Обзор на методите и протоколите за маршрутизация при безжични мрежи (MANETs и WMNs)

докторант Илия Костов, доц. д-р Васил Фурнаджиев

/Настоящият доклад бе изнесен на семинар на департамент „Информатика” на 19 април 2012 г./

I. Мобилни разпределени мрежи. Безжични многосвързани мрежи (WMNs)

1. Мобилни разпределени мрежи

В последните десетина години сме свидетели на непрекъснат прогрес в областта на безжичните комуникации. Налице е огромен напредък в съществуващата мрежова инфраструктура, броя на достъпните приложения както и появата на множество устройства използващи безжична комуникация: портативни и джобни компютри, преносими компютри, клетъчни телефони, персонални асистенти (PDAs). Тези устройства непрекъснато увеличават своята мощност и възможности и започват да играят все по-важна роля в нашия живот. Показателен е факта, че освен, че стават все по-малки, по-евтини, по-удобни и по-мощни, те вече изпълняват все повече приложения и мрежови услуги.

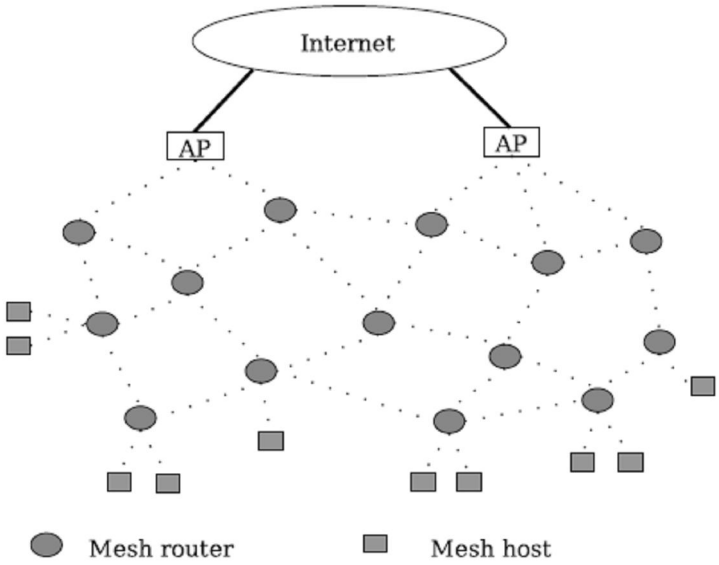
Мобилните разпределени мрежи (Mobile Ad-hoc Networks - MANETs) се състоят от устройства, който са в състояние самостоятелно да се организират в безжични мрежи. Тъй като разпределената мрежа се изчерпва с устройствата от който е изградена имаме възможност за лесно разгръщане на една динамична, самоорганизираща се и сравнително евтина мрежа. Отделните мобилни станции имат възможност да се движат напълно произволно като по този начин топологията може да се променя доста бързо и непредсказуемо. Този тип мрежи могат да съществуват като самостоятелни или да бъдат свързвани към по-големи мрежи и Интернет. Тези предимства на разпределените мрежи имат все пак и своята цена, която е за сметка на по-сложни технологични решения, които се изискват на всичките слоеве на използвания комуникационен модел. Както и останалите безжични мрежи и разпределените такива се изправят пред традиционните проблеми на безжичната комуникация като: оптимално използване на честотната лента, контрол върху изразходваната мощност, подобрения върху качеството на предаване. Освен това характеристики като липсата на фиксирана инфраструктура и факта, че мобилните станции освен като крайни устройства действат и като маршрутизатори, препращайки пакетите до останалите станции по пътя им към крайния получател (т.нар. **multihop routing**) са уникални за този тип мрежи и крият нови проблеми за изследване като: конфигурация на мрежата, откриване на съседи, поддържане на топологията, адресиране, маршрутизиране. [6]

Появили се първоначално, за да изпълняват изцяло военно-тактически задачи днес пред мобилните разпределени мрежи съществуват все по-голямо разнообразие от възможности за тяхното приложение. Това е особено вярно в последните няколко години, когато рязко нарасналия интерес към тяхното изследване, води до засилване на интереса от страна на индустрията и комитетите за стандартизация. Появата на нови технологии като Bluetooth, IEEE 802.11 и Hyperlan значително улесняват използването на разпределените мрежи извън военния сектор. Някои от новопоявилите се приложения на мобилните разпределени мрежи включват: изграждане на мрежи от сензори, използването им при спешни спасителни операции, изграждане на виртуални класни стаи, комуникация по време на конференции, събирания или лекционни часове,

роботизирани домашни любимци, достъп до Интернет извън границите на дома или офиса, изграждане на WLAN и PAN мрежи в дома и офиса, електронна търговия, мобилни офиси, транспортни услуги: разпространение на новини, на информация за времето, кооперирание с останалите автомобили на пътя за предварително известяване за пътни събития и инциденти.

2. Безжични многосвързани мрежи (WMNs)

WMNs са нов клас мрежи, появили се наскоро. Основните им компоненти включват безжични mesh рутери, безжични mesh възли (хостове) като: лаптопи, PC, PDA и др. и точки на достъп, които действат и като Интернет рутери и като безжични mesh рутери.



Фиг. 1 Структура на WMNs

Mesh рутерите в WMNs осигуряват многоскокова връзка от един хост на друг или към Интернет през точките на достъп. WMNs се самоорганизира и конфигурира динамично с възли, които автоматично установяват и поддържат връзки помежду си. Това свойство осигурява много предимства на WMNs като: ниска цена за инсталация, широк обхват, надеждност и самоуправление.

Безжичните многосвързани мрежи (WMNs) са във фокуса на много изследвания, тъй като те дават възможност за увеличаване на покритието, като се запазват ниската цена и лесното внедряване. WMNs са били идентифицирани като ключова технология, която има за цел да подобри съществуващите мрежови инсталации и да осигури достъп до Интернет на места, където традиционните технологии не са на разположение или са твърде скъпи за инсталиране. WMNs се състои от mesh маршрутизатори (MR), които са статични и mesh клиенти (MC), които често са напълно подвижни. Mesh рутерите формират гръбнака на мрежата, чрез който клиентите получават достъп до мрежата.

Много от протоколите, които се прилагат за WMNs са еволюирали от безжичните локални мрежи (WLAN) и мобилните ad-hoc мрежи (MANET). Въпреки това и двете мрежи, имат характеристики, които ги различават от WMNs. Така например докато WLAN имат относително статична топология, MANET са напълно подвижни. Следователно използването на протоколи, проектирани само за някоя от тези мрежи, не ни дава възможност да използваме всички предимства на WMNs. При MANET мрежите всички възли са рутери, които имат ограничена подвижност и

пропускателна способност (честотна лента). При WMNs mesh рутерите имат по-големи ресурси, отколкото mesh клиентите, които могат да бъдат използвани. Въпреки, че са направени много изследователски проучвания за справяне с тези проблеми и са предложени някои специализирани алгоритми за WMNs, все още има много нерешени проблеми в тази област. Един от тези проблеми е изготвянето на оптимален график за достъп до мрежата. Без изготвянето на такъв график за безжичните многосвързани мрежи ще бъде изключително трудно изграждането на една мрежа, в която всички потребители очакват относително равноправен достъп до мрежата. Много от съществуващите решения не отчитат така наречените алчни потребители или потоци, което създава възможност за изключително неравностоен достъп до мрежата от различните потребители. Много от съществуващите протоколи са проектирани без да се отчитат възможността за приоритетен достъп до мрежата. Тези протоколи са фокусирани главно върху други характеристики като например високата пропускателна способност на мрежата.

Тъй като при безжичните многосвързани мрежи има много скокове при предаването на едно съобщение съществуват доста повече проблеми, с които трябва да се справим в сравнение с традиционните жични и безжични мрежи. Безжичния канал е бродкаст среда, което означава че в определени граници всички възли са подложени на смущения и не могат да предават едновременно. В същото време е трудно да се долови дали се извършва комуникация в други части от мрежата, тъй като е възможно да има проблем когато има междинен възел между двата възела, които се опитват да си комуникират едновременно, но са на голямо разстояние един от друг. Решаването на много от тези проблеми може да стане като се направи график за предаването на съобщенията. Изграждането на график за достъп до мрежата е въпрос на балансиране между два основни елемента: от една страна осигуряване на справедлив достъп до мрежата (т.е. приоритетен достъп за спешните съобщения) и от друга страна осигуряването на максимално добро качество на вразката при предаването на съобщенията. Целта на един добър алгоритъм за планиране е да се намери баланс между тези две цели.

Мотивацията за създаването на такъв график за работа на мрежата е свързана с това, че в търговските приложения например всеки потребител плаща за достъп до мрежата и е добре всеки потребител да получи еднакво качество на услугата (QoS). Също така е важно да се дефинират параметрите, по които ще се определя ефективността на даден алгоритъм по отношение на осигуряването на приоритетен достъп до мрежата. Така например един алгоритъм за създаване на график може да осигури добра пропускателна способност на мрежата, но в същото време да не може да отчете закъснението, което може да се получи при предаването на данните. Така някои възли от мрежата могат да се окажат без възможност за предаване на данни по мрежата, докато други възли имат възможността да комуникират свободно. [8]

Особено важен е въпроса за подобряване на достъпа при комуникационните системи на диспечерите за спешна помощ. Необходима е безжична система за спешни съобщения, която да поддържа комуникацията между различните агенции (пожарна, полиция, бърза помощ) в реално време. Така например ще е полезно ако парамедиците могат да използват портативни сканиращи устройства, докато транспортират пациентите до болницата, изпращайки снимки и видео към спешното отделение, за да диагностицират навременно пациента и да определят лечението.

3. Протоколи за маршрутизация

При безжичните многосвързани мрежи много важен е проблема за осигуряването на оптимална маршрутизация и бърз достъп до мрежата, тъй като при тях имаме множество точки за достъп (предлагащи интернет) и крайни мобилни

устройства нар. възли. Възлите в мрежата служат като „релета”, които препращат трафика към други възли и по този начин те се явяват като междинни устроства (шлюзове), благодарение на които се постига желания резултат. Така се осигурява оптимално използване на всички възли и точки на достъп. Като колкото по – голяма е гъстотата на потребителите, толкова по – малко точки на достъп са нужни като цяло. За осигуряването на оптимална маршрутизация в такъв тип мрежи е необходимо маршрутизиращият протокол, който оперира с възлите да е надежден независимо от движението на устройствата. Освен това отделните възли в мрежата трябва да имат непрекъснат достъп до интернет и да не губят връзката с отделните точки, т.е. от голямо значение е и проблема за управлението на мобилните възли в многосвързаните безжични мрежи.

По отношение на осигуряването на ефективен достъп до данните при многосвързаните безжични мрежи съществуват разработени XML приложения за маршрутизация, които изследват вида на заявката за съвпадение с интересите на потребителите. Приложенията като VoIP, аудио и видео поставят изискванията за по – високочестотна лента. Тези приложения в реално време не понасят закъсненията в мрежата. Доказано е, че процеса на сканиране напрактика допринася за 90% от закъсненията в мрежата. Закъсненията по време на предаването на данни в мрежата могат да доведат до влошаване на качеството на услугата, поради това намаляването им е изключително важно. В тази посока са разработени няколко стратегии за намаляване на времето за сканиране при предаване на данни в безжичните мрежи. За осигуряването на оптимална маршрутизация на пакетите в мрежата има разработени различни протоколи за маршрутизация, които се различават по своите характеристики. Те предлагат избор между дългите маршрути, състоящи се от много надеждни връзки и късите маршрути състоящи се само от няколко, но често ненадеждни връзки. Като надеждността на връзката се оценява на базата на средната измерена сила на предавания сигнал.

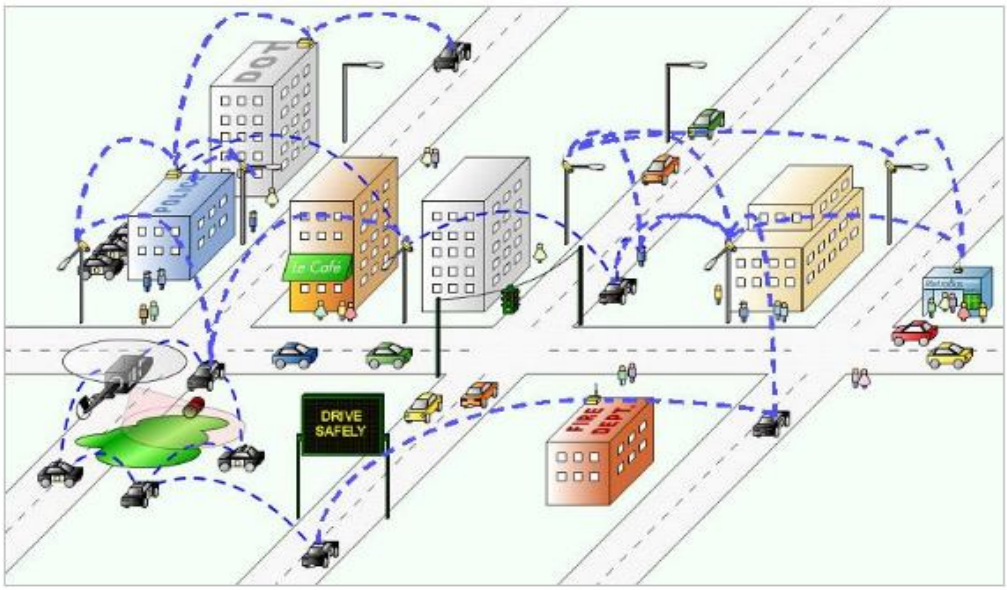
Маршрутизиращите протоколи трябва да отговарят на множество изисквания. Те трябва да са достатъчно прости и лесни за конфигуриране и да осигуряват надеждна и стабилна работа на мрежата. Отпадането на маршрутизатори или връзки между тях не бива да пречи на нормалното функциониране на останалите маршрутизатори, които трябва да бъдат в състояние да открият алтернативни пътища за доставяне на пакетите, ако такива съществуват. Минимизирането на времето за закъснение и максимизирането на общия поток в мрежата са други две цели на маршрутизиращите протоколи. Тези две цели са противоречиви - минимизирането на времето за закъснение е свързано с по-малък престой на пакетите в междинните възли, докато максимизирането на общия поток предполага буферите в маршрутизаторите да работят на максимален капацитет. Освен това максимизирането на общия поток може да влезе в противоречие с изискването мрежовите ресурси да могат да се използват от всички потребители в мрежата. Като вземем в предвид тези изиквания към маршрутизиращите протоколи можем да насочим изследванията си към сравнителен анализ на различните протоколи за маршрутизация и да предложим подобрения, които да доведат до осигуряването на оптимален път за предаване на данни в безжични мрежи с многосвързана топология. Освен това могат да се направят подобрения свързани с осигуряването на приоритетен достъп до мрежата при спешни случаи. Така например първоначално мрежата е адаптирана да работи в нормален режим, но при спешни случаи да има възможност за приоритетен достъп от потребителите със спешна нужда.

WMNs намират приложение в:

1. Служби за сигурност, отбрана, борба с бедствия и аварии, тъй като те позволяват:
    - моментално разгръщане на мрежата веднага след пристигане на екипите

- директна гласова връзка, получаване на данни и видео информация от мястото на събитието

2. определяне на месторазположението на участниците в операциятаДоставяне на мобилен достъп до Internet и обществени база данни
3. За управление и оптимизиране на работата в големи производствени комплекси (рудодобивни, индустриални и др.)
   - осигуряване на гласови комуникации и видео наблюдение
   - събиране на данни от производствения цикъл
   - визуализиране на текущото състояние на производствените обекти
4. Организация на пътния трафик
   - организиране на „интелигентни" транспортни системи
   - управление на сигнализацията за пътно движение
   - определяне на състоянието на товара
   - дистанционно управление на транспортни средства
5. Управление на градски транспорт
   - гласова и видео връзка с водачите на транспортните средства
   - определяне на местоположението на транспортните средства
   - визуализация на информацията за движението на транспортните средства
6. Другото основно приложение на Mesh топологията, е на места, където е много скъпо да се пусне широколентов достъп поради отдалеченост на самото място или малкия брой абонати.



Фиг. 2 Примерна илюстрация на WMNs

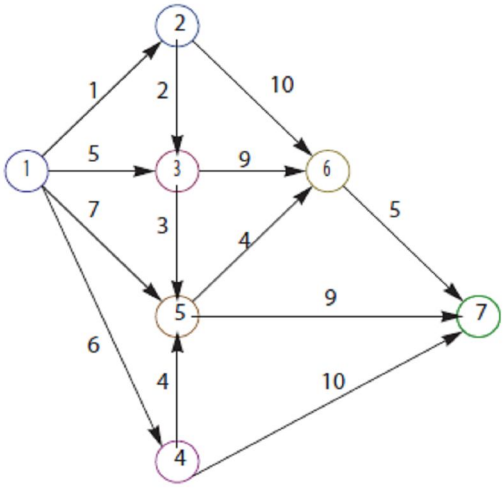
II. Динамични методи за маршрутизация

1. Разпределена динамична маршрутизация (маршрутизация с вектор на разстоянието Distance vector routing)

Характерно за разпределената маршрутизация е, че дейтаграмата носи в себе си само адреса на крайния получател. Маршрута се определя разпределено като всеки рутер определя само следващия скок от маршрута. Това той извършва на базата на адреса на крайния получател и на алгоритъм заложен в таблицата за маршрутизация. Рутерите разменят само с директно свързаните към тях съседни рутери съобщения с информация от маршрутните си таблици за всички възли в мрежата. Предполага се, че всеки рутер знае метриката на връзките до своите съседи. Ако метриката е брой скокове, разстоянието до всеки съсед е 1. Ако метриката е натоварване на възела,

разстоянието до всеки съсед е броя на пакетите в изходящата опашка към този възел. Ако метриката е време-закъснение, рутерът периодично изпраща "ехо" пакети до съседните му рутери и измерва закъснението на техния отговор. [1]

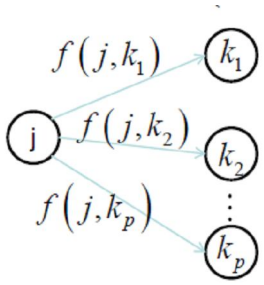
Нека разгледаме следния модел на безжична мрежа с многосвързана топология (фиг.3), където отделните възли в мрежата са означени като върхове на граф, а ребрата на графа ни показват време-закъснението при предаването на даден пакет от един възел на друг. Тогава задачата, която си поставяме е да определим кой е маршрута, по който даден пакет ще се предаде от източника (възел 1) до получателя (възел 7) с минимално време-закъснение.



Фиг. 3 Модел на WMNs

Ако за всички върхове с номера k по-големи от j е определен пътя с минимално време-закъснение и той е равен на $F(k)$ и от върха j може да се стигне до върховете k_s $s \in \{1,2,...,p\}$ с дължини на съответните дъги $f(j,k_s)$, то

$$F(j) = \min\{f(j,k_s) + F(k_s) : s \in \{1,2,...,p\}\}$$



Нека $F(i)$ е минималното време-закъснение за предаване на пакета от възел i до получателя. Тогава $F(7) = 0$, тъй като възел 7 е крайния получател. Реализираме връщане към предишните възли и последователно изчисляваме:

$$F(6) = \min\{f(6,7) + F(7)\} = 5$$

$$F(5) = \min\begin{Bmatrix} f(5,6) + F(6) \\ f(5,7) + F(7) \end{Bmatrix} = \min\begin{Bmatrix} \underline{4+5} \\ \underline{9+0} \end{Bmatrix} = 9$$

$$F(4) = \min\begin{Bmatrix} f(4,5) + F(5) \\ f(4,7) + F(7) \end{Bmatrix} = \min\begin{Bmatrix} 4+9 \\ \underline{10+0} \end{Bmatrix} = 10$$

$$F(3)=\min\begin{Bmatrix} f(3,5)+F(5) \\ f(3,6)+F(6) \end{Bmatrix}=\min\begin{Bmatrix} \underline{3+9} \\ 9+5 \end{Bmatrix}=12$$

$$F(2)=\min\begin{Bmatrix} f(2,3)+F(3) \\ f(2,6)+F(6) \end{Bmatrix}=\min\begin{Bmatrix} \underline{2+12} \\ 10+5 \end{Bmatrix}=14$$

$$F(1)=\min\begin{Bmatrix} f(1,2)+F(2) \\ f(1,3)+F(3) \\ f(1,4)+F(4) \\ f(1,5)+F(5) \end{Bmatrix}=\min\begin{Bmatrix} \underline{1+14} \\ 5+12 \\ 6+10 \\ 7+9 \end{Bmatrix}=15$$

Следователно минималното време-закъснение при предаването на пакета с данни от възел 1 към възел 7 е 15 секунди и то се реализира при предаването на пакета по един от следните два маршрута: $1\to 2\to 3\to 5\to 7$ или $1\to 2\to 3\to 5\to 6\to 7$. Ако към разгледания пример въведем и допълнителното условие за минимален брой скокове, то предпочитания маршрут тогава ще бъде $1\to 2\to 3\to 5\to 7$. Ако пък поради някаква външна причина връзката между възли 5 и 7 е нарушена, то може да се избере алтернативния маршрут $1\to 2\to 3\to 5\to 6\to 7$ и отново ще се гарантира минимално време-закъснение при предаването на пакета с данни.

2. Маршрутизация със следене състоянието на връзката (Link state routing)

При маршрутизирането със следене състоянието на връзката(link state routing), всеки рутер трябва да извършва следните пет основни действия:

1. Откриване на съседните рутери и техните мрежови адреси.
2. Измерване на цените на връзките до съседните рутери.
3. Конструиране на пакети с информация за състоянието на връзките.
4. Изпращане на тези пакети до всички останали рутери.
5. Изчисляване на най-късия път до всеки рутер в мрежата.

В резултат на тези пет действия се събира и разпространява до всички рутери информация за цялата топология на мрежата.

1) Откриване на съседните рутери

След включването на един рутер неговата първа задача е да научи кои са съседите му. Това се постига чрез изпращане на “ехо” пакет по всяка от изходящите линии на рутера. От своя страна, всеки от съседите отговаря като съобщава името си. Това име трябва да бъде уникално в мрежата.

2) Измерване на цените на връзките

Всеки рутер трябва да може да определи време-закъснението до своите съседи. Най-простият начин е рутерът да изпрати "ехо" пакет към всеки свой съсед, на който трябва директно да се отговори. Времето от изпращането на "ехо" пакета до получаване на отговора се дели на две и по този начин се получава времето-закъснение до съответния съсед. За по-точно измерване, този процес може да се повтори няколко пъти и да се вземе средната стойност.

Като критерий за избор при определяне на цената на връзката може да се избере също така надеждността при предаването на пакета с данни по тази връзка или пък шумоустойчивостта на връзката на външни смущения. При безжичните мрежи с многосвързана топология имаме възможност за предаване на данни по различни маршрути. Избора на даден маршрут пред друг може да се определи според различни критерии. Задачата, която сме си поставили е да определим този маршрут, който ще

предаде пакета с данни с минимално време-закъснение и максимална надеждност. При така поставената задача броя скокове не е определящ, защото може да се окаже, че път с по-голяма дължина (по-голям брой скокове) реализира по-надеждно и по-бързо предаване на пакета с данни в сравнение с друг по-къс, но по-ненадежден маршрут. Надеждността на даден маршрут се определя от това дали пакета с данни е пристигнал до получателя или не. Неполучаването на даден пакет с данни може да се дължи на грешка в блока с данни или на загуба на потвърждението в резултат на комуникационна грешка. И в двата случая ще се наложи повторно предаване на блока с данни, което ще забави значително процеса на предаване на данните. Ето защо избора на надежден маршрут е от голямо значение, когато се цели мининално време-закъснение при предаването на съобщенията. Надеждността на връзката при предаването на пакетите с данни е от особено значение, когато се предават спешни съобщения. Тогава основната цел е съобщението да не се загуби при предаването му по мрежата. Ето защо дори с риск за по-дълго време-закъснение е по-добре да се избере този маршрут, който осигурява максимална надеждност и гарантира доставяне на спешното съобщение до съответния получател.

3) Подготвяне на пакети с информация за състоянието на връзките (link state packets)

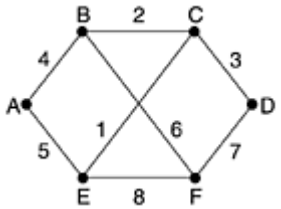
След като събере необходимата информация за състоянието на връзките си, следващата задача на рутера е да конструира пакет, който съдържа тази информация.

Пакетът трябва да съдържа уникалното име на подателя, пореден номер, време на живот и списък със съседите на подателя, като за всеки съсед е указана цената на връзката до него.

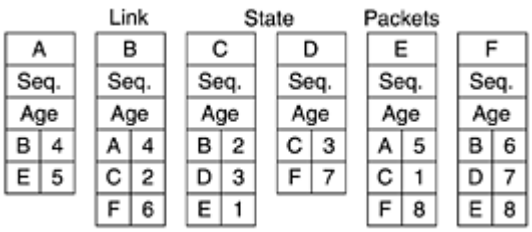
Определянето на момента, в който трябва да бъдат подготвени и изпратени пакетите е важна задача.

Един възможен начин е това да става през определени равни интервали от време. Друга по-добра възможност е пакетите да се подготвят и изпращат само при промяна в топологията на мрежата - след отпадане или поява на нов съсед или промяна в цената на някоя връзка.

Нека да разгледаме следната примерна мрежа. Ребрата имат етикети със съответното време-закъснение.



Пакетите със състоянието за връзките за шестте маршрутизатора изглеждат по следния начин:



4) Разпространяване на пакетите с информация за състоянието на връзката

Най-съществената част на алгоритъма е надеждното доставяне на пакетите с информацията за състоянието на връзката до всички рутери.

За разпространението на пакетите се използва методът на наводняването (flooding). При него всеки пакет се изпраща по всички линии, освен линията по която е пристигнал.

Обработката на всеки пристигнал пакет започва с проверка дали пакетът има по-голям пореден номер в сравнение с най-големия пореден номер, който е пристигнал до този момент от този източник. Ако номерът е по-голям, информацията от пакета се записва в таблицата с информация за състояние на връзките и пакетът се предава по останалите линии. Ако номерът е по-малък или равен, пакетът се отхвърля.

В полето за време на живот рутерът-подател указва продължителността на времето в секунди, през което пренасяната от него информация трябва да се счита за валидна. Всеки рутер, който получи даден пакет намалява с единица стойността на това поле преди да го предаде към своите съседи. Освен това, след като рутерът запише данните от пакета в своята таблица, той продължава да намалява времето на живот на тези данни на всяка следваща секунда. Ако времето на живот стане 0, данните се изтриват. По този начин се премахва опасността остаряла информация за състоянието на връзките да се разпространява и използва прекалено дълго време от рутерите.

5) Изчисляване на новите маршрути

След като един рутер получи пълна информация за състоянието на връзките на всички останали рутери, той може да приложи алгоритъма на Дейкстра. Всъщност всяка връзка се представя два пъти, по веднъж за всяка посока. Двете цени могат да се усреднят или да се използват отделно. Изчислените маршрути се записват в маршрутните таблици.

Необходимата памет за съхраняване на информацията за състоянието на връзките за мрежа с n рутери, всеки от които има по k съседи е пропорционална на nk.

Така големите по размер мрежи изискват използване на рутери с голям обем памет.

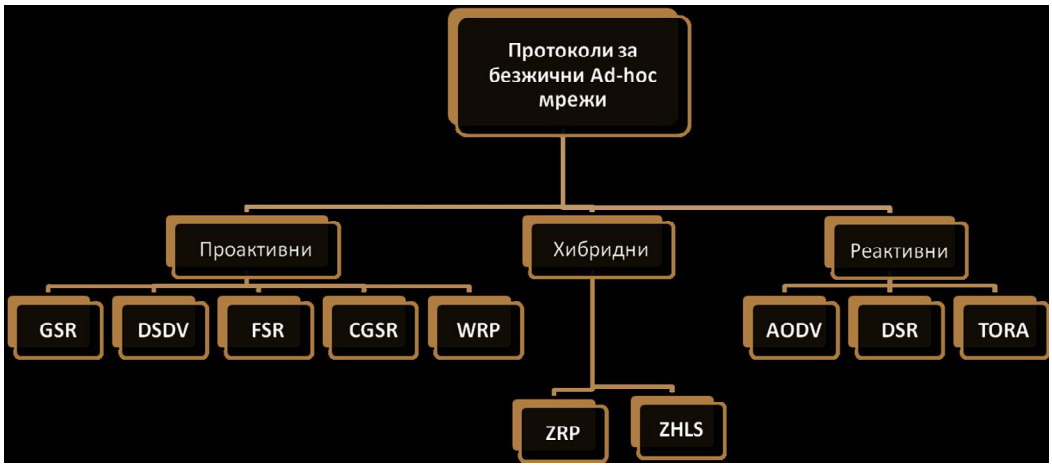
3. Йерархична маршрутизация

С увеличаването на размерите на мрежата нараства обемът на маршрутните таблици, което изисква повече памет и процесорно време за тяхната обработка. Това налага въвеждането на йерархично маршрутизиране, при което мрежата се разделя на **области**. Рутерите в една област знаят всичко за вътрешната структура на своята област, но не знаят вътрешната структура на останалите области. За по-големи мрежи може да е необходима йерархия с повече от две нива.

Ако n е броят на маршрутизаторите в една мрежа, може да се покаже, че оптималният брой области, всяка с по равен брой маршрутизатори е най-близкото цяло до $\sqrt{n}$.

III. Видове маршрутизиращи протоколи при мобилни разпределени мрежи

Съществуващите маршрутизиращи протоколи за мобилни разпределени мрежи най-общо могат да бъдат разделени в три категории: проактивни, реактивни и хибридни.



Проактивните маршрутизиращи протоколи поддържат информация за пътищата между кои да е две станции в мрежата. Тъй като тази информация обикновено се пази в таблици те се наричат още table-driven протоколи. Реактивните маршрутизиращи протоколи от друга страна изграждат път между две станции, само когато възникне нужда от това. Обикновено посредством процедура за откриване на нов път инициирана от източника на информацията. Веднъж открит, маршрута се пази докато е наличен и докато се използва. След определен период без да бъде използван той се отстранява и при следваща необходимост се търси наново. Предимството на проактивните маршрутизиращи протоколи е времето за използване на маршрута, тъй като той е наличен може да се използва веднага, докато при реактивните е необходимо време за неговото откриване, което довежда до забавяне на предаването на първия пакет. Въпреки това проактивните протоколи са свързани с поддържане на таблици, т.е. необходимо е мобилните устройства да имат по-голям капацитет от памет, а също така при тях изразходването на пропускателната способност за целите на маршрутизирането е много по-голямо. Третия тип протоколи, хибридните имат за цел да спечелят от предимствата на другите два използвайки както реактивен така и проактивен подход. Около всяка станция се формира зона, вътре в зоната се използва проактивно маршрутизиране, а за всеки пакет към станция извън зоната на източника се прилага реактивно маршрутизиране.

1. Проактивни маршрутизиращи протоколи

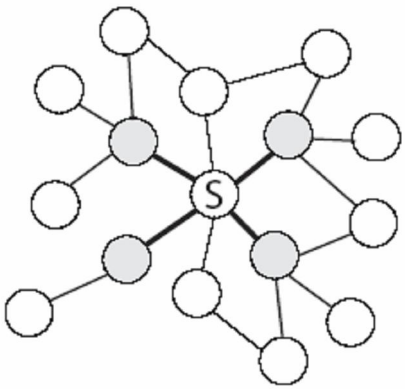
Към проактивните протоколи принадлежат: Destination-Sequenced Distance-Vector (DSDV), Wireless Routing Protocol (WRP), Global State Routing (GSR), Fisheye State Routing (FSR), Optimized Link State Routing (OLSR), Cluster-head Gateway Switch Routing (CGSR), Hierarchical State Routing (HSR), Topology broadcast reverse path forwarding (TBRPF), Distance routing effect algorithm for mobility (DREAM).

Протоколът **DSDV** намира единствен път между всеки две мобилни устройства, който гарантирано не съдържа цикъл и е с минимална дължина. За намиране на най-къс път се използва Белман-Форд алгоритъма. Избягването на цикли се постига с поредни номера. Всяка станция поддържа последователно нарастващ номер за себе си и списък

от номерата на всички останали станции. С цел намаляване на големината на служебната информация се използват два типа съобщения за опресняване на пътищата: пълни (изпраща се цялата маршрутизираща таблица) и частични (изпращат се само настъпилите промени). Въпреки това DSDV все още използва значително количество от пропускателната способност на мрежата и не може да бъде използван за мрежи съдържащи голям брой станции. [10]

Протоколът **WRP** също гарантира, че намерените пътища не съдържат цикли. Той също както DSDV принадлежи към класа на distance-vector маршрутизиращите протоколи. Недостатък на този протокол е, че поддържа четири маршрутизиращи таблици, което консумира значителна част от ресурсите памет на мобилните станции, която нараства с нарастването на размерите на мрежата. Друг недостатък е, че разчита на надеждно и в правилен ред получаване на маршрутизиращите съобщения. За станциите с ограничена мощност недостатък е периодичното обменяне на т.нар. hello съобщения между съседите, когато няма предаване на пакети, което не позволява на станциите да преминат в спящ режим и да намалят консумацията си.

Протоколът **OLSR** е оптимизирана версия на класическия link-state маршрутизиращ протокол какъвто е OSPF. Оптимизирането идва от използване на концепцията за Multipoint Relays (MPRs) (фиг. 4), това е множество от съседни станции, които ще извършват разпръскването на маршрутизиращите съобщения до станциите отдалечени на две и повече стъпки от източника. По този начин значително се намалява броя на broadcast съобщенията в мрежата. Маршрутизиращите съобщения се обменят през определен период от време, като определянето на този период е критично за работата на протокола. Протоколът дава значително подобрение спрямо традиционните link-state протоколи за мрежи, в които мобилните станции са разположени нагъсто.



фиг. 4 Многоточкови релета

Протоколът **CGSR** принадлежи към класа на йерархичните маршрутизиращи протоколи. Отделните станции са групирани в клъстери, но вътре в клъстера не се налага да се поддържа йерархичност. За всеки клъстер се избира една главна станция, т.нар. cluster-head, която управлява отаналите. Всяка комункация между клъстерите задължително минава през главната станция на съответния клъстер. Останалите станции трябва да пазят информация само за пътя до своята главна станция. Станциите, които попадат в два клъстера е наричат gateway станции и чрез тях се осъществява връзка между отделните клъстери. Въпреки, че се явява сериозно подобрение спрямо протоколите използващи механизма на наводнението (flooding) количеството на допълнителната контролна информация необходима за поддържането на клъстерите е значително. Причината е, че всяка станция периодично разпръсква своята таблица със съседствата в клъстера и я обновява с новополучената информация от останалите.

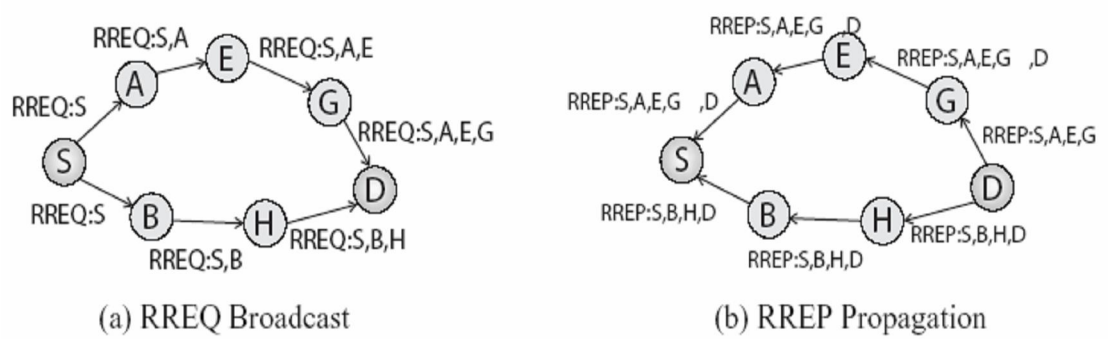
В заключение проактивните маршрутизиращи протоколи не са подходящи за мрежи състоящи се от по-голям брой станции поради повишаването на количеството маршрутизираща информация, което би попречило на обменянето на полезна информация. Някои от разгледаните протоколи биха работили добре и при по-голям брой станции, но относително ниска мобилност. Използването им би било уместно, само когато се цели преследване на качество на услугата (QoS), което не може да бъде осигурено от реактивните маршрутизиращи протоколи.

2. Реактивни маршрутизиращи протоколи

Реактивните маршрутизиращи протоколи, наричани още *on-demand* са проектирани така, че да намалят допълнителната контролна информация, която се обменя при проактивните, като се поддържа информация само за активните пътища. Това означава, че пътища се изграждат и поддържат само за станции, които се нуждаят да изпратят данни до определен получател. Откриването на пътища в този случай обикновено се осъществява по механизма на наводняването (flooding). Когато бъде достигнат получателя той потвърждава пътя използвайки междинните станции в обратен ред ако връзките са двупосочни или отново с наводнение ако съществуват еднопосочни връзки. Реактивните маршрутизиращи протоколи се разделят от своя страна на две под-категории: *source routing* и *hop-by-hop routing.* При source routing реактивните маршрутизиращи протоколи заглавната част на всеки обменен пакет включва адресите на всички междинни станции между източника и получателя. По този начин се избягва необходимостта междинните станции да поддържат маршрутизираща информация за всеки активен път, който минава през тях за да могат да препратят информацията към крайната станция. Нещо повече, не е необходимо да се поддържа свързаност със съседните станции посредством периодични сигнализиращи съобщения. Този подход обаче прави използването им в големи мрежи трудно поради две причини: първо с нарастването на броя на междинните станции нараства и вероятността за пропадане на пътя и второ с нарастване на дължината на пътищата силно нараства и допълнителната служебна информация (overhead) включвана в заглавната част на всеки пакет. При hop-by-hop маршрутизирането всеки пакет съдържа само адресите на получателя и на следващата станция. Всяка междинна станция проверява маршрутизиращата си таблица, за да реши накъде да препрати пакета по пътя му към своя получател. Този подход позволява по-голяма адаптивност към динамичната среда на мобилните разпределени мрежи, защото всяка станция може да опреснява маршрутизиращата си таблица с по-нова информация, която получава и да препредава пакетите по нови и по-добри пътища. Недостатък е необходимостта междинните станции да поддържат маршрутизираща информация за всеки активен път през тях, както и да поддържат свързаност със своите съседи. Към реактивните протоколи принадлежат: Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporary Ordered Routing Algorithm (TORA), Associativity-based Routing (ABR), Location-aided Routing (LAR), Ant-colony-based Routing Algorithm (ARA), Flow Oriented Routing Protocol (FORP), Cluster-based Routing Protocol (CBRP). [10]

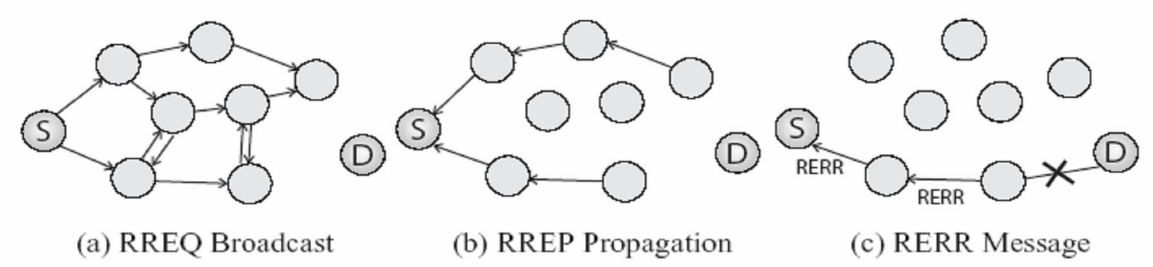
Протоколът **DSR** принадлежи към source routing реактивните маршрутизиращи протоколи и за него са валидни недостатъците описани по-горе. За динамични и много големи мрежи значителна част от пропускателната способност се използва за обмяна на маршрутизираща информация затова не е обосновано използването му. Въпреки това той има значителни преимущества пред останалите реактивни протоколи и за малки до средни мрежи и такива с умерена мобилност работи значително добре. Когато станция се нуждае да изпрати пакет до друга, за която не знае маршрут тя наводнява мрежата с route request съобщения. Всяка станция, която получи тези съобщения ги препраща,

включвайки себе си в заглавната част на съобщението (фиг. 5), освен ако не е крайната станция или няма информация за път до нея, като в този случай отговаря с route reply съобщение. Отговорът се изпраща до източника по същия механизъм. Ако има промяна някъде по пътя се изпраща *route error* съобщение и отпадналата предишна информацията се изтрива. Недостатък е недостатъчно ефективното отстраняване на остарели пътища което освен, че е свързано с повишено използване на пропускателната способност е свързано и с препълване с невярна информация на маршрутизиращата памет (route cache) на междинните станции. Предимството на този протокол пред останалите е откриването на повече от един маршрут, които се пазят временно и при отпадане на текущо използвания той може веднага да бъде заменен, което може да бъде много ефективно при ниска мобилност на станциите. Друго предимство е, че не е необходимо периодичното обменяне на hello съобщения и станциите могат да влязат в спящ режим, като намалят консумацията на енергия и пропускателна способност. [10]



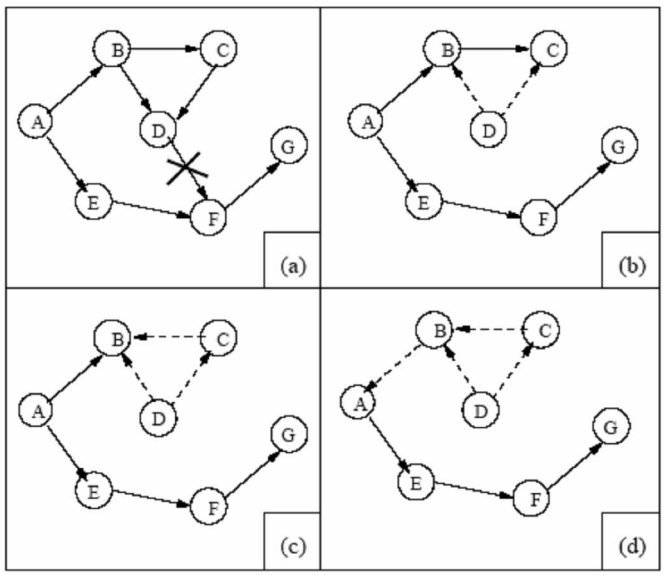
Фиг. 5 Механизъм на откриване на маршрут при DSR

Протоколът **AODV** е друг пример за реактивен маршрутизиращ протокол, който обаче използва подхода hop-by-hop routing. За насочване на съобщенията се използва информацията в маршрутизиращата таблица. За предотвратяване на цикли и разпознаване на по-нови пътища се използва идеята за последователните номера на DSDV протокола. Тези номера се включват във всяко маршрутизиращо съобщение, при получаване на съобщение с по-нов номер старият път се изтрива от маршрутизиращата таблица независимо, че пътя може все още да е активен. Освен тях се използват и таймери, след изтичането на които информацията отново се изтрива без значение дали пътя е активен или не. Протоколът поддържа използването на най-много един път до получател. Въпреки, че се адаптира добре и за по-големи мрежи откриването на нов маршрут може да е свързано с голямо закъснение, а отпадането му довежда до допълнително закъснение и консумира повече пропускателна способност. Модификация на протокола наречена Ad-hoc On-demand Multipath Distance Vector (AOMDV) позволява използването на алтернативни пътища за намаляване на броя на процедурите за откриване на нов път, което води до значителни подобрения. На фигура 6 е показан механизма на откриване и поддържане на пътища. [11]



Фиг. 6 Откриване и поддържане на маршрути при AODV

При протокола **TORA** процедурата по откриване на нови маршрути изчислява множество пътища до крайната станция, всички те несъдържащи цикли. За целта се използва т.нар. Destination-oriented directed acyclic graph (DAG) граф. Въпреки, че разпределените мрежи се представят от ненасочени графи, в концепцията на TORA се използва логическа насоченост на ребрата на графа по посока от източника до получателя. При отпадане на всички връзки в графа водещи до крайната станция започва процедура по обръщане на посоките на ребрата (връзките), т.нар. link reversal процедура (фиг. 7), докато отново се стигне до състояние, при което графа отново е насочен към крайната станция. Протоколът TORA използва модифицирана версия на алгоритъма за обръщане на посоките на ребрата, който дава възможност за откриване на несвързани сегменти в графа, което е полезна черта, липсваща в голяма част от другите протоколи. По-нови пътища се откриват едва, когато отпаднат всички стари, което е аналогично на AODV протокола. Недостатък на TORA е, че разчита на надеждно и в правилен ред получаване на маршрутизиращите съобщения. Също така използвайки процедурата за обръщане на посоките на връзките прави много трудно използването на метрики за определяне на по-предпочитани пътища. Последното почти елиминира предимството на множеството маршрути до крайната станция. Въпреки това TORA остава предпочитан избор за мрежи, в които се изисква множество станции да имат маршрут до една крайна станция. [11]



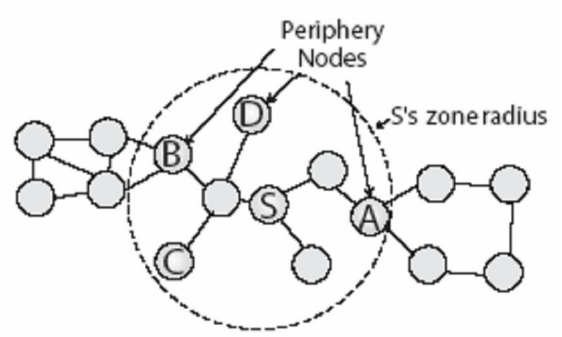
Фиг. 7 Фази по откриване и поддържане на маршрут при TORA

3. Хибридни протоколи за маршрутизация

Повечето от съществуващите хибридни протоколи се базират на понятието за зона, т.е. от гледна точка на отделните станции мрежата е разделена на зони, които може да се препокриват или не. Най-известните от хибридните маршрутизиращи протоколи са: Zone Routing Protocol (ZRP) и Zone-based Hierarchical Link State (ZHLS).

Протоколът **ZRP** е типичен пример за хибриден маршрутизиращ протокол. Всяка станция представлява център на зона, като по този начин мрежата е разделена на множество зони, които се застъпват. Всяка зона е с радиус ρ (фиг. 8) като радиуса не оказва някакви физически граници, а е цяло число даващо броя на стъпките до станциите по ръба на зоната. Стойността на радиуса контролира размерите на проактивната и реактивната част на мрежата. Станциите в зоната са разделени на вътрешни и периферни. Периферни са всички станции отдалечени на ρ на брой стъпки

от централната станция. ZRP протокола се състои от три различни компонента. Локалната проактивна компонента се нарича Intra-zone Routing Protocol (IARP), а глобалната реактивна компонента съответно Inter-zone Routing Protocol (IERP). Трябва да се подчертае, че IARP и IERP не са конкретни маршрутизиращи протоколи, сбор от проактивни, съответно реактивни маршрутизиращи протоколи. Факта, че топологията вътре в зоните е известна може да бъде използван при откриване на глобални пътища. Това се осъществява чрез концепцията на т.нар. bordercasting. Тя се изразява в насочването на информацията за топологията предоставена от IARP към граничните станции на зоната. Компонентата, която се занимава с тази задача се нарича Bordercast Resolution Protocol (BRP). За откриването на нови и отпаднали стари съседи ZRP разчита на протокол на каналния слой наречен Network Discovery Protocol (NDP). Протоколът ZRP е атрактивен с това, че може да се трансформира в изцяло проактивен, в изцяло реактивен или в нещо между тях само с променянето на един единствен параметър - радиуса на зоната. При класическата версия на протокола радиуса е предварително фиксиран. Версията на протокола Adaptive ZRP предлага алгоритъм за неговото динамично променяне.



Фиг. 8 Маршрутизираща зона на ZRP с радиус 2

Протоколът ZRP има плоска структура. За разлика от него **ZHLS** е йерархичен протокол. При него мрежата е разделена на зони, които не се препокриват. Всяка станция има два идентификационни номера: node ID и zone ID, втория от които се изчислява чрез информация от GPS. Йерархичната структура е на две нива: топология на ниво станция и топология на ниво зона. За разлика обаче от останалите йерархични протоколи тук липсва усложненията за избор на главна станция и за поддържане на клъстери. При ZHLS е намален размера на служебната информация, пътищата са устойчиви на движение на станциите, стига да е в рамките на зоната. Недостатък на ZHLS е изискването всички станции да имат предварително зададени статични карти на зоните, което не винаги е приложимо.

IV. Маршрутизация при WMNs

Безжичните многосвързани мрежи (WMNs) са вид мрежи с комутация на пакети. В мрежите с комутация на пакети маршрутизиращите протоколи препращат пакетите с данни от източника до получателя чрез междинни възли. Има много протоколи за маршрутизация за този тип мрежи. Всеки протокол използва различна стратегия за маршрутизация. Според това каква стратегия за маршрутизация използват протоколите за WMNs могат да бъдат групирани в две основни групи проактивни и реактивни протоколи.

Проактивните протоколи са познати също като неадаптивни и те са характерни за мрежи, при които маршрутите са предварително изчислени и топологията на мрежата е статична или се променя много бавно.

Реактивните протоколи са познати също като адаптивни и са характерни за мрежи с динамично променяща се топология, при които маршрутите се изчисляват при необходимост (при поискване).

Хибридните протоколи са друга категория, която напрактика комбинира част от характеристиките на проактивните и реактивните протоколи.

Има и други стратегии за маршрутизация, които също могат да обединят различните протоколи в групи. Съществува алтернативна маршрутизация, която се основава на случайни решения или на решения взети в зависимост от съответното състояние на мрежата. Това е т. нар. разпределена стратегия, при която за определяне на маршрута се използва информацията получена от съседните възли. Тази стратегия се противопоставя на централизираната стратегия, базирана на master/slave идеята, при която главния възел (master) определя маршрута на предаване на пакетите с данни и подчинения възел (slave) не е в състояние сам да управлява трафика.

Тези стратегии за маршрутизиране спомагат за създаването на маршрутизиращи протоколи, които по принцип са различни, но са и подобни, тъй като се опитват да постигнат комбинация от следните желани свойства:

- устойчивост (robustness) – алгоритъма за маршрутизация трябва да се справи с промените в мрежовата топология
- стабилност (stability)
- оптималност (optimality)
- пропускателна способност (throughput)
- балансиране на натоварването (load balancing)
- управление на претоварването на мрежата (congestion control)

Всеки протокол избира върху кои от тези свойства да се съсредоточи.

Процесът на изпращане пакети от един възел към друг през междинни възли – маршрутизирането – е само част от процеса на предаване на съобщението. По-точно, той е само последната част на целия процес. Не забравяйте, че при безжичните мрежи може да има повече от един път от източника до получателя. Изборът на най-подходящия пътя за пакета се нарича селекция на пътя (path selection).

1. Метрики за избор на път (Path Selection Metric)

Избора на маршрут е процес, при който се избира един път от списък с възможности и този път е или част от маршрута или целият маршрут на пакета до неговия получател. Този процес включва прилагането на метрики за маршрутизация към няколко маршрута, с цел да се изберът (или предвидят) най-добрите маршрути. Метриката е свойство на маршрута, състоящо се от различни стойности използвани от алгоритмите за маршрутизация, за да се определи дали даден маршрут е по-добре да се изпълни отколкото друг. Метриката може да включва информация като:

- пропускателна способност (скорост на предаване, bandwidth)
- мрежово закъснение (network delay)
- процент на загуба на пакети (packet loss rate)
- брой скокове (hop count)
- цена на пътя (path cost)
- натоварване (load)
- надеждност (reliability)
- разходи за комуникация (communication cost)

Други метрики са изградени върху техники, които могат да включват метрики като споменатите по-горе. Усъвършенстването на мерките улеснява избора на по-добри пътища. Като цяло тези метрики служат за представяне на цената на връзката между два възела в мрежата. Някои от най-популярните метрики, използвани за WMNs са:

- очакван брой предавания (Expected Transmission Count – ETX) – това е скоростта на загуба на пакети при предаването им между двойка възли
- време-закъснение (Round Trip Time – RTT) – това е закъснението при обмена (изпращане и получаване) на пакети между два възела в мрежата
- брой скокове (Hop Count) – това е броя на връзките между два възела в мрежата

2. Протоколи за маршрутизация при WMNs

Съществуват голям брой протоколи за маршрутизация при WMNs. Според едни основната причина за това е липсата на стандарт, който ще определи точно операциите по маршрутизация на съобщенията. Въпреки, че IEEE 802.11 е набор от стандарти, които определят много аспекти на функционирането на WMNs в момента няма приет стандарт за маршрутизация. Това оставя редица въпроси за различните аспекти на функционирането на WMNs, отворени за обществен дебат и много последващи решения на този проблем. Друга важна причина за изобилието от протоколи за WMNs е диапазона на приложения на тази технология. Безжичните многосвързани мрежи намират широко приложение в: службите за сигурност, отбрана, борба с бедствия и аварии, за управление и оптимизиране на работата в големи производствени комплекси, за военни комуникационни и т.н. Такива приложения може да имат различни оперативни изисквания като мащабност (голяма площ на достъп), сигурност (защитена комуникация), QoS (качество на услугата и опит съответно).

Други автори пък посочват, че наличието на толкова много протоколи за маршрутизация се дължи на различните начини за използване на безжичната среда и на комбинация от съществуващи и нови идеи. Различните начини за използване на средата дават на протоколите присъщата им природа.

Сега ще разгледаме част от протоколите за WMNs като не забравяме, че те са разделени в три основни групи: реактивни, проактивни и хибридни протоколи. Към реактивните протоколи спадат: Adhoc on Demand Distance Vector (AODV), Dynamic Source Routing (DSR), SRCRR, Link Quality Source Routing (LQSR), Multi radio LQSR(MRLQSR). Към проактивните протоколи спадат: Optimized Link State Routing (OLSR), Destination Sequence Distance Vector (DSDV), Scalable routing using heat protocols. Представител на хибридните протоколи е протокола MeshNetworks Scalable Routing (MSR). Сега ще представим подробностите за всеки протокол. Като първи са тези, класифицирани като реактивни протоколи.

2.1 Реактивни протоколи за маршрутизация

- **DSR – dynamic source routing:**

При този протокол източника проверява в своята памет за маршрутизация дали има валиден маршрут до получателя и ако има маршрут източника използва този маршрут, а ако няма източника генерира пакет за заявка за маршрут. Хостът, който получава заявката за маршрут изпълнява следните операции:

- ✓ Ако ID на заявката за маршрут се намира в списъка на хоста за наскоро изпълнени заявки, тогава той (хоста) пренебрегва пакета за заявка за маршрут, защото вероятно има такъв маршрут
- ✓ Ако ID на заявката за маршрут се намира в списъка на хоста за наскоро изпълнени заявки, тогава пакета за заявка за маршрут се пренебрегва и не се обработва по нататък
- ✓ Ако двойката адрес на източника и ID на заявката за маршрут се намират в списъка на хоста за наскоро изпълнени заявки, тогава пакета за заявка за маршрут се игнорира и не се обработва по нататък

- ✓ В противен случай адреса на хоста се добавя към записа на маршрута в пакета за заявка за маршрут и заявката се препраща отново до всички.

Предимството на този протокол е, че не изисква периодично обновяване (beacon) и така възелът може да спести енергия, което го прави подходящ за нискоенергийни устройства. В същото време неговите недостатъци са, че няма механизми за справяне със задръстването получено от голям трафик в мрежата. При нарастване на закъснението поради нарастването на размера на мрежата, протокола не може да разшири обхвата си.

- **AODV – Ad-hoc On-demand Distance Vector:**

При AODV протокола само временни мершрути се създават по заявка и само активни маршрути се поддържат. Това намалява допълнителната служебна информация, която се предава по маршрута, но въвежда първоначално забавяне поради създаването на маршрут по заявка. Този протокол използва прост Request-Reply (заявка–отговор) механизъм за намиране на маршрут подобен на този на DSR. Преимуществата на този протокол са, че той реагира бързо на топологичните промени и не създава цикли, и избягва проблема на броенето до безкрайност. От друга страна има също недостатъци като например: няма постоянни маршрути създадени по заявка и само активни маршрути се поддържат. Това намалява предаването на допълнителна служебна информация по маршрута, но въвежда първоначално забавяне поради създаването на маршрут по заявка. Също така не е подходящ за нискоенергийни устройства. Освен това процентът на доставени пакети значително намалява с нарастване на броя на връзките.

- **SrcRR:**

Това е разширение на DSR протокола, което използва ETX метрика. Занимава се основно с пропускателната способност, като взема в предвид загубата на връзка и процента на предадени битове и временните прекъсвания. Когато един възел иска да изпрати данни до друг възел, за който няма известен път тогава се следва същия процес като при DSR и AODV с една допълнителна особеност: възелът, който получава пакета за заявка на маршрут добавя ETX метриката от възела, от който е получил заявката. За да се подсигури маршрутизирането единствено на актуална информация, ако метриката на връзката не се обновява на 30 секунди, то предаваната информация отпада от паметта на връзката. Преимуществото на този протокол е, че той намира матршрути с голяма пропускателна способност. Недостатъкът е, че не подлежи на мащабиране (разширяване на обхвата си) поради високия брой заявки, който увеличава значително трафика в мрежата.

- **LQSR – Link Quality Source Routing:**

Също като SrcRR това е разширение на DSR протокола, което добавя някои метрики към DSR. Метриките са: HOP (най-късия маршрут между два възела в мрежата), Round Trip Time (RTT) (време – закъснение при предаването на пакета (отиване и връщане)), Packet Pair Delay (PktPair) (забавянето между предаването на два последователни пакета), ETX (очакван брой предавания). Преимуществото на този протокол е, че той увеличава пропускателната способност, тъй като взема в предвид ETX метриката.

- **MR – LQSR:**

Основава се на използването на метрика нар. мулти – радио (MR) с LQSR. Идеята е, че ако един възел има множество радио честоти, то те са настроени на

различни неинтерфериращи станции. Протоколът използва натоварването на връзката, за да намери подходящ път до даден получател. Преимуществата са подобни на тези, които се забелязват при използването на мулти – радио: баланс на натовареността, компромис между забавяне и пропускателна способност, тъй като използва канали с добро качество. Недостатъка е, че не може да разширява обхвата си (notscalable).

2.2 Проактивни протоколи за маршрутизация

- **DSDV:**

Всеки възел в мрежата притежава две основни характеристики: възрастта на възела, която периодично нараства и множеството на текущите съседи. Като цяло съобщението включва възрастта и дължината до всеки възел в мрежата в таблицата за марщрутизация. За да се намали трафика причинен от процесите на обновяване на таблицата за маршрутизация могат да се извършат две неща: full dump (премахване на складирани данни, разпространени сред много пакети), или увеличаваме честотата на обновяванията, тогава само част от таблицата за маршрутизация ще се променя в даден момент. Предимствата на този протокол са, че той гарантира пътища без цикли и по-висока ефективност при откриването на маршрути за разлика от реактивните протоколи, където имаме забавяне при откриването на маршрут. Недостатъка е, че процентът на доставени пакети намалява с увеличаване на размера на мрежата. Също така мрежовите ресурси са ненужно използвани, когато мрежата е стабилна и контрола на задръстванията е по-лош.

- **OLSR:**

Това е оптимизирана версия на протоколите за състояние на връзката. Като при този протокол топологичните промени причиняват наводняване с информация за топологията на мрежата. За да се намали претоварването на мрежата протоколът използва Multipoint Relay (MPR) за намаляване на предаването в някои участъци на мрежата. Като съществуват два вида контролни съобщения: HELLO (за намиране на хост и състояние на връзката) и Topology control (за предаване на списъка на избраните MPR и за уведомяване на съседите). Съобщенията за контрол на топологията се предават периодично само от MPR хостовете. Предимството на този протокол е, че е подходящ за многосвързани мрежи, където източника и получателя се сменят непрекъснато. Недостатъка е, че честотната лента се изразходва много при съобщенията за контрол на топологията и този факт се утежнява още повече с нарастване на мрежата.

- **Маршрутизация с разширяване на обхвата и използване на HEAT протокол:**

При тази маршрутизация рутерите в мрежата са моделирани като топлинни източници, които създават температурни полета в мрежата. Колко е по-висока температурата на един възел, толкова по-близо е той до точката на достъп. Пакетите се предават по възлите на мрежата с най-висока температура докато достигнат топлинен източник (напр. интернет рутер). Ключовата идея на HEAT е да осигури мащабност (свързана с предаваната допълнителна контролна информация по мрежата) и стабилност на мрежата (свързана със сривовете на връзката). Когато се добавя, отстранява или променя някои елемет на мрежата температурната стойност се преизчислява. Предимството е, че се постига мащабност с по-малко изразходване на ресурси и честотна лента и се улеснява процеса на маршрутизацията. Недостатъкът е, че външната топлина на средата може да засегне рутерите, и че ненужно се изразходва

енергия при балансиране на натовареността, което също може да засегне топлинния параметър на възела.

Като цяло можем да кажем, че изборът на ефективен протокол за маршрутизация на съобщенията в мрежата изисква да обърнем внимание на поведението на протокола при различни условия, за да преценим кога един протокол е по-добър от друг. Производителността на протоколите за маршрутизация при WMNs зависи от самата мрежа.

Обощение

Особеностите на различните протоколите за маршрутизация при WMNs са показани в долните таблици:

Протокол	Сложност на съхранение (storage)	Времева сложност	Контрол на големината на пакета	Сложност на комуникацията
DSDV	$O(N)$	$O(D)$	$O(N)$	$O(N)$
GSR	$O(N.A)$	$O(D)$	$O(N)$	$O(N)$
FSR	$O(N.A)$	$O(D)$	$O(N)$	$O(N)$
CGSR	$O(2N)$	$O(D)$	$O(N)$	$O(N)$
WRP	$O(N.A)$	$O(D)$	$O(N+A)$	$O(N)$
DSR	$O(D)$	$O(2D)$	$O(D)$	$O(2N)$
AODV	$O(D_d)$	$O(2D)$	$O(D_d)$	$O(2N)$
TORA	$O(D_d.A)$	$O(2D)$	$O(1)$	$O(2N)$
ZRP	$O(M+B+D_d)$	Intrazone: $O(M)$ Interzone: $O(2D)$	Intrazone: $O(M)$ Interzone: $O(1)$	Intrazone: $O(M)$ Interzone: $O(2B.D)$
ZHLS	$O(M+N/M)$	Intrazone: $O(M)$ Interzone: $O(D)$	Intrazone: $O(A)$ Interzone: $O(N/M)$	Intrazone: $O(M)$ Interzone: $O(N)$

Сравняване на сложността на протоколите за маршрутизация при безжични Ad-hoc мрежи

Значението на символите в таблица 1 е следното:

- M – среден брой възли в зоната
- N – общ брой възли в мрежата
- A – среден брой съседни възли
- B – среден брой гранични възли (gateway) в зоната
- D_d – брой на най-желаните получатели

Протокол	Изчисление на маршрута	Структура	Маршрути	Маршрути-зация от източника (source routing)	Съхранявана информация	Период на актуализация	Актуализирана информация	Получатели на актуал. информация	Метод
DSDV	Проактивно/ Разпределено	Плоска	Единичен път	Не	Вектор на разстоянието	Хибридна	Вектор на разстоянието	Съседите	Broadcast
GSR	Проактивно/ Разпределено	Плоска	Единичен път или множество пътища	Не/Да	Цялата топология	Периодична	Състоянието на връзките за всички възли	Съседите	Broadcast
FSR	Проактивно/ Разпределено	Плоска	Единичен път или множество пътища	Не/Да	Цялата топология	Периодична	Състоянието на връзките	Съседите	Broadcast
CGSR	Проактивно/ Разпределено	Йерархична	Единичен път	Не	Вектор на разстоянието	Периодична	Вектор на разстоянието	Съседите	Broadcast
WRP	Проактивно/ Разпределено	Плоска	Единичен път		Таблица с цените на връзките по пътя до получателя	Хибридна	Вектор на разстоянието	Съседите	Broadcast
DSR	Реактивно/ Broadcast заявка	Плоска	Множество пътища	Да	Маршрути до желаните получатели	Предизвикана	ROUTE-ERROR	Източника	Unicast
AODV	Реактивно/ Broadcast заявка	Плоска	Множество пътища	Не	Следващия скок по пътя до получателя	Предизвикана	ROUTE-ERROR	Източника	Unicast
TORA	Реактивно/ Broadcast заявка	Плоска	Множество пътища	Не	Разстоянията до съседите на даден възел	Предизвикана	Разстоянията до съседите	Съседите	Broadcast
ZRP	Проактивно (intra)/ Реактивно (inter)	Плоска	Единичен път или множество пътища	Interzone: Да	Локалната топология на зоната	Периодична	Състоянието на връзките между възлите в зоната	Съседите	Broadcast
ZHLS	Проактивно (intra)/ Реактивно (inter)	Йерархична	Единичен път	Не	Локалната топология на зоната	Периодична/ Предизвикана	Състоянието на връзките между възлите в зоната	Всички възли/ възлите в зоната	Broadcast

Сравнителна таблица на протоколите за маршрутизация при безжични Ad-hoc мрежи

Библиография

[1] Боянов К., Компютърни мрежи и интернет, София, 1998
[2] Ганчев И., Компютърни мрежи и комуникации. Пловдив, ИМН, 1999.
[3] Тужаров, Хр. Компютърни мрежи, ПИК,В.Търново, 2000.
[4] Цонев Ив., Компютърни мрежи и комуникации, Шумен, 2007
[5] Шиндлър Д., Компютърни мрежи, Софтпрес, 2004
[6] Basagni, S., Conti, M., Giordano, S., Stojmenovic, I. „Mobile Ad Hoc Networking", IEEE Press, ISBN: 0-471-37313-3, 2004
[7] Chakeres, I., „AODV Routing Protocol Implementation Design". *Proceedings of the International Workshop on Wireless Ad Hoc Networking (WWAN)*, 2004, 698-703
[8] Ernst J., „Scheduling techniques in WMN", 2009
[9] Jiang, X., Camp, T. (2002) „A Review of Geocasting Protocols for a Mobile Ad Hoc Network". *Proceedings of the Grace Hopper Celebration (GHC '02)*
[10] Royer E., „A review of current routing protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, 1999
[11] Sklyarenko G., „AODV Routing Protocol", 2006