FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
UNSKA 3, ZAGREB
ZAVOD ZA ELEKTRONIČKE SUSTAVE I OBRADU INFORMACIJA

SUSTAVI ZA PRAĆENJE I VOĐENJE PROCESA

SEMINARSKI RAD

MOBILNE AD-HOC MREŽE (MANET)

Domagoj Rudančić
0036356782

Zagreb, 31.5.2004.

Sadržaj

UVOD

Područje mobilnih računala sve je više popularno u zadnjih nekoliko godina. Mobilna računala postaju sve manja, snažnija i ima ih sve više počevši od prijenosnih računala (laptopa), ručnih računala (PDA), pa sve do mobilnih telefona. Uskoro će biti više od milijardu bežičnih uređaja u svijetu.
Kako su mobilni telefoni potpuno promijenili značenje pojma biti dostupan, sličan preobrazba čeka i korisnike prijenosnih računala, te je samo pitanje vremena kada će nov način korištenja prijenosnih računala promijeniti navike i učiniti život lakšim. Kada govorimo o preobrazbi pri tom mislimo na razvoj rješenja koja će učiniti Internet dostupan od bilo kuda i bilo kada.
Kako se suvremeni čovjek sve više navikava na dostupnost "mreže" (Interneta)na kojoj može pronaći gotovo svaku potrebnu informaciju, polako je integrira u svoj život, tako npr. želimo na brzinu saznati gdje se može kupiti knjiga od specifičnog autora ili o specifičnoj temi, koje su ljekarne otvorene, pronaći ulicu itd. .
Danas se već nudi bežični pristup Internetu na aerodromima, Internet cafee-ima, hotelima, a takvi pristupi su bazirani na predhodno postavljenoj infrastrukturi kao npr. bežična pristupna točka (eng. wierless access point) preko koje se svojim bežičnim uređajem spajate na Internet ili komunicirate s drugom osobom i razmjenjujete podatke.
Takav način pristupa Internetu dok ste u pokretu preko vašeg prijenosnog računala zahtijevalo bi infrastrukturu kao za GSM mrežu. Za to se pristupilo razvoju drukčijeg modela mreža a to su ad- hoc mreže, odnosno MANET-u (eng. Mobile Ad-hoc Networks), kao pod vrsti ad-hoc mreža.

Što je to?

Mobile Ad-Hoc Network je dinamična pokretna mreža koja omogućuje bežično umrežavanje u pokretu bez potrebe za prethodno izgrađenom mrežnom infrastrukturom, a sastoji se od pokretnih čvorova (node), gdje čvor može biti čovjek s ručnim računalom (opremljenim s odgovarajućim uređajem za bežičnu komunikaciju), također prijenosno računalo, roboti bez posade, tj. bilo tko može biti čvor tko je opremljen s odgovarajućom opremom za bežičnu komunikaciju itd. .

Čvorovi u takvoj mreži mogu biti vrlo pokretni te uzrokuju vrlo brzu promjenu položaja čvorova, a time i stvaranje i gašenje veza među njima. Kako su čvorovi neprestano u pokretu znači da je topologija mreže promjenljiva. Time se zahtjeva da mreža mora biti sposobna da izlaskom nekog čvora ili više njih, odaslana informacija ne propadne već da sama pronađe novi put do odredišnog čvora.

Svrha MANET-a je da osigura mrežu koja se može odmah postaviti u proizvoljnom komunikacijskom okruženju te da se brzo prilagođuje na topološke promjene u mreži.

Moguće situacije u kojima bi se mogle koristiti ovakav način komunikacije: pri zajedničkoj akciji spašavanja policije, vatrogasaca i hitne pomoći, u vojnim operacijama, sastanci i konferencije gdje se razmjenjuju podaci bez potrebe za posebnom mrežnom infrastrukturom, mreža senzora – u komunikaciji među inteligentnim senzorima.

Model MANET-a i komunikacijsko okruženje

Spomenut ćemo pretpostavke vezane uz komunikacijske parametre, mrežnu arhitekturu i mrežni promet

- čvorovi su opremljeni prenosivim komunikacijskim uređajima koji se napajaju iz baterija, a vijek trajanja baterije nameće ograničenja u području dometa signala, a time i u komunikacijskoj

aktivnosti (slanje i primanje podataka) i u računalnoj snazi takvih uređaja

- veza između čvorova nije prijelazna, tj. ako čvor A može komunicirati izravno s čvorom B, a čvor B izravno komunicira s čvorom C, to ne znači da čvor A može izravno komunicirati s čvorom C. To je tzv. problem skrivenog terminala
- pretpostavit ćemo da čvorovi koriste stalne indentifikacijske oznake (kao npr. IP adrese)
- svaki čvor ima jednake mogućnosti, odnosno svaki čvor je sposoban izvršavati neku od funkcija iz iste grupe mrežnih servisa, pa ipak svi čvorovi ne moraju, nužno, izvršavati istu funkciju istovremeno. Također, ako čvor ima neku zadanu funkciju u mreži to ne znači da je njegova funkcija nepromjenjiva te se s vremenom i potrebama mijenja.

MANET je peer-to-peer mreža koja omogućuje izravnu komunikaciju s bilo koja dva čvora kad postoje uvjeti za slanje signala i kada čvorovi imaju dovoljno snage za odašiljanje signala.
Ako između početnog i odredišnog čvora ne postoji izravna veza tada se koristi multihop način uspostave veze (vidi dio "Kako radi?").
Dakle, cjelokupna komunikacija među entitetima ove mreže se ostvaruje slanjem radio signala, ali propagacija takvog signala jako je osjetljiva na različita pogoršanja u komunikacijskom kanalu pa spojenost čvorova u mreži nije garantirana, štoviše povremeni prekidi a i povremena spojenost su gotovo normalna pojava.
Većina prijenosnih uređaja imaju ograničene izvore energije (baterije), pa zbog toga snagu kojom se odašilje signal treba što je moguće više smanjiti. Osim toga domet signala svakog uređaja je ograničen, a i kanal kojeg koristi svaki mobilni uređaj je i prostorno ograničen, jer više uređaja može koristiti isti komunikacijski kanal samo ako su dovoljno udaljeni jedan od drugoga. To ima za posljedicu, pošto je domet svakog uređaja mnogo manji nego što je raspon mreže, da komunikacija među dva čvora ovisi o čvorovima koji

se nalaze između njih, tj. bez njih ne bi ni mogla biti uspostavljena komunikacija između dva najudaljenija čvora.
Zbog mogućih brzih kretanja čvorova i promjenjivih uvjeta širenja signala (propagacije) mrežne informacije , kao što su ruting tabele. postaju jako brzo nekorisne. Tako česta rekonfiguracija mreže može uzrokovati čestu izmjenu kontrolnih informacija među čvorovima, a koje služe da bi se ruting tabele obnovile i da bi svaki čvor mogao znati oblik i trenutno stanje mreže. Međutim, kako te informacije imaju kratko trajanje, što znači da se izmjenjuje veliki broj kontrolnih poruka, većina tih informacija neće biti ni iskorištena. To znači da je bandwith korišten za slanje kontrolnih informacija uzaludno trošen, odnosno na taj način može doći do zagušenja veze.

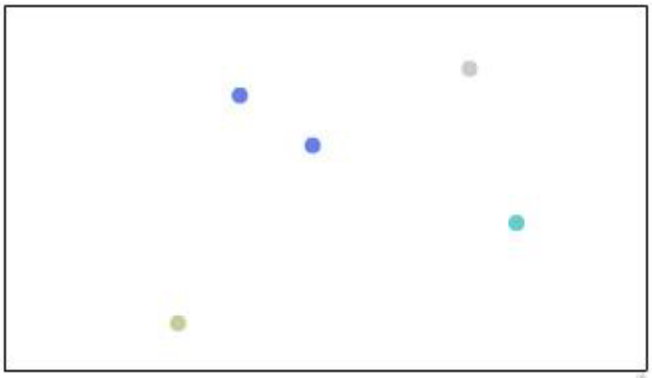
Zahtjevi za MANET

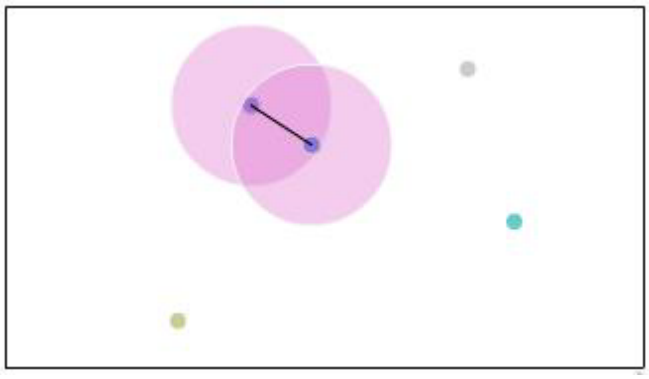
Dakle na temelju prethodno predočenog modela od MANET-a se očekuje:

- robusno usmjeravanje (eng. robust routing) i algoritmi za praćenje promjene topologije mreže da bi se povećala pouzdanost i dostupnost – da se smanji mogućnost da dio mreže ostane izoliran od ostatka mreže
- adaptivni algoritmi i protokoli da se čvorovi mogu prilagoditi čestoj promjeni propagacije signala, promjeni topologije mreže i uvjetima prometa u mreži
- protokole i algoritme koji će slati što manje kontrolnih poruka da štede komunikacijske reseurse (kanale)
- višestruke (različite) rute između izvorišnog i odredišnog čvora – da ne dolazi do protoka prometa samo između određenih čvorova, tj. da ne dolazi do zagušenja na toj ruti, te da se poveća pouzdanost
- robusnu mrežnu arhitekturu da se izbjegne osjetljivost na greške u mreži, zagušenja na čvorovima koji imaju veliki broj čvorova vezanih na sebi

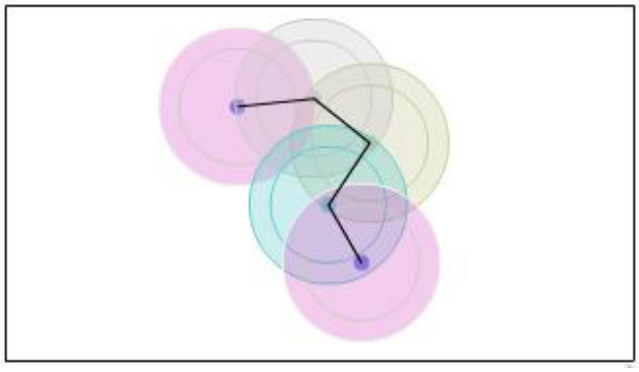
Kako radi ?

Ako odredimo dva čvora koji žele međusobno komunicirati (na slici plavi), a moći će direktno komunicirati ako se nalaze jedan drugome u području dosega signala i takav način komunikacije među čvorovima naziva se Singlehop.





Dok Multihop način komuniciranja se odvija kada čvorovi koji žele komunicirati nisu u dosegu, ali vezu mogu ostvariti samo ako među njima postoji dovoljan broj čvorova tako da je između svaka dva susjedna čvora ostvarena direktna komunikacija (singlehop).



Svaki čvor u takvoj mreži osim što je odredište informacijskih paketa i također vrši funkciju usmjerivača za pakete koji imaju druge odredišne čvorove. Znači čvorovi međusobno ovise jedan o drugome da bi veza u mreži postojala.
Pošto ne postoji centralni element u takvoj mreži neophodno je koristiti posebne protokole, koji osim što osiguravaju prosljeđivanje paketa od čvora do čvora, moraju pronaći odgovarajući put od izvorišnog do odredišnog čvora te provjeravati da li veza još postoji ili da li je prekinuta te u slučaju prekida određene rute pronaći novu i uspostaviti vezu.

Protokoli

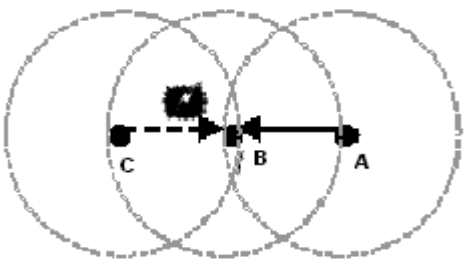
Za razliku od standardnih i bežičnih mreža u ad-hoc mrežama ne postoji postavljena infrastruktura te neka centralna jedinica koja bi nadgledala i upravljala radom mreže. Zbog takve mrežne arhitekture i prirode ad-hoc mreže (česte promjene topologije mreže) standardni protokoli za usmjeravanje (eng. routing) i ostali standardni protokoli ne mogu biti korišteni, te se koriste tzv. distributivni protokoli.
Zato najvažniju ulogu u razvoju MANET-a ima upravo razvoj algoritama za protokole koji će se moći prilagoditi mreži i zahtjevima koje smo ranije naveli.

Protokol za MAC sloj u MANET-u

Upotrebljivost nekog od postojećih protokola za MAC sloj, kao npr. CSMA (Carrier Sense Multiple Access) u području radio signala je ograničena zbog problema *"Skrivenog čvora"* i "I*zloženog čvora"*.

Problem skrivenog čvora

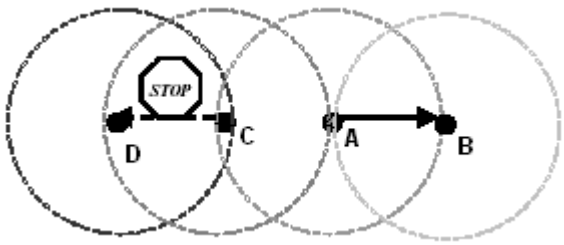
Problem se javlja jer su mreže koje rade s radio signalima potpuno drukčije od mreža kao npr. LAN jer primjerice ne garantiraju tako dobru spojenost kao LAN. Kao što smo već rekli veza među čvorovima nije prijelazna. Znači dok čvor A komunicira s čvorom B čvor C također želi komunicirati s čvorom B, ali kako je veza neprijelazna on pomoću standardnog protokola



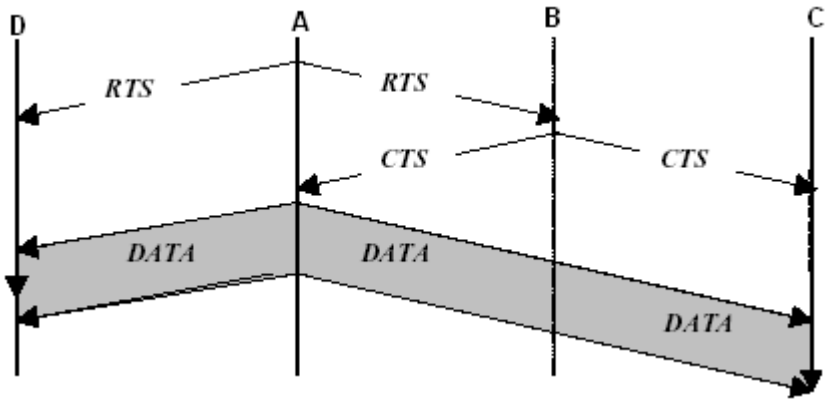
CSMA ne može čuti da je A trenutno u komunikacijskom kanalu zbog "prepreke", čvora B, pa zaključuje da je medij slobodan i da može komunicirati s čvorom B. Što za posljedicu ima da dolazi do kolizije na čvoru B.

Problem izloženog čvora

U ovom slučaju čvor A komunicira s čvorom B, dok čvor C želi uspostaviti komunikaciju s čvorom D. Koristeći CSMA protokol, čvor C osluškuje da li netko koristi medij, te čuje čvor A da je trenutno koristi medij, pa ne pokušava komunicirati s čvorom D. Iako nema razloga zašto čvor C ne bi mogao komunicirati s čvorm D dok je A u komunikaciji s B, jer čvor B nije u dometu signala čvora C te ne bi došlo do kolizije kao što ni D nije u dometu čvora A.



Problemi su riješeni korištenjem MACA protokola (Medium Access Collision Avoidance). U MACA protokolu, prije slanja podataka prvo se uspostavlja tzv. RTS/CTS komunikacija. Čvor A želi komunicirati i prvo što čini je da šalje kontrolni paket RTS (Request To Send), kojeg čuju svi čvorovi te ne će pristupati komunikacijskom kanalu dok RTS/CTS dijalog ne završi. Odredišni čvor nakon primitka RTS paketa odgovara sa drugim kratkim kontrolnim paketom CTS (Clear To Send). Taj paket također čuju svi čvorovi te neće pokušati pristupati kanalu dok god traje slanje paketa s podacima. Dok za čvor A primitak CTS paketa da je RTS/CTS komunikacija uspješno završila i da može početi slati pakete s podacima.



Ruting protokoli u MANET-u

Problem usmjerivanja (routing-a) u osnovi je problem pronalaženja najkraćeg puta.
Osnovni zahtjevi za čvorove u procesu usmjerivanja paketa i pronalaženja rute do odredišnog čvora:

- svaki čvor mora imati informaciju o svojim susjednim čvorovima, odnosno kuda oni mogu prosljediti pakete
- svaki podatkovni paket sadrži informaciju o odredišnom čvoru u svom zaglavlju
- svaki čvor ima svoju routing tabelu u kojoj se nalazi popis čvorova u mreži, za koje čvor trenutno zna da postoje, odnosno ne zna zbog česte promjene topologije mreže, na osnovu koje prosljeđuje pakete
- kada čvor primi podatkovni paket, on ga prosljeđuje susjednom čvoru. To se prosljeđivanje vrši svaki čvor koji se nalazi na ruti prema odredištu dok paket ne stigne na odredište

Routing protokoli se mogu podijeliti ovisno kako reagiraju na promjenu topologije mreže na *proactive* – upravljani routing tablicom i *reactive* – protokoli koji se koriste na zahtjev.

Proactive protokoli

Svaki čvor koji koristi ovaj tip protokola, održava svoju routing tabelu te šalje kontrolne poruke susjednim čvorovima koji mijenjaju svoje routing tabele, koje sadrže listu svih raspoloživih odredišta, broj točaka koliko treba proći do odredišta te slijedni broj kojeg dodjeljuje odredišni čvor, s novim informacijama. Svaki susjedni čvor šalje dalje kontrolnu poruku svom susjednom čvoru. Kada se topologija mreže promijeni čvorovi šalju poruku kroz cijelu mrežu tako da svaki čvor obnovi svoju routing tabelu, pa se tako u svakom trenutku može znati kako izgleda topologija mreže odnosno preko kojih čvorova paketi mogu doći do svog odredišta.

Neki od proactive protokola:

- Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV)
- Wierless Routin Protocol (WRP)
- Global State Routing (GSR)
- Fisheye State Routing (FSR)
- Hierarchical State Routing (HSR)
- Zone-based Hierarchical Link State Routing Protocol (ZHLS)
- Clusterhead Gateway Switch Routing (CGSR)

Reactive protokoli

Za razliku od proactive protokola ovi protokoli ne održavaju redovno routing tabele, već se one obnavljau samo kad postoji potreba da se uspostavi veza. Temelje se na nekoj vrsti "query-replay" (pitaj –odgovori) dialoga. Ako postoji potreba za uspostavom veze, reactive protokoli pozivaju proceduru za traženje rute (puta) do odredišta, a takve procedure uključuju "flooding" (preplavljivanje) mreže paketima koji ispituju i traže rute do odredišta. Takav način traženja najbliže rute može znatno usporiti cijelu uspostavu veze, a također može i zagušiti mrežu s previše paketa.

Neki od proactive protokola:

- Cluster Based Routing protocol (CBRP)
- Ad hoc On-demand Distance Vector Routing (AODV)
- Dynamic Source Routing Protocol (DSR)
- Temporally Ordered Routing Algorithm (TORA)
- Associativity Based Routing (ABR)
- Signal Stability-Based Adaptive Routing protocol (SSR)

U daljnjem tekstu opisat ćemo dva routing protokola koji su jedni od najčešśće korištenih, analiziranih i testiranih protokola u MANET-u.

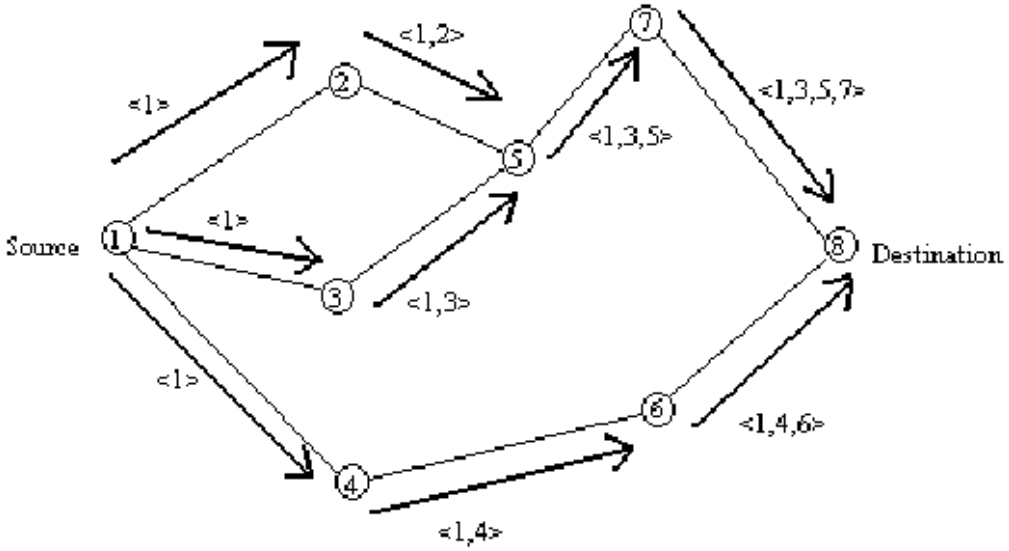
Dynamic Source Routing Protocol (DSR)

Dynamic source routing protokol sastoji se od dvije glavne komponente: pronalaženje puta (rute) i održavanje rute.

Pronalaženje rute

Kada čvor želi poslati pakete na neko odredište on prvo provjerava u svom međuspremniku (cache) popis ruta preko kojih mu je dostupno neko odredište. Ako ruta do odredišta postoji tada je koristi za slanje paketa. Ako izvorni čvor nema spremljenu rutu do odredišta ta se inicira proces pronalaženja rutu tako što se broadcast načinom šalju tzv. "route request" paketi RREQ tj. ranije spominjani "flooding".

RREQpaketi sadrže adresu izvorišnog i odredišnog čvora te jedinstveni indentifikacijski broj.



Type=REQ	Option Length	Idetification	
Target Address			
index1	index2	index3	index4
Address1			
Address2			
Address3			
Address4			

RREQpaket

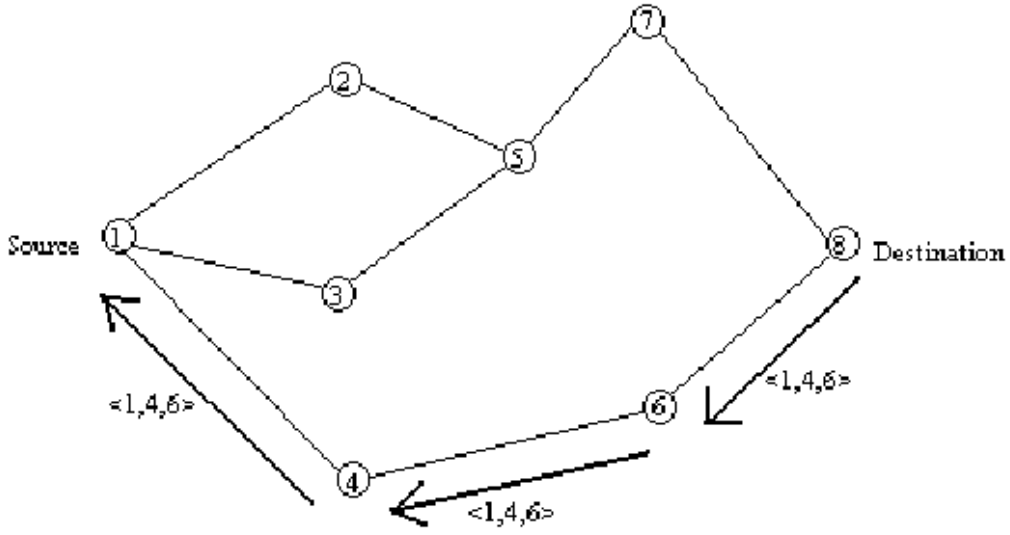
Svaki čvor koji se nalazi na putu između izvorišnog i odredišnog čvora, provjerava da li on ima spremljenu rutu do odredišta u svom međuspremniku. Ako nema, onda dodaje svoju adresu u RREQpaket i prosljeđuje ga dalje susjednim čvorovima. Da se u mreži ne pojavljuje veliki broj paketa, tj. da se ograniči broj poslanih paketa susjednim čvorovima međučvor šalje dalje paket samo ako paket nije prošao kroz taj čvor i ako ne postoji adresa tog čvora zapisana u RREQpaketu.

Ako je paket stigao na odredište ili do nekog međučvora koji ima pohranjenu rutu do odredišta u svom međuspremniku, onda se generira "route replay" paket RREP.

Type=REPLY	Option Length	R	F	Reserved
Target Address				
Index1	Index2	Index3	Index4	
Address1				
Address2				
Address3				
Address4				

RREP paket

Kako je RREQpaket prolazio mrežom, tako su se u njega upisivale adrese čvorova kroz koje je prolazio. Ako je RREP paket odaslao odredišni čvor tada on popis adresa iz RREQpaketa prebacuje u RREP paket. Ako RREP paket šalje neki međučvor tada on u RREQpaket upisuje svoj popis adresa do odredišta i zaim ih sve zajedno prebacuje u RREP paket. RREP paket se zatim



šalje unicastom, ali sada u suprotnom smjeru, prema izvoru, po novoj, otkrivenoj, routi ili po već nekoj drugoj ruti koja je odredišnom čvor već od prije poznata. Po primitku RREQpaketa, odredišni čvor,
sprema tu rutu u svoj međusprmenik (cache) tako da u slučaju ponovne uspostave veze ne prolazi kroz proceduru traženja rute, već da odmah krene s uspostavom veze i slanjem paketa, naravno ako ta ruta još uvijek postoji.

Održavanje rute

DSR protokol koristi dvije vrste paketa za održavanje rute "route error" pakete RERR i pakete potvrde (acknowledgments) .

Kada čvor ustanovi problem u slanju na podatkovnom sloju, tj. da nemože poslati paket nekom rutom on generira slanje route error paketa i kad izvorišni čvor primi route error paket on briše adresu tog čvora iz svog međuspremnika i sve rute koje su koristile taj čvor se brišu , te će izvorišni čvor ponovno pokrenut proces pronalaženja rute.

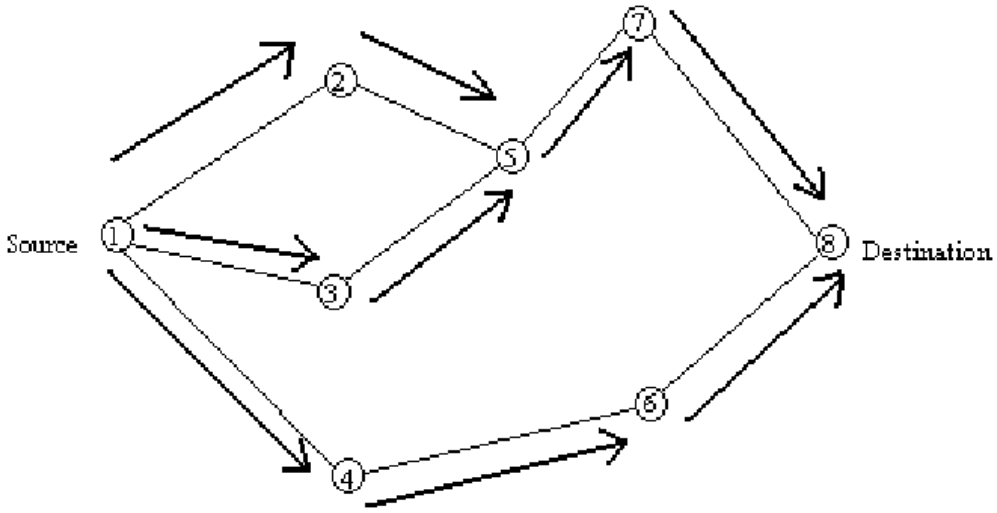
Type=ERROR	Option Length	Index
Originator Address		
From Hop Address		
Next Hop Address		

route error paket

Paketi potvrde se koriste kako bi se potvrdila ispravnost veze koju koristi za slanje paketa.To uključuje i tzv. pasivnu potvrdu pri kojoj čvor osluškuje sljedeći čvor na ruti prosljeđujući mu paket.

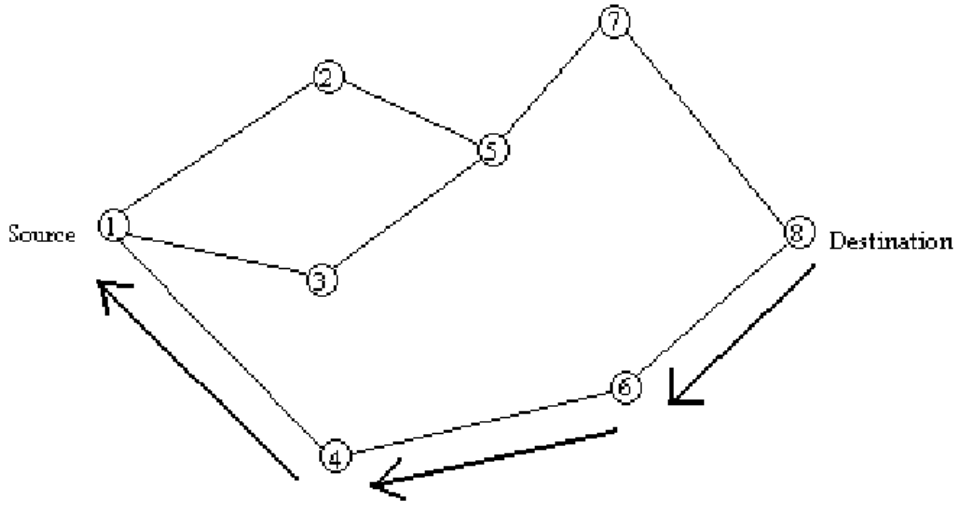
Ad hoc On-demand Distance Vector Routing (AODV)

Da bi pronašao put do odredišta, izvorišni čvor šalje RREQpakete svim susjednim čvorovima, oni zatim, također, šalju te pakete svojim susjednim čvorovima sve dok se ne pronađe prvi čvor kojem je poznata putanja do odredišta ili dok paketi ne stignu do odredišta.



Čvorovi odbacuju one RREQpakete koji su već prošli kroz njega. RREQpaket koristi sljedni broj kako bi bio siguran da na ruti ne postoji petlja, te da bude siguran, u slučaju da neki međučvor odgovori na RREQpaket, da čvor u RREP paket upiše posljednju primljenu inforamciju o ruti do odredišta koju sadrži, to se kod ovog protokola očituje u promjeni sekvencnog broja.
Prilikom prosljđivanja paketa susjednim čvorovima, svaki čvor upisuje u svoju routing tabelu inforamciju o čvoru koji je inicirao slanje RREQpaketa. Ta informacija se kasnije koristi da bi se kreirala veza za RREP paket, koji ustvari koristi istu putanju kaou i RREQpaket ali u suprotnom smjeru. Prilikom slanja RREP paketa svaki čvor na toj putanji obnavlja svoju routing tabelu s novom putanjom do izvorišnog čvora. Na taj način se routing tabela čvora s novim rutama i popisom čvorova s kojima može uspostaviti vezu.
U slučaju da se izvorišni čvor pomakne, tj. da se izgubi veza s prijašnjim čvorvima tada izvorišni čvor mora ponovno pokrenuti proces traženja rute. Ako se pomakne neki od međučvorova, tada njegov susjedni, predhodni, čvor na

temelju slanja tzv. HELLO paketa utvrđuje da li veza postoji te u slučaju neodazivanja šalje RREP paket svim prethodnim čvorovima koji koriste tu putanju i taj čvor, da ponište rutu u svojim routing tabelama te ujedno javlja izvorišnom čvoru da ponovno pokrene proces pronalaženja rute.



Literatura

http://www.ietf.org/html.charters/manet-charter.html

http://www.ietf.org/1id-abstracts.html

http://www.watersprings.org/pub/id/draft-ietf-manet-aodv-13.txt

http://www.watersprings.org/pub/id/draft-ietf-manet-dsr-09.txt

http://wnl.ece.cornell.edu/Publications/ency01.pdf

http://www.adhoc-nets.de/