УДК 004.732

Л.В. Буланая, асистент,
В.Г. Павлов, кандидат технических наук, доцент
(Национальный авиационный университет, Украина)

ЗАЩИТА ИНФОРМАЦИИ В БЕСПРОВОДНЫХ MESH-СЕТЯХ

В статье анализируются особенности защиты информации в беспроводных сетях: безопасность аутентификации и обеспечение доступности информации. Рассмотрены проблемы, связанные с ограниченной зоной покрытия в беспроводных сетях из-за специфики распространения радиоволн. Продемонстрированы преимущества, которыми обладают беспроводные ячеистые сети - Wireless Mesh Network: масштабируемость и надежность.

Прошло чуть больше 10 лет, как был впервые разработан и опубликован стандарт беспроводного Ethernet IEEE 802.11 (Wi-Fi), но сегодня трудно представить себе офис учреждения или учебный класс ВУЗа без возможности беспроводного подключения компьютеров к локальной сети. Причины такого быстрого распространения беспроводных технологий очевидны:

- быстрота развертывания и подключения;
- отсутствие необходимости в прокладке громоздких кабельных линий;
- простота в наращивании сети и изменении ее конфигурации;
- меньшие затраты по сравнению с традиционными проводными сетями.

Правда, в беспроводных сетях сложнее реализовать процедуру аутентификации при подключении нового пользователя к сети. Понятно, что для компьютеров, стационарно подключенных к определенным узлам сети, построить так называемый список доступа ACL (Access Control List) можно однократно, а изменения в него будут вноситься только при перераспределении прав пользователей. Появление «чужих» компьютеров в таких сетях является событием неординарным и будет требовать вмешательства администратора, а в крайнем случае может рассматриваться как несанкционированное подключение, несущее угрозу информационной безопасности. В беспроводных сетях количество подключенных компьютеров не является постоянным, а появление в зоне покрытия каких-либо иных компьютеров – вещь вполне обычная. Таким образом, процедура аутентификации здесь не основана на наличии обязательного физического подключения компьютера кабелем, а значит, алгоритм аутентификации должен быть более сложным.

В процессе эволюции протокола IEEE 802.11 мы можем наблюдать, как постепенно совершенствовалась и усложнялась процедура аутентификации.

Первоначально для опознания «своего» компьютера использовался его MAC-адрес, а для поиска «своей» точки доступа - идентификатор беспроводной локальной сети - SSID (Service Set Identifier). SSID позволяет логически отличать сети друг от друга, но ни в коей мере не обеспечивает конфиденциальность данных. Аутентификация, при которой для подключения достаточно знать SSID называется открытой (Open Authentication).

Более защищенной является аутентификация с общим ключом (Shared Key Authentication). Она подразумевает наличие у абонента статического ключа шифрования WEP (Wired Equivalent Privacy), иначе подключение к сети невозможно. Далее с помощью данного ключа шифруется специальное сообщение (Challenge Text), которое отправляется точке доступа, где с помощью такого же WEP-ключа расшифровывается. Если расшифровывание проходит успешно, то подключение абонента к сети разрешается.

Как видим, в данном случае используется классическая система с симметричным шифрованием. Однако здесь один и тот же ключ используется для всех абонентов точки доступа, а значит, на основе статистической обработки большого количества перехваченных зашифрованных сообщений может быть вычислен WEP-ключ. По этой причине аутентификация с

общим ключом не считается достаточно надежной и на сегодняшний день не рекомендуется для применения.

В ноябре 2002 г. была анонсирована спецификация WPA (Wi-Fi Protected Access), которая обеспечивает уровень безопасности больший, чем WEP. Это обусловлено тем, что в WPA поддерживается шифрование по стандарту TKIP (Temporal Key Integrity Protocol). В нем используется пофреймовое изменения ключей шифрования, что значительно уменьшает шансы взлома ключей на основе статистической обработки.

Спецификация WPA2 представляет еще более высокий уровень защиты процедуры аутентификации в беспроводных сетях, поскольку поддерживается шифрование по стандарту AES (Advanced Encryption Standard), который считается более криптоустойчивым по сравнению с применяемым в WEP алгоритмом RC4.

Однако сложность аутентификации в Wi-Fi сетях не является единственной проблемой. Дело в том, что беспроводные сети чувствительны к условиям распространения радиосигнала. Даже в идеальном случае дальность распространения сигнала не превышает 100 м при мощности передатчиков порядка 100 мВт. Такие физические факторы, как строительные материалы и характер конструкций (многоэтажные бетонные здания, толстые стены и потолки), значительно уменьшают зону надежного приема радиосигнала. В результате ухудшается показатель доступности информации, что, конечно, недопустимо.

Увеличение зоны покрытия может быть достигнуто за счет более рационального расположения точек доступа, когда формируется ячеистая структура, наподобие сот мобильной телефонной связи. Для определения границы действия точек доступа на практике используется ноутбук с установленной программой измерения скорости передачи, например, ***Network Stumbler*** (www.stumbler.net). Перемещая ноутбук по офису можно определить расстояния, на котором скорость падает до порогового значения и где требуется установить новую точку доступа. Понятно, что такой способ «оптимизации» не предполагает гибкого расширения сети и имеет ограниченное применение.

Поиск решения проблемы потери мощности сигнала и ограниченности зоны покрытия для сетей Wi-Fi привел к разработке технологии Wireless Mesh Network (WMN - ячеистая сеть). В отличие от вышеупомянутых ячеек, образованных точками доступа, здесь все основано на объединении абонентских компьютеров. За основу взята существующая в стандарте 802.11 возможность специального режима Ad-Hoc (точка-точка), которая была первоначально предназначена для создания одноранговой (P2P) сети беспроводных клиентов. В этом режиме каждый узел представляет собой также маршрутизатор, способный передавать трафик другим узлам. Подход P2P обеспечивает высокую производительность, требуемую в ячеистых сетях.

WMN образуется на основе множества соединений «точка-точка» узлов находящихся в области радиопокрытия друг друга, расширяет функциональность беспроводного доступа в Интернет и позволяет реализовывать точки доступа с охватом на порядок более высоким, чем у привычных хот-спотов. С возможностью обеспечения защищенного беспроводного покрытия как внутри помещений, так и на улицах, в городской местности или в крупных населенных пунктах, Wireless Mesh может быть использована для быстрого развертывания, в частности, сети связи для целей внутренней безопасности или в случаях чрезвычайных ситуаций в городе.

Для применения в WMN режим Ad-Hoc был расширен в части поддержки возможности маршрутизации. В беспроводной ячеистой сети протокол маршрутизации аналогичен IGP (Interior Gateway Protocol). Поэтому внутри ее собственного «домена» организация маршрутов «точка-точка», многоточечных и многоадресных выполняется способом, полностью совместимым с внешними протоколами коммутации и маршрутизации.

Каждый узел в WMN вычисляет исходное дерево, которое определяет пути ко всем соседним узлам в пределах досягаемости радиосигнала. Соседние узлы связываются друг с другом посредством специальных служебных пакетов, распространяемых в сети. Поскольку ситуация в сети может со временем меняться из-за изменения состава и расположения або-

нентов, процесс опроса периодически повторяется, что обеспечивает динамическую сквозную реконфигурацию.

Для максимизации производительности при передаче трафика от одного края сети к другому могут вычисляться метрики канала, как и в других протоколах маршрутизации. Эти метрики способны базироваться на полосе пропускания, уровне сигнала, его стабильности, задержке или других параметрах канала.

Помимо обеспечения высокой производительности и качественной связи Wireless Mesh обеспечивает высокую надежность сети, поскольку отключение или выход из строя одного из абонентских компьютеров вызовет лишь изменение маршрута передачи сообщений. Сеть автоматически переопределяет маршруты передачи данных между абонентами, что позволяет предотвратить сбои коммуникаций. При этом управление такого рода сетями является децентрализованным. Поскольку у каждого абонента имеется свой сетевой процессор и беспроводной интерфейс, то исчезает необходимость в централизованной коммутации. Иными словами, топология ячеистых сетей предусматривает либо непосредственную связь между абонентами, либо транзитную передачу данных по целой цепочке абонентов. Следовательно, перед тем как начать обмен данными, каждый абонент должен «решить», будет ли он выполнять функции точки доступа, служить транзитным устройством или сочетать обе роли. Далее абоненты определяют своих соседей, используя протокол типа «запрос/ответ», а также замеряют характеристики коммуникационных каналов: мощность принимаемого сигнала, пропускную способность, задержку и частоту ошибок. Абонентские компьютеры обмениваются этими значениями, а затем каждый из них на основе этой информации выбирает наилучший маршрут коммуникаций со своими соседями.

Процессы обнаружения и выбора наиболее благоприятного маршрута выполняются в фоновом режиме, так что каждый абонентский узел располагает актуальным списком соседей. В случае недоступности по тем или иным причинам какого-либо абонента соседние могут быстро реконфигурировать свои таблицы и вычислить новый оптимальный маршрут. Способность самоконфигурации и самовосстановления делает ячеистые сети очень надежными. Беспроводные ячеистые сети могут состоять из сотен и даже тысяч абонентов, что позволяет легко расширять их и обеспечивать необходимую избыточность.

Интеллектуальность вообще является одной из особенностей сетей Wireless Mesh, и можно сказать, что она интегрирована непосредственно в сеть и обеспечивает высокий уровень надежности, а это немаловажно как в экстренных случаях, так и для мобильных удаленных сотрудников. Это исключает необходимость ручного администрирования сети и играет важную роль для оперативного развертывания оборудования. Как только сеть запускается в эксплуатацию, она начинает автоматически управлять своей работой, благодаря функциям самовосстановления и самоадаптации.

Еще один фактор, определяющий перспективность применения WMN, это повышение скорости передачи информации. Дело в том, что физические параметры радиоканалов таковы, что на более коротких расстояниях пропускная способность сети выше. Причиной могут быть помехи и другие факторы, чье действие накапливается по мере увеличения расстояния. И потому одним из способов повышения пропускной способности сети становится передача данных через несколько узлов, разделенных небольшими расстояниями.

Следует учесть, что пространственное разделение — еще одно преимущество сетей Wireless Mesh по сравнению с сетями, использующими одну точку доступа. Если несколько абонентов пытаются одновременно пользоваться сетью, могут возникать виртуальные «заторы», замедляющие ее работу. Этот эффект «бутылочного горлышка» характерен для крупных корпоративных сред. Он выражается в виде резкого снижения пропускной способности сети, даже при условии достаточно широкого внешнего канала, соединяющего интрасеть с внешним миром. Дело здесь в том, что точки доступа стандартов 802.11 предоставляют среду с разделением по времени, в которой в данный момент времени лишь одна из них может вести передачу данных.

В противоположность этому в сетях ячеистой топологии множество устройств могут подключаться одновременно через разные цепочки коммутируемых узлов, благодаря чему формируются параллельные каналы передачи информации, что в большинстве случаев не снижает производительность сети.

Абонентские узлы остаются вполне автономными устройствами, способными самостоятельно управлять своим функционированием, и в то же время являются компонентом общей сети, допускающим управление из центральной точки. Используя SNMP, системный администратор может выполнять мониторинг и конфигурировать отдельные элементы, узлы, домены или всю сеть, а протокол обнаружения лишь упрощает данную задачу посредством поиска и локализации отдельных узлов для их отображения на дисплее управления.

Все указанные особенности сетей Wireless Mesh нашли свое отражение в разработке протокола IEEE 802.11s, который практически не затрагивает физический уровень распространения сигнала, а посвящен вопросам маршрутизации пакетов. Начатая в 2003 году разработка была практически завершена к 2008 году, поэтому разработчики сетевого оборудования (CISCO, NORTEL и др.) на сегодняшний день предлагают целый спектр уже готовых решений.

Выводы

1. Рассмотрены основные факторы, определяющие особенности беспроводных сетей:
   - необходимость применения более защищенного алгоритма аутентификации;
   - обеспечение доступности информации за счет формирования зоны надежного приема сигнала.
2. Проанализированы преимущества, которыми обладают ячеистые беспроводные сети WMN:
   - высокая надежность передачи информации за счет дублирования каналов связи;
   - самовосстановление и саморегулирование, что не требует ручной настройки;
   - более высокая скорость передачи, определяемая уменьшением расстояния между источником сигнала и приемником;
   - имеются значительно большие возможности по расширению или изменению топологии сети.
3. По вышеуказанным причинам перспективность широкого внедрения сетей Wireless Mesh не вызывает сомнений.

Список литературы

1. IEEE P802.11s/D1.08. Amendment: Mesh Networking. – IEEE, January 2008.
2. Беспроводные сети Wi-Fi / А. В. Пролетарский, И.В. Баскаков, Д. Н. Чирков; – М.: БИНОМ, 2007. – 178 с
3. Wi-Fi. Беспроводная сеть / Джон Росс; пер. с английского В.А. Ветлужских. – М.: НТ Пресс, 2007. – 320 с.
4. http://juniper.kz/nortel/12_4.htm
5. http://www.lastmile.su/issue/2008/2/6
6. http://ko.com.ua/node/24637
7. http://habrahabr.ru/blogs/the_future_is_here/79360/
8. http://research.microsoft.com/en-us/projects/mesh/
9. http://www.meshwlan.com/