Продолжение. Начало в № 4`2009

Конвенциональные широкополосные технологические радиосети обмена данными

повышенной надежности и живучести. Часть 2

Сергей Маргарян
Александр Харламов, к.т.н.
Алексей Хромцев
Алексей Сабунин

Оборудование УКВ-диапазона на практике является идеальным решением для создания технологических радиосетей обмена данными для большинства ответственных приложений. В связи с этим на протяжении последних десятилетий узкополосные технологические радиосети обмена данными оставались основным инструментом сбора данных и управления. Однако с развитием информационных технологий возросли потребности в пропускной способности радиосетей, используемых для обеспечения работы отдельных ответственных приложений. С целью удовлетворения этих возросших потребностей были созданы образцы аппаратуры УКВ-диапазона, имеющие более высокие технические характеристики и позволяющие обеспечить передачу в оперативном режиме достаточно большого объема данных. Для достижения таких характеристик разработчикам пришлось использовать широкополосные сигналы[1]. Это решение позволило увеличить скорость обмена данными и пропускную способность радиосетей, сохранив дальность передачи, характерную для УКВ-диапазона.

В настоящее время количество представленных на российском рынке моделей широкополосной аппаратуры, работающей в УКВ-диапазоне, относительно невелико. Технические характеристики некоторых моделей широкополосных радиомодемов представлены в таблице 4.

Все широкополосные радиомодемы обеспечивают работу в радиосетях с архитектурой «точка – много точек». Так, радиомодемы Mercury-900 и Sentry 4G-900 могут использоваться для строительства как подвижных, так и стационарных радиосетей (в последнем случае поставляются без встроенного навигационного приемника). Надежность работы этих устройств в составе радиосети обеспечивается реализацией разнесенного приема (технология MIMO — multiple in multiple out), при котором радиосигнал принимается одновременно на две антенны, установленные на расстоянии одна от другой. В Mercury-900 разнесенный прием используется для работы в радиосети WiMax, в Sentry 4G-900 — в радиосетях WiMax и WiFi.

Построение технологических радиосетей повышенной надежности и живучести на оборудовании Sentry 4G-900

Надежность и живучесть технологических радиосетей на перспективном оборудовании Sentry 4G-900 обеспечивается за счет возможности создания на их базе единого информационного поля, функционирующего по IP-протоколу, доступ к которому с каждого устройства организуется по двум выделенным каналам — 900 МГц IEEE802.16e-2005 WiMax и IEEE802.11b/g WiFi. Кроме того, при наличии в оперативной зоне радиосетей стандарта WiFi общего пользования они могут использоваться в качестве резервных каналов доставки информации, повышая живучесть разворачиваемой технологической радиосети.

Упрощенная схема радиосети обмена данными на радиомодемах Sentry 4G-900 представлена на рис. 13.

Представленная на рис. 13 радиосеть обмена данными функционирует по IP-протоколу и является «прозрачной» для любого программного обеспечения, поддерживающего работу через локальную или глобальную вычислительную сеть. Задействуемая для работы в составе радиосети аппаратура может автоматически сопрягаться между собой по каналам WiMax или WiFi, используя автоматическую маршрутизацию сообщений и «прозрачное» объединение обеих технологий, чем обеспечивается высокая надежность и живучесть радиосети и функционирующей на ее базе информационной системы в целом.

Радиосеть имеет следующие функциональные возможности и порядок функционирования:

1. Стационарная базовая станция WiMax широкополосной технологической радиосети обмена данными.
2. Мониторинг и оперативно-диспетчерское управление подвижными дежурными силами при выдвижении в район оперативного предназначения в зоне работы постоянной действующей технологической радиосети.
3. Управление светофорными комплексами по каналам технологической радиосети в интересах приоритетного пропуска подвижных дежурных сил служб общественной безопасности на регулируемых

[1]Радиочастотный сигнал, база которого существенно больше единицы (ГОСТ 24375-80. «Радиосвязь. Термины и определения»).

Таблица 4. Характеристики специализированных радиомодемов для подвижных и стационарных технологических радиосетей обмена данными

Наименование радиомодема (производитель)	Рабочий диапазон частот, МГц	Полоса, кГц/вид модуляции	Скорость передачи информации	Тип протокола	Выходная мощность передачи, Вт	Чувствительность приема
ExaLink-900, 900M, 900MT (Exergia Division II, США)	902–928	Нет данных	935 кбит/с	TCP/IP	0,125	–101 дБм, BER 10×10^{-4}
Phantom-900 (CalAmp, США)	902–928	490 кГц/2FSK, 4FSK	256 или 512 кбит/с	прозрачный, TCP/IP	0,1–1	–98 дБм, BER 10×10^{-6}, 512 кбит/с –102 дБм, BER 10×10^{-6}, 256 кбит/с
Sentry 4G-900, бортовой радиомодем со встроенным навигационным приемником[2] и встроенной точкой доступа WiFi IEEE802.11b/g (CalAmp, США)	902–928	3,5 МГц/OFDMA TDD (IEEE802.16e-2005 WiMax), QPSK, 16QAM, 64QAM	1–3 Мбит/с (6 Мбит/с пиковая)	TCP/IP	0,1–1	Нет данных
Mercury-900, бортовой радиомодем со встроенным навигационным приемником и встроенной точкой доступа WiFi (GE MDS, США)	902–928	1,75, 3,5 МГц/ OFDMA (IEEE802.16d-2004 WiMax)	800 кбит/с	прозрачный, TCP/IP	0,1–1	Нет данных
TransNET 900 (GE MDS, США)	902–928	CPFSK	115,2 кбит/с	прозрачный	0,1–1	–108 дБм, BER 1×10^{-6}

[2]Ведется разработка встроенного навигационного приемника системы ГЛОНАСС.

перекрестках на маршруте выдвижения в район оперативного предназначения.

4. Оперативное управление и информационное обеспечение сил и средств служб общественной безопасности в районе оперативного назначения, находящемся в зоне действия технологической радиосети по каналам связи WiMax.
5. Локальная сеть управления силами и средствами служб общественной безопасности в районе оперативного предназначения по каналам связи WiFi в оперативной зоне постоянной действующей технологической радиосети.

6–9. Разнородные подвижные силы и средства служб общественной безопасности различной ведомственной принадлежности в удаленной зоне.

10. Локальная сеть WiFi для взаимодействия разнородных подвижных сил и средств служб общественной безопасности различной ведомственной принадлежности в удаленной зоне
11. Локальная сеть WiFi общего пользования.

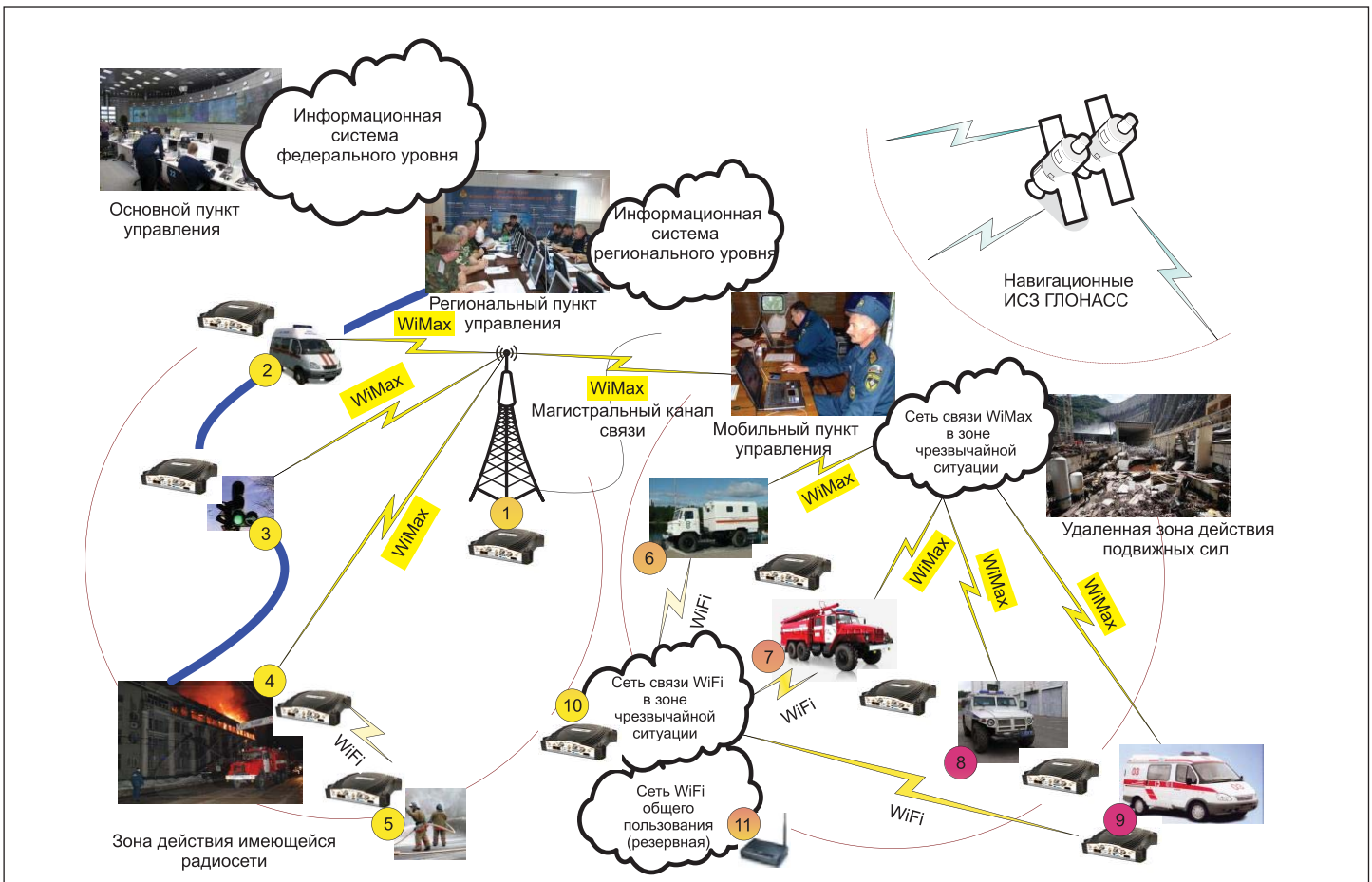

Рис. 13. Упрощенная схема радиосети обмена данными на радиомодемах Sentry 4G-900: 1 — радиомодем Sentry 4G-900; 2 — точка доступа WiFi радиосети связи и передачи данных общего пользования; 3 — канал связи IEEE802.16e-2005 WiMax; 4 — канал связи IEEE802.11b/g WiFi

Широкополосная технологическая радиосеть обмена данными имеет в своем составе группу стационарных базовых станций WiMax и обеспечивает функционирование подвижных и стационарных объектов в оперативной зоне. Встроенный протокол позволяет организовать автоматический перевод подвижных объектов между соседними базовыми станциями с минимальной задержкой по времени. Базовые станции подключаются к региональному пункту управления по проводным или беспроводным магистральным каналам связи, работающим по IP-протоколу.

Региональный пункт управления осуществляет мониторинг и оперативно-диспетчерское управление подвижными дежурными силами при выдвижении в ходе решения функциональных задач в районе оперативного предназначения в зоне работы постоянной действующей технологической радиосети. Он обеспечивает автоматизированный контроль действий подвижных сил с самого начала их оперативного использования и до завершения операции. По каналам радиосети с заданной периодичностью транслируются данные о текущем местоположении подвижных сил и средств и характере их использования, передаются команды управления и сигналы оповещения, а также обеспечивается удаленный доступ к массивам информации, которая может потребоваться в процессе решения задач оперативного предназначения.

По каналам технологической радиосети осуществляется оперативно-техническое управление стационарной инфраструктурой, в частности, светофорными комплексами. Наличие такой возможности позволяет организовать приоритетный пропуск подвижных средств дежурных сил служб общественной безопасности на регулируемых перекрестках при их выдвижении в район оперативного предназначения. Реализация данной функциональной задачи позволяет существенно сократить время реагирования на аварии и происшествия и свести к минимуму тяжесть их последствий.

Оперативное управление и информационное обеспечение сил и средств служб общественной безопасности в районе оперативного назначения, находящемся в зоне действия технологической радиосети, осуществляется по каналам связи WiMax, которые обеспечивают обмен мультимедийной информацией. Относительно высокая пропускная способность радиосети позволяет передавать достаточно большие массивы графической и видеоинформации.

В районе оперативного предназначения разворачивается беспроводная локальная сеть управления силами и средствами служб общественной безопасности по каналам связи WiFi. Она сопрягается с действующей стационарной технологической радиосетью обмена данными WiMax и обеспечивает доступ пользователей к ресурсам информационной системы на региональном и федеральном уровнях. В результате подвижные силы имеют функциональные возможности, аналогичные тем, которыми они располагают при работе в стационарных условиях. Применение WiFi позволяет организовать подключение к сети абонентов различной ведомственной принадлежности через коммерческие терминалы и стандартное программное обеспечение, используемое в сетях данного типа.

Полевой (мобильный) пункт управления подвижными силами служб общественной безопасности может разворачиваться в удаленном районе при отсутствии постоянно действующей технологической радиосети обмена данными либо на границе данной сети. В последнем случае он может выступать как ретранслятор, увеличивая дальность связи. Связь обеспечивается техническими средствами, разворачиваемыми в оперативной зоне на период проведения совместной операции. В рамках взаимодействия технологическая радиосеть обеспечивает обмен данными между всеми участниками операции, независимо от их ведомственной принадлежности.

Локальные подсети обмена данными разнородных подвижных сил и средств служб общественной безопасности различной ведомственной принадлежности в удаленной зоне разворачиваются на период проведения операции. Они позволяют предоставить подвижным силам функциональные возможности, аналогичные тем, которыми они располагают при работе в стационарных условиях. Разворачиваемая в удаленной зоне локальная вычислительная сеть на базе WiFi обеспечивает взаимодействие разнородных подвижных сил и средств служб общественной безопасности различной ведомственной принадлежности.

При наличии в удаленной зоне сети WiFi общего пользования она может использоваться в качестве резервной или аварийной для обеспечения обмена данными участников операции между собой и с соответствующими пунктами управления верхнего звена. Навигационное обеспечение участников операции данными, поступающими от системы спутниковой связи ГЛОНАСС, осуществляется через внешние или встроенные навигационные приемники аппаратуры Sentry 4G-900.

Таким образом, рассмотренная технология широкополосной передачи данных и реализованные на ее основе образцы оборудования позволяют создавать мобильные и стационарные интегрированные технологические радиосети обмена данными повышенной надежности и живучести для служб общественной безопасности и управления удаленными объектами.

Обеспечение безопасности информации в стационарных и подвижных технологических радиосетях обмена данными

Безопасность данных в стационарных и подвижных технологических радиосетях является одним из ключевых условий их использования, а строительство таких радиосетей осуществляется с учетом полного исключения или максимального затруднения компрометации передаваемой по ним информации. В радиосетях обмена данными широко применяются различные методы и способы защиты информации. Степень защиты данных оказывает непосредственное влияние на надежность радиосети и ее живучесть, поскольку постороннее вмешательство в работу может существенно снизить эти параметры. Ниже представлена информация о возможностях данных радиосетей противостоять основным угрозам: перехвату данных, несанкционированной работе в составе радиосети и радиоэлектронным помехам[3].

Обеспечение безопасности данных в стационарных радиосетях

Одним из наиболее важных требований к технологическим радиосетям обмена данными является обеспечение их безопасности. Следует отметить, что защита данных в любой системе представляет собой непрерывный комплекс организационно-технических и специальных мероприятий, ни одно из которых самостоятельно не позволяет добиться поставленной задачи. Тем не менее, рассматриваемые средства обмена данными обладают свойствами, позволяющими значительно снизить существующие угрозы, главными из которых являются перехват и несанкционированный доступ к работе в радиосети, что обусловлено уже самой средой передачи.

Устойчивость к перехвату данных

На первый взгляд, перехват данных в проводных технологических сетях связи сопряжен с серьезными трудностями. Однако эта задача не так сложна для специалиста, имеющего соответствующую подготовку (подтверждением этому являются многочисленные успешные атаки хакеров[4] на информационные системы). Кабельная сеть прокладывается внутри здания или комплекса зданий. При этом отдельные сегменты могут укладываться в подвалах зданий, коллекторах, потернах и т. п., не контролируемых службами безопасности, и представлять собой потенциальные точки для несанкционированного подключения. Теоретически любой человек, знающий структуру кабельной системы, может получить доступ к ней в этих точках. После подключения к проводной системе связи получение доступа к информации является делом техники, поскольку во всех открытых проводных сетях используются стандартные протоколы связи и обмена данными, а также серийно выпускаемые и общедоступные программно-технические средства.

Средой передачи данных в радиосетях являются радиоволны, которые могут приниматься любым приемником на относительно большом расстоянии от передатчика. Однако радиосигналы, передаваемые в системах обмена данными с использованием современных радиомодемов, не так доступны, как это может показаться на первый взгляд.

Во-первых, для организации перехвата необходимо точно знать номинал рабочей частоты, используемой для обмена данными. При соблюдении пользователями минимальных правил безопасности получение этой информации крайне затруднено. Поскольку передаваемые

[3] Вопросы противодействия профессиональным средствам радиоэлектронной борьбы и радиоэлектронного подавления в настоящей статье не рассматриваются.

[4] Хакер (от англ. hack — разрубать) — особый тип компьютерных специалистов. Как правило, это компьютерные взломщики, осуществляющие неправомерный доступ к компьютерам и информации.

данные не могут восприниматься на слух, то при использовании для определения номинала рабочей частоты доступных средств перехвата, например, частотных сканеров, фиксируется только факт передачи сигналов на определенной частоте, которые представляют собой набор шумов. Определение принадлежности этих сигналов тому объекту, поиск которого ведется, без доступа к передаваемой информации оказывается практически невозможным.

Во-вторых, оборудование использует специальные схемы модуляции сигнала и собственные преамбулы (структуру пакета данных). На практике это приводит к невозможности получения доступа собственно к передаваемой информации при отсутствии соответствующего радиомодема или специального оборудования для анализа сигналов. В отличие от проводных модемов, распространение радиотехнического оборудования имеет известные ограничения, а все его пользователи регистрируются. В связи с этим вероятность легального приобретения злоумышленниками оборудования, которое может использоваться для обеспечения доступа к передаваемой в технологических радиосетях обмена данными информации, практически равна нулю.

В-третьих, в большинстве радиосетей, особенно имеющих топологию типа «звезда», в которых обмен данными производится через базовую станцию, в отдельно взятой точке могут приниматься только данные, передаваемые в одном направлении (от базовой станции к удаленному объекту). Это связано с принципами построения сети, в которой базовая станция разворачивается на возвышенности и имеет высоко подвешенную приемо-передающую антенну, что обеспечивает возможность организации связи со всеми удаленными станциями сети. Для организации перехвата используемое для него оборудование необходимо разместить на такой же выгодной позиции, что в большинстве случаев оказывается невозможным. В противном случае обеспечивается перехват только данных от базовой станции, которые в большинстве стационарных технологических радиосетей представляют наименьший с точки зрения перехвата интерес (например, запросы, которые дают минимальное представление о работе информационной системы). И, наконец, в отличие от проводных сетей обмена данными, где кабельная инфраструктура и аппаратура для ретрансляции сигналов распределены на больших территориях, радиооборудование для передачи данных может быть полностью развернуто в охраняемых помещениях, физический доступ в которые строго ограничен.

Совокупность всех перечисленных выше качеств делает радиосети обмена данными более безопасными в части перехвата данных по сравнению с технологическими проводными сетями связи и обмена данными.

Устойчивость к несанкционированному подключению

При подключении к сети обмена данными обычно ставится цель получения доступа для работы в составе информационной системы или «просмотра» передаваемых данных. Для решения этой задачи требуется соответствующий терминал, поддерживающий используемые в сети обмена данными протоколы. Такой терминал может быть легко реализован на базе современного компьютера, но решение второй части задачи представляется не таким простым.

Перечисленные выше трудности, возникающие при организации перехвата, возникают и при попытке получить доступ к работе в составе сети обмена данными. Кратко описанные ниже свойства применяемых протоколов связи и обмена данными в равной степени относятся к радио- и проводным сетям и характеризуют их способности по обеспечению безопасности информации.

Большинство коммерческих пользователей синхронных систем (например, банков) используют протоколы «опроса» (например, синхронный протокол SDLC), в которых заложены определенные возможности по обеспечению безопасности. Чтобы терминал распознавался системой, он должен быть внесен в «опросную таблицу», которая ведется и поддерживается на центральном компьютере. Несмотря на то, что система может самостоятельно распознавать новые терминалы и автоматически вносить их в таблицу, содержание таблицы постоянно контролируется администратором сети и специальными программами, которые могут локализовать нового пользователя, получившего доступ к системе, и предпринять соответствующие меры по исключению возможности его работы в составе информационной системы. Если терминал не будет внесен в таблицу, он не сможет работать в составе сети.

Значительная часть стационарных технологических радиосетей (например, технологические радиосети управления телемеханикой на объектах топливно-энергетического комплекса) используются для обслуживания строго определенного количества терминалов, поэтому появление в их составе новых терминалов вообще не предусматривается.

Возможно, что профессиональный крэкер[5] или хакер сможет перепрограммировать компьютер таким образом, чтобы получать данные без внесения дополнительного адреса в «опросную таблицу», однако в этом случае он не сможет передавать свои данные в центральный компьютер (что в большинстве случаев является основной целью).

Попытки работы через технологическую радиосеть обмена данными под «прикрытием» другого терминала за счет дублирования его идентификационного номера приводят к генерации некорректных данных и подтверждений, получаемых центральным компьютером. Этот факт незамедлительно привлечет внимание администратора сети. На данном этапе достаточно просто выявить попытку получения несанкционированного доступа к работе в сети и предпринять соответствующие меры для предоставления контролируемой работы или предотвращения доступа к сети. Поскольку основным условием успешного проникновения в сеть является скрытность, уже сам факт выявления попытки несанкционированного доступа делает его дальнейшие действия бессмысленными.

На практике выявить и локализовать несанкционированную работу в технологической радиосети обмена данными намного проще, чем в проводной системе связи. В случае предоставления крэкеру или хакеру возможности продолжения контролируемой работы в сети, излучаемые его приемопередатчиком сигналы при посылке запросов и подтверждении приема сообщений могут быть легко запеленгованы (поскольку работа в сети управляется с базовой станции администратором, последний может инициировать работу передатчика злоумышленника с необходимой периодичностью), что существенно проще, чем определить точку подключения к проводной сети обмена данными.

Устойчивость к подавлению и воздействию помех

Подавление или намеренная постановка помех работе радиосистемы — задача существенно более сложная, чем физическое нарушение соединения в проводной системе, и для большинства коммерческих систем маловероятна.

Подверженность радиосигналов воздействию помех и возможность их подавления являются непреложным фактом. Однако для выполнения этой задачи необходимо знать номинал рабочей частоты системы обмена данными, установить который не так просто, поскольку передача ведется короткими сеансами. Факт появления помех немедленно выявляется администратором радиосети, а источник излучения становится объектом пеленгования и локализации, в том числе при поддержке соответствующих организаций, контролирующих использование радиочастотного спектра.

Поэтому гораздо проще незаметно перекусить кусачками пару проводов, чем поставить помеху радиосистеме, используя сложное и дорогостоящее специализированное оборудование, серьезно рискуя при этом быть пойманным. Работа кусачками займет не более 30 секунд, а установка и использование специального оборудования радиопротиводействия требует времени и крупных финансовых затрат, но при этом его воздействие не может быть продолжительным.

Подвижные радиосети

Подвижные технологические радиосети обмена данными подвергаются тем же угрозам, что и стационарные. Однако степень этих угроз существенно выше, поскольку удаленные объекты постоянно перемещаются, и контроль за ними оказывается более сложным, причем количество одновременно работающих в составе подвижной радиосети пользователей динамически изменяется. В подвижных радиосетях более высока угроза утраты радиотехнического оборудования и его использования для несанкционированного доступа к радиосети.

Устойчивость к перехвату

Практический опыт эксплуатации подвижных технологических радиосетей обмена данными

[5]Крэкер (англ. cracker) — тип компьютерного взломщика: человек, взламывающий системы защит информационных систем или создающий программные средства для взлома систем защит. Вне профессиональной среды применяется общий термин «компьютерный взломщик» или чаще «хакер», что также часто не является правильным. В абсолютном большинстве случаев «крэкер» не располагает исходным кодом программы, поэтому программа изучается связкой дизассемблера и отладчика с применением специальных утилит.

позволяет рассмотреть возможные угрозы на примере двух наиболее типовых ситуаций:

- целенаправленный перехват;
- угон служебного автомобиля, оснащенного бортовым радиотехническим оборудованием для работы в составе радиосети.

Необходимо отметить, что в современных технологических подвижных радиосетях обмена данными используется схема централизованного управления радиосетью, а все данные передаются через базовые станции. В них применяется асимметричная схема адресации, то есть аппаратура базовой станции и подвижного объекта ведут себя по-разному, а сообщения, передаваемые в эфир одним подвижным объектом, не могут приниматься и использоваться другим без «разрешения» базовой станции. Таким образом, архитектура подвижной технологической радиосети обладает определенными свойствами, повышающими ее надежность и живучесть в условиях внешних воздействий.

Целенаправленный перехват

Организация перехвата сообщений в подвижной радиосети обмена данными связана с теми же трудностями, что и в стационарной. Дополнительные «препоны» создаются путем использования уникальных адресов, которые «прошиваются» в радиотехническую аппаратуру в заводских условиях и не могут быть изменены пользователем. Каждый радиомодем для подвижного объекта имеет несколько адресов (индивидуальный, групповой и циркулярный). Все сообщения, за исключением циркулярных, направляются в адрес строго определенного пользователя и не могут приниматься другим радиомодемом, работающим в составе радиосети.

Таким образом, даже при наличии незарегистрированного в радиосети комплекта бортового радиотехнического оборудования, можно получить доступ только к циркулярным сообщениям, транслируемым базовой станцией. Комплект базового оборудования теоретически позволяет принимать адресованные базовой станции сообщения. Однако для этого необходимо сменить адрес имеющегося базового радиомодема на адрес радиомодема, реально используемого в составе радиосети, и развернуть оборудование в точке, обеспечивающей прием сообщений от всех или хотя бы от значительной части подвижных объектов, работающих в достаточно большой зоне. Но даже в этом случае эффект от перехвата данных будет мизерным, поскольку основную оперативную ценность в большинстве подвижных технологических радиосетей представляют исходящие данные (управляющие сигналы, команды, распоряжения, результаты обработки обращений к базам данных и т. д.), передаваемые в адрес мобильных пользователей со стороны базовой станции.

Дополнительная безопасность обеспечивается в том числе парольной защитой и закрытием данных. И хотя такое препятствие не может рассматриваться как серьезное для специалиста, оно достаточно надежно страхует от «случайного доступа». Обеспечение более высокого уровня безопасности информации достигается за счет применения штатной аппаратуры шифрования.

Угон служебного автомобиля с подключенным к радиосети радиотехническим оборудованием

В случае угона служебного автомобиля при включении установленного в нем оборудования невозможно получить такой же полный доступ ко всей информации, как в голосовой радиосети. В отличие от конвенциональных голосовых радиосетей, где каждый подключившийся к сети пользователь может принимать циркулирующие в ней сообщения, в радиосетях обмена данными это полностью исключено.

Поскольку устанавливаемый на подвижных объектах радиомодем имеет свой уникальный адрес, он может принимать только общие циркулярные сообщения и сообщения, адресованные только данному подвижному объекту в составе группы или индивидуально. Но, получив сообщение об угоне служебного автомобиля, администратор информационной системы может оперативно исключить адрес установленного на нем оборудования из общего списка адресов, предотвратив тем самым передачу данных на установленный в угнанном автомобиле компьютер. Передача циркулярных сообщений на период локализации ситуации с угоном служебного автомобиля также может быть временно прекращена, а доведение данных до остальных пользователей — производиться с использованием групповых и индивидуальных адресов.

Поскольку управление работой всей сети обмена данными строго централизовано и происходит дистанционно с базовой станции, аппаратура на угнанном автомобиле может быть просто отключена. Факт блокировки радиомодема легко подтверждается, поскольку каждая переданная в его адрес команда автоматически контролируется и фиксируется. В этом случае передача циркулярных сообщений в радиосети обмена данными может беспрепятственно продолжаться.

В некоторых реально действующих системах реализована специальная функция, обеспечивающая трансляцию на компьютер в похищенном автомобиле ложных сообщений, имитирующих реальный радиообмен, что позволяет ввести похитителя в заблуждение и, в большинстве случаев, побудить к выполнению действий, направленных на его задержание.

В современных системах, использующих навигационные средства, обеспечивается автоматическая передача диспетчеру данных о местоположении подвижного объекта. Таким образом, в случае угона служебного автомобиля администратор радиосети имеет возможность дистанционно его контролировать. Поскольку управление работой бортовой аппаратуры и передачей навигационной информации с подвижного объекта также производится дистанционно через базовую станцию, имеется возможность изменения режима ее работы в сторону увеличения интенсивности трансляции навигационных данных с борта угнанного автомобиля, что опять же способствует задержанию угонщика и возврату автомобиля.

Несанкционированное подключение

Целью «криминального» подключения к подвижной технологической радиосети обмена данными в большинстве случаев является получение доступа к базам данных или просто «просмотр» передаваемых данных. Эта задача решается с использованием соответствующего специального оборудования, поддерживающего применяемые в радиосети обмена данными протоколы. Получить в распоряжение такое оборудование достаточно просто, но решение второй части задачи представляется существенно более сложным.

Перечисленные выше трудности, возникающие при попытке незаконно использовать полученное оборудование для целенаправленного перехвата, сопровождают и попытку получить доступ к работе в составе подвижной радиосети обмена данными. Применяемая схема адресации исключает возможность подключения к сети обмена данными нового пользователя без автоматического уведомления администратора радиосети. Несмотря на то, что функционально оборудование для подвижных радиосетей обмена данными обеспечивает динамическое подключение к сети новых пользователей, информация о вновь появившихся адресах фиксируется и анализируется, что позволяет предпринять любые ответные действия из описанных выше. Поскольку изменение «прошитого» в заводских условиях адреса подвижного радиомодема невозможно, а сам он является уникальным для каждого устройства, оказывается невозможным организовать «незаконную» работу под одним из адресов, официально «прописанных» в системе.

Кроме того, в этой ситуации достаточно просто запеленговать передатчик «нового пользователя», предоставив ему контролируемый доступ в систему на период, необходимый для проведения мероприятий по его локализации и задержанию либо дезинформированию. При этом для упрощения процесса пеленгования можно легко организовать интенсивную передачу данных со стороны компьютера «нового пользователя».

Устойчивость к подавлению и воздействию помех

Трудности по постановке помех для стационарных радиосетей обмена данными в полном объеме относятся и к подвижным радиосетям. Поток цифровых данных в подвижных технологических радиосетях более устойчив к воздействию помех по сравнению с речевыми сообщениями вообще, а серьезная устойчивость к воздействию помех дополнительно обеспечивается встроенными функциями контроля и коррекции ошибки. Применяемые в составе подвижных радиосетей обмена данными технические средства имеют более высокую, по сравнению со стационарными радиосетями, выходную мощность, что также осложняет их подавление.

Целенаправленное подавление сигналов подвижных радиосетей связано с еще бóльшими трудностями, если они имеют в своем составе несколько базовых станций и, тем более, если соседние базовые станции имеют полностью перекрывающиеся оперативные зоны. Поскольку

передатчик помех всегда будет иметь меньшую зону охвата, значительная часть технологической радиосети обмена данными будет продолжать функционировать даже в случае полного подавления одной из базовых станций.

Физическая безопасность технологической радиосети

Обеспечение безопасности данных, передаваемых по кабельной линии связи, необходимо на всей ее протяженности. В случае с технологической радиосетью обмена данными достаточно защитить отдельные помещения, в которых размещается приемопередающая аппаратура.

Таким образом, первое впечатление действительно обманчиво: «присущая» кабельным системам связи и обмена данными безопасность информации — такой же миф, как и слабая защита данных в технологических радиосетях. Высокий уровень защиты передаваемых в технологических радиосетях данных обеспечивает их высокую надежность и живучесть.

Технология параллельного декодирования (интеллектуального объединения радиосигналов) как средство повышения надежности и живучести технологических радиосетей обмена данными

Современные подвижные узкополосные технологические радиосети обмена данными строятся на специализированном оборудовании, позволяющем наряду с увеличением их пропускной способности поддерживать высокие характеристики надежности и живучести. Функционирование таких радиосетей организуется, как правило, на базе IP-протокола, что обеспечивает их совместимость с любым программным обеспечением, поддерживающим этот протокол.

Использование IP-протокола стало возможным и целесообразным только после достижения достаточно высоких скоростей обмена данными в радиосети (выше 19,2 кбит/с)[6]. Однако повышение скорости обмена связано с решением ряда технических задач. Известно, что увеличение скорости обмена данными требует дополнительных энергетических затрат. Расчеты и практические измерения показывают, что, при прочих равных условиях, радиосеть обмена данными, работающая на скорости 19,2 кбит/с, имеет рабочую зону примерно в четыре раза меньше, чем аналогичная радиосеть, работающая на скорости 4,8 кбит/с, при одинаковом соотношении сигнал/шум. При удвоении скорости для обеспечения той же чувствительности необходимо увеличить мощность выходного сигнала на 3 дБ. Увеличение скорости обмена данными с 4,8 до 19,2 кбит/с приводит к минимально возможной потере чувствительности в 6 дБ или выходной мощности в четыре раза.

На практике потери составляют около 9 дБ, поскольку теоретический минимум потерь рассчитан для идеальных условий распространения сигнала. Компенсация потери в 9 дБ требует увеличения выходной мощности применяемой аппаратуры примерно в восемь раз, или до 250 Вт для подвижного объекта и 800 Вт для базовой станции. Использование таких мощностей в реальных системах невозможно. Потери в 9 дБ относятся к стационарным системам. Значение этого параметра еще более возрастает в подвижных системах, где более ощутимо влияние эффекта замирания в результате многолучевого распространения сигнала.

Взаимосвязь скорости обмена данными и соотношения сигнал/шум хорошо известна. Более 50 лет назад она была описана в теореме Шеннона, а приведенный выше вывод подтверждается расчетами, выполненными по следующей формуле:

$$C = BW\mathrm{Log}2\times(1+S/N),$$

где

C — пропускная способность канала (бод);

BW — ширина канала (Гц);

S/N — соотношение сигнал/шум.

Даже не выполняя операцию с логарифмами, можно легко заметить, что если соотношение сигнал/шум равно 1, пропускная способность канала равна BW, а если соотношение сигнал/шум равно 3, то пропускная способность канала равна $2BW$ (удваивается). Другими словами, при увеличении соотношения сигнал/шум увеличивается пропускная способность канала передачи данных. И наоборот, при уменьшении соотношения сигнал/шум пропускная способность канала уменьшается.

Отношение энергетических затрат на бит данных в зависимости от уровня шума можно определить по следующей формуле:

$$Eb/N_0 = (S/N)\times(W/R),$$

где

Eb/N_0 — отношение энергетических затрат на бит данных в зависимости от уровня шума;

S/N — соотношение сигнал/шум несущей частоты;

W — ширина канала (Гц);

R — скорость передачи (бит).

Для упрощения расчетов можно предположить, что $S/N = 1$ и $W/R = 1$. В этом случае значение $Eb/N_0 = 1$. Таким образом, при прочих равных условиях, в случае удвоения скорости передачи R до $2R$ величина Eb/N_0 будет равна 0,5. Переведя ее в дБ (мощность сигнала), получаем значение 3 дБ. Другими словами, на передаче одного бита данных теряются 3 дБ. Для достижения одинаковой производительности системы необходимо увеличить значение соотношения сигнал/шум на 3 дБ либо увеличить ширину канала до 2 В, то есть удвоить ее.

Если величина Eb/N_0 не увеличивается, то это приводит к возрастанию вероятности ошибок при передаче. Для обеспечения заданного числа минимальных вероятных ошибок в случае увеличения скорости передачи необходимо увеличить ширину канала или мощность сигнала, либо обоих параметров одновременно.

Поскольку ширина канала является величиной постоянной, единственным способом обеспечить минимально допустимый уровень ошибок при передаче является увеличение соотношения сигнал/шум. В этом случае для компенсации потерь, например, в 8 дБ, теоретически необходимо увеличить мощность сигнала в 6,3 раза. То есть, если в системе со скоростью обмена данными 4,8 кбит/с удовлетворительная работа обеспечивается при использовании передатчика мощностью 25 Вт, то для работы с такой же достоверностью доведения данных на скорости 19,2 кбит/с потребуется передатчик мощностью более 150 Вт.

Как следует из представленных выше расчетов, увеличение мощности передатчика нельзя назвать эффективным решением. Но можно увеличить количество базовых станций при уменьшении оперативной зоны каждой из них (как это делается в сотовой связи). В этом случае потери мощности сигнала при передаче снижаются, поскольку мобильные пользователи находятся на более близком расстоянии от базовой станции. При этом для рассмотренного выше варианта, в котором потери мощности сигнала составляют 8–9 дБ, число базовых станций, которые смогут обеспечить работу в заданной зоне на скорости 19,2 кбит/с, должно быть увеличено в четыре раза по сравнению с аналогичной системой, работающей на скорости 4,8 кбит/с.

Как правило, владелец технологической радиосети обмена данными имеет ограниченные возможности по расширению базовой инфраструктуры, которая связана, в частности, с дополнительными затратами на обеспечение безопасности системы и увеличением эксплуатационных затрат. В связи с этим в современных технологических радиосетях применяется специализированное оборудование, реализующее методы работы и алгоритмы обработки сигналов, позволяющие сохранить приемлемые размеры оперативной зоны базовой станции при наращивании скорости обмена данными.

Наряду с сокращением оперативной зоны базовой станции возрастает количество ошибок при передаче, которые обусловлены замиранием сигнала при многолучевом распространении, поскольку радиоволны достигают приемной антенны, проходя путь различной длины. Одни сигналы приходят в точку приема по прямой, другие — многократно отражаясь от различных предметов (зданий, складок местности, автомобилей и т. д.). Такая ситуация наиболее типична для крупных городов.

Замирание сигнала возникает в результате того, что различные радиосигналы, проходя различное расстояние и достигая приемной антенны в различное время, усиливают или, наоборот, подавляют друг друга. Обычно подавление сигнала составляет 30 дБ (то есть коэффициент подавления составляет 1000). Любой пользователь сотового телефона ощущал помехи от замирания сигнала. Изменение положения «мобильника» всего на несколько десятков сантиметров может очень сильно повлиять на качество принимаемого сигнала. Обмен данными подвержен более серьезному воздействию «затухания» по сравнению с речевым обменом.

В определенной степени влияние затухания сигнала может быть компенсировано путем восстановления потерянных во время передачи данных. Оно производится за счет избыточности данных, добавляемых к исходному

[6] Далее в расчетах принимается скорость обмена данными, равная 19 200 бит/с, как минимально целесообразная для организации обмена данными по IP-протоколу.

сообщению перед его передачей. Эта технология, получившая наименование «коррекция ошибки» (FEC — Forward Error Correction), основывается на том, что лучше пожертвовать частью пропускной способности радиоканала и передать сообщение увеличенного объема, чем повторно передавать сообщение полностью (в последнем случае потери пропускной способности радиосети и задержки в доставке данных будут значительно выше).

Как и любая другая, технология коррекция ошибки имеет свои ограничения. На определенном этапе объем избыточных данных, необходимых для надежной передачи сообщения, приводит к заметному снижению эффективности работы радиосети и увеличению накладных расходов, поскольку наиболее мощные алгоритмы коррекции ошибок требуют увеличения объема исходного сообщения в два раза. С увеличением скорости обмена возрастает и объем избыточных данных, необходимых для восстановления переданного сообщения, поскольку удвоение скорости приводит к удвоению потерь в результате затухания. Таким образом, при увеличении скорости обмена данными с 9,6 до 19,2 кбит/с для компенсации этого эффекта необходимо увеличить объем избыточных данных в четыре раза. В случае использования IP-протокола объем передаваемых в радиосети данных существенно увеличивается за счет служебной информации, связанной с этой технологией. Все это ведет к заметному снижению эффективности радиоканала с точки зрения его пропускной способности.

Оборудование нового поколения Dataradio Paragon/Gemini и ParagonG3/GeminiG3

Технические проблемы, связанные с наращиванием скорости обмена данными, получили решение в современных образцах радиомодемов, использующих технологию «параллельного декодирования/интеллектуального объединения» радиосигналов (Parallel Decoding/Smart Combining). Затухание радиосигнала возникает в определенных точках оперативной зоны базовой станции. На практике расположение таких точек определяется комбинацией сигналов, принимаемых в заданной точке оперативной зоны, и соотносится с длиной их волны. Если использовать два приемника с двумя разнесенными антеннами, то вероятность одновременного попадания двух антенн в точку затухания сигнала существенно снижается. Другими словами, если одна антенна попадет в зону затухания сигнала, вторая, как правило, будет находиться вне этой зоны.

Впервые данный принцип был реализован в радиомодемах Paragon/Gemini и получил дальнейшее развитие в радиомодемах ParagonG3/GeminiG3. Пространственное разнесение приемных антенн не является новым методом, но представляется чрезвычайно эффективным. Радиомодемы оснащены двумя приемниками с антеннами, позволяющими использовать данный принцип.

Пространственно разнесенный прием может быть реализован двумя способами. Наиболее известной и широко применяемой является коммутация, при которой из двух поступающих от приемных антенн сигналов детектируется только наиболее мощный. Данный способ позволяет увеличить процент успешно принятых сообщений, но на этом его преимущества и заканчиваются.

Таблица 5. Практические результаты оценки эффективности технологии параллельного декодирования/интеллектуального объединения

Модель затухания	Один приемник	Два приемника (PD)	Разница
Стационарный прием	−110,7 дБм	−113,5 дБм	2,8 дБм
Городская застройка	−98,7 дБм	−108,2 дБм	9,5 дБм
Сельская местность	−99,5 дБм	−109,5 дБм	10 дБм
Пересеченная местность	−99,3 дБм	−108,5 дБм	9,2 дБм

Разработчики вышеуказанных радиомодемов создали и запатентовали более совершенный способ, позволяющий использовать одновременно оба принимаемых сигнала. Одновременное использование двух потоков данных позволяет почти в два раза (реально — в 1,91) увеличить чувствительность приемника независимо от влияния эффекта затухания сигнала. Эта технология и получила наименование «параллельное декодирование/интеллектуальное объединение». В результате одновременного приема сигнала на две антенны становится возможным использовать их в различных комбинациях, а не просто выбирать наиболее мощный. Разработанная компанией технология «интеллектуального объединения» позволяет применять различные алгоритмы обработки — в зависимости от относительной мощности и тренда (тенденции изменения) параллельно принятых сигналов. Например, если более мощный сигнал имеет тенденцию к ослаблению, предпочтение отдается менее мощному сигналу достаточной интенсивности, имеющему тенденцию к усилению.

Практические результаты оценки эффективности технологии параллельного декодирования/интеллектуального объединения представлены в таблице 5. Эти данные демонстрируют преимущества рассматриваемой технологии при сравнении с работой аналогичной радиоприемной системы, использующей одну антенну, в различных условиях приема. Сравнение производилось для условий успешного приема 99% сообщений длиной 800 бит каждое.

Как видно из таблицы, радиомодемы Paragon и Gemini позволяют улучшить параметры принимаемого сигнала практически на 10 дБм, что соответствует увеличению мощности передатчика базовой станции в аналогичной по характеристикам радиосети в 10 раз. Это обеспечивает расширение зоны уверенного приема радиосигнала без использования дополнительных базовых станций. В случае, когда необходимость расширения зоны электромагнитной доступности отсутствует, рассматриваемая технология позволяет серьезно увеличить надежность радиосети и ее живучесть, поскольку обеспечивает увеличение процента корректно принимаемых с первой попытки сообщений, в том числе в сложной помеховой обстановке. Размер оперативной зоны и сокращение количества повторно передаваемых сообщений приводит к существенному росту пропускной способности и сокращению времени реакции системы. В случае возникновения необходимости повторной передачи сообщений в радиосети обмена данными, работающей на скорости 19,2 кбит/с, ее пропускная способность для отдельных видов данных (коротких сообщений) может сократиться в 10 раз.

Другим фактором, влияющим на снижение пропускной способности, является избыточная информация, необходимая для реализации функции коррекции ошибок. Нельзя считать корректным утверждение типа: «Наш протокол использует алгоритм коррекции ошибки, имеющий 25% избыточности, поэтому пропускная способность в нашей радиосети составляет 19,2×0,75 = 14,4 кбит/с». Такое утверждение в принципе соответствует действительности, но только частично.

В простых расчетах, подобных приведенному выше, игнорируются многие важные факторы, которые должны учитываться при оценке пропускной способности. К ним, в частности, относятся адресация, порядковые номера пакетов данных, алгоритмы обнаружения ошибки и подтверждения приема сообщений. Все данные, которые добавляются к информационному сообщению не пользователем, а средствами системы (не только избыточные данные, необходимые для реализации функции коррекции ошибки), являются непроизводительными (служебными) и отражаются на ее пропускной способности.

Не менее серьезное влияние на пропускную способность оказывает время «атаки» передатчика (набор передатчиком мощности, необходимой для начала передачи данных, PTT — Power To Transmit) и стабилизации по частоте. Этот важный компонент «накладных расходов» очень часто недооценивается, поскольку он не оказывает серьезного влияния на работу речевых каналов связи, где процесс нажатия тангенты радиостанции и начала передачи речевого сообщения занимает не менее четверти секунды. В случае с обменом данными все обстоит иначе.

Для иллюстрации этого были проведены сравнительные испытания радиомодема Gemini (время «атаки» — менее 10 мс) и другого радиомодема с аналогичными параметрами, подключенного к серийно выпускаемой современной мобильной радиостанции одного из ведущих производителей оборудования этого класса (время «атаки» передатчика — 80 мс). В обоих случаях передавались одинаковые сообщения. В результате модель Gemini затратила на передачу 52 мс, а ее «соперница» — 87 мс, или на 40% больше. При скорости обмена данными 19,2 кбит/с это соответствует дополнительной пропускной способности, равной 7680 бит/с.

Таким образом, повышение скорости обмена данными в узкополосных радиосетях, работающих в УКВ-диапазоне, связано с решением комплекса проблем, обусловленных необходимостью сохранения размеров зоны уверенного приема и поддержанием высокой пропускной способности. Эта задача может эффективно решаться благодаря современным технологиям, реализованным в специализированном оборудовании и позволяющим обеспечить достаточно высокий уровень надежности и живучести технологических радиосетей обмена данными.