

Разработка радиоканальных охранно-пожарных систем

Виталий Германов
germanov@isca.su

В последнее время рынок оборудования и услуг охранной и противопожарной безопасности неуклонно растет. Правда, с повышением спроса также увеличиваются и предъявляемые к системам требования, что заставляет производителей постоянно совершенствовать существующие и создавать принципиально новые охранно-пожарные системы (ОПС).

В соответствии с ФЗ №123 «Технический регламент о требованиях пожарной безопасности», вступившим в силу 01.05.09, в проектах нормативных документов радиоканал наравне с проводными средствами стал одним из вариантов организации линий связи в системах пожарной сигнализации, оповещения и автоматики.

Беспроводные, или радиоканальные ОПС существуют на рынке давно, но первоначально из-за

невысокой надежности и высокой стоимости по сравнению с их проводными аналогами занимали очень маленький сегмент рынка. Сейчас, благодаря развитию беспроводных технологий и соответствующей элементной базы, появилась возможность создавать беспроводные ОПС, не только не уступающие по своим параметрам проводным системам, но и имеющие огромное преимущество. Для их установки не требуется прокладки дополнительных проводов, что позволяет производить монтаж не только на этапе строительства или капитального ремонта зданий, но и в жилых помещениях без необходимости проведения последующего ремонта.

В соответствии с ГОСТ Р 53325-2009 «Техника пожарная. Технические средства пожарной автоматики. Общие технические требования. Методы испытаний» радиоканальные системы пожарной безопасности должны удовлетворять следующим требованиям:

- ППКП и ППУ, а также иные технические средства противопожарной защиты, взаимосвязь с которыми осуществляется по радиоканальным линиям связи, должны быть адресными и обеспечивать между собой двухсторонний обмен данными.
- Достоверность передачи информации по радиоканальным линиям связи должна быть обеспечена техническими решениями, определяемыми производителями систем. В качестве данных технических решений могут быть предусмотрены возможности перехода на резервные частотные каналы, использование специальных протоколов обмена и иные способы повышения достоверности и надежности системы связи.
- При отсутствии связи с любым компонентом радиоканальной системы в течение определенного времени, но не более 300 с, ППКП и/или ППУ должны информировать о возникшей неисправности.
- Интервал времени с момента начала воздействия на адресный пожарный извещатель (АПИ) контролируемого фактора пожара с величиной, превышающей порог срабатывания АПИ, до перехода адресной системы пожарной сигнализации в режим «ПОЖАР» не должен превышать 10 с.

Учитывая все вышеизложенные требования к радиоканальным охранно-пожарным системам нового поколения, специалистами ЗАО «Институт Систем Комплексной Автоматизации» был разработан беспроводной протокол передачи

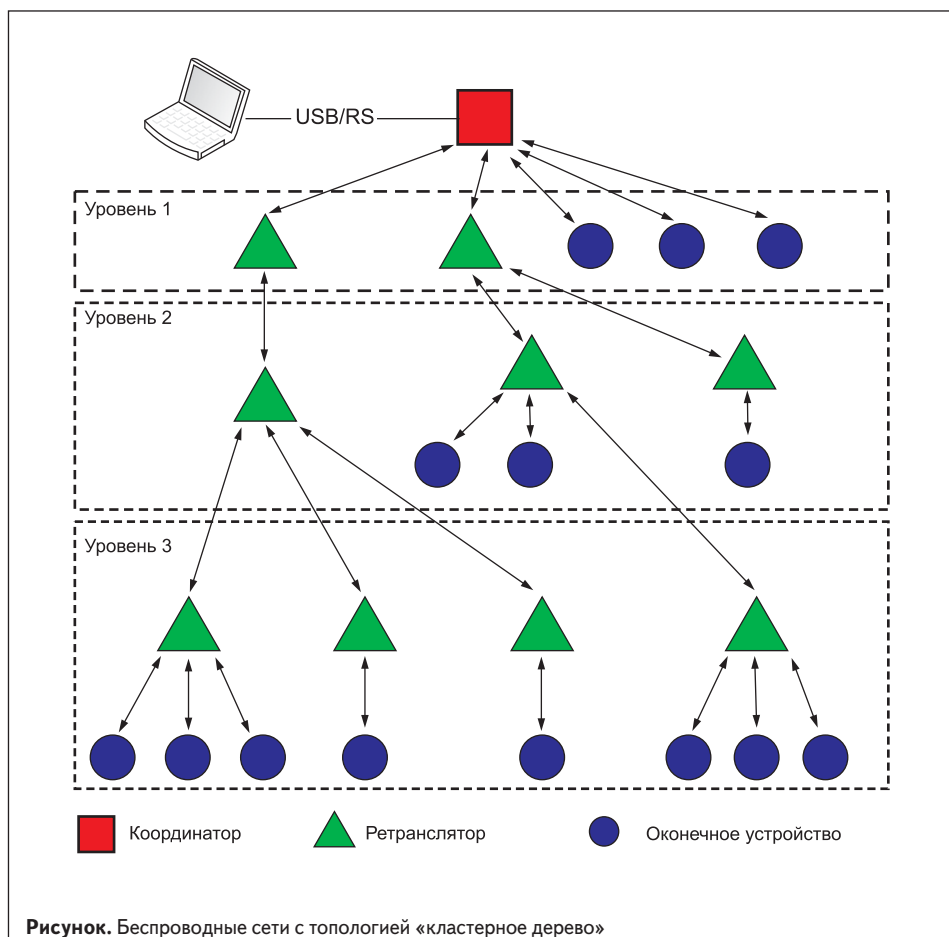


Рисунок. Беспроводные сети с топологией «кластерное дерево»

данных Hognet. Протокол реализован на базе ядра реального времени CEMCore и является аппаратно независимым в отличие от большинства представленных на рынке. В частности, на его основе могут быть спроектированы многоканальные беспроводные охранно-пожарные системы, работающие в радиочастотных диапазонах 433, 868 МГц и 2,4 ГГц.

В рамках протокола Hognet реализованы следующие механизмы взаимодействия устройств: конфигурирование, самоорганизация и самовосстановление, маршрутизация, контроль присутствия устройств в сети, переход на резервный маршрут, переход на резервный канал, аутентификация, гарантированная передача данных.

Благодаря применению адаптивных алгоритмов доступа к каналу, механизмов смены маршрута доставки сообщений и возможности перехода на резервные каналы, системы, построенные на базе протокола Hognet, обладают повышенной помехозащищенностью и живучестью.

Для защиты от подмены данных и устройств в протоколе Hognet реализован механизм динамической аутентификации и контроля наличия устройств в составе сети.

Для удобства развертывания беспроводных систем в них заложены механизмы самоорганизации, позволяющие автоматически определять оптимальные маршруты доставки сообщений, что значительно упрощает развертывание и настройку. Также сохранена возможность задать желаемую топологию, которая будет понятна оператору и обслуживающему персоналу и может быть нанесена на планы помещения.

Системы, построенные на базе протокола Hognet, обладают высокой оперативностью доставки сообщений — в среднем 20 мс на оповещение (при работе сети из 120 узлов, с 6-уровневой ретрансляцией). Протокол ориентирован в первую очередь на использование в системах с автономными беспроводными устройствами, поэтому большое внимание при его разработке было уделено энергосбережению. Это позволило обеспечить автономную работу оконечного устройства в течение 9 лет при контрольном интервале 12 с. (Оконечное устройство — без индикации, без измерений, один раз в 12 секунд передающее пакет «Норма»,

емкость батареи с учетом коэффициента утилизации — 0,7×2,4 А/ч. Средний срок службы реального датчика, снимающего отсчеты с АЦП раз в 50 мс и индицирующего свое состояние раз в 12 с, составляет 6 лет.)

В протоколе Hognet можно выделить следующий ряд устройств, отличающихся по своей функциональности:

- координатор сети;
- ретранслятор;
- оконечное устройство.

Координатор сети является центральным узлом и, как правило, имеет проводной интерфейс с внешним миром. Через него осуществляется конфигурирование устройств сети, контроль за топологией и состоянием устройств.

Ретрансляторы применяются для передачи сообщений от оконечных устройств на координатор. Помимо своей основной функции они также осуществляют подстройку времени выхода оконечных устройств в зависимости от загруженности радиофира. Микросота, контролируемая ретранслятором, может работать на своем канале, и, в случае обнаружения длительных радиочастотных помех, ретранслятор переводит ее на резервный канал. Датчики в топологии «кластерное дерево» сами определяют ретранслятор по вложенности и уровню сигнала. В случае выхода из строя ретранслятора или сильного ухудшения связи с ним датчик выбирает другой ретранслятор в области радиовидимости.

Оконечные устройства (датчики, устройства управления или исполнительные устройства) в зависимости от алгоритма работы делятся на автономные или неавтономные, с контролем присутствия в сети или без него. Автономное устройство с контролем присутствия работает от батареи, большую часть времени проводит в спящем режиме и «просыпается» только для измерений, передачи сигналов тревоги или контрольных пакетов в сеть. Координатор отслеживает присутствие таких устройств в сети и выдает соответствующее сообщение при их «пропаже». Автономное устройство без контроля присутствия работает от батареи, но контроль над ним не требуется. Устройства данного типа передают только по своей инициативе. Неавтономные устройства могут вы-

полняться как с контролем, так и без контроля присутствия в сети, основная их особенность — они не уходят в режим сна и всегда «слушают» радиоэфир. Как правило, это исполнительные устройства, работающие от стационарных источников питания.

Радиопrotocol Hognet позволяет строить беспроводные сети с топологией «кластерное дерево», что позволяет значительно увеличить зону покрытия.

Основные характеристики радиопrotocol Hognet:

- Топология радиосети — «кластерное дерево».
- Узлы сети имеют иерархическую систему адресации с интегрированной маршрутизацией.
- Максимальное число ретрансляторов, функционирующих одновременно в радиосети, — от 0 до 32.
- Максимальная вложенность ретрансляторов — 0–7.
- Максимальное число ретрансляторов, осуществляющих передачу через один ретранслятор следующего уровня, — не более 16.
- Максимальное число дочерних устройств на отдельный ретранслятор — до 256.
- Максимальное число устройств на один координатор — 256.
- Максимальное число устройств с точки зрения адресации — 65536.
- Ретранслятор осуществляет равномерное распределение устройств датчиков по свободным микроинтервалам.
- Организация доступа к каналу передачи данных осуществляется псевдослучайным образом с применением алгоритмов «анализа радиоэфира» и «временной коррекции».
- Интервалы передачи контрольных сигналов — от 10 с до 2 мин.
- Число резервных каналов — 1–16.
- В сети реализованы механизмы динамической аутентификации и динамического регулирования мощности.
- Переход микросоты (группы датчиков, обслуживаемых одним ретранслятором) на резервный канал в случае локальной помехи.
- Гарантированная доставка сообщений.