

**Шогенов**

Тимур Коммунарович, начальник кафедры специально-технической подготовки Северо-Кавказского института повышения квалификации сотрудников МВД России (филиал) Краснодарского университета МВД России, к.ф.-м.н., доцент, полковник полиции

Деятельность органов внутренних дел тесно связана с использованием специальных технических средств и современных информационных технологий. Во многих регионах Российской Федерации развиваются и функционируют системы «Безопасный город», внедряются навигационно-мониторинговые спутниковые системы управления нарядами, достаточно широко используются радиосети передачи данных для обеспечения удаленного доступа мобильных и стационарных абонентов органов внутренних дел к ведомственным информационным системам, внедрена единая информационно-телекоммуникационная сеть. Однако при всей функциональности и специфике решаемых с помощью них задач эти информационные системы в настоящее время развиваются автономно и, зачастую, вне зависимости друг от друга.

По нашему мнению, делом ближайшей перспективы станет разработка концептуальной программы создания единого информационного сетевого пространства, которое позволит оптимизировать и связать существующие и вновь разрабатываемые информационные системы органов внутренних дел.

Очевидно, что при реализации такой информационной транспортной инфраструктуры нельзя ограничиться только каналами связи на основе проводных и волоконно-оптических линий. Системы широкополосного

К вопросу об использовании систем широкополосного радиодоступа в деятельности органов внутренних дел

радиодоступа (ШПД) должны в такой инфраструктуре занять ключевое место. Это позволит обеспечить информационный обмен с мобильными объектами органов внутренних дел, а при необходимости – и других правоохранительных органов. Следует отметить, что возможность создания и использования систем широкополосного радиодоступа подразделениями органов внутренних дел закреплена в Наставлении, утвержденном Приказом МВД России от 28 декабря 2006 года.

Как известно, системы беспроводного широкополосного радиодоступа предназначены для помехоустойчивой передачи (приема) по радиоканалу информации с использованием сигналов относительно малой мощности, при этом в системах ШПД используется значительно более широкая полоса частот, чем это требуется при обычной передаче, как, например, в конвенциональных радиосетях. За счет высокой информационной избыточности достигается хорошая помехоустойчивость сигнала и достаточно высокая скорость информационного обмена.

Технологии ШПД позволяют организовать сети различных типов и решать широкий спектр задач – от развертывания сети в отдельно взятом помещении до распределенной сети в масштабе обслуживаемой органом внутренних дел территории.

Особенностью систем широкополосного радиодоступа является их мультисервисность, т.е. возможность обеспечивать:

- передачу аудио-видеоинформации в реальном времени;
- доступ к базам данных;
- услуги IP-телефонии;
- подключение к телефонным системам общего пользования;
- организацию беспроводных локальных сетей.

Традиционно системы ШПД включают в себя следующие базовые элементы:

- точки доступа;

- серверы авторизации;
- специальные коммутаторы и маршрутизаторы, обеспечивающие управление сетью и повышение ее защищенности.

Беспроводной широкополосный радиодоступ обеспечивает высокое качество связи, что позволяет решить проблему организации передачи аудио-видеоинформации и данных в районах, где использование проводных или волоконно-оптических каналов связи невозможно или экономически неэффективно.

Наиболее важными этапами проектирования мультисервисных сетей широкополосного радиодоступа для обеспечения деятельности подразделений органов внутренних дел являются:

- определение оптимальной топологии сети с учетом взаимной удаленности объектов, характеристики местности, наличия и состояния действующих линий связи и элементов сетевой инфраструктуры, согласно требованиям по приоритетности трафика, распределению пропускной способности и надежности сети,
- выбор сетевых технологий, протоколов, схем адресации, систем мониторинга и управления и средств обеспечения информационной безопасности сети;
- выработка рекомендаций по внедрению, эксплуатации, расширению и модернизации сети.

Для реализации беспроводного широкополосного радиодоступа могут быть использованы различные стандарты, наибольшее распространение среди которых получили стандарты семейства IEEE 802.11, что, вероятно, связано с относительно невысокой стоимостью оборудования¹.

Как известно, сети широкополосного радиодоступа могут иметь одноузловую и многоузловую структуру. Наибольшую привлекательность

1. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.: Эко-Трендз, 2005.



имеет многоузловая ячеистая топология сети.

В традиционной беспроводной сети стандарта 802.11 несколько абонентов подключаются по прямому соединению с точкой доступа. Такие сети называются одноузловыми. Основным недостатком таких сетей является существенное снижение скорости передачи данных с увеличением количества подключаемых к точке доступа терминалов (оконечных устройств).

В многоузловой сети любое устройство беспроводной связи способно выступать в роли как маршрутизатора, так и точки доступа. Если ближайшая точка доступа перегружена, данные перенаправляются к ближайшему незагруженному узлу. Пакеты данных продолжают перемещаться от одного узла к другому, пока не достигнут места назначения – получателя информации.

Одним из решений по построению многоузловых ячеистых сетей является технология Mesh^{2,3,4}. Сама идея применения Mesh-технологии не нова и уже достаточно давно реализована в практике деятельности специальных подразделений зарубежных стран.

Главной особенностью Mesh-сети является ее «интеллектуальность». Как только точка доступа установлена и включена, она автоматически обнаруживает другие точки доступа и «выясняет» свою роль в сети. Это снижает необходимость ручного администрирования сети, играет важную роль для оперативного развертывания оборудования. Как только сеть запускается в эксплуатацию, она начинает автоматически управлять своей работой благодаря функциям самовосстановления и самоадаптации. Если точка доступа отключается или какой-либо сегмент сети оказывается перегруженным, сеть автоматически переопределяет маршруты передачи данных между точками, что позволяет предотвратить сбои коммуникаций.

Топология ячеистых сетей предусматривает либо прямую связь между образующими их узлами, либо тран-

зитную передачу данных между источником и получателем. Перед тем как начать обмен данными, каждый узел должен «решить», будет ли он выполнять функции точки доступа, служить транзитным устройством или сочетать обе роли. Далее индивидуальные узлы определяют своих соседей, используя протокол типа «запрос-ответ». После окончания процедуры обнаружения узлы определяют характеристики коммуникационных каналов: мощность принимаемого сигнала, пропускную способность, задержку пакетов и частоту ошибок. Узлы обмениваются этими значениями, а затем на их основе каждый узел выбирает наилучший маршрут коммуникаций со своими соседями.

Процессы обнаружения и выбора наиболее благоприятного маршрута выполняются в фоновом режиме, так что каждый узел располагает актуальным списком «соседей» (по IP или MAC-адресам). В случае недоступности по тем или иным причинам какого-либо узла соседние могут быстро переконфигурировать свои таблицы и вычислить новый оптимальный маршрут. Способность самоконфигурации и самовосстановления делает ячеистые сети очень надежными. Беспроводные ячеистые сети могут состоять из сотен и даже тысяч узлов, что позволяет легко расширять их и обеспечивать необходимую избыточность. Использование множественных маршрутов доставки данных повышает пропускную способность сети.

Физические свойства беспроводных коммуникационных каналов таковы, что на более коротких расстояниях пропускная способность сети выше. Причиной могут быть помехи и иные влияющие на потерю данных факторы, чье действие накапливается по мере увеличения расстояния. В связи с этим одним из способов повышения пропускной способности сети становится передача данных через несколько узлов, разделенных небольшими расстояниями. Такой механизм реализуется в сетях ячеистой топологии. Благодаря тому, что для передачи данных на более короткие расстояния требуется меньшая мощность, многоузловая сеть может обеспечить более высокую общую пропускную способность, одновременно удовлетворяя всем законодательным требованиям к устройствам радиосвязи, ограничивающим максимальную мощность передатчиков.

Узлы остаются вполне автономными устройствами, способными само-

стоятельно управлять своим функционированием, и в то же время являются компонентом общей сети, допускающим управление из центральной точки. Системный администратор при необходимости может выполнять мониторинг и конфигурировать отдельные элементы, узлы, домены или всю сеть.

Еще одним важным преимуществом сетей ячеистой топологии по сравнению с одноузловыми сетями является их пространственное разделение. Как уже было отмечено, в одноузловой сети все оконечные устройства совместно используют одну точку доступа. Если несколько оконечных устройств пытаются одновременно взаимодействовать с сетью, то возникающие задержки в ее работе существенно снижают скорость обмена данными. В противоположность этому в сетях ячеистой топологии множество оконечных устройств могут подключаться одновременно через разные узлы, но пропускная способность сети при этом практически не ухудшается. Более короткие расстояния передачи данных в сетях ячеистой топологии позволяют уменьшить влияние помех и осуществить одновременную передачу пространственно разделенных потоков информации.

Информационная безопасность беспроводной системы доступа является достаточно серьезной проблемой, что обусловлено широким распространением устройств беспроводного доступа среди населения, а также наличием большого количества доступного программного обеспечения для несанкционированного доступа в беспроводные сети. Для решения этой проблемы используются различные средства, вплоть до запрещения использования беспроводного доступа в системе с организацией службы радиомониторинга и радиопротиводействия. Системы мониторинга позволяют не только идентифицировать вторжение в сеть, но и определять место, откуда оно ведется.

Использование шлюзов Mesh в сети обеспечивает аутентификацию пользователей, шифрование данных и необходимое качество обслуживания трафика, реализует безопасный роуминг между подсетями.

Подсистема безопасности в оборудовании Mesh-сетей включает в себя механизмы криптографической защиты, препятствующие несанкционированному доступу к сетевым ресурсам и нанесению им ущерба, а также перехват и дешифровку передаваемой информации. Большинство контрол-

- Осипов И. Е. Mesh-сети: технологии, приложения, оборудование // Технологии и средства связи. 2006. №4. С. 39-45.
- Технология Mesh – надежное профессиональное решение по гарантированной передаче широкополосных данных с мобильных объектов. Интернет-ресурс http://www.sagatelecom.ru/radiosystems/wireless_system/mesh.php.
- Вишневецкий В.М., Лаконцев Д.В., Сафонов А.А., Шпилев С.А. Mesh-сети: в ожидании стандарта IEEE 802.11s. // Электроника. 2008 г., № 3, С. 98 – 106.



леров доступа Mesh-сети используют для аутентификации пользователей встроенную базу данных. Однако наиболее надежным средством является использование сервера аутентификации RADIUS (Remote Authentication Dial-In User Service). Также следует проработать вопрос по использованию при передаче критически важных данных сертифицированных по требованиям обеспечения информационной безопасности программных продуктов.

В настоящее время на рынке линейка оборудования Mesh представлена целым спектром продуктов от известных мировых производителей, таких как Motorola⁵, Cisco^{6,7,8}, D-Link⁹, Proxim Wireless¹⁰ и др. Однако, на наш взгляд, для решения задач органов внутренних дел предпочтение все же следует отдавать отечественным разработкам, в частности продукции предприятий оборонно-промышленного комплекса Российской Федерации. Привлекательным по тактико-техническим характеристикам и технико-экономическим показателям является также предложение российского концерна «Созвездие» линейки Mesh оборудования K-Line¹¹.

Предлагаемые на рынке средств беспроводной связи внешние точки доступа по технологии Mesh поддерживают стандарты беспроводной связи IEEE 802.11a/b/g и предназначены для организации высокоэффективной беспроводной сети. Они выполняются в металлическом, влагозащитном

корпусе, имеют класс защиты IP-66 (всепогодное исполнение), предназначены для наружной установки, сохраняют работоспособность в широком диапазоне внешних температур.

Внешние и внутренние точки доступа, функционирующие по технологии Mesh с одной стороны, обеспечивают радиосигналом зону своего покрытия, с другой стороны – одновременно осуществляют передачу трафика между аналогичными точками доступа с помощью протокола динамической маршрутизации. Такие точки доступа, как правило, могут работать в диапазоне 2,4 ГГц для большего радиуса действия системы, или в диапазоне 5 ГГц для минимизации частотной интерференции. Точки доступа оснащены соответствующими разъемами, с помощью которых к ним можно подключать самые разнообразные антенны в зависимости от структуры беспроводной сети и условий ее построения.

Чтобы облегчить задачу администрирования сети Mesh крупного масштаба, например населенного пункта, разработчики поставляют совместно с оборудованием централизованное управляющее программное обеспечение, которое может контролировать все узлы Mesh-сети и управлять ими. Графический интерфейс программного обеспечения позволяет администратору контролировать статус сети в реальном времени.

Таким образом, основой Mesh-сети является совокупность внешних точек доступа, размещаемых на различных конструктивных элементах зданий, высотных сооружениях, опорах электропередач и столбах городского освещения.

Основным требованием при территориальном планировании размещения внешних точек доступа является обеспечение условий прямой радиовидимости по крайней мере трех узлов между собой в одном кластере и двух точек доступа в двух различных кластерах.

Очень важным аспектом проектирования сети является обеспечение электромагнитной совместимости на основе анализа электромагнитной обстановки в местах монтажа оборудования. Также необходимо решать вопросы по надежному обеспечению электропитанием точек доступа.

Вторым элементом сети является сервер аутентификации и доступа, оснащенный Mesh-шлюзом и внутренней либо внешней Mesh-точкой доступа, обеспечивающей взаимодействие

сервера с внешней инфраструктурой сети. Сервер должен размещаться на центральном контрольном пункте подразделения органа внутренних дел и обеспечивать конфигурирование информационной сети по IP и MAC-адресам, а также формировать политику безопасности сети в целом.

Кроме этого, сервер может быть интегрирован с существующими информационными системами ОВД, ЕИТКС, системами «Безопасный город», что, в случае необходимости, позволит обеспечить оперативный доступ к информационным ресурсам и базам данных, видеoinформации от камер наружного наблюдения в реальном времени с любого мобильного терминала, поддерживающего стандарты IEEE 802.11 и размещаемого, например, в автомобиле.

Третьим элементом сети является комплекс оборудования, устанавливаемого на объекте оперативной заинтересованности, в который входят: внешняя или внутренняя Mesh-точка доступа, IP-камеры видеонаблюдения, видеосерверы с подключенными средствами аудио и видеонаблюдения (например, акустический датчик и телевизионная камера). Если используются беспроводные IP-камеры видеонаблюдения, то их взаимодействие с точками доступа Mesh-сети осуществляется непосредственно по радиоканалу.

В заключение отметим, что рассмотренная в статье реализация широкополосного радиодоступа на основе мультисервисной Mesh-сети требует сравнительного анализа оборудования различных производителей, практического апробирования на основе тщательного изучения тактико-технических характеристик и технико-экономических показателей, проведения испытаний в реальных условиях и сертификации по требованиям МВД России.

Проведение научно-исследовательских и опытно-конструкторских работ по существующим и перспективным техническим решениям реализации распределенных закрытых мультисервисных сетевых инфраструктур широкополосного радиодоступа, а впоследствии и внедрение их результатов позволят существенно оптимизировать расстановку сил и средств органов внутренних дел, повысить эффективность мероприятий органов внутренних дел по обеспечению общественного порядка и общественной безопасности в нашей стране.

5. Сети Mesh. Интернет-ресурс <http://www.motorola.com/Business/RU-RU/Business+Product+and+Services/Wireless+Networks/Wireless+Broadband+Networks/Mesh+Networks>.
6. Cisco wireless Mesh. Интернет-ресурс <http://www.cisco.com/global/RU/products/downloads/mesh.pdf>.
7. Проектирование городских Wi-Fi Mesh-сетей. Интернет-ресурс http://www.cisco.com/web/UA/expo2008/download/pdf_pre/29.pdf.
8. Cisco Aironet 1520 Series Lightweight Outdoor Access Point. Интернет-ресурс http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/product_data_sheet090aecd8066a157.pdf.
9. Беспроводное решение D-Link для Mesh-сетей. Интернет-ресурс <http://www.ediscom.ru/index.php?chp=showpage&fromi=1&num=682>.
10. Системы для построения Wi-Fi Mesh-сетей снаружи и внутри зданий. Интернет-ресурс http://asvagrroup.com/proxim_mesh.htm.
11. Беспроводная самоорганизующаяся Mesh-сеть. Интернет-ресурс http://www.sozvezdie.su/catalog/wifi_tochka_dostupa_kline_oborudovanie/.