

06, июнь 2016

УДК 004.057.4

Анализ и выбор наилучшего протокола маршрутизации для сетей 802.11s с количеством конечных узлов менее 100

*Гурьев Н. Н., студент
Россия, 105005, г. Москва, МГТУ им. Н. Э. Баумана,
кафедра «Системы обработки информации и управления»*

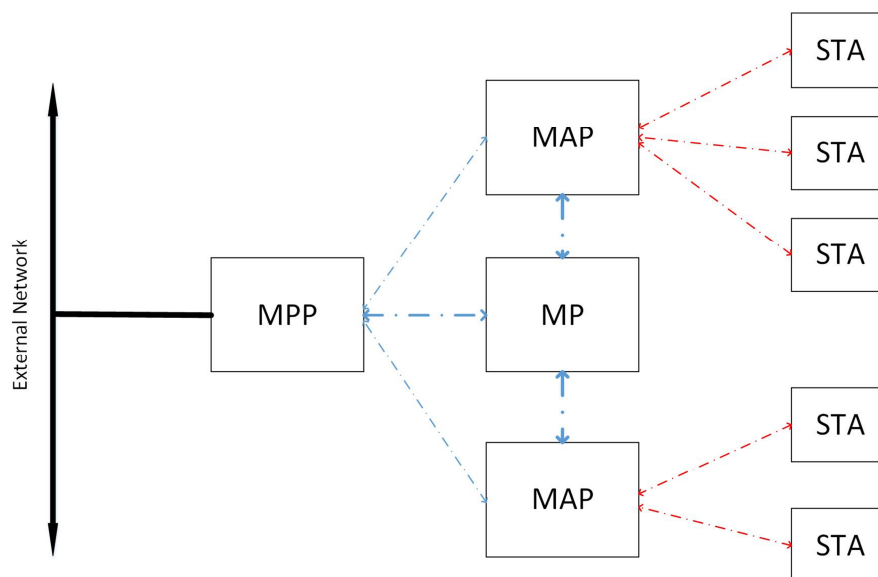
*Кочетков А. А., студент
Россия, 105005, г. Москва, МГТУ им. Н. Э. Баумана,
кафедра «Системы обработки информации и управления»*

*Научный руководитель: Аксенов А.Н., старший преподаватель
Россия, 105005, г. Москва, МГТУ им. Н. Э. Баумана,
кафедра «Системы обработки информации и управления»
aksenovan@bmstu.ru*

Введение

Беспроводная ячеистая сеть (WMN – Wireless Mesh Network) – это распределенная, одноранговая сеть с ячеистой топологией, в которой каждый узел имеет равные права.

Архитектура WMN сети на базе 802.11s изображена на рисунке.



Mesh Point (MP) – узел сети, обеспечивающий маршрутизацию и передачу пакетов по сети.

Mesh Portal Point (MPP) – граничный узел сети, обеспечивающий связь ячеистой сети с внешней сетью.

Mesh Access Point (MAP) – узел сети, позволяющий различным беспроводным устройствам, поддерживающим стандарт 802.11, подключаться к WMN.

Stations (STA) – беспроводные устройства с поддержкой стандарта 802.11, которые подключаются к MAP.

Mesh-сети бывают двух видов:

- самоорганизующиеся – автоматическое подключение к существующим участникам, самостоятельный выбор оптимального маршрута, самонастройка оборудования внутри сети
- настраиваемые – необходимость настроить сеть перед использованием

Особенности данной сети:

- независимость от провайдера
- возможность построить с относительной легкостью свою небольшую сеть
- каждый новый подключившийся элемент увеличивает емкость сети
- динамическая маршрутизация
- устойчивость сети при отказе отдельных элементов
- расширяемость сети
- мобильность станций

Mesh-сети описывает стандарт IEEE 802.11s. Основными целями этого стандарта является оптимизация маршрутов в беспроводных сетях с ячеистой топологией, а также интегрирование возможностей WMN в существующие сети 802.11 на MAC уровне.

Маршрутизация в сетях 802.11s

Изменения в 802.11s почти не затрагивают физический уровень (модели OSI). Большинство нововведений касаются MAC-подуровня канального уровня. Также в данном стандарте рассмотрены аспекты маршрутизации пакетов в сети, т.е. затрагивается сетевой и транспортный уровни модели OSI.

Существуют три основных типа протоколов:

- проактивный

- реактивный
- гибридный

Самая популярная реализация гибридного типа так и называется: гибридный протокол маршрутизации (HWMP – Hybrid Wireless Mesh Protocol). Данный протокол может работать в проактивном и реактивном режимах, таким образом являясь реализацией сразу двух типов.

Для нахождения оптимального маршрута применяются критерии, которые называются метриками. Наиболее распространенной метрикой является длина пути. Длина пути – это сумма длин каналов (путь между двумя соседними узлами) от узла отправителя к узлу источника .

Надежность также является распространенным критерием. Под данной метрикой обычно подразумевается процент потери пакетов при передаче по данному каналу. Но существуют и другие факторы, влияющие на данную метрику. Например, некоторые каналы имеют малый период восстановления соединения после разрыва, что положительно сказывается на показании данной метрики.

Другая важная метрика – задержка. Это время доставки пакета от отправителя к получателю. Эта метрика зависит от нескольких важных факторов, таких как физическое расстояние, которое необходимо преодолеть, пропускная способность каналов, загрузка сети и очередь в портах.

Пропускная способность нередко используется для выбора оптимального маршрута. Эта метрика подразумевает объем данных, который может быть передан по каналу в единицу времени.

Напрямую связана с пропускной способностью метрика загрузка. Она отражает степень занятости сетевых ресурсов, таких как каналы и маршрутизаторы. Важно отметить, что отслеживание показаний загрузки сети само по себе может потребовать значительных ресурсов.

В 802.11s присутствует обязательная для использования метрика времени передачи в канале (ALM – Airtime Link Metric). Эта метрика определяется формулой:

$$C_a = \left[O + \frac{B_t}{r} \right] \times \frac{1}{1 - e_f},$$

где O – константа, отражающая время доступа к каналу, зависит от применяемого протокола: 802.11a или 802.11b;

B_t – число битов в тестовом пакете, всегда 8192;

r – скорость передачи данных в канале. Измеряется в Мбит/с;

e_f – вероятность возникновения ошибки в тестовом пакете.

Вероятность возникновения ошибки e_f , если ошибки в пакете независимы друг от друга, определяется следующей формулой:

$$e_f = 1 - (1 - p_o)^n \approx np_o.$$

Метрика определяет оценку времени передачи пробного пакета длиной B_t с учетом возможных ретрансляций при потерях в канале. Способ определения параметров r и e_f в стандарте не приводится, однако можно предположить, что для этого должна использоваться периодическая рассылка пробных пакетов длиной $B_t = 8192$ бита.

Гибридный беспроводной mesh-протокол маршрутизации (HWMP)

Гибридный протокол маршрутизации HWMP использует стандартный набор служебных пакетов, правил их создания и обработки, подобно распространенному протоколу дистанционно-векторной маршрутизации по запросу (AODV – Ad Hoc On Demand Distance Vector). Однако HWMP работает с адресами MAC-уровня и метриками путей. Данному протоколу было дано название «гибридный», поскольку в нем объединены два режима построения путей: реактивный и проактивный. Они могут использоваться как одновременно в одной сети, так и по отдельности:

- реактивный режим – маршрутные таблицы в узлах mesh-сетей строятся по запросу непосредственно перед передачей данных. Данная процедура инициируется узлом-отправителем, а ее результатом является итоговое значение метрики пути «отправитель-получатель»;
- проактивный режим – маршрутные таблицы в узлах mesh-сетей периодически обновляются. Данная процедура инициируется корневым узлом, а ее результатом является граф путей, построенный на сети, в качестве вершины которого выступает сам корневой узел;

При реактивном режиме построения путей протокола HWMP узел-отправитель посылает широковещательный пакет запроса пути (PREQ – Path Request). Через соседние узлы пакет распространяется по всей сети, пока не достигнет узла-адресата. Критерием выбора пути служит метрика, информация о которой содержится в специальном поле служебных пакетов запроса пути. Поле метрики пути от отправителя до текущего узла модифицируется по мере продвижения от узла к узлу. В результате для пути «отправитель-получатель» формируется полная метрика. Узел-адресат посылает инициатору итоговое значение метрики пути «отправитель-получатель» в пакете

подтверждения (PREP – Path Reply). Таким образом, узел-инициатор, приняв его, получает сведения об установленном пути.

До получателя пакеты запроса в mesh-сетях, как правило, доходят по множеству путей через различные узлы. Широковещательные пакеты запроса пути PREQ могут передаваться циклически (по замкнутым маршрутам), неоднократно проходя через один и тот же узел. Для предотвращения данной ситуации применяется нумерация запросов. По стандарту 802.11s у каждого устройства mesh-сети имеется собственный порядковый номер назначения (DSN – Destination Sequence Number). Также в стандарте 802.11s существует понятие DSN инициатора поиска пути (OSN – Originator's DSN). При рассылке пакетов запроса пути данный параметр служит порядковым номером. Перед отправкой пакета PREQ в его поле OSN записывается увеличенное на единицу значение DSN инициатора. Также в пакет запроса записывается адрес начала пути (адрес инициатора). В полях «адрес отправителя», «метрика пути» и «порядковый номер» служебных пакетов передаются сведения, позволяющие всем узлам mesh-сети обновлять хранимую о каждом узле информацию.

Каждый узел сравнивает значение OSN полученного пакета PREQ с ранее сохраненным значением того же отправителя, если таковое имеется. Пакет запроса пути будет принят, обработан и ретранслирован при условии, что OSN текущего пакета больше OSN ранее сохраненного пакета, а в случае равенства OSN двух пакетов дополнительно необходимо, чтобы метрика вновь полученного пакета была лучше, чем метрика ранее полученного. Таким образом, исключена возможность приема и ретрансляции одного и того же пакета. В реактивном режиме все успешно принявшие пакет запроса пути PREQ промежуточные узлы могут так же, как и узел назначения, отправлять пакеты подтверждения PREP. Для этого в пакете запроса пути должны быть установлены необходимые флаги.

Второй важный параметр, который может изменяться в пакете запроса по мере прохождения от узла к узлу – время жизни (TTL – Time to Live). Значение данного поля характеризует число узлов, которые пакету разрешено пройти. В случае использования данного параметра он декрементируется с каждым последующим узлом. В случае достижения полем TTL значения нуля прекращается обработка и трансляция пакета.

В проактивном режиме протокола HWMP, в отличие от реактивного, в сети назначается один или несколько корневых узлов, которые производят периодическую рассылку пакетов PREQ, распространяющихся по всей сети. Каждый узел, принявший проактивный пакет PREQ, сохраняет адрес узла-отправителя, через который лежит путь к

корню, изменяет поля метрики и TTL, широковещательно ретранслирует пакет с измененными полями и отправляет PREP корневому узлу (в зависимости от установок, может не отправлять).

Реактивный и проактивный режимы построения путей протокола HWMP могут использоваться одновременно, например, в следующей ситуации: в штатном режиме сеть использует проактивный режим протокола HWMP, но один из узлов для установления прямого соединения с другим заданным узлом использует реактивный режим, выбирая путь по запросу.

Протокол маршрутизации HWMP является протоколом по умолчанию стандарта IEEE 802.11s и обязателен для всех устройств. Протокол маршрутизации HWMP является протоколом по умолчанию стандарта IEEE 802.11s и обязателен для всех устройств.

Оптимизированный протокол состояния канала для беспроводной сети (RA-OLSR)

Ранние версии стандарта IEEE 802.11s, помимо HWMP, предполагали использование модификации для беспроводной сети (RA-OLSR – Radio Aware OLSR) оптимизированного протокола маршрутизации по состоянию канала (OLSR – Optimized Link State Routing). OLSR является очень популярным проактивным протоколом маршрутизации для мобильных ad hoc сетей, который крайне эффективен в больших и плотных сетях. Он основан на механизме широковещательной рассылки для обновления информации о топологии сети. В данном протоколе при помощи сообщений приветствия и контроля осуществляется периодическое обновление маршрутной информации в сети, благодаря чему все узлы получают сведения о топологии сети и в них поддерживаются актуальные таблицы маршрутизации. Протокол описан в документе IETF RFC 3626.

В OLSR предусмотрен метод оптимизации рассылки сетевой информации, называемый многоточечной передачей (MPR – MultiPoint Relay). Каждым узлом m по таблице топологии сети выбирается несколько таких одношаговых соседей (neighbors) с симметричной связью, которые являются одношаговыми соседями хотя бы одному двухшаговому соседу (two-hop neighbor) данного узла. В результате для узла m в сети образовывается набор узлов $MPR(m)$, формирующийся таким образом, что все узлы в сфере радиусом 2 шага от m (соседи соседей) имеют симметричные с $MPR(m)$ каналы. В результате узлы MPR имеют связь со всеми узлами в сфере радиусом 2 шага от m . MPR выбираются каждый раз при обнаружении изменений в сфере радиусом 1 или 2 шага.

Посылаемые узлами широковещательные служебные пакеты выбора маршрута (ТС – Topology Control) распространяют по всей сети информацию о топологии сети, на основании которой каждый узел формирует свою таблицу маршрутизации. Пересылать ТС-пакеты могут только MPR-узлы, остальные узлы принимают эти пакеты, производят их обработку, но не участвуют в их дальнейшей пересылке.

Число передач служебных пакетов значительно снижается по сравнению с лавинной рассылкой благодаря механизму переключателя многоточечной передачи (MPRS – MPR Selectors), который для каждого MPR формируется из соседних узлов, выбравших его в качестве MPR. Информация о MPRS может пересылаться только между двумя соседними узлами. Передача происходит при помощи специальных приветственных пакетов (HELLO-пакетов), в которых сообщается об изменениях в топологии сети. В сообщениях содержится адрес узла-отправителя и перечень всех его доступных соседей с указанием их адресов и типов соединения (симметричное или ассиметричное). Таким образом узел сообщает своим соседям о доступных ему связях, передаются данные об одношаговых и двухшаговых соседях. Пакеты отправляются с заданным интервалом. Если узел не принимает HELLO-сообщение от соседа в течение определенного промежутка времени, связь с ним разрывается. Эта информация вносится в таблицу топологии сети абонента. ТС-пакеты в сеть отправляют только сведения о состоянии соединений между MPR и MPRS (то есть с одношаговыми соседями).

По полученной из ТС- и HELLO-сообщений информации узел строит граф, описывающий представление о построении сети для данного узла. С помощью этого графа для каждого узла строится таблица кратчайших расстояний. Существует серьезный недостаток подобного способа организации связи между узлами. Возможна ситуация, когда двухшаговый сосед является одношаговым для более, чем одного одношагового соседа передающего узла. Иными словами, существует несколько путей между узлами, находящимися на расстоянии двух шагов. В такой ситуации двухшаговый сосед будет получать несколько раз одно и то же HELLO-сообщение. Данная проблема решена методом оптимизации рассылки сетевой информации MPR, который позволяет уменьшить трафик широковещательной рассылки.

Служебные сообщения в OLSR содержат последовательные номера, которые увеличиваются в последующих сообщениях по аналогии с DSN в гибридном протоколе HWMP. Благодаря этому, даже если контрольные сообщения пришли в обратном порядке, получатель сообщений может легко определить более свежую информацию.

В беспроводных сетях часто происходит потеря широковещательных пакетов. Каждый узел при использовании оптимизированного протокола маршрутизации шлет контрольные пакеты периодически, что повышает устойчивость в случае потери части этих сообщений. OLSR не зависит от корневых узлов – это совершенно распределенный протокол.

Ранние версии стандарта IEEE 802.11s детально описывают RA-OLSR, однако от присутствовавшего опционально протокола отказались, начиная с версии D1.07. Поводом послужило то, что RA-OLSR дублирует функциональность гибридного протокола маршрутизации HWMP, который является проактивным и реактивным одновременно, при этом стандартом допускается использование любых других сторонних протоколов. Модификация RA-OLSR отличается от оригинального протокола OLSR энергопотреблением. Также не фиксирована процедура выбора узлов MPR, которую задает производитель устройств. В остальном протокол RA-OLSR схож с OLSR. Несмотря на чрезмерный размер самого описания протокола, которому посвящена пятая часть всего документа 802.11s, было очень много замечаний, указывающих на неточность формулировок в тексте стандарта. Таким образом, разработчики оставили выбор альтернативного протокола маршрутизации производителям оборудования, и отказ от RA-OLSR не связан с его недостатками. Таким образом, отказ от RA-OLSR не связан с его недостатками, рабочая группа просто решила оставить вопрос выбора альтернативного механизма маршрутизации производителям оборудования.

Сторонние протоколы

Адаптивный беспроводной протокол пути (AWPP – Adaptive Wireless Path Protocol) – протокол маршрутизации, от компании Cisco Systems для беспроводных ячеистых сетей. Применяется в беспроводной платформе Cisco Aironet 1520 Series. Он динамически определяет соседние радиоузлы и вычисляет качество всех возможных путей к проводной сети. Даже после того, как оптимальный путь к проводной сети был установлен, вычисления продолжают и данные обновляются. В случае нахождения более эффективного пути протокол автоматически переназначает маршрут. Функции управления и мониторинга сети берет на себя специальное устройство – контроллер беспроводной сети (Cisco Wireless LAN Controller). Рекомендуется использование контроллеров серии 4400. Так как данные о путях постоянно обновляются, это приводит к увеличению трафика в сети. Это недостаток данного протокола, но благодаря этому, он хорошо работает в нестатических средах, где возможны частые разрывы соединений.

Кроме того, протокол неплохо справляется с подвижностью узлов. Также недостатком является ограничение использования только оборудования компании Cisco Aironet.

Динамическая маршрутизация от источника (DSR – Dynamic Source Routing) – реактивный протокол маршрутизации от компании Microsoft. Формирует маршрут по требованию, передавая broadcast-запрос. Использует явную маршрутизацию, не полагаясь на таблицы маршрутизации на каждом промежуточном устройстве. Благодаря этому вся информация о маршрутах непрерывно обновляется мобильными узлами. Это позволяет избежать периодической проверки маршрута. В результате остаются только фазы поиска и поддержки. Таким образом, маршрут генерируется, только если сообщение с запросом достигло намеченного узла адресата. Динамический протокол маршрутизации от источника (DSR) создавался для того, чтобы уменьшить трафик, потребляемый управляющими пакетами в беспроводных сетях, устраняя сообщения обновления таблицы, требуемые в подходе с формированием маршрута при помощи таблиц. Основной подход этого протокола состоит в том, что во время фазы конструкции маршрута узел устанавливает маршрут, рассылая шировещательные пакеты RouteRequest по сети. Узел адресата при получении пакета RouteRequest отвечает, отсылая пакет RouteReply назад к источнику, который несет маршрут, пройденный полученным пакетом RouteRequest. Этот протокол использует реактивный подход, который избавляется от необходимости периодические засорять сеть сообщениями обновления таблицы, которые требуются в подходе с формированием маршрутов при помощи таблиц маршрутизации. В реактивных протоколах маршрут устанавливается только, когда он требуется, и следовательно, потребность в поиске путей ко всем другим узлам в сети отсутствует. Промежуточные узлы также эффективно используют информацию кэша маршрута, чтобы уменьшить издержки. Недостаток этого протокола – то, что механизм обслуживания маршрута в местном масштабе не восстанавливает разорванные соединения. Устаревшая информация из кэша маршрута может также привести к несогласованностям во время фазы реконструкции маршрута. Задержка установки подключения выше, чем в протоколах, использующих таблицы. Даже при том, что протокол хорошо работает в статических средах и средах с низкой подвижностью узлов, производительность быстро ухудшается с увеличивающейся подвижностью. Кроме того, значительные издержки маршрутизации появляются из-за маршрутизации от источника, используемой в DSR. Эти издержки прямо пропорциональны длине пути.

Интеллектуальный беспроводной протокол маршрутизации (PWRP – Predictive Wireless Routing Protocol) – протокол компании Tropos Networks. Его метрика основана на

оценке пропускных способностей каналов. Протокол является ориентированным на обеспечение связи клиент-сервер. Яркий пример применения данного протокола – сеть Google WiFi, объединяющая более 400 маршрутизаторов в опорной сети, 15 тысяч домов, 25 тысяч пользователей. Как следует из примера, этот протокол идеально подходит для больших сетей.

Протокол пересылки для mesh-сетей (FLAME – Forwarding Layer for Meshing) – протокол маршрутизации, разработанный в Голландском институте беспроводной и мобильной связи (Twente Institute for Wireless and Mobile Communications). Протокол работает на втором с половиной виртуальном уровне модели OSI, также как и протокол LQSR. Это дает FLAME те же преимущества, что есть у LQSR, а именно прозрачность с точки зрения протоколов верхних уровней и независимость от среды передачи данных. Однако протокол FLAME не использует никаких метрик. Первый пришедший от узла пакет считается пришедшим по кратчайшему пути, который и используется в дальнейшем. Любой полученный пакет является основанием для обновления информации о его источнике. При этом в таблицу маршрутизации заносится интерфейс и соседний узел, через которые пролегает путь к источнику пакета. Для этого в сети под управлением FLAME ко всем передаваемым пакетам добавляется FLAME-заголовок. Данный протокол эффективен только в статичных средах. Плохо работает в больших и сложных сетях.

Заключение

В статье представлен краткий обзор стандарта IEEE 802.11s и анализ протоколов маршрутизации в беспроводных сетях с ячеистой топологией, построенных на данном стандарте. 802.11s не имеет общепринятого протокола маршрутизации (HWMP должен обязательно поддерживаться, но не обязателен к использованию). В настоящее время количество протоколов маршрутизации от сторонних производителей постоянно растет. Каждый из них имеет достоинства и недостатки. Наиболее подходящими протоколами для небольшой сети, включающей в себя до 100 узлов, являются адаптивный беспроводной протокол пути (AWPP) и протокол динамической маршрутизации от источника (DSR). AWPP следует применять для сети с нестатичной средой и подвижными узлами. DSR следует применять для сети со статичной средой и слабо подвижными узлами. Беспроводные сети с ячеистой топологией – перспективная технология. В будущем уже реализованные протоколы будут совершенствоваться, и будет появляться большое количество новых протоколов маршрутизации.

Список литературы

- [1]. Дугаев Д.А. Архитектура и гибридный протокол маршрутизации для беспроводных ячеистых сетей на базе стандарта IEEE 802.11s. Режим доступа: <http://cyberleninka.ru/article/n/arhitektura-i-gibridnyy-protokol-marshrutizatsii-dlya-besprovodnyh-yacheistyh-setey-na-baze-standarta-ieee-802-11s.pdf> (дата обращения: 20.01.2016).
- [2]. Таненбаум Э., Уэзеролл Д. Компьютерные сети: пер. с англ. 5-е изд. СПб.: Питер, 2012. 960 с. [Andrew S. Tanenbaum, David J. Wetherall. Computer Networks. 5th ed. New Jersey: Prentice Hall, 2011. 960 p.]
- [3]. Вишневский В. М. Mesh-сети стандарта IEEE 802.11s: технологии и реализация // Первая Миля. Электрон. журн. 2008. № 2. Режим доступа: http://www.lastmile.su/files/article_pdf/2/article_2099_241.pdf (дата обращения: 23.01.2016).
- [4]. Вишневский В. М. Mesh-сети стандарта IEEE 802.11s: протоколы маршрутизации // Первая Миля. Электрон. журн. 2009. №1. Режим доступа: http://www.lastmile.su/files/article_pdf/2/article_2055_382.pdf (дата обращения: 23.01.2016).
- [5]. Ricardo C. Carrano, Luiz C.S. Magalhaes, Debora C. Muchaluat Saade and Celio V.N. Albuquerque. IEEE 802.11s Multihop MAC: A Tutorial. Available at: <http://documents.mx/documents/ieee-80211s-multihop-mac-a-tutorial.html>, accessed: 24.01.2016.