Создание эффективных каналов управления устройствами GSM/GPRS через Интернет

Александр Елисеев (г. Вильнюс, Литва)

Приведён обзор технологий управления через Интернет встраиваемыми устройствами, оборудованными модемами GSM/GPRS. Описаны методы преодоления ограничений, наложенных межсетевыми экранами и серверами трансляции адресов (NAT). Показаны преимущества, предоставляемые виртуальными частными каналами.

Введение

Эффективное управление устройствами через глобальную сеть Интернет является большим удобством для пользователя. Однако надёжная связь со встраиваемыми устройствами через десятки маршрутизаторов и сред распространения сигналов является сложной задачей, особенно при связи на большие расстояния и через границы государств. Каналы связи GSM/GPRS успешно решают проблему расстояний, покрытия и глобализации управления, но устанавливают значительные ограничения на пропускную способность, стоимость передачи данных и способы доступа по протоколу TCP/IP.

Проблемы с доставкой пакетов TCP/IP приводят к ошибкам в работе прикладных программ, таких как web-браузеры, FTP-клиенты, почтовые клиенты, Telnet и т.д. Если на настольном компьютере или планшете пользователь может предпринять ряд шагов по устранению неполадок, включая смену коммуникационного канала и переустановку программы, то встраиваемое устройство должно автоматически настроиться для установления связи. Разработчики встраиваемых устройств, естественно, не могут создать более интеллектуальные программы, чем работающие на настольных компьютерах, поэтому неизбежны компромиссы, ограничивающие возможности и выбор используемых интернет-технологий. Ниже мы опишем некоторые методы, применяемые при реализации интернет-каналов связи поверх GPRS.

Модемы GPRS

GPRS является технологией пакетной связи, работающей на базе GSM. Редкий GSM-модем на сегодняшний день не является одновременно и модемом GPRS. Такие модемы получили широкое распространение и значительно дешевле модемов, оснащённых протоколами 3G и EDGE. Сети GSM повсеместно предлагают услугу GPRS, чего нельзя сказать про EDGE и, тем более, 3G. Максимальная пропускная способность GPRS составляет до 48 Кб/с. Модемы GPRS могут иметь встроенный стек TCP/IP либо прозрачно передавать пакеты TCP/IP. В последнем случае модемы GPRS используют протокол PPP в качестве контейнера для пакетов TCP/IP. С помощью сервисов встроенного в модемы протокола PPP внешние устройства могут получить информацию о полученном адресе IP и адресе шлюза для выхода в Интернет.

Адрес IP, предоставленный оператором, 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 диапазонах (в шестнадцатеричной кодировке) 0A.xx.xx.xx, AC.1x.xx.xx и C0.A8.xx.xx.

Устройство с частным адресом не может указывать его в качестве адреса отправителя при посылке пакетов в Интернет. Обратный адрес должен быть публичным, иначе до устройства не дойдёт ответ адресата и в принципе станет невозможной двухсторонняя связь. Для решения этой задачи, в сети оператора связи существуют специальные серверы трансляции адресов (NAT).

Трансляторы сетевых адресов

В 2012 г. во всемирной сети закончились свободные публичные IP-адреса, основанные на протоколе IPv4; переход на протокол IPv6 затянулся, но при этом количество клиентов, желающих использовать сеть Интернет как инструмент удалённого управления, непрерывно растёт. Дефицит публичных адресов является серьезным препятствием на пути развития служб удалённого управления встраиваемыми устройствами.

На рисунке 1 показана типичная структурная схема сети оператора мобильной связи с точки зрения внешнего пользователя. Когда оператор выделяет модему GPRS частный IP-адрес, это означает, что в сети работает сервер NAT, задачей которого является преобразование частных адресов в

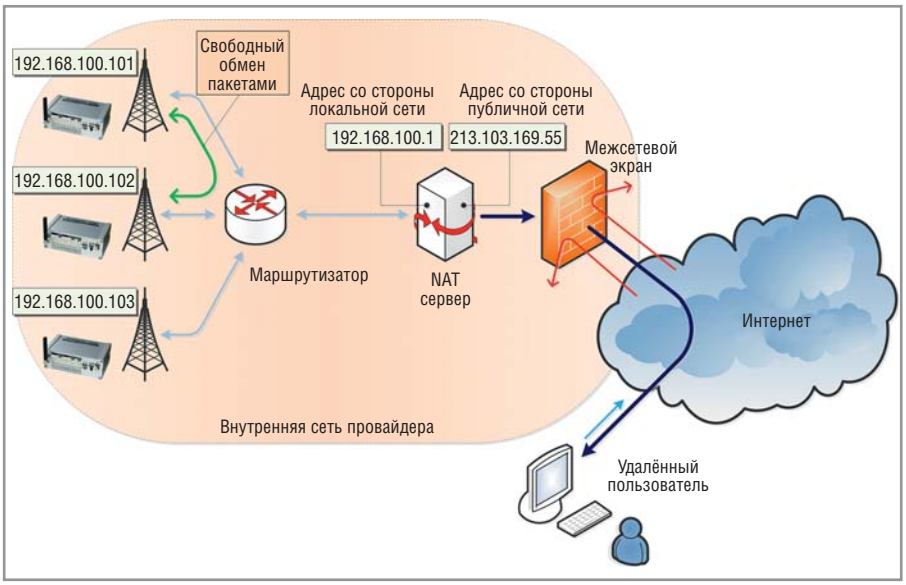

Рис. 1. Структурная схема сети оператора связи

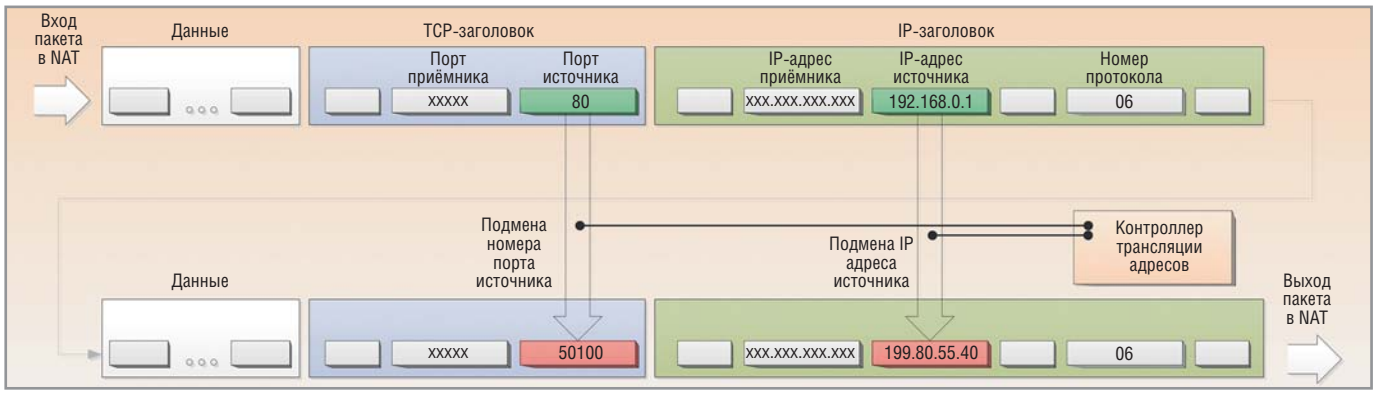

Рис. 2. Алгоритм работы сервера NAT при передаче пакета TCP в Интернет

публичные и обратно при прохождении данных между Интернетом и сетью оператора.

Целью использования NAT является экономия публичных адресов, которая достигается за счёт того, что они назначаются не устройствам в сети оператора, а только одному серверу NAT. Внутри сети оператора применяются только частные адреса. Маршрутизатор по адресу назначения определяет, какие пакеты IP надо направлять серверу NAT. Обычно модемы GPRS, 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 подсети, и тогда, оказавшись в разных подсетях, модемы GPRS не смогут установить между собой связь по внутренним адресам, если последние выделяются динамически (сервером DHCP). Поэтому соединение по частным адресам внутри сети оператора не может рассматриваться как надёжный канал управления устройствами.

Принцип работы сервера NAT достаточно простой, если рассматривать его на уровне отдельных соединений TCP/IP. На рисунке 2 показан алгоритм работы сервера NAT при передаче пакета TCP из внутренней сети оператора в Интернет. Трансляция частных IP-адресов через один публичный во многом становится возможной именно из-за наличия такого элемента адресации, как номер порта в пакетах TCP. Когда приходит ответ из сети Интернет от удалённой стороны, серверу NAT достаточно провести обратный поиск в таблице подмен по номеру порта назначения из полученного пакета, чтобы узнать порт TCP и адрес IP-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 Интернет. Запись удаляется, если в течение определённого времени не было обменов либо после явного разрыва связи узлами.

Сервер NAT способен анализировать состояние каждого логического соединения TCP и определять фазы установления и прекращения соединений. Всё сказанное выше относится и к пакетам UDP, которые также содержат номер порта. Это не означает, что сервер NAT способен пропускать только пакеты TCP и UDP, в других протоколах поверх IP могут быть различные атрибуты, уникально доопределяющие источник во внутренней сети. Например, команда PING протокола ICMP имеет уникальный атрибут Sequence number, который может быть выбран NAT в качестве индекса для построения таблиц трансляции IP-адресов.

Таким образом, модем GPRS с присвоенным ему частным адресом обязан первым инициировать связь с другими узлами в Интернете. Инициировать связь в обратном направлении невозможно, поскольку сервер NAT пропускает только пакеты, соответствующие записи трансляции. Впрочем, запись может существовать, если предыдущий сеанс связи не был явно разорван, а первый пакет нового соединения имеет те же номер порта и адрес IP. Однако межсетевой экран (файрвол) оператора, который более «пристально» следит за подключениями TCP, может иметь жёсткую политику безопасности, не допускающую таких коллизий.

Управление через канал TCP, инициированный модемом GPRS

Благодаря технологии NAT, модемы GPRS имеют возможность устанавливать полнофункциональные соединения TCP и работать, используя протокол UDP, хотя и должны первыми начинать сеанс связи. Модемы могут свободно высылать и принимать электронную почту, осуществлять поиск web-страниц, пересылать файлы на FTP-серверы, запрашивать информацию у серверов DNS и серверов точного времени, и т.д. Для управления устройствами через GPRS удобно использовать соединения TCP, поскольку они гарантируют доставку данных. Использование протокола UDP нежелательно, т.к. в нём отсутствует контроль доставки данных, а в сетях GSM потеря пакетов или их недопустимая задержка – явление весьма частое. Поскольку модем первым инициирует соединение, на удалённой стороне связь с модемом должен поддерживать сервер TCP, разумеется, с публичным IP-адресом.

Протокол TCP не определяет, какие данные, как и когда передаёт или принимает устройство. Этим должно заниматься приложение пользователя на сервере, работающее поверх протокола TCP. Такие приложения обычно создаются индивидуально под заказчика. Дело осложняется тем, что клиентами серверов приложений являются простые встраиваемые устройства, не обладающие ресурсами и возможностями ПК и не поддерживающие возможности программных структур типа .NET.

Система распределённого управления «Полигон»

Ниже представлена реализация системы управления тактическим мобильным полигоном (см. рис. 3), разработанная в рамках исследования возможностей применения связи GPRS. Концепция «полигона» заключалась в том, чтобы его можно было развернуть на любом участке подготовленной местности, покрытой связью GPRS, в кратчайшие сроки и гибко управлять из нескольких центров наблюдения,

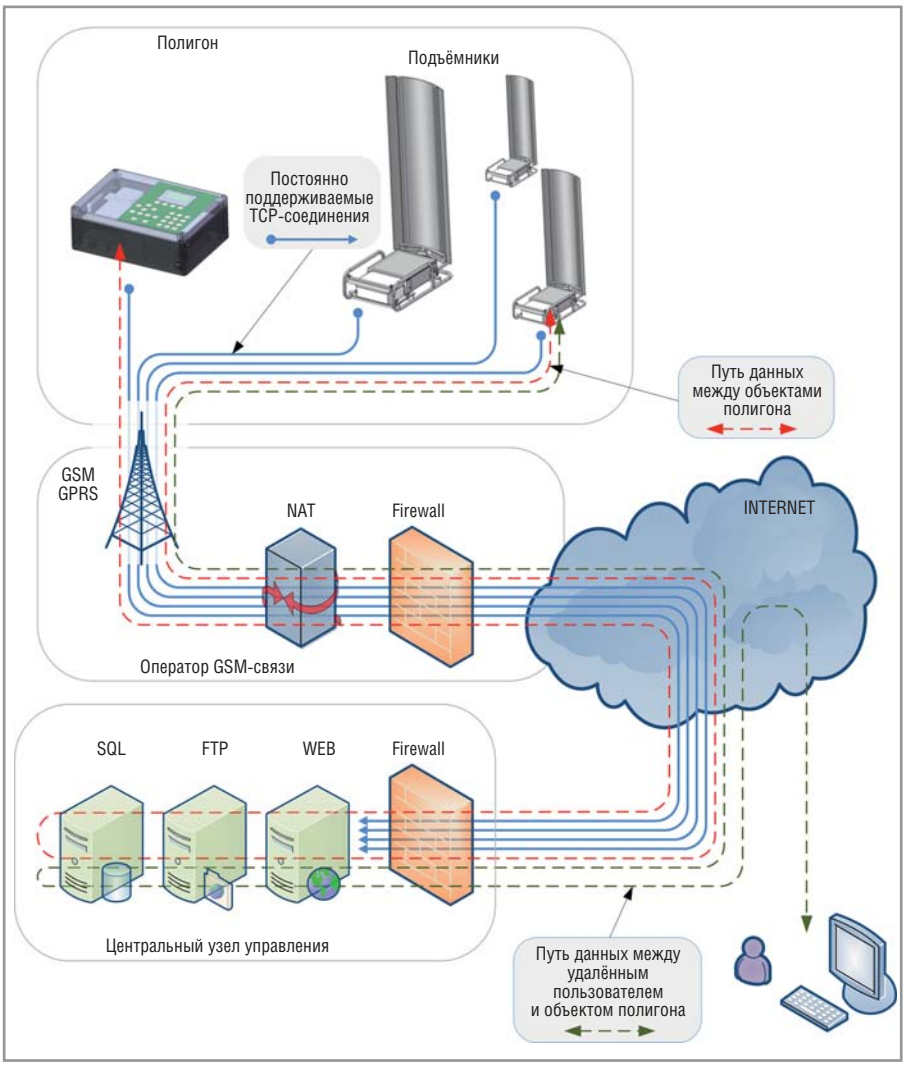

Рис. 3. Система управления полигоном

включая офис технической поддержки разработчика и с мобильных пультов координаторов учений. Для полного использования своих возможностей высокотехнологичные подъёмники, рассчитанные на автономную работу в дневное и ночное время, оснащённые 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.

Практика управления подъёмниками допускала некоторые задержки реакции на ручные команды, выдаваемые с пультов операторов. Такие команды, в основном, инициировали автоматические алгоритмы управления, реализованные в подъёмниках. При этом пульты и подъёмники соединялись через канал связи GPRS с центральным сервером приложений в офисе. Сервер приложений работал в режиме прослушивания запросов на соединения TCP от объектов полигона. По требованию последних сервер открывал соединение и, согласно бизнес-логике приложения, обрабатывал команды, посылаемые объектами.

Определённые команды содержали данные, предназначенные для сохранения в базе данных на сервере, другие команды ретранслировались по определённым алгоритмам на подключённые к серверу объекты. Таким образом, благодаря трансляции команд на сервере, пульты могли передавать команды подъёмникам, а подъёмники – передавать информацию пультам. Маршрутизация в этом случае осуществлялась специальным приложением. База данных на основе SQL-сервера 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 простым и универсальным для авторизированных пользователей, в частности, для администрации полигона. Он осуществлялся как посредством web-браузеров, так и с помощью офисных программ, поддерживающих связь с удалёнными SQL-серверами.

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

Чтобы определить задержку передачи команд, обусловленную Интернетом, были проведены замеры по месту установки системы, которые проводились в течение 2 суток с интервалом 1 мин на шести объектах, оснащённых модемами GPRS. Результаты распределения задержек показаны на рисунке 4. В сумме было передано 14 073 пакета, из них 27 пакетов было доставлено с задержкой более 5 с.

Мобильные объекты полигона (пульты и подъёмники) имели возможность обновлять собственное программное обеспечение путём скачивания с внешних FTP-серверов, а также сохраняли возможность управления посредством SMS. При этом все действия объектов стартовали по команде, пересылаемой через основное TCP-соединение с сервером.

Виртуальные частные сети

Приведённая выше схема с использованием сервера удобна при разработке специализированных приложений с большим бюджетом. Однако при необходимости организации доступа к одному или нескольким устройствам стоимость такого решения становится сдерживающим фактором, поскольку необходимо приобрести стандартный пакет серверного ПО (web-, SQL-, FTP-сервер, почтовый сервер и т.д.) и специальный сервер приложений. Даже если применяется свободное серверное ПО, остаются расходы на его инсталляцию, конфигурирование, поддержание работоспособности и хостинг. Такое решение невозможно предложить частным клиентам ввиду необходимости квалифицированной технической поддержки.

Альтернативой является использование технологии виртуальных частных сетей (Virtual Private Network, VPN), которые нашли широкое применение на персональных компьютерах для преодоления проблем, связанных с NAT и межсетевыми экранами. По сути VPN является постоянным соединением

между компьютерами, через которое передаются пакеты всех других соединений, включая IP, TCP, UDP и др. Эта схема подобна тоннелю, которым является первоначально созданное соединение на основе протокола IP. Не имеет значения, какая сторона инициировала соединение, важно, что пакеты VPN свободно[1] пропускают серверы NAT и межсетевые экраны, не пытаясь их анализировать и модифицировать.

Технология VPN появилась сразу же, как появились серверы NAT и межсетевые экраны, и быстро стандартизировалась, и потому тоннели VPN приобрели специальные номера портов назначения в заголовках TCP и UDP, а также идентификаторы в заголовке IP, что позволяет отличать их пакеты от пакетов остальных протоколов. Всё сетевое оборудование должно распознавать протоколы VPN, если оно соответствует рекомендациям IETF. Провайдеры мобильной связи в большинстве своём не блокируют протоколы VPN, следуя правилам остальных сетей, поскольку в противном случае они могут потерять значительную часть трафика.

Хотя преимущества виртуальных частных сетей известны, приведём 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 подключение IP, через которое осуществляется туннелирование, применяет шифрование данных, защищая пакеты от несанкционированного просмотра и модификации.

Протокол туннелирования PPTP

В настоящее время применяется несколько протоколов VPN. Самые известные из них обозначают аббревиатурами PPTP (point-to-point tunneling protocol) и L2TP (Layer 2 Tunnelling Protocol). Это два конкурирующих протокола различаются механизмами работы. Протокол PPTP возник несколько раньше и поэтому чаще встречается на старом или давно выпускаемом оборудовании. Далее мы будем рассматривать только протокол PPTP из-за характеристик, делающих его привлекательным для использования во встраиваемых устройствах.

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

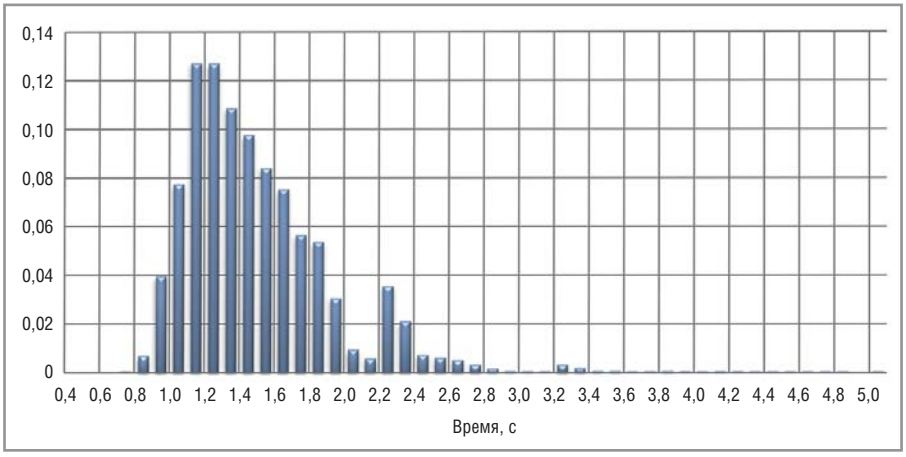

Рис. 4. Нормированная гистограмма распределения времени прохождения пакетов между объектами в системе «Полигон»

На рисунке 5 представлены форматы пакетов протокола PPTP, который использует IP-пакеты для организации двух каналов транспортного уровня: одного канала TCP для управления тоннелем и одного канала GRE для передачи данных туннелируемых протоколов. GRE (Generic Routing Encapsulation, общая инкапсуляция маршрутов) – это протокол туннелирования, разработанный для инкапсуляции пакетов сетевого уровня. В случае с PPTP – это пакеты протокола PPP.

Сначала протокол PPTP устанавливает с удалённой стороной соединение TCP, через которое «договаривается» о параметрах тоннеля; после достижения договорённости начинают передаваться пакеты GRE, которые, в свою очередь, транспортируют пакеты PPP. С помощью последних внутри тоннеля организуется сетевое соединение по какому-либо сетевому протоколу поверх PPP. Схема достаточно сложная, учитывая, что между PPP и переносимыми им пакетами может присутствовать «прослойка» протокола MPPE, отвечающего за шифрование данных. Тем не менее, дополнительный объём заголовков, добавляемый протоколом PPTP к первичному IP-потоку данных, не превышает 36 байт, что составляет 2,5% максимального объёма пакета IP (1500 байт). Если посмотреть на типичный пакет данных, отправляемый на web-сервер через модем GPRS с помощью тоннеля PPTP, мы увидим следующую цепочку вложенных заголовков: PPP → IP → GRE → → PPP → MPPE → IP → TCP → HTTP → → данные. Как правило, всё, что следует после заголовка MPPE, зашифровано.

По умолчанию, на протяжении существования соединения PPTP, по управляющему каналу непрерывно (с периодичностью раз в минуту в конфигурации Windows) передаются эхо-запросы (56 байт), в ответ на которые противоположная сторона должна посылать эхо-ответы (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 данных; его можно отключить и, таким образом, наблюдать за пакетами в тоннеле в процессе отладки.

Создание виртуальной частной сети на примере встраиваемой платы ARMGeoSpyder2

Для использования преимуществ VPN необходимо иметь модем GPRS или модуль, поддерживающий протоколы VPN. Модули GPRS с поддержкой VPN – большая редкость. В составе универсальных маршрутизаторов модемы

[1] *Маршрутизаторы иногда фильтруют отдельные протоколы VPN. – Прим. ред.*

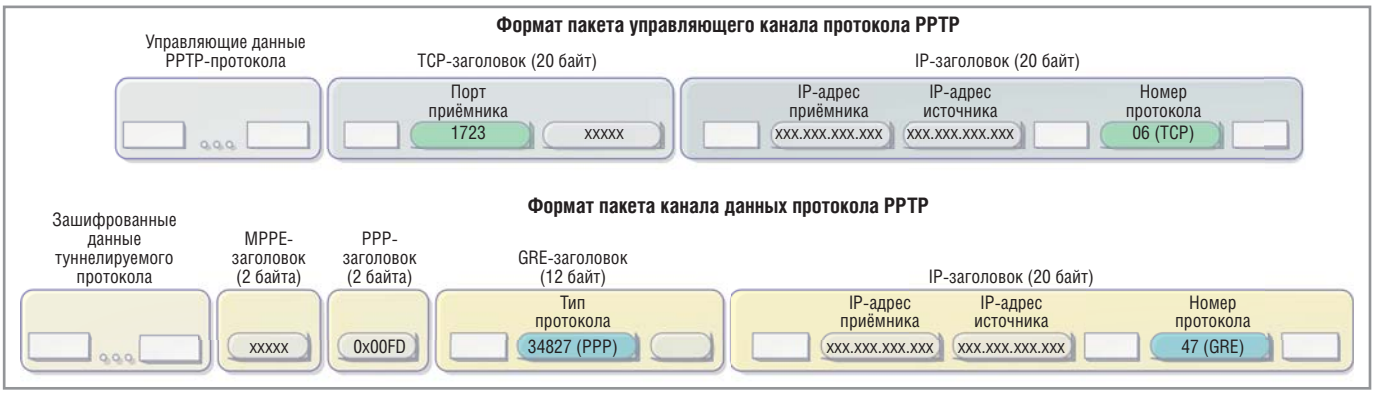

Рис. 5. Форматы пакетов протокола PPTP

GPRS можно найти в большом ассортименте. Однако в основном они плохо адаптированы для мобильных и встраиваемых применений ввиду большой потребляемой мощности, неадаптированного диапазона питающих напряжений, отсутствия интеграции с источниками резервного питания, гибкой политики экономии трафика, адаптации под меняющиеся сети операторов и работы в роуминге, а также неразвитой самодиагностики. Интернет-страница www.indemsys.ru предлагает для приобретения встраиваемые платы с модулями GPRS и готовые устройства, в значительной степени свободные от перечисленных выше недостатков.

На рисунке 6 изображена схема управления платой ARMGeoSpyder2 через Интернет. Плата установлена на мобильном объекте и выполняет ряд функций по управлению оборудованием, слежению за перемещениями транспортного средства и записью сигналов с бортового оборудования. Ключевое отличие этой схемы от схемы, представленной на рисунке 3, заключается в том, что не требуется создавать центральный узел управления с работающим приложением и несколькими специализированными серверами. Вместо этого необходим только компьютер или отдельный недорогой маршрутизатор, подключённый к сети Интернет и имеющий открытый канал (порт 1723) для протокола PPTP. Например, в такой схеме можно применить обычный домашний компьютер или домашний маршрутизатор с выходом в Интернет через оптоволоконный, DSL, телефонный или другой кабель.

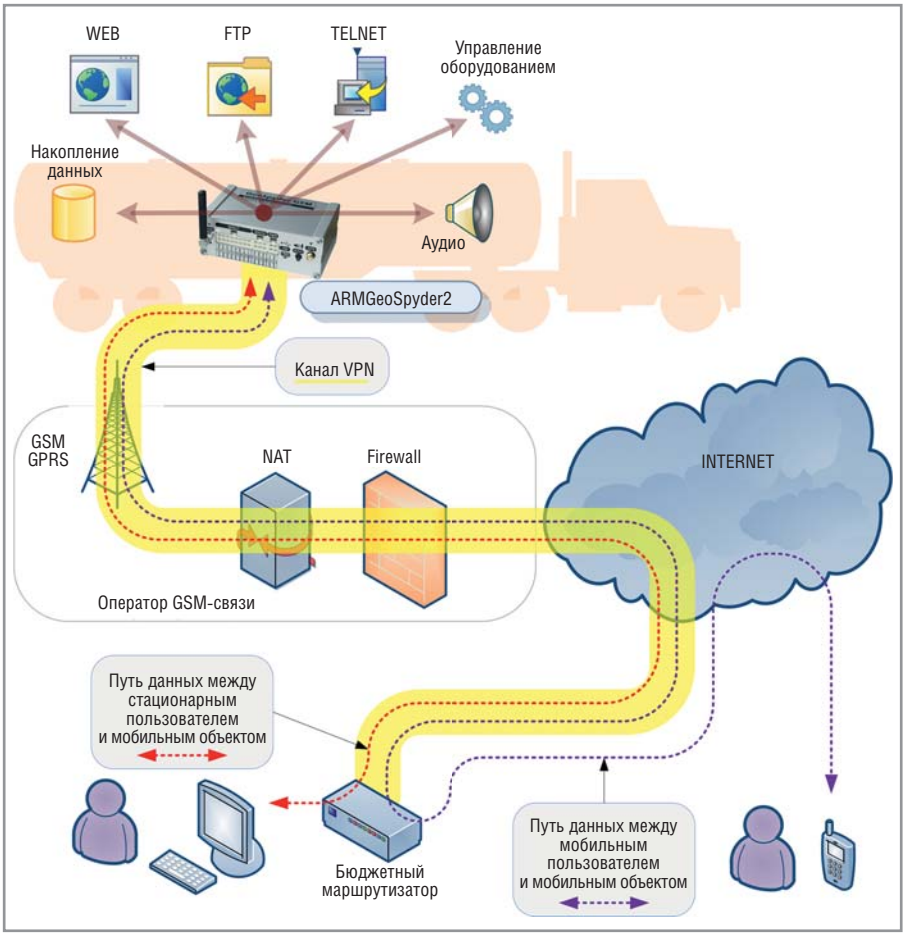

Рис. 6. Схема управления мобильным объектом с использованием VPN

При подаче питания на плату ARMGeoSpyder2, встроенное ПО платы организует подключение GPRS по заданному публичному IP-адресу, который имеет компьютер или маршрутизатор пользователя. Задать или изменять адрес можно заблаговременно, послав плате конфигурационную команду по SMS. Если соединение установлено, то со стороны платы поступает запрос на установление PPTP-тоннеля. На стороне пользователя тоннель может устанавливать ПО, установленное либо на компьютере, либо на маршрутизаторе. Стационарные маршрутизаторы, поддерживающие туннелирование по протоколу PPTP, доступны для приобретения. В процессе установления тоннеля PPTP плата ARMGeoSpyder2 авторизируется 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 смену ключа при передаче каждого пакета.

Если подключение к Интернету с домашнего компьютера не обеспечивается постоянным IP-адресом, последний выделяется при каждом подключении. В нашем случае это не является проблемой, поскольку существуют бесплатные сервисы для связывания динамических IP-адресов с постоянными доменными именами, получаемыми на этих сервисах бесплатно. Такие сервисы называются динамическими серверами DNS. Домашние маршрутизаторы, поддерживающие

VPN, обычно поддерживают и функцию взаимодействия с DDNS. Плата ARMGeoSpyder2 может устанавливать тоннель как по IP-адресу, так и по доменному имени.

После установления тоннеля PPTP с платой ARMGeoSpyder2, в локальной сети пользователя появляется новый 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 и мосты к портам RS232 платы через Интернет, чтобы управлять другим оборудованием на мобильном объекте. Плата ARMGeoSpyder2 позволяет одновременно управлять двумя портами RS232 через Интернет, причём в режиме Telnet-сессий, что удобно при использовании программ 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 порта TCP компьютера или маршрутизатора на IP-адрес и номер порта web-сервера платы. Например, для работы с web-сервером платы можно указать, что с внешнего порта маршрутизатора с номером 8080 (поскольку порт 80 пользователь, возможно, захочет оставить за домашним web-сервером) 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 Интернет. Тогда за определённую плату и пользователь, и плата ARMGeoSpyder2 получают доступ по статическому публичному IP-адресу к арендованной VPN для организации беспрепятственной связи.

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

Устройством на мобильном объекте можно напрямую управлять через собственный встроенный web-сервер, как это делается в стационарных встраиваемых устройствах. Виртуальный канал расширяет возможности по выбору провайдеров связи GSM, не привязываясь к определённым планам и не приобретая специальные услуги по предоставлению публичных IP-адресов, и удешевляет работу в роуминге. Расширяются возможности резервирования каналов связи, поскольку удалённое устройство может «выбирать» среди многих VPN-подключений, уведомляя пользователей о смене подключения через SMS или e-mail. Кроме того, обмен данными между пользователями и удалёнными устройствами надёжно защищается от перехвата и модификации, что может иметь большое значение в транснациональных бизнес-процессах.