Создание эффективных каналов управления устройствами GSM/GPRS через Интернет

Александр Елисеев (г. Вильнюс, Литва)

В статье приведён обзор технологий управления через Интернет встраиваемыми устройствами, оборудованными модемами GSM/GPRS. На примерах описаны методы преодоления ограничений, обусловленных межсетевыми экранами и серверами трансляции адресов (NAT).

Многие разработчики хотели бы эффективно управлять удалёнными устройствами через Интернет. Однако надёжная связь по глобальной сети через десятки маршрутизаторов и сред распространения сигналов является сложной задачей, особенно на больших расстояниях и через границы государств. Технология GSM/GPRS успешно решает проблему покрытия и глобализации управления, но устанавливает ограничения на пропускную способность, способы доступа по протоколу TCP/IP и вынуждает оптимизировать стоимость передачи данных.

Проблемы с протоколом связи TCP/IP или наложение ограничений на его работу вызывают некачественное функционирование или отказы прикладных программ, таких как web-браузеры, FTP-клиенты, почтовые клиенты, Telnet и т.д. И если на настольном компьютере или ноутбуке пользователь может предпринять ряд действий по устранению неполадок, включая смену коммуникационного канала, переустановку ПО и обращение в сервисный центр, то встраиваемое устройство должно автоматически настроиться для установления связи, не «надеясь» на помощь извне.

Разработчики встраиваемых устройств, естественно, не могут создать более «интеллектуальные» программы, чем работающие на персональных компьютерах, поэтому они вынуждены идти на компромиссы, ограничивающие возможности и выбор используемых технологий связи. Ниже мы опишем некоторые методы реализации интернет-каналов связи поверх GPRS.

Модемы GPRS

Технология GPRS, как известно, обеспечивает пакетную передачу данных на базе GSM-связи. Сегодня редкий GSM-модем не является одновременно и GPRS-модемом. Эти модемы получили широкое распространение и значительно дешевле модемов, поддерживающих технологии 3G и EDGE. Сети GSM повсеместно предлагают услугу GPRS, чего нельзя сказать про EDGE и, тем более, 3G. Максимальная пропускная способность канала GPRS составляет 48 Кбит/с.

Модемы GPRS могут иметь встроенный стек протоколов TCP/IP либо прозрачно пропускать трафик TCP/IP. В последнем случае GPRS-модемы используют протокол PPP в качестве контейнера для пакетов TCP/IP. С помощью сервисов встроенного в модемы протокола PPP внешние устройства могут получить информацию об IP-адресе, который получил модем от оператора, и IP-адресе шлюза оператора в Интернете.

Адрес, полученный модемом от оператора, может быть либо публичным, либо частным – это зависит от плана подключения для конкретной SIM-карты и особенностей сети оператора. Как правило, адрес назначается из пула частных адресов, если SIM-карта приобретена без дополнительных условий. Частные адреса находятся в трёх диапазонах (в шестнадцатеричном представлении): 0A.xx.xx.xx; AC.1x.xx.xx; C0.A8.xx.xx.

Устройство, имея частный адрес, не может указывать его как адрес отправителя при посылке пакетов в Интернет. Обратный адрес должен быть публичным, иначе до устройства не дойдёт ответ адресата и станет невозможной двухсторонняя связь. Для решения этой проблемы в сети оператора связи существуют специальные серверы трансляции адресов (NAT).

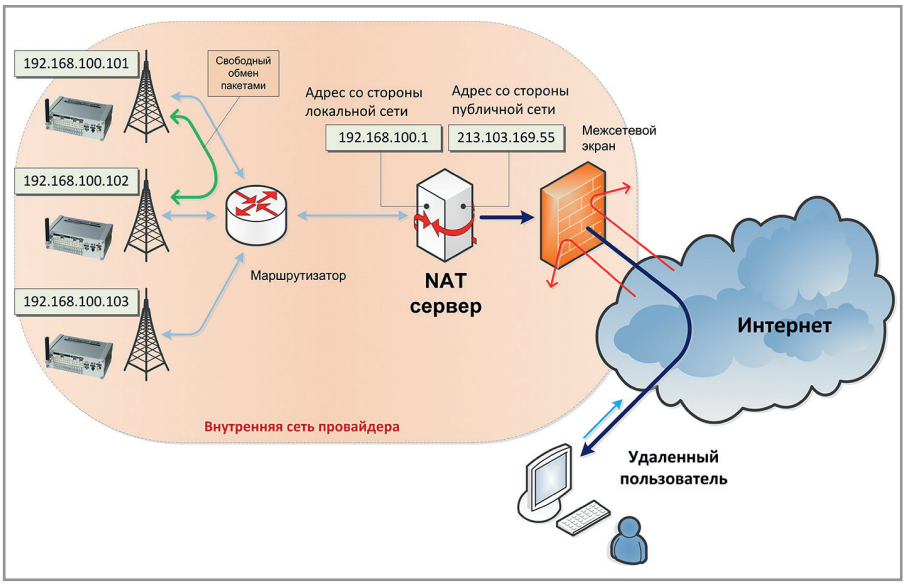

Рис. 1. Структурная схема сети оператора связи

Трансляторы сетевых адресов

В этом году во всемирной сети закончились свободные публичные IP-адреса, основанные на протоколе IPv4; переход на протокол IPv6 затягивается, но при этом количество клиентов, желающих использовать Интернет как инструмент удалённого управления, непрерывно растёт. Дефицит публичных адресов является серьёзным препятствием на пути развития сервисов управления встраиваемыми устройствами.

На рисунке 1 показана типичная структурная схема сети оператора мо-

бильной связи с точки зрения внешнего пользователя. Когда оператор выделяет GPRS-модему частный IP-адрес, это означает, что в сети работает сервер NAT, задачей которого является преобразование частных адресов в публичные и обратно при обмене данными между Интернетом и сетью оператора. Целью применения NAT является экономия публичных адресов, поскольку у оператора есть ограниченный пул публичных адресов, а приобрести дополнительные адреса скоро станет практически невозможно. Экономия достигается за счёт того, что публичные адреса назначаются не устройствам в сети оператора, а только серверам NAT. Внутри сети оператора применяются только частные адреса. Маршрутизатор в сети оператора по адресу назначения определяет, когда IP-пакеты надо направлять серверу NAT, а когда – другим узлам во внутренней сети.

Обычно GPRS-модемы, присоединённые к одной сети оператора и с одинаковым параметром APN (задаётся при установлении соединения), могут общаться между собой беспрепятственно, используя частные адреса. Однако внутренняя сеть оператора может быть поделена на несколько подсетей, и тогда, попав в разные подсети, GPRS-модемы не смогут установить между собой связь по внутренним адресам. Поскольку динамические IP-адреса модемам выделяются случайным образом, то случайным образом может появляться возможность соединения модемов между собой по внутренней сети. Поэтому соединение по частным адресам внутри сети оператора не может рассматриваться как универсальный и надёжный канал управления устройствами.

Принцип работы сервера NAT достаточно прост, если рассматривать его на уровне отдельных TCP/IP-соединений. На рисунке 2 проиллюстрирована передача пакета TCP из внутренней сети оператора в Интернет. Пакет содержит IP-заголовок и TCP-заголовок. Сервер NAT заменяет в IP-заголовке обратный частный адрес устройства на свой публичный адрес из пула публичных адресов, находящихся в собственности провайдера. Затем в TCP-заголовке сер-

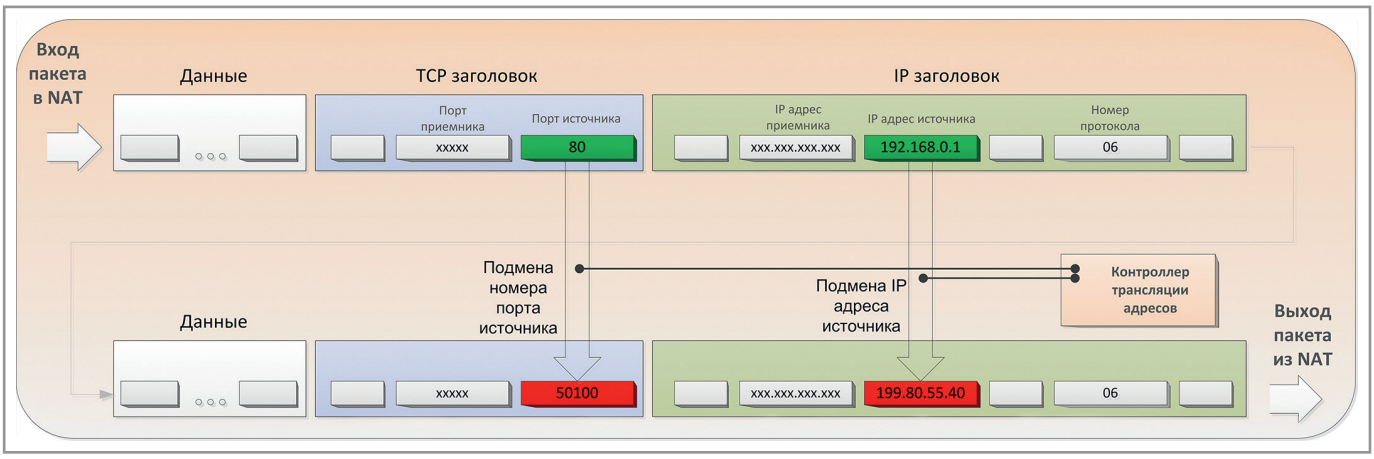

Рис. 2. Принцип работы сервера NAT при передаче пакета TCP в Интернет

вер NAT заменяет номер порта источника на другой, из пула свободных внешних портов для выбранного публичного IP-адреса.

Трансляция внутренних, частных IP-адресов через один публичный во многом становится возможной именно из-за наличия такого атрибута адресации, как номер порта в пакетах TCP. Когда по Интернету приходит ответ от удалённой стороны, серверу NAT достаточно провести обратный поиск в таблице подмен по номеру порта назначения из полученного пакета, чтобы узнать TCP-порт и IP-адрес узла во внутренней сети, которому предназначается пакет. Каждая новая запись в таблице подмен появляется, когда устройство во внутренней сети инициирует связь с удалённым узлом в Интернете. Запись удаляется, если в течение определённого времени не было обмена данными либо после явного разрыва связи узлами. Сервер NAT способен анализировать состояние каждого логического TCP-соединения, проходящего через него, и определять фазы установления и прекращения соединений.

Всё сказанное в равной мере относится и к пакетам UDP, которые также имеют атрибут адресации в виде номера порта. Однако это не означает, что сервер NAT способен пропускать только пакеты TCP и UDP; в других протоколах поверх IP могут быть переданы различные атрибуты, уникально доопределяющие источник во внутренней сети. Например, команда PING протокола ICMP имеет уникальный атрибут Sequence number, который может быть выбран сервером NAT в качестве индекса для построения таблиц трансляции IP-адресов.

Модем GPRS с присвоенным ему частным адресом обязан первым начинать установление связи с другими узлами в Интернете. Инициировать связь в обратном направлении невозможно, поскольку сервер NAT пропускает только пакеты, соответствующие записи трансляции, а на момент попытки установить связь снаружи такой записи не будет. Впрочем, она может присутствовать, если предыдущий сеанс связи не был явно разорван, а первый пакет нового соединения имеет тот же номер порта и адрес IP. Но тогда в игру вступит межсетевой экран оператора, который отслеживает TCP-подключения и может осуществлять жёсткую политику безопасности, не допускающую подобных коллизий.

Итак, сервер NAT – неплохой компромисс для операторов связи, являющийся, однако, серьёзным препятствием на пути использования всего богатства протоколов и сервисов Интернета.

Управление через канал TCP, инициированный GPRS-модемом

С учётом наличия NAT, GPRS-модемы всё же имеют возможность устанавливать полнофункциональные TCP-соединения и работать, используя UDP-протокол, хотя и должны всегда первыми начинать сеанс связи. Во-первых, модемы могут свободно посылать и принимать электронную почту, осуществлять просмотр интернет-страниц, могут в пассивном режиме пересылать файлы на FTP-серверы, запрашивать информацию у серверов DNS, серверов точного времени и т.д. Значительно труднее придумать способ, чтобы «добраться» до web- или FTP-сервера на стороне самих модемов, но об этом ниже.

Для управления устройствами через GPRS, наиболее удобно использовать TCP-соединения, т.к. они гарантируют доставку данных. Использование протокола UDP менее надёжно, поскольку на уровне UDP нет контроля доставки данных, а в сетях GSM потеря пакетов или их недопустимая задержка – явление весьма регулярное. Поскольку модем инициирует соединение, то на удалённой стороне связь с модемом должен поддерживать TCP-сервер с публичным IP-адресом.

Сам по себе протокол TCP ещё не определяет, какие данные, как и когда должны посылаться или приниматься устройством. Этим должно заниматься приложение пользователя на сервере, работающее поверх протокола TCP. Такие приложения обычно создаются под конкретные задачи, и общей схемы не существует. Дело осложняется тем, что клиентом серверов приложений являются простые встраиваемые устройства, не обладающие ресурсами ПК и поэтому не поддерживающие возможности MS .NET Framework, например.

Система распределённого управления по GPRS «Полигон»

На рисунке 3 представлена реализация системы управления тактическим мобильным полигоном, разработанная в рамках исследования возможностей применения GPRS-связи. Концепция «Полигона» заключалась в том, чтобы его можно было развернуть на любом участке подготовленной местности, покрытой GPRS-связью, в кратчайшее время и гибко управлять из нескольких центров наблюдения, включая офис технической поддержки разработчика, и с мобильных пультов координаторов учений. Высокотехнологичные подъёмники, рассчитанные на автономную работу в дневное и

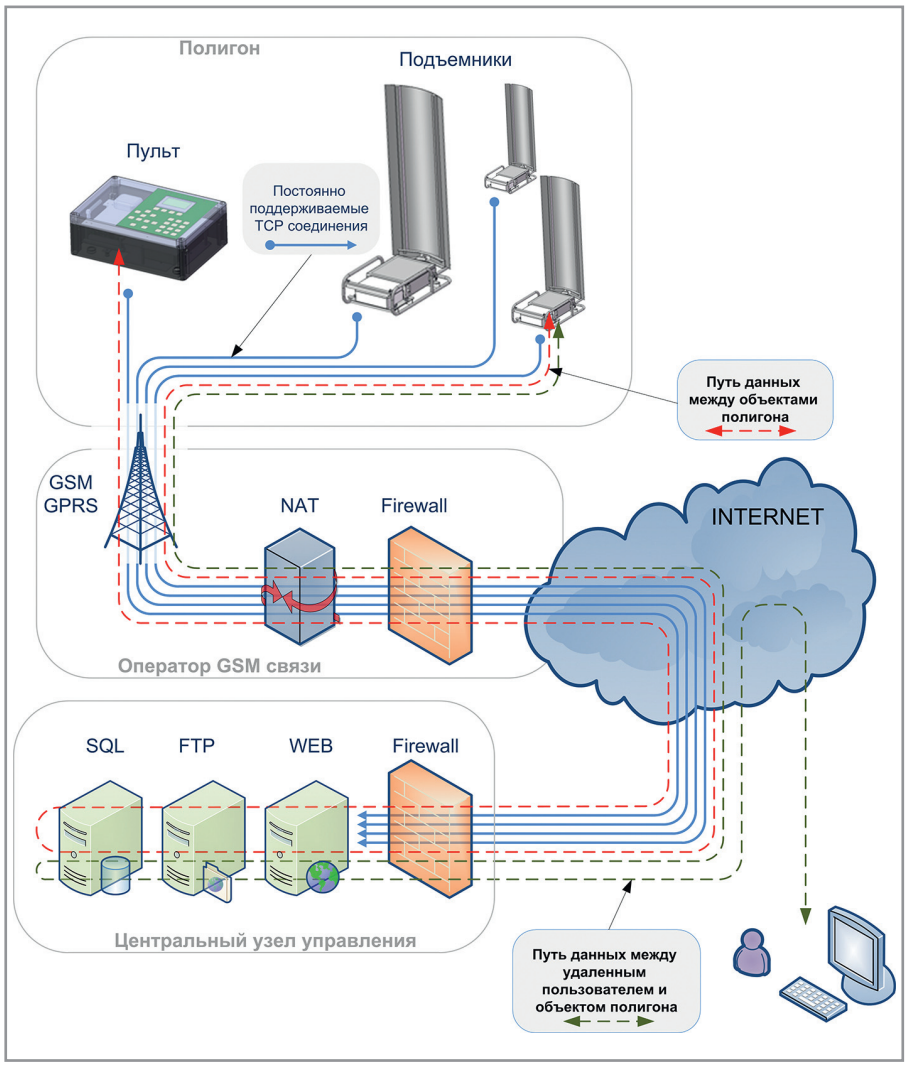

Рис. 3. Система управления «Полигон»

ночное время, со звуковыми и световыми системами имитации огня, с адаптерами автоматической системы определения координат попаданий и направлений обстрела, с возможностью подключения видеокамер и с модулями определения собственных координат требовали универсальных каналов связи для полного использования своих возможностей.

Практика управления подъёмниками допускала некоторые задержки реакции подъёмников на ручные команды, выдаваемые с пультов операторов. Эти команды в основном инициировали автоматические алгоритмы управления, реализованные в подъёмниках. При этом пульты и подъёмники соединялись через канал связи GPRS с центральным сервером приложения в офисе, который работал в режиме прослушивания запросов на TCP-подключения от объектов полигона. По требованию сервер открывал соединение и обрабатывал команды, посылаемые объектами. Обработка команд была подчинена бизнес-логике приложения. Определённые команды несли данные, предназначенные для сохранения в базе данных на сервере, другие команды транслировались подключенным к серверу объектам по определённым алгоритмам.

Таким образом, через трансляцию команд на сервере пульты могли передавать команды подъёмникам, а подъёмники – передавать информацию пультам. Маршрутизация в этом случае осуществлялась специально написанным разработчиками «Полигона» приложением. База данных сервера была реализована на основе SQL-сервера и работала в тесном взаимодействии с web-сервером, через который осуществлялся доступ из Интернета к информации о работе системы. Доступ к данным и функциям их анализа был сравнительно прост и универсален для авторизованных пользователей, в частности, для администрации полигона. Доступ мог быть осуществлён как посредством web-браузеров, так и с помощью офисных программ,

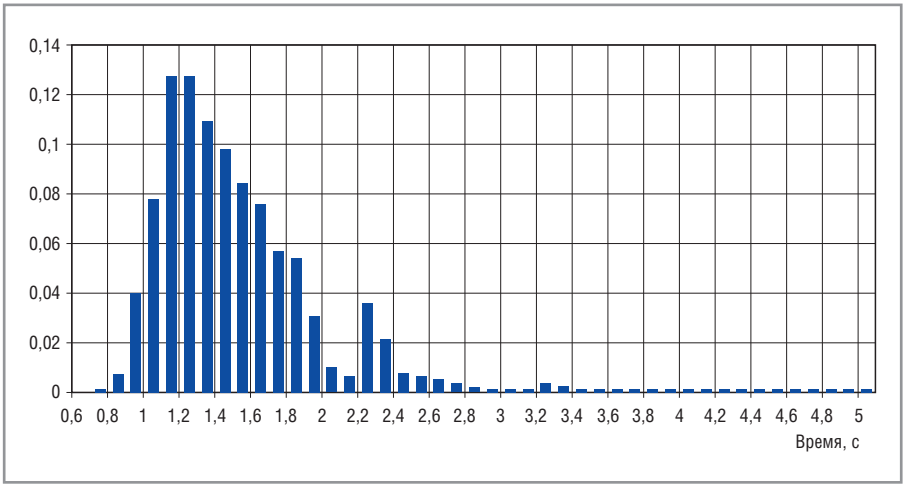

Рис. 4. Нормированная гистограмма распределения времени прохождения пакетов между объектами в системе «Полигон»

поддерживающих связывание с удалёнными SQL-серверами.

После того как мобильные объекты полигона (пульты и подъёмники) устанавливали TCP-соединение с сервером, они не разрывали его в течение всего времени работы, и таким образом создавался симметричный канал обмена асинхронными сообщениями по схеме запрос-ответ.

Чтобы определить задержку передачи команд, обусловленную использованием Интернета, по месту установки системы в течение двух суток проводились замеры с интервалом 1 мин на шести объектах с GPRS-модемами. Результаты распределения задержек показаны на рисунке 4. В сумме было передано 14 073 пакета, из которых 27 пакетов было доставлено с задержкой более 5 с.

Мобильные объекты полигона имели возможность обновлять собственное программное обеспечение путём его скачивания с внешних FTP-серверов. Также объекты сохраняли возможность управления по SMS, однако все действия запускались по команде, пересылаемой через основное TCP-соединение с сервером.

Виртуальные частные сети

Приведённая выше схема с использованием сервера удобна при разработке специализированных приложений с достаточно большим бюджетом. Однако при необходимости организации доступа к одному или нескольким устройствам стоимость такого решения становится сдерживающим фактором. Она складывается из необходимости приобретения стандартного пакета серверного ПО (web-сервер, SQL-сервер, FTP-сервер, почтовый сервер и т.д.) и специального сервера приложений. Даже если применять свободное ПО, то остаются расходы на его инсталляцию, конфигурирование, поддержание работоспособности и услуги провайдера. Такое решение невозможно предложить частным клиентам ввиду необходимости квалифицированной и, следовательно, дорогой технической поддержки.

В этом случае становится привлекательным использование технологии виртуальных частных сетей (VPN). Эти сети нашли широкое применение на персональных компьютерах для преодоления проблем, связанных с NAT и межсетевыми экранами. По сути VPN – это постоянно поддерживаемое соединение между компьютерами, через которое передаются пакеты всех других соединений, включая IP, TCP и UDP. Такая схема подобна тоннелю, созданному на основе протокола IP. Не имеет значения, какая сторона инициировала соединение, – важно, что пакеты этого соединения свободно пропускают серверы NAT и межсетевые экраны, не пытаясь их анализировать и модифицировать.

Технология VPN появилась одновременно с серверами NAT и межсетевыми экранами и была стандартизована, поэтому тоннели VPN приобрели специальные номера портов назначения в заголовках TCP/UDP и идентификаторы в заголовке IP, что позволяет легко отличать их пакеты. Сетевое оборудование должно распознавать протоколы VPN, если оно соответствует общепризнанным рекомендациям IETF. Провайдеры мобильной связи в подавляющем числе не блокируют протоколы VPN, следуя правилам остальных сетей, поскольку в противном случае они могут потерять значительную часть трафика.

Хотя преимущества виртуальных частных сетей известны, перечислим их ещё раз:

- узлы виртуальной частной сети не нуждаются в публичных IP-адресах;
- внутри виртуальной частной сети открыты все порты TCP и UDP и доступны любые конфигурации подключений между узлами;
- первичное IP-подключение, через которое осуществляется туннелирование, применяет шифрование своих данных, защищая передаваемые по тоннелю пакеты от несанкционированного просмотра и модификации.

Протокол PPTP

В настоящее время применяются несколько протоколов VPN, самые известные из которых обозначаются аббревиатурами PPTP (point-to-point tunneling protocol) и L2TP (Layer 2 Tunnelling Protocol). Это – два конкурирующих протокола, имеющие сильно различающиеся механизмы работы. Протокол PPTP появился несколько раньше и потому чаще встречается в устаревшем оборудовании. Далее мы будем рассматривать только протокол PPTP ввиду нескольких характеристик, делающих его привлекательным во встраиваемых устройствах.

Во-первых, протокол PPTP реализует повторное использование протокола PPP, который является первичным протоколом при «общении» с GPRS-модемами. Во-вторых, протокол PPTP поддерживают все ПК с операционной системой Windows, начиная с Windows 95. Единственно доступное входящее VPN-подключение в операционных системах Windows XP класса Home edition выполняется именно по протоколу PPTP. В-третьих, протокол PPTP использует алгоритм шифрования RC4, который работает в 3 – 7 раз быстрее алгоритмов, применяющихся в протоколе L2TP (DES3, AES), и быстрее обеспечивает аутентификацию. Скорость и простота – важные факторы во встраиваемых системах.

На рисунке 5 представлены форматы пакетов протокола PPTP. Этот протокол использует пакеты IP для организации двух каналов транспортного уровня: один для управления тоннелем и один (GRE) – для передачи данных туннелируемых протоколов. Протокол GRE (общая инкапсуляция марш-

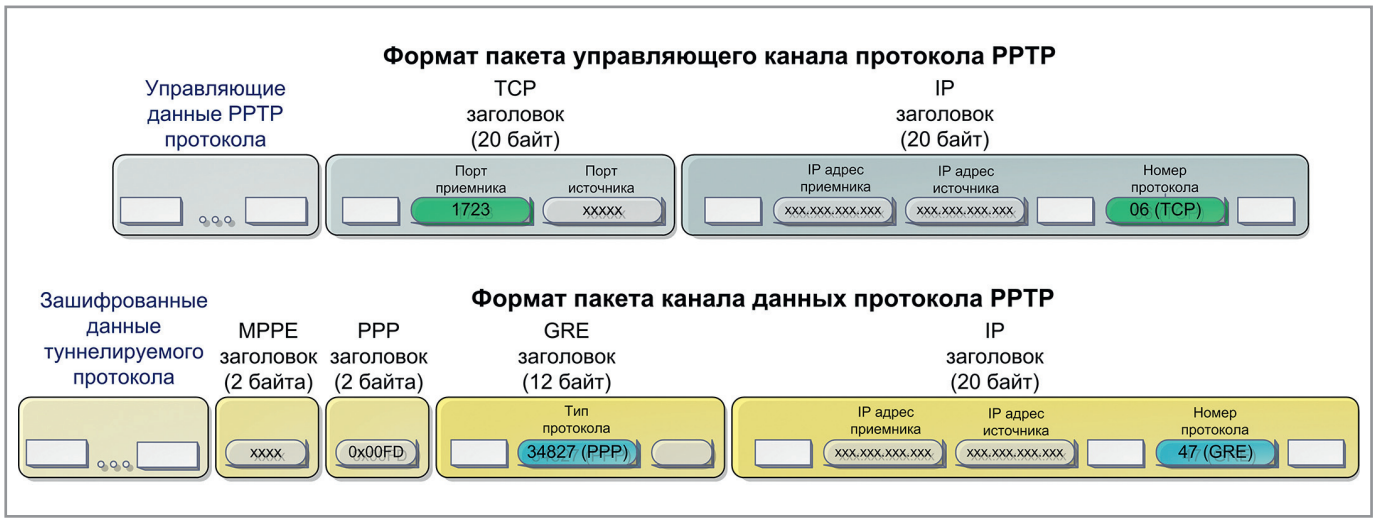

Рис. 5. Форматы пакетов протокола PPTP

рутов) – это протокол, разработанный специально для инкапсуляции пакетов сетевого уровня, т.е. PPP. Сначала протокол PPTP устанавливает с удалённой стороной TCP-соединение, через которое «договаривается» о параметрах тоннеля; после достижения договорённости с удалённой стороной начинают передаваться пакеты GRE. Эти пакеты, в свою очередь, переносят пакеты PPP, с помощью которых внутри тоннеля организуется сетевое соединение по какому-либо сетевому протоколу поверх PPP. Схема получается достаточно сложной для восприятия, учитывая, что между PPP и переносимыми им пакетами может присутствовать «прослойка» в виде протокола MPPE, отвечающего за шифрование данных.

Тем не менее, дополнительный объём заголовков, добавляемый протоколом PPTP к первичному IP-потоку данных, не превышает 36 байт. При максимальной длине IP-пакетов в 1500 байт, дополнительные заголовки занимают не более 2,5%. Если проанализировать типичный пакет данных, отправляемый на web-сервер через тоннель PPTP, то мы увидим следующую цепочку вложенных заголовков: PPP → IP → GRE → → PPP → MPPE → IP → TCP → HTTP → → данные. Обычно всё, что идёт после заголовка MPPE, будет зашифровано.

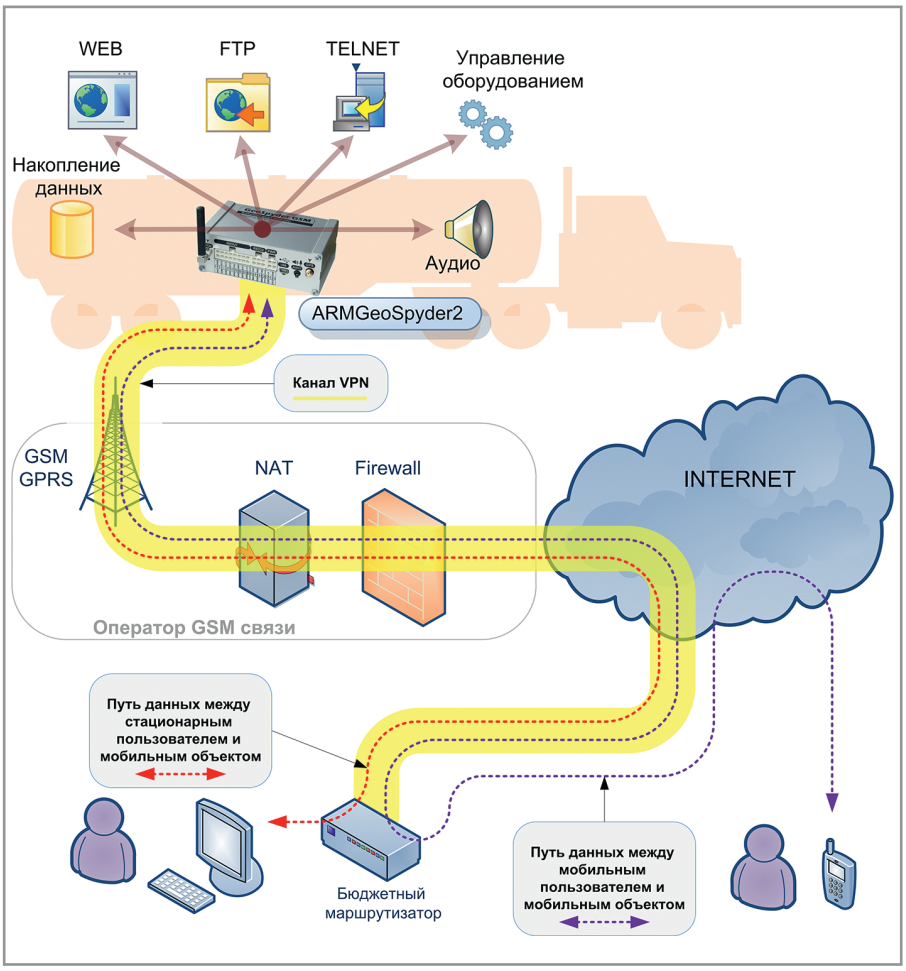

Рис. 6. Схема управления мобильным объектом с использованием VPN

Следует упомянуть о некоторых других особенностях протокола PPTP. По умолчанию, на протяжении существования PPTP-соединения, по управляющему каналу с периодичностью один раз в минуту (в конфигурации Windows) передаются эхо-запросы (размером 56 байт), в ответ на которые противоположная сторона должна отвечать эхо-ответами (размером 60 байт). В результате создаётся дополнительный трафик объёмом около 5 Мб в месяц. Во встраиваемых устройствах с целью экономии интервал эхо-запросов можно увеличить. Протокол PPTP не обязывает использовать шифрование передаваемых данных; его можно отключить в целях отладки, чтобы наблюдать за пакетами, передаваемыми в тоннеле.

Создание виртуальной частной сети на примере платы ARMGeoSpyder2

Для использования преимущества VPN необходимо иметь GPRS-модем или модуль, поддерживающий протоколы VPN. GPRS-модули с поддержкой VPN – большая редкость. GPRS-модемы в составе универсальных маршрутизаторов с функцией VPN можно найти в достаточно большом ассортименте. Но как правило, они плохо адаптированы для мобильных и встраиваемых применений. Их отличает большая потребляемая мощность, отсутствие интеграции с источниками резервного питания, гибких политик экономии трафика, адаптации под сети операторов и роуминг, а также слабый контроль за собственной работоспособностью.

На интернет-странице www.indemsys.ru можно ознакомиться с встраиваемыми платами, оборудованными GPRS-модулями, и готовыми устройствами, в значительной степени свободными от перечисленных выше недостатков. На рисунке 6 изображена схема управления платой ARMGeoSpyder2 через Интернет. Плата устанавливается на мобильном объекте и выполняет ряд функций по управлению оборудованием, слежению за перемещениями транспортного средства и записи сигналов с бортового оборудования. Ключевое отличие такой схемы связи от схемы, приведённой на рисунке 3, состоит в том, что не требуется создавать центральный узел управления с работающим на нём прикладным приложением и несколькими специализированными серверами. Вместо этого используется только компьютер или недорогой маршрутизатор, подключенный к Интернету и имеющий открытый порт 1723 для протокола PPTP. В данной схеме можно применить обычный домашний компьютер или домашний маршрутизатор с выходом в Интернет через оптоволоконный, xDSL-, телефонный или другой канал.

При подаче питания на плату ARMGeoSpyder2 встроенное ПО платы организует GPRS-подключение по заданному публичному IP-адресу в Интернете (адресу компьютера или маршрутизатора пользователя). Задать или поменять адрес можно заблаговременно, передав на плату конфигурационную команду при помощи SMS. Если соединение установлено, то со стороны платы посылается запрос на установление тоннеля PPTP.

На стороне пользователя тоннель может устанавливать программа либо на компьютере, либо на маршрутизаторе. Стационарные маршрутизаторы, поддерживающие туннелирование по протоколу PPTP, стоят недорого и повсеместно распространены. В процессе установления PPTP-тоннеля плата ARMGeoSpyder2 авторизуется на стороне пользователя с использованием протокола MSCHAP-v2. Далее происходит согласование алгоритмов шифрования. Плата ARMGeoSpyder2 поддерживает шифрование по протоколу MPPE с длиной ключа до 128 бит и сменой ключа при передаче каждого пакета.

Подключение к Интернету с домашнего компьютера, как правило, обеспечивается динамическим публичным IP-адресом, который выделяется при каждом сеансе. В нашем случае это не представляет проблемы, поскольку существуют бесплатные службы в Интернете для связывания динамических IP-адресов с постоянными доменными именами, получаемыми бесплатно на этих сервисах. Такие сервисы называются динамическими серверами DNS. Домашние маршрутизаторы, поддерживающие VPN, обычно поддерживают и функцию взаимодействия с динамическими DNS. Плата ARMGeoSpyder2 может устанавливать тоннель как по IP-адресу, так и по доменному имени.

После установления PPTP-тоннеля с платой ARMGeoSpyder2, в локальной сети пользователя появляется виртуальный локальный компьютер с частным IP-адресом. Этот адрес назначается плате ARMGeoSpyder2 из списка, который ранее пользователь ввёл для VPN-подключения на своём компьютере или на маршрутизаторе. Теперь пользователь с домашнего компьютера может свободно обращаться к web- и FTP-серверам на плате ARMGeoSpyder2, организовывать Teltet-подключения, мосты к портам RS-232 платы через Интернет, чтобы управлять другим оборудованием на мобильном объекте. Плата ARMGeoSpyder2 позволяет одновременно управлять двумя портами RS-232 через Интернет, причём в режиме Telnet-сессий, что очень удобно для таких бесплатных программ, как HyperTerminal и TeraTerm.

Для доступа к web-серверу платы ARMGeoSpyder2 из Интернета с других мобильных устройств, таких как смартфоны, планшеты и т.д., пользователю на домашнем компьютере достаточно выполнить несложную конфигурацию по перенаправлению пакетов с определённого внешнего TCP-порта компьютера или маршрутизатора на IP-адрес и номер порта web-сервера платы. Например, для работы с web-сервером платы указать, что с внешнего порта маршрутизатора с номером 8080 данные должны передаваться на IP-адрес 192.168.1.100 и порт 80 во внутренней сети. Здесь предполагается, что адрес 192.168.1.100 выделен плате ARMGeoSpyder2, а порт 80 по умолчанию обслуживается web-сервером платы.

Даже если пользователь не имеет собственного постоянного выхода в Интернет либо свободный доступ в Интернет затруднён межсетевыми экранами, остаётся возможность аренды внешнего сервиса VPN в Интернете. Тогда и пользователь, и плата ARMGeoSpyder2 получают от сторонних организаций доступ по статическому публичному IP-адресу к арендованной виртуальной сети для организации беспрепятственной связи между собой, – за определённую плату.

Таким образом, организация виртуальной частной сети с удалённым устройством по GPRS-каналу позволяет перенести многие сервисы, в частности, web, FTP и Telnet, на само устройство, избавившись от выделенного сервера приложений в Интернете и связанных с этим расходов.

Устройство на мобильном объекте может напрямую управляться через встроенный web-сервер, как это делается у стационарных встраиваемых устройств. Виртуальный канал расширяет возможности выбора провайдеров GSM-связи, не привязываясь к определённым планам и не приобретая специальных услуг по предоставлению публичных IP-адресов. Кроме того, применяя местные sim-карты, можно отказаться от роуминга. Расширяются возможности резервирования каналов связи, поскольку удалённое устройство может выбирать среди многих VPN-подключений, уведомляя пользователей о смене подключения посредством SMS или e-mail. Обмен данными между пользователями и удалёнными устройствами надёжно защищается от перехвата и модификации, что имеет важное значение в бизнес-процессах.