M2M-системы удаленного управления и мониторинга.

Законченные решения на базе резервируемых GSM/GPRS-терминалов

Игорь Дианов
igor@analytic.ru
Владимир Серганов
vladimir@analytic.ru
Алексей Упоров
uporov@analytic.ru

Статья посвящена особенностям передачи данных в сети GSM/GPRS и законченным решениям по организации устойчивого канала обмена в модемах AnCom RM производства компании "Аналитик-ТС" (http//www.analytic.ru).

На Российском рынке беспроводных систем M2M широкое распространение получили GSM/GPRS-модули, терминалы и законченные системы передачи данных различных производителей. Их использование предпочтительно в проектах с ограниченным финансированием, когда создание каналов проводной связи нецелесообразно: это системы телеметрии и телемеханики, безопасности и АСКУЭ, торговые и платежные терминалы, банкоматы и парковочные счетчики, подвижные объекты и т.п.

Сервисы, предоставляемые сетью GSM для M2M

В GSM-сети для передачи данных используются сервисы: SMS (Short Message Service), CSD (Circuit Switched Data) и GPRS/EDGE (General packet radio Service / Enhanced Data for Global Evolution).

SMS – в связи с ограничениями на объем передаваемых данных (160 символов), относительно высокой стоимостью и отсутствием "гарантированной доставки" в основном применяется в охранно-пожарных системах.

CSD – сервис с коммутацией каналов, скорость до 9.6 кбит/с (14.4 кбит/с при использовании HSCSD в одном слоте). Данные передаются в выделенном при установлении соединения канале. Поддерживается протокол сжатия и коррекции ошибок V.42bis. Преимущества: если соединение установлено, то данные дойдут за фиксированное время. Недостатки: повременная оплата и сложность использования в системах, требующих быстрой реакции на событие (необходимо время, чтобы дозвониться).

GPRS/EDGE – сервис с пакетной передачей данных, скорость до 171/473 кбит/с, постоянное соединение с сетью (не надо дозваниваться до абонента). Передача пакетов идет по неиспользуемым в данный момент голосовым каналам, которые всегда есть в промежутках между разговорами абонентов. Использование для передачи сразу нескольких каналов обеспечивает повышение скорости. Плюсы: постоянная готовность к передаче данных и тарификация объема передаваемых данных, а не времени соединения. Минус: выделение слотов по остаточному принципу.

Особенности передачи данных в сети GPRS

При организации каналов передачи данных по GPRS необходимо четко разделять понятия:

- скорость передачи (максимум 171 кбит/с, а на реальной "московской" сети в среднем 10 кбит/с);
- время доставки данных (до 15 и более секунд);
- девиация времени доставки (до ±15 с).

Как следствие, временные тайм-ауты при опросной схеме должны составлять более 30 секунд, и необходимо учитывать возможные временные разрывы передачи самого сообщения (если не

используются специальные средства по их сборке-разборке), например, несколько байтов приходят через 2с после отправки, а оставшаяся часть задерживается на 13с.

Рассмотрим причины задержек доставки данных:

- собственно задержка доставки кадров канального уровня, определяемая:
  - задержкой на интерфейсе передачи (например, вызванной механизмом RTS/CTS);
  - временем сборки-разборки кадров и их обработки, включающей в себя помехоустойчивое кодирование, перемежение, диспетчеризацию потоков с разным качеством обслуживания, шифрование и др.;
  - задержкой передачи кадра, включающей выделение свободных слотов и распространение сигнала в физическом канале;
- потери кадров канального уровня при их передаче по радиолиниям:
  - возникновение канальных ошибок, свойственное мобильным сетям;
  - разрыв линии связи, возникающий, например, во время процедуры хэндовера (handover) — перехода мобильного терминала из одной соты в другую;
- транспортный протокол со своим механизмом защиты от ошибок иногда некорректно взаимодействует с аналогичными механизмами канального уровня, осуществляя повторную передачу задержанных или утерянных пакетов наряду с их повторной передачей канальным протоколом.

IP-адресация в сети GPRS

Соединение GPRS подразумевает использование сетевого протокола TCP/IP (Transmission Control Protocol/Internet Protocol). Оператор GSM предоставляет для мобильного терминала точку входа в сеть — APN (Access Point Name). Сетью может быть Интернет, локальная сеть оператора, корпоративная сеть пользователя. Сервер выдаёт мобильному терминалу IP-адрес, тип которого определяется тарифным планом:

- локальный - принадлежит оператору и невидим со стороны Интернета,
- публичный - доступен со стороны Интернета,
- динамический - меняется при переустановке соединения,
- статический - жестко привязан к SIM-карте.

Локальные статические адреса позволяют организовать передачу данных между мобильными терминалами без выхода в Интернет. Обеспечивается максимально быстрое установление соединения. Обмен данными локализован в сети оператора. Недостаток — соответствующие тарифные планы относительно дорогие.

Локальные динамические адреса используются для доступа к ресурсам Интернета без возможности опроса мобильного терминала со стороны Интернета – самые дешевые тарифы, но их использование в системах не всегда удобно.

Публичные динамические адреса видны в Интернете, позволяют организовать различные схемы передачи данных и во многом оптимальны по соотношению цены и возможностей. Обмен текущими адресами осуществляется через буферный FTP-сервер или SMS.

Публичные статические адреса в основном используются в системах с VPN-туннелями.

Обеспечение безопасности передачи данных

Многих волнуют вопросы, связанные с безопасностью передачи данных по сети GPRS. Понимая всю сложность темы, рассмотрим хотя бы часть обеспечивающих её системных средств:

- непосредственно в мобильном терминале безопасность обеспечивается на уровнях:
  - SIM карты: идентификатор абонента (IMSI), ключ аутентификации (Ki), алгоритмы шифрации (A8) и аутентификации (A3), PIN код доступа;
  - терминального оборудования: идентификатор IMEI, алгоритм шифрации A5;
- при передаче данных от терминала к обслуживающему узлу данные шифрируются в соответствии с алгоритм GEA1,2,3;
- защита локальной сети оператора обеспечивается блокировкой доступа из внешних сетей по RFC 1918.

Отдельно можно выделить сервис, значимость и количество инсталляций которого постоянно возрастают, а стоимость падает – VPN-туннель (Virtual Private Network). Цель VPN – обеспечить прозрачный защищенный доступ к ресурсам локальной сети пользователя с мобильного терминала через незащищенную сеть Интернет (или выделенные каналы). Оператор связи создаёт уникальную точку доступа — APN-сервер, поддерживающий IP-адреса, выделенные оператором, либо принадлежащие пользователю. Организуется туннель от сервера до локальной сети пользователя (протоколы: L2TP, GRE, IPSec…). В дополнительные сервисы включено полноценное шифрование туннелированных данных.

”Управляющий” модем

Большое количество выпускаемых GSM/GPRS-модулей и терминалов имеют встроенную поддержку стека протоколов POP3/SMTP, FTP, TCP/IP/UDP/DNS. Простота организации на их базе доступа компьютеров в Интернет и аналогии с применением проводных модемов могут создать ощущение отсутствии сложностей при использовании в промышленных системах телеметрии и телеуправления.

Подключение к модулю управляющего контроллера, обеспечивающего формирование AT-команд, внешнего источника питания и антенны в конечном счете не вызовет затруднений у опытных разработчиков. Основные вопросы начинают возникать при решении задачи обеспечения устойчивой работы:

- системы, работающие на столе, вдруг начинают сбоить и ”виснуть” при переходе на реальные объекты, при изменении оператора или увеличении загрузки сети;
- выясняется, что необходимы существенные усилия для обработки нештатных ситуаций, по тестированию, поддержке работы с динамическими IP-адресами, обеспечению доступа к состоянию модема и сети в процессе передачи данных и т.п.

Безусловно, найдутся организации, которые смогут решить возникающие проблемы – но оправдано ли это экономически для большинства?

Всё это приводит к появлению на рынке предложений законченных решений. Их стоимость, безусловно, немного выше, но это цена за своеобразный Plug and Play («включил и работай»). Подобные системы могут содержать управляющий контроллер, но современные GSM/GPRS-модули позволяют от него избавиться, сделав ”управляющим” сам модем. Встроенные программы превращают модем в законченную систему передачи данных, а во многих случаях в систему сбора, обработки и передачи данных. Примеры подхода к программированию модемов представлены в таблице.

Таблица. Примеры подхода к программированию модемов

Производитель	Выполнение в модуле пользовательских программ
Wavecom www.wavecom.com	Программы, написанные на C++ с использованием API-функций среды Open AT, загружаются в Flash-память модуля и исполняются под управлением ОС
Siemens Communications www.communications.siemens.ru	Встроенный интерпретатор для Java, IMP 2.0
Telit Communication S.p.A www.telit.co.it	Встроенный интерпретатор для Python
Enfora www.enfora.com	Настраиваемые пользователем встроенные программные блоки, в том числе, обеспечивающие отслеживание внешних событий и реакцию на них

Законченные решения на базе резервируемых модемов AnCom RM

ООО “Аналитик-ТС” построило свои решения на базе модемного модуля фирмы Wavecom и собственного встроенного программного обеспечения Socket mode.

AnCom RM — законченное решение для промышленных систем, чувствительных к перерывам связи. Семейство резервируемых модемов с автоматическим переходом на запасной

канал передачи данных и возвратом на основной при его восстановлении. Прозрачный канал автоматически активируется после включения питания.

Рис.1. Внешний вид модема AnCom RM/E

AnCom RM/E (рис.1) — в модеме реализовано резервирование каналов связи, разделенных на физическом уровне (проводные и беспроводные каналы). Модульная архитектура (до 5 модулей, устанавливаемых в мини крейт) обеспечивает выпуск широкой номенклатуры модемов: с различными интерфейсами (RS-232C, RS-485 или USB), типами первичного питания, проводными (встроенный модем AnCom STF) и беспроводными (GSM/GPRS модуль) каналами связи (два канала в любой комбинации).

AnCom RM/D (рис.2) — модем оптимизирован для беспроводных GSM/GPRS-систем передачи: два держателя SIM-карт со встроенной программной поддержкой автоматического переключения между ними (резервирование оператора связи), интерфейс RS-232C, встроенная или внешняя антенна, различные виды первичного питания.

Рис.2. Внешний вид модема AnCom RM/Д

Встроенное программное обеспечение ”SOCKET_MODE”

Назначение и возможности

После включения питания загруженное в модем приложение обеспечивает автоматическое подключение к сети GSM/GPRS и установление между двумя модемами прозрачного канала обмена данными (TCP/IP-сокета). В процессе работы контролируются нештатные ситуации (сбои SIM-карты, уровень GSM-сигнала, регистрация в сети GSM/GPRS, сбои в сети оператора связи, передача данных через TCP/IP-сокет, активность на порту данных и т.п.) и обеспечивается максимально быстрое восстановление соединения, в том числе, за счет перезагрузки или перехода на резервный канал.

Особенности реализации

Для настройки режимов работы модема введено расширение AT-команд с префиксом AT@ATS. Настройка модема производится на скорости COM-порта 115200 бод. При переходе модема в режим передачи данных скорость COM-порта изменятся на скорость указанную при настройке модема (AT@ATSSPEED=”xxxx”, где xxxx — скорость в диапазоне 300-57600 бод).

Поддерживается режим работы с одной или двумя SIM-картами, команда AT@ATSSIMCARD со значением 1 или 2. Возможна работа с публичными динамическими IP-адресами (обмен адресами через FTP сервер или SMS). Для корректной работы приложения необходимо подключение сотовым оператором услуги определения номера звонящего и поддержки публичного динамического (либо локального или публичного статического) IP-адреса.

Для исключения ситуации ”зависания” модема все этапы установления соединения и передачи данных охвачены контролем времени завершения (более 30 контролируемых тайм-аутов). В том числе, реализованы тайм-аут на отсутствия приема-передачи данных по интерфейсу (AT@ATSPRRESET) и тайм-аут на попытку возврата с резервного канала на основной.

Модем имеет расширенный до 16 кбайт внутренний буфер данных, что позволяет применять его в системах с ”3-проводным” интерфейсом (только RxD и TxD). При передаче без программного квитирования пакетов данных размером более 16 кбайт необходимо включить управление потоком CTS/RTS.

На всех этапах осуществляется светодиодная индикация уровня входного сигнала, состояния процесса установления соединения и работы.

Дополнительные средства обеспечения безопасности данных

В модемах AnCom RM реализовано несколько дополнительных уровней аутентификации на этапах инициализации, установления соединения и передачи данных:

- для предотвращения возможности использования SIM-карт не по назначению при настройке модема вводятся значения их PIN-кодов, которые в дальнейшем хранятся в памяти модема, проверяются при запуске и недоступны по чтению (AT@ATSPINCODE= “pin code” и AT@ATSPINCODEREZ=”pin code” – ввод PIN-кодов для основной и резервной SIM-карты);
- для предотвращения несанкционированного соединения модемов с неизвестными мобильными устройствами осуществляется аутентификация доступа на APN-сервер и доступа на системный FTP-сервер
  (AT@ATSGPRS=”APNSERVER”,”LOGIN”,”PASWORD”;
  AT@ATSFTP=”FTPSERVER”,”USER”,”PASWORD”);
- контролируются номера телефонов входящих синхронизирующих вызовов и номера отправителей SMS-сообщений;
- при обмене динамическими адресами контролируются идентификаторы модемов;
- при установлении TCP-соединения происходит контрольный обмен идентификаторами, при их несовпадении соединение разрывается, передача данных невозможна (AT@ATSREMUIN=”REMUIN”).

Алгоритм открытия TCP/IP-сокета между двумя модемами

После включения питания модемы инициализируют актуальные SIM-карты, проверяют правильность введенных PIN-кодов и контролируют уровень GSM-сигнала. Обмен звонками с идентификацией номера звонящего позволяет синхронизировать работу и определить каналы, на которых работают модемы (основной или резервный).

Посредством активации соответствующего PDP-контекста (Packet Data Protocol) открывается GPRS-сессия и, как результат, модемы получают IP-адреса (PDP-контекст задается для основного и резервного оператора командами AT@ATSGPRS=”apn”,”login”,”password” и AT@ATSGPRSREZ=”apnrezerv”,”loginrezerv”,”passwordrezerv”).

Если IP-адреса динамические, то модемы обмениваются ими через FTP-сервер или SMS. Затем инициализируется TCP/IP-соединение (с учетом введенного режима работы ”Клиент” или ”Сервер”). Модемы переводятся в режим передачи данных. Между модемами организуется прозрачный канал обмена с контролем состояния GSM/GPRS-сети и TCP/IP-соединения.

Обеспечение совместимости

При разработке встроенного программного обеспечения необходимо обеспечить корректную реакцию модемов на особенности, свойственные сетевым операторам (например, формат выдачи номера звонящего), различные тарифные планам и т.п.

Выход один – комплексное тестирование. Все изменения ПО Socket_mode проверяются на стационарных и движущихся объектах; в сетях операторов: МТС, Beeline, ”Мегафон” и др.; на тарифных планах с IP-адресами: локальными статическими, публичными динамическими, VPN-канале с динамическими адресами из заданного диапазона.

Перспективы развития

ООО ”Аналитик-ТС” продолжает разработки в области расширения функциональности встроенного ПО (на подходе масштабируемый программный комплекс, обеспечивающий прозрачный канал обмена данными через VPN-туннель между GSM/GPRS-модемом и компьютером, находящимся в локальной сети). Осуществляются заказные разработки встроенного ПО.

Технологическое программное обеспечение

GTem — свободно распространяемое терминальное приложение, обеспечивающее существенное упрощение процедур настройки и тестирования модемов. Основные режимы работы:

- настройка режима COM-порта, к которому подключен модем, с индикацией сигналов CTS, DSR, RING и DCD;
- программирование модулей Wavecom (с поддержкой протокола Xmodem);
- настройка модема:
  - передача в модем AT-команд: сформированных вручную, выбранных из редактируемого списка или представленных в виде AT-скриптов (последовательности AT-команд);
  - создание, редактирование и исполнение AT-скриптов, которые могут быть созданы вручную или при помощи специальных формы (скрипт из 18 команд выполняется примерно за 10 секунд);
  - в комплект поставки ПО входит набор библиотек AT-команд и AT-скриптов;
- тестирование канала передачи с возможностью передачи:
  - строки или массива символов ASCII (однократно или через определенные интервалы времени);
  - заданного файла.

В процессе работы GTem ведутся журналы, которые могут быть сохранены и использованы как отчетные документы:

- журнал исполнения последнего скрипта (поданные команды и ответы на них);
- журнал передачи последнего файла (порядок передачи пакетов данных и результаты передачи);
- копия данных, которые были переданы в COM-порт и приняты из него (журнал создается при запуске программы, в имени файла содержится дата и время его создания).

FTPmonitor — свободно распространяемое приложение, предназначенное для помощи пользователям, использующим модемы AnCom RM:

- функционально представляет собой FTP-клиента с возможностью работы с директориями и файлами на FTP-сервере, в том числе, получение списка файлов и директорий через заданные промежутки времени;
- обеспечивается наблюдение за обменом файлами, содержащими информацию о динамических IP-адресах модемов при инициализации их соединения.

Литература

1. Пушкарев О. EDGE технология высокоскоростной передачи данных в GSM-сетях// Беспроводные технологии 2005. №1
2. Пушкарев О. GSM/GPRS-модемы Wavecom для быстрой разработки и внедрения GSM-решений//Беспроводные технологии 2006. №2
3. AT Commands Interface for TCP/IP. For eDsoft-302 v0.1. F. D. eDevice. WAVECOM SA. Jan, 2003.
4. Проблемы передачи данных в сетях мобильной связи http://www.ccc.ru/magazine/depot/02_05/read.html?0302.htm
5. VPN и IPSec на пальцах http://www.opennet.ru/docs/RUS/vpn_ipsec/index.html
6. Enabler-IIG AT Command Set Version 1.08; http://www.enfora.com