алгоритма.

В сети с маячками используется слотовый (тактированный) механизм доступа CSMA/CA, в котором начало временного слота должно совпадать с границей суперфрейма сетевого координатора, то есть начало слота для каждого устройства должно быть синхронизировано с началом передачи маячка сетевым координатором. Поскольку устройство не может начать передачу, пока не найдёт маячок, а маячки рассылаются только сетевым координатором, то сетевой координатор с помощью маячков выполняет тактирование актов обмена во всей сети. При этом уровень PHY должен обеспечить, чтобы все передачи в сети начинались одновременно с началом слотов. Введение описанной синхронизации позволяет уменьшить вероятность одновременной передачи сообщений несколькими узлами сети.

Для устройств, которые требуют срочной доставки или большой пропускной способности канала, сетевой координатор может зарезервировать часть суперфрейма, в котором будет отсутствовать конкуренция за канал (рис. 4), поскольку в это время сетевой координатор запрещает любую передачу всем другим устройствам. Эта часть слотов суперфрейма называется гарантированными временными слотами (Guaranteed Time Slots — GTSs). ●

Литература

1. Денисенко В.В. Компьютерное управление технологическим процессом, экспериментом, оборудованием. — М. : Горячая линия — Телеком, 2008. — 608 с.
2. Specification of the Bluetooth System. Master Table of Contents & Compliance Requirements. Covered Core Package version: 2.0+ EDR. — Issued: 4 November 2004. — 1230 p.
3. ZigBee Alliance Document 053474r13: ZigBee Specification. — ZigBee Standards Organization, 1 Dec. 2006. — 534 p.
4. IEEE Std 802.15.4™-2003. IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) — IEEE Computer Society. IEEE-SA Standards Board, 12 May 2003. — 679 p.
5. Vieira M.A.M., Junior D.C.S. Survey on wireless sensor network devices // Proceedings of the IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA'03), 16–19 Sept. 2003. — Vol. 1. — P. 537–544.
6. ANSI/IEEE Std 802.11, 1999 Edition. Information technology —Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications — IEEE-SA Standards Board, 12 June 2003. — 528 p.
7. Willig A., Matheus K., Wolisz A. Wireless technology in industrial networks // Proceedings of the IEEE, June 2005. — Vol. 93. — Issue 6. — P. 1130–1151.
8. Akyildiz I.F., Wang X. A survey on wireless mesh networks // IEEE Communications Magazine. — Sept. 2005. — Vol. 43. — Issue 9. — P. S23–S30.
9. Баскаков С.И. Радиотехнические цепи и сигналы. — М. : Высшая школа, 1983. — 536 с.
10. Hirai J., Kim T.-W., Kawamura A. Practical study on wireless transmission of power and information for autonomous decentralized manufacturing system // IEEE Trans. Ind. Electron. — 1999. — Vol. 46. — No. 2. — P. 349–359.
11. O'Brien K., Scheible G., Gueldner H. Analysis of wireless power supplies for industrial automation systems // The 29th Annual Conference of the IEEE (IECON '03.), 2–6 Nov. 2003. — Industrial Electronics Society, 2003. — Vol. 1. — P. 367–372.
12. Wiberg P.-A., Bilstrup U. Wireless technology in industry — Applications and user scenarios // Proceedings of the IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA'01). — P. 123–133.
13. Willig, A. Redundancy Concepts to Increase Transmission Reliability in Wireless Industrial LANs // IEEE Transactions on Industrial Informatics. — 2005. — Vol. 1. — No. 3. — P. 173–182.
14. Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11. — М. : Издательский дом «Вильямс», 2004. — 304 с.
15. Решение № 04-03-04-003 от 6 декабря 2004 года : Государственная комиссия по радиочастотам (ГКРЧ). — М.: 2004. — 7 с.
16. Sairam K.V.S.S.S.S., Gunasekaran N., Redd S.R. Bluetooth in wireless communication // IEEE Communications Magazine. — June 2002. — Vol. 40. — Issue 6. — P. 90–96.
17. Hac A. Wireless Sensor Network Designs. —John Wiley & Sons, Ltd; 2004. — 391 p.
18. Shen X., Wang Z., Sun Y. Wireless sensor networks for industrial applications // Fifth World Congress on Intelligent Control and Automation (WCICA 2004), 15–19 June 2004. — Vol. 4. — P. 3636–3640.
19. Low K.S., Win W.N.N., Er M.J. Wireless Sensor Networks for Industrial Environments // International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce, 28–30 Nov. 2005. — Vol. 2. — P. 271–276.
20. Bonivento A., Carloni L.P., Sangiovanni-Vincentelli A. Platform-Based Design of Wireless Sensor Networks for Industrial Applications // Design, Automation and Test in Europe (DATE '06), 6–10 March 2006. — Vol. 1. — P. 1–6.
21. Gutierrez J.A., Durocher D.B., Bin Lu, Habetler T.G. Applying Wireless Sensor Networks in Industrial Plant Energy Evaluation and Planning Systems // Pulp and Paper Industry Technical Conference, 18–23 June 2006. — P. 1–7.
22. Jiang P., Ren H., Zhang L., Wang Z., Xue A. Reliable Application of Wireless Sensor Networks in Industrial Process Control // The Sixth World Congress on Intelligent Control and Automation (WCICA 2006), 21–23 June 2006. — Vol. 1. — P. 99–103.