ВОПРОСЫ БЕЗОПАСНОСТИ И РАЗРАБОТКИ СТАНДАРТОВ ДЛЯ ПРОМЫШЛЕННЫХ БЕСПРОВОДНЫХ СЕТЕЙ

ЯН ВЕРХАППЕН (IAN VERHAPPEN), Industrial Automation Networks

В статье рассмотрены способы повышения надежности промышленных беспроводных сетей, а также методы и инструменты обеспечения безопасности, предусмотренные в перспективных протоколах промышленных беспроводных сетей, — WirelessHART, WIA-PA и ISA-100. Затронуты вопросы разработки основных стандартов промышленных беспроводных сетей. Статья представляет собой перевод [1].

Промышленные беспроводные сети являются перспективным направлением развития систем промышленной автоматики. Однако темпы их внедрения пока отстают от количества заказов на поставку оборудования, благодаря которым компании-разработчики технологии намерены возвратить свои инвестиции, по крайней мере, в ближайшей перспективе. Опыт показал, что любая новая технология в промышленности следует традиционной модели развития новой технологии на рынке. Это справедливо для компаний, впервые ее применивших, и для большинства компаний, которые вводят в действие опытные мелкосерийные производства или испытательные комплексы для изучения особенностей конкретной технологии. Результаты испытаний в условиях мелкосерийного производства закладывают в основу корпоративных стандартов и методик для крупносерийного производства и внедрения новой технологии.

Последнее исследование компании ON World (www. ControlDesign.com/onworld) подтверждает, что эта тенденция характерна и для промышленных беспроводных сетей, поэтому маловероятно, что их широкое внедрение произойдет до середины нынешнего десятилетия. Если проблемы безопасности и стандартизации в области промышленных беспроводных сетей не будут решены, то их распространение отодвинется на неопределенный срок.

Все промышленные протоколы в качестве базы для проектирования используют 7-уровневую модель OSI, а радиомодули стандарта 802.15.4, на которых основаны протоколы промышленных беспроводных сетей, используют два нижних уровня модели — физический и канальный (см. рис. 1). Для различных протоколов это позволяет использовать один и тот же базовый радиомодуль, несмотря на то, что каждый из них имеет свою специфику, которая определяет механизмы работы в сети в соответствии с требованиями конкретного приложения.

БЕЗОПАСНОСТЬ

К счастью, инженеры, которые разрабатывают коммуникационные протоколы для промышленных сетей, знают о проблемах безопасности и разрабатываемых в этой области нормативных документах, в частности, о стандартах Североамериканского совета по электрической надежности NERC/CIP (www. ControlDesign.com/nerccip). Эти стандарты регламентируют вопросы безопасности электросети, в том числе кибербезопасности. Фактически, в круг обязанностей комиссии по стандарту ISA-100 входит совместная работа по этой проблеме с комиссией стандарта ISA-99, а также сотрудничество с комиссией стандарта ISA-84 в части вопросов безопасности.

Разработчики стандартов для промышленных беспроводных сетей включают в протоколы разнообразные функции защиты. Распространенным инструментом сохранения целостности данных и предотвращения преднамеренного или случайного перехвата данных между двумя узлами в сети является кодиро-

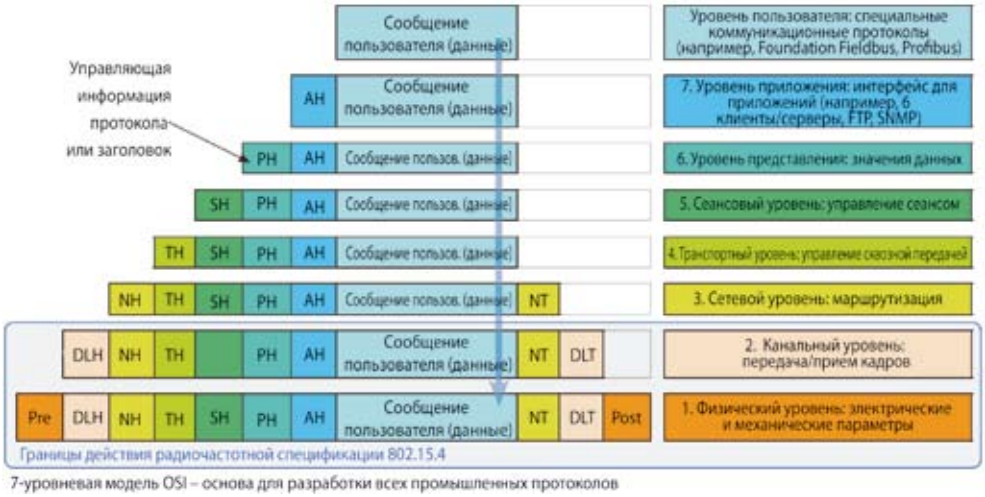

Рис. 1. **Уровни модели OSI и передача сообщений**

вание сообщений. В беспроводных протоколах для систем автоматизации технологических процессов предусмотрено 128-разрядное AES-кодирование, ставшее стандартным в отрасли, и, кроме того, используются уникальные ключи шифрования для каждого сообщения и ключи шифрования с циклическим изменением для точек доступа при выполнении обработки запросов устройств на подключение к сети.

Другими функциями, включенными в стандарты промышленных беспроводных сетей, являются проверка целостности данных (искажены ли данные?) и аутентификация устройства (действительно ли это то устройство, за которое оно себя выдает?). Это два из трех важнейших принципов кибербезопасности. Третий принцип — это права устройства, т.е. имеет ли устройство достаточно полномочий при выполнении запрашиваемой коррекции какого-либо параметра.

Для устройства, которое не является частью сети, функция переключения каналов (channel hopping) осложняет возможность определения частоты, на которой будет происходить следующая передача, т.е. у этого устройства нет доступа к ключу переключения.

Другой важной функцией является множество уровней ключей защиты для доступа разных лиц с разными полномочиями. Это позволяет еще больше усилить принцип наделения правами, который, как уже отмечалось, является третьим основным принципом обеспечения безопасности. Регулируемые уровни мощности передачи позволяют пользователю управлять возможностью выхода сигнала за пределы границ предприятия. Если радиосигналы не выходят за границу объекта, становится намного сложнее овладеть информацией или перехватить достаточное количество пакетов для того, чтобы иметь возможность расшифровывать формат пакета данных.

Беспроводные сети имеют защитные серверы, подобные серверам RADIUS для условий офиса, и администратор сети записывает каждую попытку подсоединения к сети. Сохранение записей этих попыток позволяет поддерживать сложную таблицу маршрутизации, что обеспечивает реализацию сети на базе более простой электроники и требует использования памяти меньшего размера.

Спецификация ISA-100.11a допускает использование программируемых уровней мощности для выходных радиомодулей. Такой подход можно использовать совместно с индикатором мощности принятого сигнала для оптимизации мощности радиопередачи в сети. Эта функция также может привести к нарушению безопасности сети, т.к. дальность распространения радиочастотного сигнала зависит от мощности передачи.

ТЕХНОЛОГИЯ WIRELESSHART

Такие методы как расширение спектра сигнала с применением кода прямой последовательности (разнообразие кодировки) и регулируемая мощность передачи (разнесение по мощности) используются и в технологии WirelessHART для того, чтобы обеспечить надежную связь даже в зоне действия других беспроводных сетей. Кроме того, WirelessHART использует синхронизированную во времени связь (разнесение во времени) для того, чтобы минимизировать вероятность возникновения коллизий путем блокирования каналов, используемых другими устройствами и сетями. В технологии WirelessHART все прямые соединения между устройствами выполняются в заранее заданном интервале времени, что обеспечивает обмен сообщениями без возникновения коллизий. Кроме того, каждое сообщение имеет определенный приоритет, чтобы гарантировать приемлемое качество сервиса (quality-of-Service — QoS) доставки. Интервалы фиксированного времени также позволяют администратору сети управлять ею без вмешательства пользователя.

ТЕХНОЛОГИЯ WIA-PA

Шеньянским институтом автоматизации Китайской академии наук была предложена технология беспроводной сети для промышленной автоматики (Wireless Network for Industrial Automation-Process Automation — WIA-PA) на базе стандарта IEEE 802.15.4. Сеть WIA-PA поддерживает иерархическую топологию, которая является гибридом топологии типа «звезда» и «сетка». Первый уровень сети представляет собой топологию «сетка», в которой используются устройства маршрутизации и шлюзы. Второй уровень использует топологию типа «звезда», в которой соединены устройства маршрутизации и полевые/портативные устройства. Как и другие протоколы, стек протоколов WIA-PA основан на 7-уровневой эталонной модели ISO/OSI и определяет только канальный подуровень (DLSL), сетевой уровень (NL) и уровень приложения (AL). Сетевые межсоединения устанавливаются с помощью шлюзов WIA-PA, которые кроме соединения с устройствами WIA-PA NM и SM способны обеспечивать соединение с другими устройствами WIA-PA для обмена информацией между ними. Шлюз WIA-PA также способен подсоединяться к другим сетям, таким как проводная промышленная сеть Fieldbus.

Стандарт WIA-PA определяет пять типов устройств, в том числе хост-компьютер, шлюз, устройство маршрутизации, полевое устройство и переносное устройство, которое обеспечивает две функции — конфигурирование сети и мониторинг характеристик сети. Подобно другим сетевым устройствам переносное устройство WIA-PA подсоединено к сети WIA-PA через шлюз и устройство маршрутизации.

СТАНДАРТЫ

Поскольку мы работаем в глобальной среде, а производители хотят, чтобы их оборудование можно было использовать повсюду, важно, чтобы и коммуникационную платформу на базе радиосвязи можно было использовать в любой стране. Исходя из того, что единственную практическую возможность связи в глобальном масштабе обеспечивает частота 2,4 ГГц, для всех трех разработанных протоколов используется диапазон ISM (Industrial, Scientific, Medical).

К сожалению, многие другие устройства, включая сотовые телефоны, беспроводные домашние телефоны и даже автомобили и игрушки с дистанционным управлением, также используют частоту 2,4 ГГц. Журнал Fortune недавно опубликовал прогноз, в соответствии с которым ожидается экспоненциальный рост количества смартфонов, в результате чего ежемесячный объем передаваемых ими данных будет измеряться экзабайтами (1 экзабайт — это 1018 байт или 1 миллиард гигабайт). Такой рост трафика осложнит проблему потери сигнала и станет фактором, который разработчики стандарта будут учитывать в следующей версии протокола. В стандарте ISA100 уже сделан первый шаг в этом направлении — введена возможность повторной проверки доступности канала для его использования.

Ряд беспроводных протоколов, использующих диапазон ISM, и соответствующие приложения учитывают, что со временем потребность в этих частотных диапазонах будет возрастать. Это, в свою очередь, вызовет потребность в том, чтобы промышленная сеть обеспечивала необходимое обновление дан-

Ряд беспроводных протоколов, использующих диапазон ISM, и соответствующие приложения учитывают, что потребность в этих частотах будет возрастать

Рис. 2. **Расширение диапазона ISM**

ных в процессах реального времени (см. рис. 2). Три организации, которые разрабатывают стандарты для промышленных беспроводных сетей, предусматривают в своих протоколах индикацию количества попыток сбоя доступа, что позволяет определить интенсивность посторонних попыток подсоединения к сети.

ISA-100

Протокол ISA-100.11a учитывает две важные характеристики, которые помогают обеспечить сосуществование сетей. С помощью медленного переключения (slow hopping) радиомодули могут переходить с одного канала на другой в поисках канала, где помехи отсутствуют. В отличие от других протоколов, в ISA-100.11a можно вернуться к предыдущему занятому каналу, чтобы проверить, доступен ли он теперь.

В других методах используется «черный список», в соответствии с которым канал объявляется запрещенным или недоступным, и его никогда заново не просматривают. Однако в ISA-100.11a используется «белый список», в котором зафиксированы каналы, пригодные для нужд сети. В стандарте ISA-100 модифицирован канальный уровень 802.15.4 с целью улучшения надежности приема сигнала в промышленной среде.

Любой протокол, соответствующий полной спецификации IEEE 802.15.4, должен уступить место стандарту IEEE 802.11 в соответствии с требованием совместимости со стандартом. Стандарт ISA100.11a не является полностью совместимым с IEEE 802.15.4. В сети ISA100 используются радиомодули IEEE 802.15.4, т.к. они недороги и доступны, однако был реализован другой протокол управления доступом к среде (MAC) для улучшения надежности и смягчения проблемы сосуществования сетей, связанной с семейством 802-х стандартов.

Профили в ISA-100.11a позволяют пользователям выбрать желаемый уровень защиты. Важнейшей функцией ISA-100.11a является возможность распределения ключей. Стандарт ISA-100.11a допускает перераспределение ключей в режиме реального времени, так что кража устройства не дает возможности получения доступа к ключу, который может быть неизменным всегда. Такое распределение выполняется по радиосвязи, поэтому персоналу обслуживания пользователей нет необходимости осуществлять доступ к каждому устройству для ввода нового ключа. Другие протоколы, присутствующие на рынке, используют ключи, введенные во время производства, поэтому их нельзя изменить. Или же их можно изменить только с помощью внеполосного сигнала от переносного устройства, которое должно иметь возможность соединения с каждым узлом в сети. Конечные пользователи, работающие в комиссии по ISA-100, согласились на кратковременный риск беспроводной передачи ключей, как на наилучший компромисс, доступный в этой ситуации.

Стандарт ISA-100.11a использует три различных подхода для оптимизации потребления электроэнергии. Протокол ячеистых сетей с синхронизацией по времени (Time Synchronized Mesh Protocol — TSMP) компании Dust Network в рамках соглашения о стандартном доступе предусматривает активизацию узлов в сети только, когда имеются сообщения, которые нужно передать. Другие протоколы ячеистых сетей требуют, чтобы питание промежуточных узлов осуществлялось без перерыва.

Спецификация ISA-100.11a допускает, чтобы конечные узлы были совершенно немаршрутизируемыми. Это позволяет использовать беспроводные датчики peel-and-stick для некоторых простых систем. Поскольку эти узлы немаршрутизируемы, их не нужно активизировать для передачи сообщений по ячейкам сети. Кроме того, не планируется их принятие Международной электротехнической комиссией (IEC). Каждый из трех стандартов находится на разной стадии рассмотрения и утверждения.

WirelessHART. Международная электротехническая комиссия приняла коммуникационный стандарт WirelessHART (HART 7.1) как общедоступную спецификацию в 2008 г. (IEC/PAS 62591, Ed. 1). В настоящее время национальные комитеты 29 стран принимают участие в обсуждении проекта стандарта, и, следовательно, он находится на самой ранней стадии среди трех стандартов промышленных беспроводных сетей, которые планируются к рассмотрению IEC.

WIA-PA. Рабочая группа по рассмотрению этого стандарта начала работу в 2006 г. на основе информации, представленной более чем 20 компаниями, институтами и университетами Китая. 31 октября 2008 г. WIA-PA прошел процедуру голосования в подкомитете IEC/SC65C, был опубликован в качестве спецификации IEC/PAS 62601 и прошел стадию проекта стандарта, рассматриваемого техническим комитетом, 5 марта 2010 г. Параллельно с этим стандарт был представлен в Управление по стандартизации Китая (Standardization Administration of China — SAC), и после его утверждения он станет национальным стандартом Китая.

ISA-100. ISA-100.11a-2009 — это стандарт, опубликованный ISA и одобренный Советом ISA по стандартам и правилам (ISA Standards & Practices Board) 8 сентября 2009 г. В ходе дальнейшего рассмотрения принятого документа было выявлено, что в ISA-100.11a-2009 необходимо внести некоторые коррективы. В настоящее время не имеет смысла представлять спецификацию ISA-100.11a-2009 на утверждение в ANSI, т.к. он требует доработки. После внесения корректив ISA представит новую версию спецификации (ISA-100.11a-2010 или -2011) на утверждение в ANSI в качестве Американского национального стандарта. До сего момента ISA-100.11a-2009 является стандартом, одобренным ISA, и он будет действовать до завершения работы над новой версией. До тех пор пока стандарт ISA-100 не будет принят в качестве стандарта ANSI, он не будет представлен на одобрение в IEC.

Подобно любой новой технологии внедрение беспроводных промышленных сетей не может не вызывать определенных проблем. Однако многие волнующие специалистов вопросы снимаются в процессе разработки тех стандартов, на базе которых на рынок выпускаются новые продукты. Беспроводные промышленные сети пока не готовы для массового применения, но, несомненно, их развитие идет именно в этом направлении.

ЛИТЕРАТУРА

1. Ian Verhappen. Security and Standards Delay Adoption and User Affinity. Industrial Wireless Worries//Industrial Networking, 2, 2010.