**Проблемы беспроводных сетей**

**Ver3**

**Mesh-сети**

Алгоритмы маршрутизации классифицируются по типам:

Статические или динамические. Статические алгоритмы представляют свод правил работы со статическими таблицами маршрутизации, которые настраиваются администраторами сети. Хорошо работают в случае предсказуемого трафика в сетях стабильной конфигурации. Динамические алгоритмы маршрутизации подстраиваются к изменяющимся обстоятельствам сети в масштабе реального времени. Они выполняют это путем анализа поступающих сообщений об обновлении маршрутизации. Если в сообщении указывается, что имело место изменение сети, программы маршрутизации пересчитывают маршруты и рассылают новые сообщения о корректировке маршрутизации. Такие сообщения пронизывают сеть, стимулируя маршрутизаторы заново прогонять свои алгоритмы и соответствующим образом изменять таблицы маршрутизации. Динамические алгоритмы маршрутизации могут дополнять, где это уместно, статические маршруты.

Одномаршрутные или многомаршрутные алгоритмы. Некоторые сложные протоколы маршрутизации обеспечивают множество маршрутов к одному и тому же пункту назначения. Такие многомаршрутные алгоритмы делают возможной мультиплексную передачу трафика по многочисленным линиям, одномаршрутные алгоритмы не могут делать этого. Многомаршрутные алгоритмы могут обеспечить значительно большую пропускную способность и надежность.

Одноуровневые или иерархические алгоритмы. Отличаются по принципу взаимодействия друг с другом. В одноуровневой системе маршрутизации все рутеры равны по отношению друг к другу. В иерархической системе маршрутизации пакеты данных перемещаются от роутеров нижнего уровня к базовым, которые осуществляют основную маршрутизацию. Как только пакеты достигают общей области пункта назначения, ониперемежаются вниз по иерархии до хоста назначения.

Алгоритмы с маршрутизацией от источника. В системах маршрутизации от источника роутеры действуют просто как устройства хранения и пересылки пакета, без всякий раздумий отсылая его к следующей остановке, они предполагают, что отправитель рассчитывает и определяет весь маршрут сам. Другие алгоритмы предполагают, что хост отправителя ничего не знает о маршрутах. При использовании такого рода алгоритмов роутеры определяют маршрут через сеть, базируясь на своих собственных расчетах.

Внутридоменные или междоменные алгоритмы. Некоторые алгоритмы маршрутизации действуют только в пределах доменов; другие - как в пределах доменов, так и между ними.

Алгоритмы состояния канала и дистанционно-векторные. Алгоритмы состояния канала направляют потоки маршрутной информации во все узлы сети. Каждый роутер отсылает только ту часть известной ему информации, которая описывает состояние его собственных каналов, но всем узлам маршрутизации. Дистанционно-векторные требуют от каждого роутера пересылки всей или части его таблицы но только соседям.

Протоколы маршрутизации подразделяют на две большие группы []: *внешние* (EGP — Exterior Gateway Protocol) и *внутренние* (IGP — Interior Gateway Protocol). Протоколы внутренней маршрутизации используются внутри так называемой *автономной* *системы*, т.е. группы маршрутизирующих узлов, находящихся под общим управлением. В свою очередь, внутренние протоколы маршрутизации подразделяются на *дистанционно-векторные* и *по состоянию канала*. Внешние протоколы предназначены для соединения автономных систем друг с другом.

Для традиционных дистанционно-векторных протоколов применяется следующая стратегия: маршрутизаторы ведут обмен всеми IP-адресами, которые могут быть достигнуты при периодическом обмене данными посредством широковещательных анонсов дистанционных векторов, т.е. «расстояние» до целевого узла, представленное в виде количества промежуточных узлов. Эти широковещательные сообщения рассылаются согласно *таймеру обновлений* (refresh timer), установленному для каждого сообщения. Таким образом, если истекает срок работы таймера обновлений и при этом поступает новая маршрутная информация, требующая пересылки соседям, этот таймер сбрасывается, и маршрутная информация не пересылается до тех пор, пока срок работы таймера снова не истечет.

В случае, если соединение или определенный маршрут становятся недоступными, то распространение маршрутной информации со сведениями о нерабочем маршруте задерживается на время до окончания срока работы таймера обновления, при этом возникает значительное замедление при обновлении маршрутной информации (конвергенция).

Такие протоколы не подходят для mesh-сетей, так как вся информация широковещательная, сеть может засоряться широковещательным трафиком, что приводит к уменьшению пропускной способности сети, так же критична большая конвергенция, так как mesh-сети постоянно изменяют свою топологию. Не смотря на недостатки такие протоколы существуют, например, AODV и DSDV.

Протоколы по состоянию канала

В протоколах по состоянию канала маршрутизаторы с некоторым количеством маршрутной информации рассылают соседям *hello*-*сообщения*. Такие сообщения являются multicast-рассылкой, что уменьшает количество широковещательных сообщений в сети. Так же в случае перестроения сети все узлы значительно быстрее смогут перестроить свои таблицы маршрутизации. Критичным для таких сетей является установка таймеров на одинаковое время, так как постоянная рассылка о том, что узел появился в сети и выбыл из сети, создаст значительную нагрузку на сеть. Примерами таких протоколов для mesh-сетей служат OLSR, TBRPF.

Существует также гибридный протокол динамической маршрутизации- AntNet. Алгоритм маршрутизации AntNet использует алгоритм муравьиной колонии. Роль муравьев выполняют активные агенты. Активный агент – специальный пакет, несущий статистику о состоянии пройденных сетевых каналов. Существуют *F-муравьи*, собирающие во внутренний стек статистику о состоянии сети, не изменяя таблиц маршрутизации, и *B-муравьи,* которые создаются, когда F-муравей достигнет узла назначения на его основе. В него копируется накопленный стек F-муравья после чего F-муравей удаляется. B-муравей отправляется обратно к узлу назначения по маршруту F-муравья. Маршрутизаторы извлекают из проходящего B-муравья информацию и обновляют свои таблицы маршрутизации. Каждый маршрутизатор, реализующий AntNet с заданной периодичностью рассылает F-муравьев в различные узлы сети для отслеживания состояния сети.

В mesh-сетях используется преимущественно протоколы по состоянию канала, хотя протоколы дистанционно-векторные проблемы маршрутизации решают лучше в случае двух или более путей к точке назначения.

Проактивные протоколы (табличные) протоколы предполагают создание на каждой мобильной станции таблиц маршрутизации, содержащих информацию обо всех станциях в сети. (DSDV, OLSR, TBRPF, FSR)

Этим резко отличаются от реактивных протоколов, которые строят таблицы маршрутизации, которые строят маршруты между конкретными узлами и только по требованию инициатора передачи. Нежелательны в сети с высоким уровнем трафика – слишком много лавинных рассылок пакетов при очередном поиске маршрута. (DSR, AODV, TORA).

Гибридные протоколы наиболее эффективны в многоуровневых сетях. (HWMP, HDVG, ZRP).

**Безопасность.**

Развитие беспроводных сетей и удобство их использования актуализирует проблему обеспечения безопасности взаимодействия составляющих элементов. В настоящее время беспроводные сети включают 3G, LTE, а также сети стандарта 802.1x. Для компрометирования проводной сети злоумышленнику необходимо получить доступ к сети изнутри: проникнуть в здание, найти сетевую розетку, подключиться к розетке со своего ноутбука. Сделать это очень трудно без применения методов социальной инженерии. В случае беспроводной сети злоумышленнику достаточно находиться недалеко от здания, чтобы получить возможность доступа к сети. Кроме того, весь трафик от точки доступа до клиента распространяется во всех направлениях в зоне покрытия данной точки доступа.

Для сетей WiFi стандарта 802.11 некоторое время использовался алгоритм шифрования данных WEP. На смену WEP пришел WPA, поддерживающий EAP (расширяемый протокол аутентификации) и шифрование AES. Алгорритм WPA является менее защищенным, чем WPA2, но более широко распространен, например, в сетях WiMAX, а также в сетях с «бесшовным роумингом», для которых необходим сервер с базой зарегистрированных пользователей RADIUS. Сервер аутентификации генерирует уникальный ключ для сеанса связи, TKIP отвечает за увеличение размера ключа, отвечает за передачу ключа пользователю.

WPA = 802.1X + EAP + TKIP + MIC

С 2006 года поддержка WPA2 является обязательным условием для сертификации WiFi-устройств. Протокол WPA2 включает два типа WPA2 Personal и WPA2 Enterprice. Разница между этими двумя типами заключается в том, откуда берутся ключи для шифрования AES: в настройке точки доступа или же на RADIUS-сервере. В отличии от WPA, WPA2 использует AES шифрование, вместо CR4.

Стандартные процедуры обеспечения защиты информации в сетях включают следующие этапы.

Аутентификация и авторизация пользователей. Аутентификация проводится на этапе соединения с точкой доступа, т.е. еще до получения пользователем ip-адреса. После успешной аутентификации пользователю необходимо дождаться авторизации, согласно которой пользователю будут доступны ресурсы.

Для разделения трафика разных классов применяются VLANы. Первоначально они использовались в проводных сетях, но также могут использоваться и в беспроводных. При этом трафик разделяется на трафик локальной сети предприятия, и “гостевой” трафик, порождаемый незарегистрированными устройствами. Это позволяет воспрепятствовать получению доступа к внутренней сети предприятия с неизвестного смартфона, даже при условии подключения зарегистрированного и незарегистрированного устройства к одной точке доступа.

Еще одной задачей является фильтрация трафика с применением фаерволов на основе ip-адресации. Такая фильтрация часто используются для обеспечения защиты доступа для удаленных сотрудников, соединяющихся с внутренними ресурсами компании, например, из дома при помощи программ VPN. Следует заметить, что межсетевые экраны рекомендовано устанавливать непосредственно на источнике пакетов, тем самым достигается значительное снижение объема трафика в сети.

**Проблемы маршрутизации**

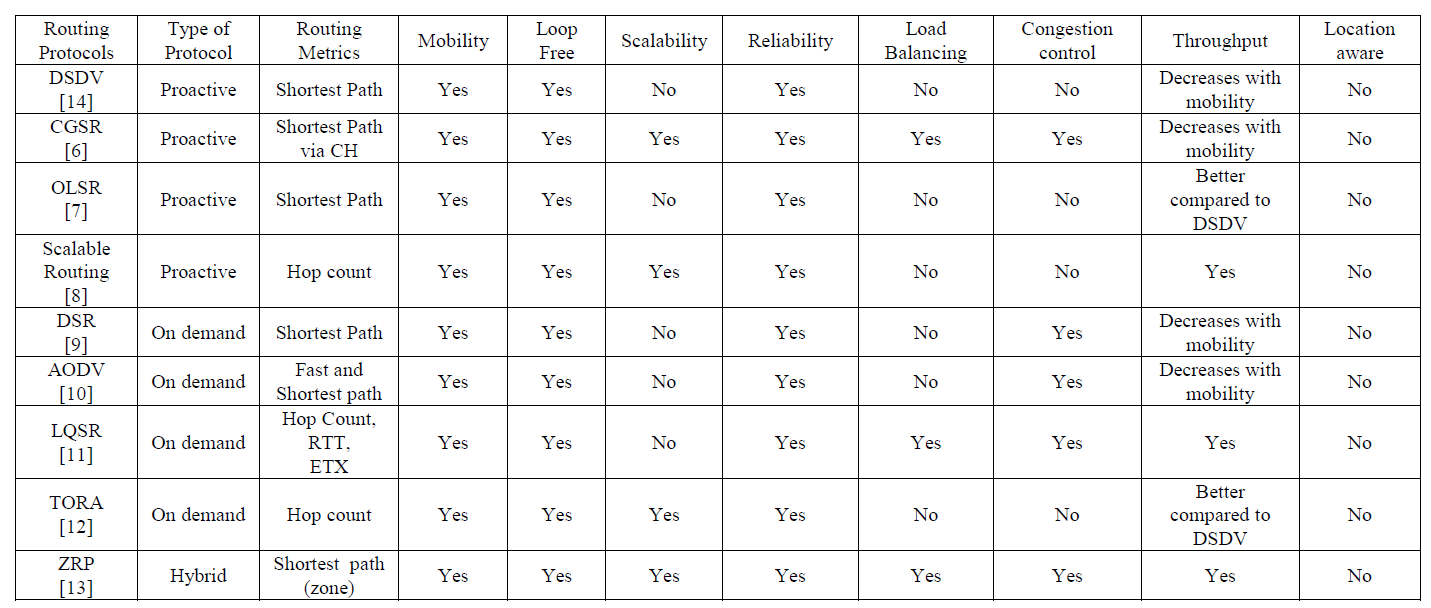
Выбор протокола маршрутизации должен быть с наибольшим QoS в данном конкретном случае.

**QoS** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) ***q****uality* ***o****f* ***s****ervice* «качество обслуживания») — этим термином в области [компьютерных сетей](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) называют вероятность того, что сеть связи соответствует заданному [соглашению](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%B3%D0%BB%D0%B0%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BE%D0%B1_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D0%B5_%D1%83%D1%81%D0%BB%D1%83%D0%B3) о трафике, или же, в ряде случаев, неформальное обозначение вероятности прохождения [пакета](https://ru.wikipedia.org/wiki/IP-%D0%BF%D0%B0%D0%BA%D0%B5%D1%82) между двумя точками сети.

В узком техническом значении, этот термин означает набор методов для управления ресурсами [пакетных сетей](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BA%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%86%D0%B8%D1%8F).

В таблице приведено сравнение различных протоколов маршрутизации для mesh-сетей.

Таблица - Сравнение протоколов mesh-сетей



Zone Based Routing Protocol (ZRP) – протокол маршрутизации на основе зоны – гибридный протокол. Использует два метода маршрутизации – маршрутизация в интрасети (IARP) и маршрутизации между интрасетями (IERP). Такой протокол применим в сотовых сетях, где есть стационарно расположенные вышки, между которыми могут перемещаться клиенты сотовой связи.

Заключение:

В данной статье рассмотрены статические и динамические, одномаршрутные и многомаршрутные, одноуровневые и иерархические типы алгоритмов маршрутизации, так же описаны алгоритмы маршрутизации с маршрутизацией от источника и междоменные и внутридоменные алгоритмы. Кроме того, приведены примеры протоколов для дистанционно-векторной маршрутизации и маршрутизации по состоянию канала.

В данной статье приведены проблемы беспроводных mesh- сетей – безопасность, создающая дополнительные проблемы при организации любых беспроводных сетей, и сама маршрутизация.

5G, Li-fi, Project Loon и беспилотники Facebook, mesh-сети и интернет вещей — все эти тренды ведут к тому, что граница между миром реальным и виртуальным окончательно теряет четкость.

С развитием технологий связано множество острых проблем, и технических, и социальных, и юридических, так что вряд ли будущее будет похоже на цифровую утопию. Но лучшее, что можно сделать, чтобы справиться с этими вызовами — обеспечить как можно большему числу людей доступ к современным технологиям связи, в надежде, что сообща они не только найдут приемлемые решения, но и сделают реальность качественно лучше.