УДК 654.026

В.А. Бабошин, Е.А. Бубнова, Р.В. Ковальчук

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ СЕНСОРНЫХ СЕТЕЙ В СИСТЕМЕ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Бабошин Владимир Александрович, *окончил Ульяновское высшее военное командное училище связи им. Г.К. Орджоникидзе. Начальник отдела ОАО «НИИ «Рубин», кандидат технических наук, доцент. Имеет статьи в области систем связи специального назначения, систем беспроводного доступа, систем хранения данных. [e-mail: boboberst@mail.ru].*

Бубнова Елена Алексеевна, *бакалавр, окончила Департамент фундаментальной подготовки Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича. Аспирант ОАО «НИИ «Рубин». Занимается исследованиями проблем сбора и обработки информации в современных сенсорных сетях. [e-mail: inforubin@rubin-spb.ru].*

Ковальчук Роман Васильевич, *окончил факультет радиосвязи Тихоокеанского военно-морского института им. адмирала С.О. Макарова. Соискатель ОАО «НИИ «Рубин». Занимается исследованиями в области систем связи специального назначения, систем беспроводного доступа, систем хранения данных. [e-mail: inforubin@rubin-spb.ru].*

Аннотация

Дальнейшим развитием технологии самоорганизующихся мобильных радиосетей являются беспроводные сенсорные сети. В статье рассмотрен общий принцип работы сенсорных сетей, некоторые стандарты беспроводных сенсорных сетей, реализация оборудования беспроводных сенсорных сетей.

Ключевые слова: система связи специального назначения, беспроводные сенсорные сети, стек протоколов.

Введение

Беспроводные сенсорные сети являются дальнейшим развитием технологий самоорганизующихся радиосетей, их возникновение связано с разработкой концепции «Интернета вещей». Этот этап эволюционного развития инфокоммуникационных сетей (Post-NGN) характеризуется тем, что разнородные сети и множество датчиков (сенсоров) объединяются под управлением единых стандартов. Официальное определение приведено в Рекомендации МСЭ-Т Y.2060, Overview of the Internet of Things, согласно которой «Интернет вещей» (Internet of Things, IoT) – это глобальная инфраструктура информационного общества, обеспечивающая передовые услуги за счет организации связи между «вещами» на основе существующих и развивающихся совместимых информационных и коммуникационных технологий [1]. «Интернет вещей» порождает понятие триллионных сетей, условием жизнеспособности которых является способность к самоорганизации,

что, в свою очередь, приводит к необходимости изменения набора протоколов, обеспечивающих сигнализацию и маршрутизацию [2].

Технологической основой для реализации концепции «Интернета вещей» и являются беспроводные сенсорные сети WSN (Wireless Sensor Networks) или всепроникающие сенсорные сети USN (Ubiquitous Sensor Networks), основанные на стандарте IEEE 802.15.4 и протоколе 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), обладающем возможностями по присвоению IP-адреса исчислимому множеству сенсорных узлов.

Основы построения беспроводных сенсорных сетей

Беспроводная сенсорная сеть или беспроводная персональная сеть WPAN (Wireless Personal Area Networks) – это распределенная сеть необслуживаемых миниатюрных электронных устройств (сенсорных узлов), осуществляющих сбор данных о параметрах внешней среды и их передачу в центр обработки посредством ретрансляции от узла к узлу. Широкое использование таких сетей возможно в области автоматизации процессов сбора информации, мониторинга и контроля характеристик разнообразных технических и природных объектов. Сенсорные узлы могут устанавливаться стационарно или иметь возможность произвольно перемещаться в некотором пространстве, не нарушая логической связанности сети, в этом случае сенсорная сеть не имеет фиксированной топологии и обладает самоорганизующейся структурой. Под самоорганизацией (SelfOrganizing) понимается автоматический выбор топологии сети, автоматическое подключение новых устройств к сети, автоматический выбор маршрутов передачи пакетов в сети без участия человека.

Стандарт IEEE 802.15.4 определяет два нижних уровня модели: физический уровень (PHY) и уровень управления доступом к радиоканалу (MAC) для диапазонов частот 868, 915 МГц и 2,4 ГГц. Уровень управления ориентирован на организацию WPAN с небольшими скоростями передачи данных (LowRate WPANs, LR WPAN), радиусом действия сетевых устройств от 10 до 75 м. Все остальные функции реализуются протоколами верхних уровней. Стек протоколов наиболее известных стандартов сенсорных сетей (ZigBee, 6loWPAN) приведен на рисунке 1.

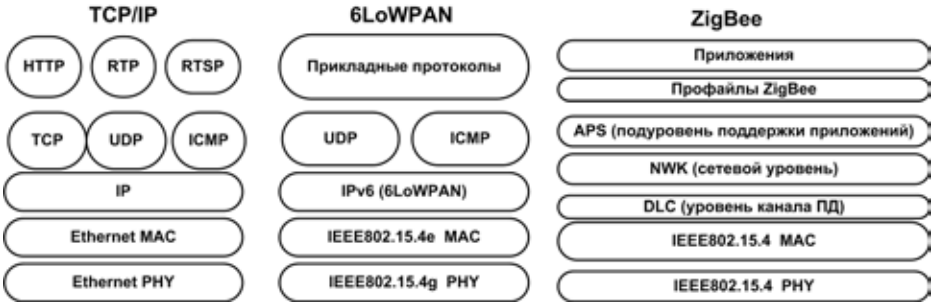

Рис. 1. Стек протоколов сенсорных сетей

В стандарте IEEE 802.15.4 (2006) выделяется четыре режима PHY:

– 868/915-МГц широкополосный спектр прямой последовательности (DSSS) PHY, использующий двухпозиционную фазовую манипуляцию (BPSK);

– 868/915-МГц DSSS PHY использует квадратурную фазовую манипуляцию со сдвигом (O-QPSK);

– 868/915-МГц широкополосный спектр обратной последовательности (PSSS) PH, использующий двухпозиционную фазовую манипуляцию (BPSK) и амплитудную манипуляцию (ASK);

– 2450-МГц DSSS PHY, использующий квадратурную фазовую манипуляцию со сдвигом (O-QPSK).

Типовой узел может быть представлен двумя типами устройств:

– сетевой координатор FFD (Fully Function Device), осуществляющий глобальную координацию, организацию и установку параметров сети, требует наибольшего объема памяти и емкого источника питания, поддерживает все типы топологий («точка – точка», «звезда», «дерево», «ячеистая сеть»);

– RFD (Reduced Function Device) поддерживает ограниченный набор функций стандарта 802.15.4 (топологии «точка – точка», «звезда»), не может осуществлять связь с другим RFD [2].

Полнофункциональное сетевое устройство FFD способно осуществлять связь как с несколькими FDD, так и несколькими RFD и может работать в трех режимах: мастер-координатор PAN, координатор и простое устройство.

Функцией мастер-координатора обладает одно FFD в сети, оно инициирует процесс самоорганизации, в его функцию входит сканирование частотных каналов для нахождения свободного канала и создания сети. После обнаружения свободного канала FDD формирует 16-разрядный адрес PAN (PAN identifier), который интерпретируется как корень дерева адресного пространства сети. После этого координатор PAN периодически передает в сеть сигналы маяка (Beacons). Сетевые устройства обнаруживают этот сигнал (функция Energy Detection) и используют для дальнейшего присоединения к существующему PAN. В адресном пространстве PAN, имеющем емкость 264, типы устройств (FFD или RFD) отличаются специальным битом в поле MAC-адреса. Для присоединения к сети удаленных от координатора PAN новых сетевых устройств могут использоваться уже присоединенные к сети FFD в режиме координатора. Из устройств, которые «слышат» своего координатора, формируются кластеры или мультикластеры сети. Функция координатора сводится к излучению кадров синхронизации доступа к радиоканалу, которые передаются между сигналами маяков, временные интервалы между ними называются «кадрами маяков» (Beacon Frame). Передача данных по сети может быть организована и без синхронизации доступа.

При передаче пакета данных (Data Frame) по сети сетевое устройство преобразует его в кадр данных, включающий адрес назначения, преамбулу для синхронизации, два проверочных байта циклического кода (CRC) для обнаружения ошибок и т. д. Кадр данных с максимальным размером 127 байт может быть зашифрован 128-битным ключом стандарта AES (Advanced Encryption Standard). Специализированный стек протоколов предусматривает функции самоорганизации и само-

восстановления сети, обеспечивает многоуровневую систему динамической аутентификации.

Узел сети содержит: датчик или множество датчиков (собственно сенсоров), принимающих данные от внешней среды; микроконтроллер; запоминающее устройство; приемопередатчик; автономный источник питания; исполнительные механизмы для передачи управляющих воздействий от узлов сети к внешней среде. Большое значение имеют способы интеграции датчиков, измеряющих значения первичных электрических величин, функционально зависимых от контролируемых параметров. Отказ от датчиков с цифровыми промежуточными интерфейсами позволяет не только экономить аппаратные средства, но и преобразовывать сигналы со всех датчиков в коды в одном многоканальном АЦП [3].

Беспроводной сенсор представляет собой плату, на которой располагаются цифровые и аналого-цифровые преобразователи, микропроцессор, оперативная и флэш-память, блок интерфейсов, приемопередатчик (радиомодем), источник электропитания, а также датчик (датчики).

Блок интерфейсов содержит иные порты ввода / вывода, например программирования или подключения внешнего датчика.

Радиомодем включает в себя низкомощный приемопередатчик и микроконтроллер, который, в свою очередь, имеет в своем составе процессор, ОЗУ, Flash-ROM, ПЗУ, EEPROM, АЦП, блок обработки прерываний, определенную номенклатуру интерфейсов и другие периферийные узлы.

В источнике электропитания реализована защита от перенапряжения и от переполюсования клемм. Питание сенсора осуществляется от батареи мощностью в несколько ватт. Возможна дополнительная схема подачи питания от внешнего источника.

В качестве опций в состав сенсора может входить блок визуализации для отображения текущего состояния устройства и блок ввода для смены режимов работы, перезагрузки и т. д. [3].

Основная обработка данных, полученных сенсором и включающих в себя информацию датчиков, а также информацию о состоянии сенсоров и результатах процесса передачи данных, производится узлом или шлюзом сети.

В рамках протокола 6LoWPAN [2] выделяются следующие типы сетей: ad-hoc, простая 6LoWPAN-сеть и расширенная 6LoWPAN-сеть.

Ad-hoc-сеть не имеет граничного маршрутизатора и подключения к внешней IP-сети. Простая 6LoWPAN-сеть имеет один граничный маршрутизатор, подключенный к внешней IP-сети напрямую (например, GPRS/3G/4G модем), или может входить в состав другой подсети. Расширенная 6LoWPAN-сеть состоит из одной или нескольких подсетей, подключенных к внешней IP-сети через несколько граничных маршрутизаторов. При этом граничные маршрутизаторы в расширенной сети разделяют один и тот же сетевой префикс. Узлы расширенной сети могут свободно перемещаться в пределах сети и осуществлять обмен с внешней сетью через любой граничный маршрутизатор (выбирается маршрут с наилучшими показателями качества сигнала – уровень ошибок, уровень сигнала).

В настоящий момент существует множество алгоритмов маршрутизации, предназначенных для использования в самоорганизующихся сетях с переменной топологией, таких как AODV (Ad-hoc On Demand Distance Vector), PWRP (Predictive Wireless Routing Protocol), DSR (Dynamic Source Routing), OLSR (Optimized Link State Routing protocol), TORA (Temporally-Ordered Routing Algorithm), HSLS (Hazy-Sighted Link State).

Протокол DSR осуществляет динамическую маршрутизацию от источника и предназначен для mesh-сетей MANET (Mobile Ad hoc Network). Так же, как и протокол AODV, он формирует маршрут по требованию посредством передачи широковещательного (broadcast) запроса, при этом используется явная маршрутизация без прямого учета таблиц маршрутизации на каждом промежуточном устройстве. Существует еще версия комбинированного протокола DSR-Flow, сочетающего в себе явную маршрутизацию и маршрутизацию по таблицам.

Протокол AODV является дистанционно-векторным реактивным протоколом, он предназначен для динамической маршрутизации в сетях MANET и других радиосетях.

Однако эффективность работы известных алгоритмов резко снижается в случае, когда скорость изменения топологии сети возрастает, что и характерно для сенсорных сетей, особенно в области специального назначения. Снижение эффективности работы реактивных алгоритмов в этой ситуации объясняется тем, что кэшированные маршруты транспортировки пакетов будут быстро устаревать ввиду разрушения составляющих их связей, поэтому при отправке пакета придется строить новый маршрут, что приведет к большим задержкам в доставке данных.

Проактивные алгоритмы, основанные на постоянной поддержке в актуальном состоянии таблиц маршрутизации в узлах сети, также малоприменимы по причине ограниченной емкости запоминающих устройств сенсорных узлов и высокой динамики изменения топологии.

В силу вышеуказанных технических и архитектурных особенностей сенсорных сетей данные решения неприемлемы, поэтому необходимо принимать меры для обеспечения эффективной маршрутизации. В частности, для этого был разработан протокол RPL (Routing Protocol for Low power and Lossy Networks), относящийся к семейству протоколов Distant Vector. Он использует принципы построения направленных ациклических графов DODAG (Destination Oriented Directed Acyclic Graph) и поддерживает маршрутизацию по множественной топологии MTR (Multi-topology routing), мобильность узлов и все механизмы для восстановления графов в случае перемещения узла [2].

Область применения беспроводных сенсорных сетей

Вышеперечисленные особенности беспроводных сенсорных сетей обусловили их применение при решении задач сбора данных в следующих областях:

- мониторинг территории охраняемых объектов, лесных массивов, акваторий;
- мониторинг территории в системах охраны государственной границы;
- мониторинг инфраструктуры телекоммуникационных сетей;

– мониторинг транспортных магистралей (железных дорог, метрополитена и др.), нефте- и газопроводов, инженерных сетей энерго- и теплоснабжения;

– контроль и анализ транспортных грузопотоков;

– выявление и предупреждение чрезвычайных ситуаций (мониторинг ледовой обстановки, сейсмической активности и вулканической деятельности, анализ атмосферы и прогноз погоды для своевременного предупреждения о наступлении стихийных бедствий);

– управление войсками и оружием в системах управления военного назначения, в частности в составе различных боевых информационно-управляющих систем, благодаря быстрой самоорганизации сети, простоте развертывания и высокой живучести, когда необходимо срочно развернуть сеть и обеспечить ее гарантированную работу даже при условии возможной потери части элементов;

– экологический, биологический и медицинский мониторинг;

– автоматизация систем жизнеобеспечения и систем класса «Умный дом».

В перечисленных сферах применения сенсорных сетей не всегда известны необходимое число датчиков и регулярность их размещения, условия обеспечения надежной межузловой связи, что требует адаптации узлов к изменению внешних факторов на основе максимальной автономности функционирования и минимальной необходимости взаимодействия узлов «по вертикали».

Технологии сенсорных сетей в системах специального назначения

Специальный (в том числе и военный) аспект применения сенсорных сетей, возможность их интегрирования в информационно-вычислительные системы открывает новые возможности и сервисы: быстрое и масштабное развертывание сенсорных сетей средствами артиллерии и авиасредствами; использование радиосвязи; сверхмалое энергопотребление и габариты; функции определения местоположения и самоорганизации. Все это позволяет решать широкий круг задач:

– отслеживание маршрутов движения объектов за счет оснащения их радиометками;

– мониторинг периметра или территории в составе объектовых охранных систем;

– охрана государственной границы;

– защита объекта (мониторинг локаций, ключевых точек, дорог);

– поддержка управления боевыми единицами, минными полями;

– разведка, обнаружение и локализация вражеских боевых единиц;

– химическая, бактериологическая, радиационная диагностика;

– передача данных между наземными, воздушными и морскими силами;

– мониторинг протяженных объектов военной инфраструктуры (дороги, трубопроводы, линии электропередач, кабельные линии).

Для решения подобных задач используются следующие типы сенсоров: акустические, сейсмические, магнитные, инфракрасные, оптические, электромагнитные, мультимодальные и другие сенсоры.

Решение специальных задач предъявляет следующие требования к оборудованию и программному обеспечению сенсорных сетей:

– защита от перехвата и декодирования сообщений, криптостойкое шифрование передаваемых данных;

– защита от «спуфинга», использование надежных механизмов аутентификации узлов в сети;

– защита целостности данных от фальсификации и атак воспроизведения за счет помехоустойчивого кодирования, проверки целостности (хэширования), криптографической обработки;

– защита от атак переполнения стека (DDOS, отказа в обслуживании);

– защита от обнаружения за счет сокращения частоты и продолжительности передачи данных;

– защита физических компонентов сети от воздействий окружающей среды (влажности, температуры, электромагнитных полей, механических воздействий) и несанкционированного доступа за счет установки элементов неизвлекаемости [4, 5].

К узлам сенсорной сети предъявляются следующие основные требования:

– возможность выполнения групповых действий, под которыми понимается функционирование выбранных узлов одного уровня системы по событиям, назначенным узлом (сетью) верхнего логического уровня для решения одной из фаз целевой задачи, при отладке и для анализа или точной диагностики аварийных ситуаций; поддержка уменьшения масштаба реального времени на период групповых действий;

– поддержка общего для всех узлов одного уровня механизма событий на основе меток единого времени или использование других доступных событий;

– непредельность реализации, возможность внесения доработок в уже эксплуатирующееся оборудование без нарушения режимов и условий его функционирования, что связано с невозможностью четкой постановки конечной задачи, вероятностью изменения задачи по мере освоения возможностей системы и / или изменения свойств среды ее размещения, влиянием «эффекта размерности системы», когда поведение большого числа одинаковых объектов становится не вполне прогнозируемым.

Сенсорным сетям отводится значительная роль в концепции сетецентрической войны, логическая модель которой приведена на рисунке 2 [6].

С технологической точки зрения основой концепции сетецентрических войн является представление любого вооруженного формирования в виде компьютерной сети, объединяющей элементы трех видов:

– сенсоры (средства вскрытия и отслеживания объектов противника);

– акторы или «стрелки» (средства огневого, радиоэлектронного и иного воздействия на вскрытые объекты);

– информационно-управляющие элементы, выполняющие функции анализа, принятия и реализации решений по управлению сенсорами и акторами.

Практическая реализация концепции сетецентрической войны невозможна без эффективного решения вопросов создания трех ключевых компонентов:

– сверхнадежной (ultreliable) коммуникационной среды, обеспечивающей эффективное функционирование на ее основе компьютерных сетей вооруженных

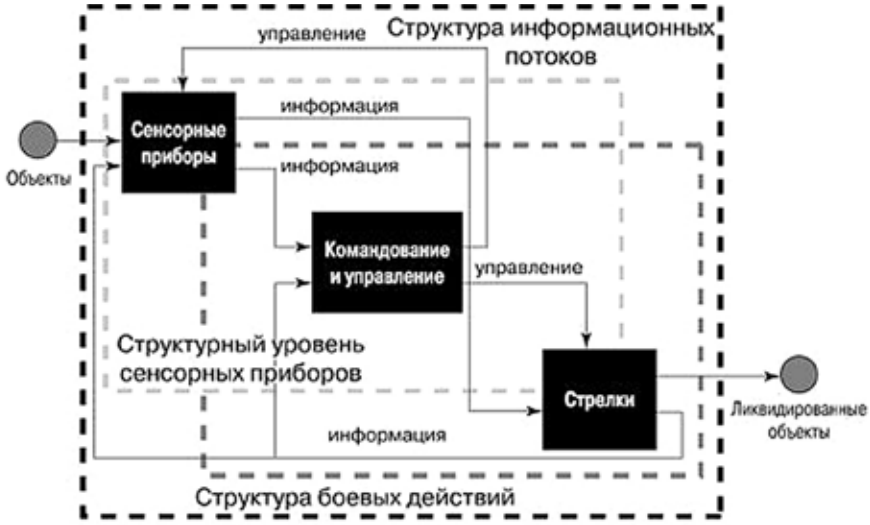

Рис. 2. Логическая модель сетецентрических боевых действий

формирований и их объединение в глобальную информационную сеть вооруженных сил;

– распределенной в пространстве группировки управляемых, достаточно информативных, надежных, долговечных и малозаметных для противника сенсоров, комплексируемых в компьютерные сети вооруженных формирований;

– распределенной программной среды, обеспечивающей в жестком реальном времени комплексную многоуровневую интеллектуальную обработку потоков малоинформативных в отдельности (а зачастую еще и противоречивых) первичных сведений о проявлениях объектов, а также позволяющей, при необходимости, оперативно изменять логику этой обработки по мере изменения состава и возможностей сенсоров, получения новых знаний о контролируемой группировке и т. п. [6].

Заключение

Беспроводные сенсорные сети на основе миниатюрных беспроводных узлов, отвечающих требованиям информационной безопасности, функционирующих в составе специализированных боевых информационно-управляющих систем, позволят повысить эффективность решения целого спектра специальных задач, а сейчас представляют собой важный объект исследования и научно-технической разработки.

СПИСОК ЛИТЕРАТУРЫ

1. Кучерявый Е.А., Молчан С.А., Кондратьев В.В. Принципы построения сенсоров и сенсорных сетей // Электросвязь. – 2006. – № 6. – С. 10–15.

2. Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А. Самоорганизующиеся сети. – СПб. : Любавич, 2011.

3. Проектирование беспроводных сенсорных сетей, 2012. – URL: http://isca.su/index.php

4. Богданов И.А., Кучерявый А.Е. Анализ особенностей обеспечения сетевой безопасности во всепроникающих сенсорных сетях. Выпуск 2, 2013. – URL: http://www.sut.ru/doci/nauka/review/.

5. Сергиевский М. Беспроводные сенсорные сети. Часть 1, 2, 3, 4 // Компьютер Пресс. – 2008. – №№ 4, 8, 11.

6. Савин Л.В. Сетецентричная и сетевая война. Введение в концепцию. – М. : Евразийское движение, 2011. – 130 с.