Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК

Игнатюк

Антон Андреевич

Анализ и характеристики методов доступа сетевых мобильных WiMAX устройств

АВТОРЕФЕРАТ
на соискание степени магистра техники и технологий

по специальности 1-458101 Системы, сети и устройства телекоммуникаций

Научный руководитель

(Королев А.И.)

Минск, 2015

ВВЕДЕНИЕ

Актуальность темы. Беспроводные сети обладают ощутимыми преимуществами, по сравнению с традиционными проводными сетями, главным из которых, конечно же, является:

- простота развёртывания;

- гибкость архитектуры сети, когда обеспечивается возможность динамического изменения топологии сети при подключении, передвижении и отключении мобильных пользователей без значительных потерь времени;

- быстрота проектирования и реализации, что критично при жестких требованиях к времени построения сети;

- также беспроводная сеть не нуждается в прокладке кабелей.

Системы беспроводной сети передачи данных существуют уже значительное время. Однако в последние 15-20 лет развиваются чрезвычайно интенсивно, став одним из основных направлений развития телекоммуникационной индустрии. Название «WiMAX» было создано WiMAX Forum — организацией, основанной в июне 2001 года с целью продвижения и развития технологии беспроводного широкополосного доступа.

На сегодняшний день технология WiMAX включила в себя не только достижения простых технологий беспроводного доступа, таких как Wi-Fi, но и современные технологии сотовых сетей 3-го и 4-го поколений. WiMAX имеет огромные преимущества в организации современной беспроводной сети. Пропускная способность каналов данной сети нисколько не уступает проводным технологиям. Дальность распространения радиоволн в несколько раз превышает, обыденных Wi-Fi сетей, что позволяет организовать крупномасштабные сети в рамках города. Главное преимущество технологии WiMAX является то, что возможно обслуживать не только статичных пользователей услуги, но и тех, кто постоянно находятся в пути. Мобильность – один из важных факторов, предоставляющий удобство для абонента.

Основной целью работы является разработка методики организации и настройки режимов передачи данных и защиты WiMAX-сетей от несанкционированного доступа. Для достижения поставленной цели в работе решались следующие задачи:

1) Исследование технологии высокоскоростной беспроводной передачи данных WiMAX стандарта IEEE 802.16;

2) Исследование топологий и методов организации режимов передачи и защиты данных от несанкционированного доступа WiMAX-сетей;

3) Исследования методов доступа сетевых устройств WiMAX-сетей к радиоканалу;

4) Разработка методик организации и настройки режимов передачи данных и защиты WiMAX-сетей от несанкционированного доступа.

Структура и объем диссертации

Общий объем диссертации составляет 65 страниц, 23 рисунка, 1 таблица, список из 28 использованных в работе источников.

ОСНОВНАЯ ЧАСТЬ

Во **введении** определена актуальность технологии WiMAX, преимущества перед проводными системами доступа, необходимость исследования по данной теме, сформулированы цель и задачи работы.

В **первой главе** изучены основные сведения о WiMAX-сетях: описана история развития технологии, дано краткое описание технологии, описаны все существующие и существовавшие ранее стандарты WiMAX-сетей. Показано, что сеть WIMAX состоит из 2-х подсистем: ASN (Access Service Network) - сеть доступа и CSN (Connectivity Service Network) - сеть обеспечения услуг; предоставлено описание ASN и CSN.

В состав сети ASN входят 2 основных элемента: BS (Base Station) и ASN Gateway.

ASN выполняет следующие основные функции:

- доступ абонентов в сеть по радиосоединению;

- передача AAA-сообщений между CSN и абонентским оборудованием для обеспечения функций аутентификации, авторизации и аккаутинга соединений (Authentication, Authorization, and Accounting);

- установление сигнальных соединений между станцией и абонентским оборудованием;- управление радиоресурсами;

- пейджинг, т.е. поиск абонентов в сети при поступлении входящего соединения;

- мобильность абонентов (управление хэндоверами);

- туннелирование между сетями ASN-CSN.

В сеть CSN могут входить такие элементы как роутеры, AAA сервер, базы данных абонентов, устройства преобразования сигнализации.

К основным функциям CSN относятся:

- распределение -адресов и параметров между пользователями сети;

- доступ к сети Internet;

- функции AAA;

- контроль доступа абонентов в сеть, основанный на профилях пользователей;

- туннелирование между сетями ASN-CSN;

- биллинг и межоператорское взаимодействие;

- туннелирование между CSN и роуминг;

- мобильность между различными ASN, т.е. хэндовер между различными сетями доступа;

- Обеспечение сервисов WIMAX, а именно определение местоположение, предоставление соединений типа "точка-точка", резервирование соединений и т.п.

Во **второй главе** приведена классификация и принцип построения топологий WiMAX-сетей. Показано, что Для соединения «точка–точка» использу-

ются две направленные друг на друга антенны. При топологии «точка–многоточка» в центре «ячейки» помещается базовая станция со всенаправленной или секторной антенной, а все обслуживаемые ей абоненты снабжаются сфокусированными на нее направленными антеннами. При использовании только всенаправленных антенн будет достигнута возможность соединения «каждого с каждым», или «многоточка–многоточка».

Показаны методы организации передачи данных WiMAX-сетей. На физическом уровне в стандарте IEEE 802.16 метод ортогонального частотного мультиплексирования OFDM значительно расширяет возможности оборудования, в частности, позволяет работать на относительно высоких частотах в условиях отсутствия прямой видимости. Кроме того, в нее включена поддержка топологии «каждый с каждым», при которой абонентские устройства могут одновременно функционировать и как базовые станции, что сильно упрощает развертывание сети и помогает преодолеть проблемы прямой видимости.

При формировании OFDM-сигнала цифровой поток данных делится на несколько подпотоков, и каждая поднесущая связывается со своим подпотоком данных. Амплитуда и фаза поднесущей вычисляются на основе выбранной схемы модуляции.

Одним из главных преимуществ метода OFDM является его устойчивость к эффекту многолучевого распространения. Для того чтобы избежать межсимвольных искажений, перед каждым OFDM-символом вводится защитный интервал, называемый циклическим префиксом. Циклический префикс представляет собой фрагмент полезного сигнала, что гарантирует сохранение ортогональности поднесущих.

Многолучевое распространение радиосигнала может приводить к ослаблению и даже полному подавлению некоторых поднесущих вследствие интерференции прямого и задержанного сигналов. Для решения этой проблемы используется помехоустойчивое кодирование.

Важной особенностью гибкости физического уровня является возможность выбора ширины для полосы пропускания канала. Стандарт предусматривает выбор ширины полосы с шагом от 1,25 МГц до 20 МГц со множеством промежуточных вариантов, что позволяет более эффективно использовать радиочастотный спектр.

В стандарте IEEE 802.16-2004 используется технология множественного доступа с разделением по времени (TDMA), согласно которой базовая станция выделяет абонентским станциям временные интервалы, чтобы они могли передавать данные в определенной очередности, а не случайным образом.

Для реализации дуплексного режима обмена данными используются две технологии: дуплексный режим с разделением по времени (TDD) нисходящего и восходящего потоков и дуплексный режим с разделением по частотам (FDD).

В соответствии со стандартом, для предотвращения несанкционированного доступа и защиты пользовательских данных осуществляется шифрование всего передаваемого по сети трафика.

После процедуры конфигурирования аутентификация АС на базовой станции происходит следующим образом:

Абонентская станция посылает запрос на авторизацию, в котором содержится сертификат X.509, описание поддерживаемых методов шифрования и дополнительная информация.

Базовая станция в ответ на запрос на авторизацию (в случае достоверности запроса) присылает ответ, в котором содержится ключ на аутентификацию, зашифрованный открытым ключом абонента, 4-битный ключ для определения последовательности, необходимый для определения следующего ключа на авторизацию, а также время жизни ключа.

В процессе работы АС через промежуток времени, определяемый администратором системы, происходит повторная авторизация и аутентификация, и в случае успешного прохождения аутентификации и авторизации поток данных не прерывается.

В **третьей главе** исследованы методы доступа сетевых устройств Wi-MAX-сетей.

Показано, что fixed WiMAX. Стандарт использует диапазон частот 10-66 ГГц. Этот частотный диапазон из-за сильного затухания коротких волн требует прямой видимости между передатчиком и приёмником сигнала.

Nomadic WiMAX. Сеансовый доступ добавил понятие сессий Fixed WiMAX, что позволяет свободно перемещать клиентское оборудование между сессиями и восстанавливать соединение уже с помощью других вышек WiMAX.

Для режима Portable Wi**MAX** добавлена возможность автоматического переключения клиента от одной базовой станции WiMAX к другой без потери соединения. Ограничена скорость передвижения клиентского оборудования - 40 км/ч.

Mobile WiMAX был разработан в стандарте 802.16e-2005 и позволил увеличить скорость перемещения клиентского оборудования до более 120 км/ч.

Показано, что централизованный ASN-шлюз предназначен для сетей большого масштаба с сотнями базовых станций и десятками тысяч абонентов внутри сети.

Достоинствами данного метода являются:

- Агрегация трафика и маршрутизация;
- MS управление доступом;
- Управление хэндовером MS между базовыми станциями;
- На основании IP сетевой платформы;
- Высокая производительность;
- Большое количество абонентов (100-600 тыс.);
- Высокая пропускная способность (5Гбит/с - 30Гбит/с агрегированного трафика);
- Легко масштабируема;
- Набор приложений безопасности, VPN и QoS;

- Высокая доступность;

- Резервная архитектура;

- Централизованная архитектура;

- Может управлять до 1000 BS и 500k сессий.

Недостатки:

- Высокая стоимость;

- При выходе из строя теряется связь со всеми подключенными.

В случае распределенной модели функции ASN-шлюзов реализуют устройства в составе БС (модуль устройства сетевой обработки NPU). Такое решение предназначено в первую очередь для сетей малого масштаба, не более 3 тыс. абонентов и до 200 Мбит/с на один ASN-шлюз.

Достоинства:

- Агрегация трафика и маршрутизация;

- На основании IP сетевой платформы;

- Высокая производительность;

- Меньший масштаб для обслуживания площадей с небольшим количеством абонентов;

- Эффективное в затратах решение.

Недостатки:

- При увеличении абонентов нужно добавлять число ASN GW, что приведет к увеличению стоимости.

В **четвертой главе** исследованы разработанные методики организации и настройки режимов передачи данных и защиты WiMAX-сетей от несанкционированного доступа.

На передачу данных и безопасность влияют многие факторы, которые необходимо исследовать от самого начала проектирования сети.

К характеристикам, которые необходимо учитывать в первую очередь, относятся:

- ширина радиоканалов и частотные диапазоны;

- чувствительность и мощность приемо-передатчиков;

- особенности реализации антенно-фидерного тракта (antenna diversity, MIMO, beam forming),

- виды предоставляемых услуг (данные, голос, видео);

- карта покрываемой территории, плотность и распределение абонентов;

- количество абонентов (фиксированных, пеших, мобильных и по видам услуг);

- наличие и процент проникновения конкурирующих технологий доступа (xDSL, MetroEthernet, оптики, Wi-Fi).

При выборе оборудования WiMAX следует еще учитывать такие характеристики базовых станций, как:

- количество радиоканалов (возможность наращивания (масштабирования), резервирования, горячей замены блоков);

- конструктивное исполнение базовых станций (внешнее, внутреннее, смешанное).

Поскольку WiMAX строится по сотовому принципу, обслуживаемая территория покрывается сетью базовых станций, связанных опорной сетью. При проектировании оценивается количество секторов в зависимости от диаграмм направленности, усиления антенн.

Максимально разрешенный радиус сот (в км) определяется категорией местности по максимальной численности населения города на обслуживаемой территории.

При частотном планировании следует учитывать, что технология OFDMA позволяет управлять мощностью передаваемых поднесущих, в связи с чем становится возможным применение различных методов повторного использования частот. При проектировании сети необходимо найти золотую середину, используя наибольший частотный диапазон, при сохранении соотношения сигнал/шум на минимально допустимом уровне.

Первый метод - увеличение количества сот в кластере. Сотовая структура позволяет увеличить пропускную способность канала, всей системы путём увеличения сот, уменьшения размеров сот и уменьшения мощности передатчиков.

Второе решение заключается в ослаблении соканальных помех при использовании секторных антенн, с шириной диаграммы направленности в 60° или 90°. То есть каждая сота разделяется на четыре или шесть секторов соответственно.

Решение проблемы связанных с соканальными помехами на краю сот, в стандарте WiMAX предложен метод, комбинированного повторного использования частоты (FFR), то есть комбинированное планирование сот.

В сотовых системах подвижной радиосвязи выделяют несколько этапов строительства. Ключевыми этапами планирования являются этап разработки частотного плана, расчёта пропускной способности и этап настройки системы. Данные этапы являются единственными, где проводятся расчёт прогнозируемых зон обслуживания базовыми станциями, интерференционный анализ и оценка распределения напряжённости поля.

Применение современных систем автоматизированного проектирования сетей подвижной радиосвязи не даёт удовлетворительных результатов. Это связанно с тем, что многие модели, заложенные в системы проектирования, являются эмпирическими или полуэмпирическими, следовательно, приближёнными моделями. Причём, невозможно в данные модели заложить всю информацию об исследуемом районе (плотность застройки, тип материалов застройки, высотную модель застройки). Если же последние факторы в какой-то степени являются детерминированными, то такие факторы, как погодные условия, движущиеся объекты, влияющие на распространения радиосигналов, случайны и не могут быть заложены в данные модели. Отсюда следует, что усовершенствование моделей, заложенных в системы проектирования зон обслуживания базовыми станциями в системах подвижной радиосвязи, является перспективным.

При разработке любой системы **безопасности** необходимо понять способы, с помощью которых безопасность может быть скомпрометирована и таким образом усилить систему в соответствующими мерами безопасности.

Стандарт WiMAX включает в себя ряд мер по защите безопасности для устранения и преодоления различных угроз безопасности, создаваемых для системы. К ним относятся методы взаимной аутентификации, гибкий инструмент управления ключами, шифрование трафика, контроль и управление защитой сообщений.

Стандарт IEEE 802.16 определяет протокол PKM (privacy and key management protocol), протокол приватности и управления ключом. Защищенная связь (Security Association, SA) — одностороннее соединение для обеспечения защищенной передачи данных между устройствами сети.

Для данных первичная защищенная связь устанавливается абонентской станцией на время процесса инициализации. Базовая станция затем предоставляет статическую защищенную связь. Что касается динамических защищенных связей, то они устанавливаются и ликвидируются по мере необходимости для сервисных потоков.

Для авторизации абонентская станция и базовая станция разделяют одну защищенную связь. Базовая станция использует защищенную связь для авторизации для конфигурирования защищенной связи для данных.

Privacy and Key Management Protocol (PKM Protocol) — это протокол для получения авторизации и ключей шифрования трафика TEK.

Стандарт IEEE 802.16 использует алгоритм DES в режиме сцепления блока шифров для шифрования данных. В настоящее время DES считается небезопасным, поэтому в дополнении к стандарту IEEE 802.16e для шифрования данных был добавлен алгоритм AES.

Показано, что в стандарте IEEE 802.16 существует ряд **уязвимостей**:

1) Атаки физического уровня, такие как глушение передачи сигнала, ведущее к отказу доступа или лавинный наплыв кадров (flooding), имеющий целью истощить батарею станции. Эффективных способов противостоять таким угрозам на сегодня нет.

2) Самозваные базовые станции, что связано с отсутствием сертификата базовой станции. В стандарте проявляется явная несимметричность в вопросах аутентификации. Предложенное решение этой проблемы — инфраструктура управления ключом в беспроводной среде (WKMI, wireless key management infrastructure), основанная на стандарте IEEE 802.11i. В этой инфраструктуре есть взаимная аутентификация с помощью сертификатов X.509.

3) Уязвимость, связанная с неслучайностью генерации базовой станцией ключей авторизации. Взаимное участие базовой и абонентской станции, возможно, решило бы эту проблему.

4) Возможность повторно использовать ключи TEK, чей срок жизни уже истек. Это связано с очень малым размером поля EKS индекса ключа TEK. Так как наибольшее время жизни ключа авторизации 70 суток, то есть 100800 минут, а наименьшее время жизни ключа TEK 30 минут, то необходимое число возможных идентификаторов ключа TEK — 3360. А это означает, что число необходимых бит для поля EKS — 12.

5) Еще одна проблема связана, как уже упоминалось, с небезопасностью использования шифрования DES. При достаточно большом времени жизни ключа TEK и интенсивном обмене сообщениями возможность взлома шифра представляет реальную угрозу безопасности. Эта проблема была устранена с введением шифрования AES в поправке к стандарту IEEE 802.16e. Однако, большое число пользователей до сих пор имеет оборудование, поддерживающее лишь старый стандарт IEEE 802.16.

ЗАКЛЮЧЕНИЕ

1) Исследованы технологии высокоскоростной беспроводной передачи данных WiMAX стандарта IEEE 802.16;

2) Исследованы топологии и методы организации режимов передачи и защиты данных от несанкционированного доступа WiMAX-сетей;

3) Исследованы методы доступа сетевых устройств WiMAX-сетей к радиоканалу;

4) Исследованы разработаные методики организации и настройки режимов передачи данных и защиты WiMAX-сетей от несанкционированного доступа.

Многие телекоммуникационные компании делают большие ставки на использование WiMAX для предоставления услуг высокоскоростной связи. И тому есть несколько весомых причин. Во-первых, технологии стандарта 802.16 позволят экономически более эффективно (по сравнению с проводными технологиями, таких как DSL) не только предоставлять широкополосный доступ в сеть новым клиентам, но и расширять спектр услуг и охватывать новые труднодоступные территории. Во-вторых, беспроводные технологии многим более просты в использовании, чем традиционные проводные каналы. WiMAX и Wi-Fi сети просты в развёртывании и по мере необходимости легко масштабируемы. Этот фактор оказывается очень полезным, когда необходимо развернуть большую сеть в кратчайшие сроки. К примеру, WiMAX был использован для того чтобы предоставить доступ в сеть пострадавшим после цунами, который произошел в декабре 2004 года в Индонезии (Aceh). Вся имеющаяся на тот момент телекоммуникационная инфраструктура области была выведена из строя и требовалось оперативное восстановление услуг связи для всего региона.

В сумме все эти преимущества позволяют снизить цены на предоставление услуг высокоскоростного доступа в Интернет, как для бизнес структур, так и для частных лиц.

Ввиду факта, что стандартам типа 802.16 необходимо непрерывно развиваться, будут выпущены дальнейшие поправки и документы, поскольку данное развитие имеет место быть. Только принимая во внимание направление движения технологии и новые требования для 802.16, это поможет идти в ногу с потребностями пользователей. Один хороший пример постоянно развивающейся технологии - Ethernet. Этот стандарт используется много лет и будет использоваться и в дальнейшем. Это было достигнуто, просто модернизируя стандарт, чтобы идти в ногу с потребностями пользователей. Это главный сетевой стандарт в течение более чем 30 лет. Это также может случиться и для IEEE 802.16 стандарта.