СПУТНИКОВЫЕ ТЕХНОЛОГИИ VSAT И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТИ

А. Гладченков

Lan №9, 2007

Для построения сетей связи крупные территориально-распределенные компании чаще всего применяют спутниковые системы VSAT. Термин Very Small Aperture Terminal (VSAT) был введён в 1983 г. для того, чтобы отличить пользовательские станции с антеннами относительно малых диаметров (до 2,4 м) от больших наземных станций. В начале 90-х гг. технология VSAT была ориентирована в основном на предоставление операторам связи закрепленных одиночных каналов (Single Channel Per Carrier, SCPC) и организацию удаленного доступа к сетям телефонии. Затем, с изменением потребностей рынка, акцент сместился с предложения исключительно голосовых услуг к комбинированным телематическим услугам, включая услуги передачи данных. Сейчас наблюдается массовая переориентация технологий VSAT на предоставление доступа к Internet. Производители оборудования VSAT, прежде всего каналообразующего, все в большей мере ориентируются на использование протоколов IP и Frame Relay на транспортном уровне своих систем.

Сети VSAT строятся на базе геостационарных спутников-ретрансляторов. В качестве примера, типичного для России, можно привести спутники «Ямал», принадлежащие компании «Газком», структурному подразделению ОАО «Газпром». Помимо самого спутника сеть спутниковой связи включает в себя ещё два основных элемента: центральную управляющую станцию (ЦУС) оператора спутниковой связи и абонентские терминалы VSAT. В состав ЦУС входят приемо-передающая аппаратура, антенно-фидерные устройства и комплекс оборудования, осуществляющий функции контроля и управления всей абонентской спутниковой сетью, перераспределение ее ресурсов, выявление неисправностей, тарификацию услуг сети и сопряжение с наземными линиями связи. Спутниковые антенны и компактные терминалы VSAT размещаются непосредственно в удалённых точках, поддерживая широкий спектр современных мультисервисных услуг, включая передачу данных, видео, голоса (см. Рисунки 1 и 2).

Рисунок 1. Спутниковый модем HughesNet

Наземные сети связи подвержены таким опасностям, как обрыв и повреждение кабеля. Свою лепту в уязвимость наземных систем связи вносят сбои и аварии в сетях электропитания, в том числе отказ сетевого оборудования. Спутниковая связь избавлена от этих опасностей. С помощью спутниковых каналов можно достаточно быстро сформировать сетевую инфраструктуру, у которой будут самые высокие показатели надёжности. Передача цифровой информации в сетях VSAT характеризуется низким уровнем ошибок (не более одной на 10 млн переданных бит информации, что соответствует примерно одной ошибке на 500 страниц текста) и надёжной работой (до 100 тыс. часов, а это почти 10 лет бесперебойной быстрой связи). Конечно, имеются и свои проблемы. Например, спутниковые сигналы подвержены ослаблению во влажной атмосфере (дождь, туман, облачность). Впрочем, погодные помехи спутниковой связи учитываются при проектировании и устраняются путем правильного выбора места установки антенного поста.

Перехват данных в одностороннем спутниковом канале

Классический односторонний спутниковый доступ по-прежнему достаточно популярен, при этом в качестве обратного канала применятся любой доступный наземный канал связи (GPRS, ADSL, и пр.). Абсолютное большинство провайдеров такого доступа не используют шифрование спутникового трафика. Поэтому все данные, которые пользователь загружает через спутник, могут быть параллельно приняты и просмотрены посторонним лицом.

Самый простой и достаточно надёжный способ защиты данных от спутникового перехвата — установка специального программного акселератора, тем более что большинство провайдеров предоставляют ее бесплатно. В таком случае задача хакера значительно усложняется. Данные, передаваемые по протоколу TCP/IP, сжимаются согласно алгоритмам компрессии (например, V.44), а работа с сеансами TCP осуществляется по технологиям посредника Web, PEP и спуфинга TCP.

И все-таки такому методу защиты не стоит доверять из-за отсутствия криптостойкого шифрования трафика. Между тем в современных двусторонних сетях VSAT используются мощные системы кодирования на программно-аппаратном уровне, что делает перехват практически невозможным.

Обеспечение безопасности в прямом и обратном спутниковом канале

Спутниковый канал в направлении от ЦУС к терминалу пользователя называется прямым спутниковым каналом (DVB-S, DVB-S2, Frame Relay). Этот канал — единый для всей сети терминалов оператора. По нему осуществляется передача конфигурационных параметров и управляющих команд оператора, а также пользовательских данных. Все передаваемые данные проходят многоступенчатую систему преобразований и шифрования. У каждого производителя спутникового оборудования свой подход к реализации такой системы (см. врезку «Структура прямого и обратного канала в сети HughesNet»). Общие принципы таковы:

- применение фирменных алгоритмов шифрования данных;
- проверка подлинности терминала при его регистрации в сети оператора (аппаратный ключ);
- шифрование как всего сеанса работы (программный ключ), так и каждого сеанса в отдельности (сеансовые ключи);
- применение фирменных алгоритмов преобразования исходных данных во внутренние форматы (структуры) данных, которые потом передаются через спутниковый канал. Тем самым решаются задачи дополнительной защиты информации, доставки служебной информации и коррекции ошибок;
- ускорение данных, передаваемых по протоколу TCP/IP. В создаваемых виртуальных каналах исходные данные в сеансах TCP группируются, сжимаются и получают приоритеты.

Спутниковые каналы в направлении от терминалов к ЦУС называются обратными спутниковыми каналами. Сети терминалов оператора могут работать сразу с несколькими обратными каналами. Само их устройство и метод работы позволяет говорить о них как о защищенных. В настоящий момент самыми распространенными способами функционирования терминалов в таких каналах являются принципы доступа с временным и частотно-временным разделением каналов (Time/Frequency Division Multiple Access, TDMA/FDMA).

Рисунок 2. Пример установки антенны

Каждый обратный канал работает в своей частотной полосе (или со своей несущей) и с определенным алгоритмом кодирования для выявления и коррекции ошибок передаваемых данных (Turbo Coding). Конкретный терминал может осуществлять передачу только в одном обратном канале. Однако многие производители спутникового оборудования уже реализовали возможность изменения частот несущих обратных каналов, на которых терминалы осуществляют передачу (FDMA) от одного пользовательского сеанса к другому. Данная возможность позволяет, с одной стороны, выполнять перераспределение всех передающих терминалов по обратным каналам в рамках их группы (балансировку нагрузки), а с другой — значительно усложняет перехват передаваемых данных.

Каждый обратный канал делится на временные составляющие. С точки зрения терминалов он не является непрерывным, а представляет собой последовательность импульсных сигналов, причем

длительность каждого не превышает несколько миллисекунд. При методе многостанционного доступа с временным разделением (TDMA) передатчики множества терминалов передают данные в выделенные им временные интервалы по одному каналу или в рамках группы каналов.

Информационная безопасность в спутниковой сети повышается за счет сложности методов организации обратных каналов, а также применения фирменных алгоритмов по работе с ними. Если терминал по какой-то причине не сможет получить управляющую информацию от серверов по зашифрованному прямому каналу, то ему не удастся передать свои данные в обратном канале. И наоборот, если он некорректно работает по обратному каналу, то не сможет правильно принимать данные.

Аппаратно-программные средства защиты в спутниковой сети

Основным способом обеспечения безопасности передачи данных в беспроводном спутниковом канале является применение аппаратно-программных средств защиты данных. Во-первых, весь обмен информацией с внешними сетями и Internet контролируется в соответствии с заданной политикой безопасности на пограничных маршрутизаторах и межсетевом экране оператора. Во-вторых, передаваемые данные шифруются с помощью фирменных алгоритмов криптозащиты производителя спутникового оборудования. В-третьих, постоянный сбор статистики по работе сети и серверов позволяет технической службе эффективно отслеживать и корректировать функционирование сети в любое время суток.

Шифрование данных в спутниковом канале осуществляется при участии как спутниковых терминалов на стороне клиента, так и специализированных высокопроизводительных серверов на ЦУС оператора. На специальном сервере оператора размещается защищенная база данных ключей шифрования и сеансовых ключей всех спутниковых терминалов. Чтобы терминал смог работать в сети оператора, информация в базе ключей оператора должна соответствовать аппаратному ключу, который хранится на интегральной схеме терминала. Это исключает несанкционированное подключение терминалов «чужого» оператора. За генерацию ключей и их распространение отвечает компания-производитель спутникового оборудования. Терминалы изготавливают таким образом, чтобы они были защищены от извлечения ключей шифрования, воздействия любых внешних сигналов, а также от вскрытия оборудования для анализа.

На серверах ЦУС для межсерверного сетевого взаимодействия операторы часто используют модифицированные транспортные протоколы. Это делается в целях обеспечения полного контроля за серверными сетевыми интерфейсами, а также для защиты от несанкционированного доступа к ним. Каждый сервер имеет «горячий» резерв — отдельно стоящий идентичный сервер, который берет на себя всю работу в случае выхода из строя основного устройства. Кроме того, сетевое взаимодействие оборудования логически разделено на виртуальные сети по технологии VLAN (IEEE 802.1Q), чтобы данные для управления и контроля были изолированы от пользовательских. В результате атаки на сеть оператора со стороны клиентов или из Internet становятся невозможными, а распространение вирусов в сети блокируется.

Спутниковые абонентские терминалы имеют необходимый набор средств для обеспечения как собственной безопасности, так и для защиты подключенных к ним сетей. Главным инструментом, конечно же, является сетевой фильтр — его функционала достаточно, чтобы исключить большинство атак по портам и протоколам на сети клиентов через спутниковые каналы связи. Расширенные возможности по регистрации различных ошибок, попыток несанкционированного доступа и взлома предоставляет сервис генерации событий. Информация о событиях автоматически передается на центральный пульт управления ЦУС оператора. Для более детального анализа работы терминала привлекаются записи в журнале событий.

Управлять спутниковыми терминалами и изменять их конфигурации разрешается только компетентным техническим специалистам ЦУС оператора. Обычно они используют программный комплекс, разработанный производителем спутникового оборудования. Посредством этого ПО эффективно решается большая часть задач по защите информации в канале: регистрация новых терминалов, контроль их состояния и доступа, управление информацией о ключах.

Защита соединения спутниковых каналов связи с наземными

Спутниковые каналы VSAT широко применяются при построении распределенных корпоративных сетей. Как уже отмечалось, для таких каналов предусматривается достаточно высокий уровень шифрования и защиты данных. Но что делать, если необходимо соединить центральный офис клиента через наземную линию связи со множеством филиалов, доступ к которым организован через спутниковый канал, причем связь должна быть защищенной?

Обычно центральный офис компаний имеет высокоскоростной доступ в Internet по наземным линиям связи или выделенную линию до центра коммутации (до площадки ММТС-9). Задача сопряжения

сетей решается путем создания защищенного туннеля VPN между ЦУС спутникового оператора и центральным офисом клиента (см. Рисунок 3). Для этого можно использовать любой из протоколов туннелирования VPN: MPLS, IPSec, PPTP, L2F и прочие. Реализованная в соответствии с такими принципами схема связи будет довлетворять заказчика как по степени информационной безопасности, так и по скорости доступа.

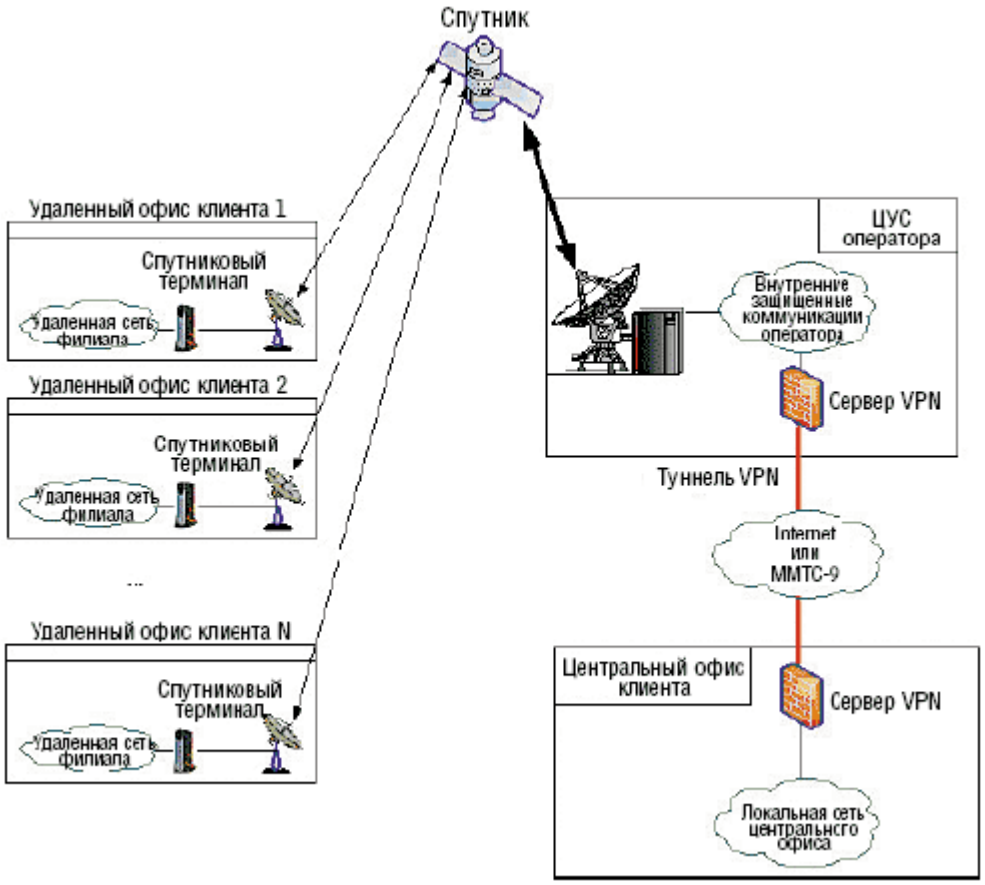

Рисунок 3. Схема построения защищенной корпоративной сети при использовании спутниковых и наземного каналов связи

В качестве примера построения защищенной корпоративной сети связи с использованием спутниковых и наземного каналов связи можно привести канал VPN, созданный для подмосковного сегмента сети автозаправочных станций компании «Сибур-Петрокон». Одним из основных требований к сети связи было наличие высокоскоростных защищенных каналов доступа через Internet, поскольку на удаленных АЗС планировалось подключение POS-терминалов для оплаты услуг посредством пластиковых банковских карт. Туннель VPN надежно защитил данные, поступающие от АЗС в процессинговый центр банка.

Передача секретной информации

При применении специализированного оборудования спутниковые каналы могут служить и для передачи информации с грифом «конфиденциально», «секретно», «совершенно секретно». Такие устройства подключаются через стандартные порты (синхронным и асинхронным интерфейсам) между компьютером или другим средством обработки информации и терминалом VSAT, обеспечивая требуемую криптографическую защиту информации. Соответствующие отечественные разработки, причем хорошего качества, уже имеются в продаже.

Резервирование каналов

Спутник предохраняет передаваемую информацию гораздо надежнее, чем другие технологии связи. Многие компании выбирают спутниковые системы VSAT для резервирования имеющихся каналов как заведомо безопасные с технической точки зрения и максимально защищённые от повреждений и сбоев. Скорость работы по спутниковому каналу для терминала VSAT составляет от 16 Кбит/с до 10 Мбит/с и более, что сопоставимо со скоростью передачи данных в наземном канале.

Приведем еще один пример. Коммерческий банк «Москомприват-банк» установил в одном из своих филиалов спутниковую систему VSAT. Вскоре после подключения к сети VSAT основная наземная

сеть банка вышла из строя. Вся система передачи данных автоматически переключилась на спутниковую связь, при этом переход на дублирующий канал произошёл столь быстро и плавно, что сотрудники банка ничего не заметили. И лишь позже, по уведомлению оператора, который отслеживал ситуацию в реальном времени, был установлен факт переключения на спутниковый канал. В итоге система работала в резервном режиме несколько дней.

Заключение

Помимо аппаратно-программных средств защиты спутниковые операторы применяют комплекс организационных и административных мер по защите своих узлов связи. Так, на ЦУС компании «Айпинэт» за безопасностью следит охрана, действует пропускной режим, ведется видеонаблюдение и установлена сигнализация. Техническими специалистами выполняются регламентные работы по полному резервному копированию баз данных и конфигурации всех ключевых серверов.

При соблюдении всего комплекса мер безопасности пользователи получают одно из самых защищенных в мире телекоммуникационных решений, отвечающее высочайшим требованиям к конфиденциальности информации. Спутниковые системы VSAT гибко настраиваются, что позволяет адаптировать их в соответствии с растущими запросами клиентов, работающих в высокотехнологичных отраслях. Так, для нефте- и газодобывающих компаний спутниковая связь VSAT считается сегодня стандартом де-факто. Это значимый довод в пользу спутниковых технологий.

***Об авторе**: Алексей Гладченков — начальник отдела развития компании «Айпинэт».*

Структура прямого и обратного канала в сети HughesNet

В случае прямого канала все передаваемые пакеты IP сначала поступают на спутниковый сервер-маршрутизатор IPGW, где упаковываются в пакеты UDP внутреннего формата. Далее эти пакеты передаются на сервер формирования пакетов MPEG (SATGW), на котором преобразуются в кадры многопротокольной инкапсуляции (Multi-Protocol Encapsulation, MPE). Каждый такой кадр состоит из нескольких компонентов:

- заголовка, в котором указывается MAC-адрес спутникового терминала назначения. MAC-адрес содержит серийный номер терминала. Поскольку всем терминалам на заводе производителя присваиваются уникальные серийные номера, получение данных другими терминалами исключается;
- порядкового номера кадра MPE (SEQ number). Он используется для учета и контроля порядка передачи последовательности кадров MPE;
- поля с зашифрованным пакетом IP. Для шифрования передаваемых пакетов IP, предназначенных для определенного терминала, сервер SATGW использует соответствующий секретный ключ шифрования. Алгоритм шифрования — собственная разработка компании Hughes;
- контрольной суммы кадра MPE. С ее помощью на терминале проверяется целостность каждого принятого кадра.

Полученная последовательность кадров MPE преобразовывается в последовательность транспортных пакетов MPEG (MPEG Transport Packets) длиной 188 байт каждый. Внутри такого пакета MPEG содержится:

- заголовок MPEG-2, в котором присутствуют уникальные данные компании-производителя спутникового оборудования. Эта информация исключает получение данных устройствами другого производителя;
- кадр MPE или фрагмент кадра MPE. Если кадр MPE не помещается в один пакет MPEG, то он разбивается на фрагменты.

На целевом терминале данные, полученные по прямому каналу Outroute, подвергаются обратному преобразованию, а вся зашифрованная информация декодируется соответствующими ключами. В итоге, терминал выдает исходные пакеты IP, которые передаются в локальную сеть.

Метод доступа терминалов к обратным каналам (Inroute) основан на собственном алгоритме, разработанном HughesNet. Функцию распределения всех передающих терминалов по обратным каналам выполняет специализированный сервер обратных каналов DNCC.

Обратный канал разбивается на временные составляющие — супер-кадры (superframe). Супер-кадр имеет длину 360 мсек и состоит из 8 кадров длительностью 45 мсек каждый. Кадр делится на слоты, измеряемые в байтах. Количество и размер слотов в одном кадре рассчитываются на основании

технических характеристик обратного канала. Пакеты IP, предназначенные для передачи терминалом, помещаются в интервальные пакеты (burst packet), которые затем распределяются по слотам и кадрам в заданное время и в заданном порядке. Контролем и управлением этим сложным процессом преобразований занимаются сервер DNCC и сервер синхронизирующих импульсов (Timing Unit Server).

Данные от терминалов поступают на ЦУС, на сервер DNCC, где интервальные пакеты проверяются на предмет их корректности и целостности, и затем они преобразуются в пакеты UDP служебного формата, которые направляются на спутниковый сервер-маршрутизатор IPGW. На его выходном сетевом интерфейсе пакеты IP получают свой первоначальный вид и теперь готовы для передачи в классическую целевую сеть доступа.