

Реализация AAA-процедур в сетях WiMAX



Михаил Светлов

Старший инженер службы IT НПЦ "Дэйтлайн"

В сетях беспроводного широкополосного доступа вообще и в сетях стандарта IEEE 802.16 в частности обеспечение безопасности является одной из важнейших задач. Оператор хочет быть уверенным в том, что абоненты, подключенные к его сети, получают доступ только к тем услугам, которые предусмотрены тарифом и производят оплату за предоставляемые им услуги. Абоненты сети хотят быть уверенными в том, что их частная информация защищена, целостность данных не нарушена и они всегда могут получить полный доступ к услугам, на которые подписаны.

Средства защиты каналов

Действительно, ожидания операторов и пользователей сети не только не противоречат друг другу, но и являются взаимодополняющими. Любая правильно спроектированная сеть нуждается в реализации средств защиты каналов от несанкционированного доступа (НСД), которые могут быть обеспечены только совместными усилиями производителей оборудования, системных интеграторов и сетевых операторов.

Профиль IEEE 802.16e-2005 определяет безопасность в сети WiMAX, на-

чиная с канального уровня (MAC), с помощью процедур аутентификации на основе алгоритмов AES, PKI, X.509. Шифрование данных на канальном уровне обеспечивает неприкосновенность частной информации и защищает трафик от перехвата.

На сетевом уровне обеспечивается защита посредством использования брандмауэров и AAA-процедур (Authentication, Authorization, Accounting). В приложениях Mobile WiMAX AAA-процедуры непосредственно задействованы в обеспечении роуминга. Для реализации AAA-процедур наиболее широко используется протокол RADIUS (Remote Authentication in Dial-In User Service), описанный в спецификациях RFC2865, RFC2866.

На транспортном уровне и уровне приложений обеспечиваются дополнительные защитные меры по желанию оператора сети или сервис-провайдера (Application Service Provider, ASP) или самого конечного пользователя с использованием протокола TLS и цифровых подписей и сертификатов соответственно.

Аутентификация

Алгоритмы безопасности канального уровня реализуют важнейшие функции аутентификации, авторизации и шифрования, существующего между конечной станцией пользователя, то есть мобильной станцией (MS), но некоторые принципы вполне применимы к станции подписчика (SS – subscriber station) и базовой станции посредством интерфейса IEEE 801.16e-2005.

Здесь, говоря о безопасности сети, будем относить различные функции

безопасности к базовой станции (BS). В действительности, как будет показано далее, все эти функции могут располагаться не только на стороне BS, но могут быть распределены между остальными узлами сети.

Существуют две формы процедуры аутентификации:

- односторонняя аутентификация – BS аутентифицирует MS;
- двухсторонняя аутентификация – BS и MS аутентифицируют друг друга.

Каждая реализация WiMAX должна иметь одностороннюю аутентификацию. Эксперименты показали, что двухсторонняя аутентификация (обоюдная) также весьма полезна.

Аутентификация реализуется путем использования протокола обмена публичными ключами, при этом обеспечивается не только собственно аутентификация, но и создание ключей шифрования. В схемах обмена публичными ключами каждый участник должен иметь публичный и частный (закрытый) ключи. Публичный ключ известен всем, частный же держится в секрете.

Стандарт WiMAX IEEE 802.16e-2005 определяет протокол управления (Privacy Key Management – PKM), поддерживающий три типа аутентификации:

- на RSA – цифровые сертификаты X.509 и RSA-шифрование;
- на EAP (опционально);
- на RSA после EAP.

Протокол аутентификации PKM устанавливает общий секретный ключ, называемый ключом авторизации (AK) между BS и MS. Как только между BS и MS установлен общий

Точки привязки сетевой эталонной модели

R1	Интерфейс между MS и ASN. Функциональность: воздушный интерфейс
R2	Интерфейс между MS и CSN. Функциональность: AAA, IP-конфигурация хостов, мобильное управление
R3	Интерфейс между ASN и CSN. Функциональность: AAA, управляющие политики, мобильное управление
R4	Интерфейс между шлюзами ASN. Функциональность: мобильное управление
R5	Интерфейс между несколькими CSN. Функциональность: роуминг, межсетевое взаимодействие
R6	Интерфейс между BTS и шлюзом ASN. Функциональность: управление IP-туннелями для установки и освобождения соединений MS
R8	Интерфейс между базовыми станциями. Функциональность: передача управления между базовыми станциями при движении абонента

АК, ключ шифрования ключей (КЕК) выводится из использования. После этого КЕК используется для шифрования в ходе РКМ последующего обмена ключом шифрования трафика (ТЕК).

В аутентификации, основанной на RSA, BS аутентифицирует MS по ее уникальному цифровому сертификату, созданному производителем MS. Сертификат X.509 содержит публичный ключ (PK) MS и ее MAC-адрес. Когда появляется необходимость в АК, MS отправляет свой цифровой сертификат на BS, которая проверяет сертификат, и затем использует проверенный PK для шифрования АК. Зашифрованный АК передается обратно на MS. Все базовые станции, которые имеют RSA-аутентификацию, имеют фабрично установленные парный частный/публичный ключ (или алгоритм для динамической генерации этих ключей) и цифровой сертификат X.509.

В случае использования аутентификации, основанной на EAP, MS аутентифицируется либо посредством уникального фактора оператора, например SIM, либо также посредством цифрового сертификата X.509, как было описано выше.

Выбор метода аутентификации зависит от выбора оператором типа EAP:

- EAP-AKA (аутентификация и согласование ключей) – для аутентификации, основанной на SIM;
- EAP-TLS – для аутентификации на основе сертификатов X.509;
- EAP-TTLS – для MS-CHAPv2 (Microsoft-Challenge Handshake Authentication Protocol).

BS ставит в соответствие MS и подписчика услуги и соответственно определяет список сервисов, к которым подписчику разрешен доступ. Таким образом, через обмен АК BS определяет подписчика и доступные для него сервисы.

Авторизация

После стадии аутентификации MS отправляет запрос на авторизацию базовой станции. Этот так называемый запрос АК, который также называют запросом Ассоциации безопасности сущности (SA identity – SAID). Запрос на идентификацию включает сертификат X.509 MS, алгоритм шифрования и криптографический ID.

В ответ BS проводит необходимую процедуру подтверждения доступа (запрашивая сервер AAA в сети) и отправляет обратно ответ авторизации (Authorization

reply), который содержит АК, зашифрованный на публичном ключе MS, ключ времени жизни (lifetime key) и SAID.

После прохождения стадии авторизации AAA посредством BS периодически проводит процедуру повторной инициализации MS.

Ассоциация безопасности

Ассоциация безопасности (SA) определяется как набор защищенной информации, разделяемой между BS и одной или несколькими MS, подключенными к этой BS, для поддержания защищенного соединения через сеть доступа WiMAX.

Определены три типа SA – первичная, статическая и динамическая. Каждая MS устанавливает первичную SA на стадии инициализации MS. Статические SA обеспечиваются посредством BS. Динамические SA создаются и уничтожаются в реальном времени в соответствии с созданием и уничтожением потоков данных сервисов. Каждая MS может иметь несколько потоков данных сервисов в каждый период времени и соответственно несколько динамических SA. При авторизации MS базовая станция удостоверяется, что соответствующие SA совместимы с типами сервисов.

ЭЛЕКТРОПИТАЮЩЕЕ ОБОРУДОВАНИЕ



Разработка и внедрение систем электропитания
Производство электропитательного оборудования
Пусконаладочные работы
Сервисное обслуживание
Обучение персонала

Системы бесперебойного питания постоянного тока
Сейсмостойкое оборудование
Дистанционное питание
Выпрямители
Стабилизаторы
Инверторы
Инверторные системы
Распределительные шкафы
Щиты рядовой защиты
Средства управления и мониторинга
Системы оперативного постоянного тока
Аккумуляторные батареи



ОАО «Юрьев-Польский завод «Промсвязь»
www.ypr.ru
(49246) 2-27-96, 2-20-04



ООО «Промсвязь-Дизайн»
www.promsvyaz.ru
(495) 947-09-69
факс 947-09-97

ГОСТ Р ИСО 9001-2001 (ИСО 9001:2000)

