SIGURNOST PROTOKOLA RUTIRANJA U *AD HOC* MREŽAMA I MOGUĆI NAPADI U MREŽI

Radiša R. Stefanović, Visoka tehnička škola strukovnih studija, Požarevac
Boban Z. Pavlović, Univerzitet odbrane u Beogradu, Vojna akademija, Katedra telekomunikacija i informatike, Beograd

DOI: 10.5937/vojtehg61-1826

OBLAST: telekomunikacije
VRSTA ČLANKA: stručni članak

Sažetak:

U članku se opisuju ad hoc mreže, specifične po svojoj mobilnosti, iznenadnoj promeni stanja i samoorganizovanju. Zbog svojih svojstava protokoli rutiranja u ad hoc mrežama moraju biti prilagođeni primenama i zadovoljavati sigurnosne zahteve – tajnost, integritet i raspoloživost. Navedena su svojstva i izazovi za razvoj protokola koji bi se suprotstavili napadima, posebno u vojnim primenama. Opisani su neki od poznatih napada i navedena jedna od metoda za ispitivanje sigurnosti protokola rutiranja.

Ključne reči: *protokoli, ad hoc mreže, sigurnost.*

Uvod

Ad hoc mreže su privremene mreže uspostavljene za neku određenu svrhu. Učesnici u mreži, mobilne stanice, ulaze i izlaze iz mreže, pomeraju se, stvaraju nove i raskidaju stare veze. Bez infrastrukture i centralnog upravljanja, moraju same da prikupljaju informacije o susednom čvoru i da upravljaju komunikacijom. Usled sve većih potreba za komunikacijom na mestima gde ne postoji infrastruktura, kao što su mesta nesreće, požari, poplave, poljoprivredno zemljište i svakako za potrebe vojske, naglo se povećava broj bežičnih uređaja. Komunikacija po principu bilo gde i bilo kada sve je traženija. U radu će težište biti na *ad hoc* mrežama za potrebe vojske. Za ove mreže je tipično da moraju prenositi taktičke informacije i u uslovima protivničkih dejstava, što zahteva da protokoli u *ad hoc* mrežama pružaju sigurnost. Svakako da je razvoj interneta i bežičnih komunikacija doveo i do ubrzanog razvoja zlonamernih postupaka kojima je cilj pristup neovlašćenim informacijama, ometanje i onemogućavanje komunikacija ili promena podataka u ličnom interesu.

radisastefanovic@yahoo.com

Specifičnosti *ad hoc* mreža

Bežične ad hoc mreže jesu dinamične samoorganizujuće mreže ravnopravnih čvorova (Omidyar, 2000). Formiraju se bez prethodnog planiranja, bez postojanja infrastrukture, tako da svaki čvor podjednako učestvuje u prosleđivanju saobraćaja. Osim što šalje svoje podatke i podatke svojih korisnika, ponašajući se kao domaćin (eng. *host*), mora usmeriti i proslediti kontrolne podatke drugih čvorova (eng. *router*). Usmeravanje se dinamički prilagođava stanju mreže u zavisnosti od njenih promena, promenom položaja, prestankom rada ili dolaskom novih čvorova. S obzirom na to da se komunikacija ostvaruje preko bežične veze javlja se i problem šuma, slabljenja i interferencije. Sve to zahteva specifične protokole koji mogu odgovoriti navedenim izazovima. Osnovne karakteristike *ad hoc* mreža su: mobilnost, višeskokovitost, decentralizacija i samoorganizovanost. Prema primeni, razlikujemo mobilne *ad hoc* mreže (eng. ***M****obile* ***A****d hoc* ***NET****works* – MANET), pristupne mreže (*mesh* mreže) i senzorske mreže.

Mobilne ad hoc mreže

MANET tehnologija izvedena u formi „petljastih" mobilnih mreža ponaša se kao robustna i isplativija alternativa koja unapređuje mobilnu mrežnu infrastrukturu baziranu na ćelijskom principu. Takođe, postojeće i buduće umrežavanje u vojnim komunikacijama zahtevaće robustniji i IP podržani prenos podataka u mobilnom bežičnom okruženju sa visoko autonomnim segmentima mrežne topologije. U kombinaciji sa satelitskim prenosom, MANET tehnologija može da obezbedi najfleksibilniji metod uspostavljanja komunikacija u slučaju bezbednosnih, protivpožarnih i spasilačkih operacija kada se zahteva funkcionalno otporno i efikasno dinamičko umrežavanje (Snow, Varshney, Malloy, 2000).

Kao što je prethodno rečeno, MANET predstavlja autonomni sistem mobilnih čvorova koji imaju mogućnost slobodne i proizvoljne promene lokacije. Sistem može da funkcioniše izolovano ili preko interfejsa i mrežnih prelaza da komunicira sa fiksnom mrežom. Bežična veza ostvaruje se na bazi slučajnog položaja mobilnih čvorova, odnosno *ad hoc* mreže, u zavisnosti od predajne snage čvorova i parametara prijema (Corson, Macker, 2009).

MANET mreže karakterišu sledeće značajne osobine:

1. Dinamična topologija: čvorovi imaju osobinu slobodnog kretanja i na taj način se mrežna topologija (koja je zapravo *multihop*) može slučajno i brzo menjati, pri čemu sadrži jednosmerne i dvosmerne linkove. Pokretljivost čvorova može obuhvatiti veliki raspon, od malog kretanja pešaka po prostoriji do velike pokretljivosti automobila na auto-putu.

2. Ograničen propusni opseg – promenljivi kapacitet linkova: ostvarena propusnost bežičnih komunikacija zbog uticaja efekata višestrukog pristupa, fedinga, šuma i interferencije najčešće je manja od maksimalne brzine radio-prenosa.

3. Ograničena energija: čvorovi u MANET mreži zavise od baterijskog ili nekog drugog izvora napajanja, tako da je najvažniji optimizacioni kriterijum prilikom projektovanja sistema održavanja energije.

4. Ograničena sigurnost komunikacije: uopšteno, mobilne bežične mreže osetljivije su na pretnje sigurnosti u odnosu na žične. Međutim, prednost MANET mreža predstavlja decentralizovana upravljačka priroda kojom se obezbeđuje dodatna robustnost pri pojavi pojedinačnih otkaza u odnosu na centralizovani pristup.

Zbog stalne promene stanja mreže, stanice moraju da prepoznaju prekid veze sa stanicom sa kojom su prethodno bile u vezi (najčešće se radi o susednoj stanici) i da pronađu novi alternativni put prema odredištu.

Mesh mreže

Bežične pristupne mreže (eng. ***W**ireless **M**esh **N**etworks* – WMN) razvijene su radi pružanja komunikacionih usluga na područjima gde se ulaganje u infrastrukturu ne isplati ili je neizvodljivo. Sastoje se od čvorova usmerača (eng. ***M**esh **R**outer* – MR) koji obezbeđuje bežičnim stanicama preko mrežnog prolaza (eng. *gateway*) pristup spoljašnjoj mreži, najčešće internetu. Za razliku od MANET mreže nema energetskih ograničenja, statičnija je i može imati više primopredajnika u jednom čvoru. Saobraćaj u ovim mrežama uglavnom je usmeren od provajdera i prema provajderu, pa su i čvorovi blizu provajdera sa najvećim opterećenjem. Mesh mreža mora imati veću propusnost, jer joj istovremeno pristupa veći broj korisnika, zbog svoje prvenstvene namene pristupa internetu.

Senzorske mreže

Bežične tehnologije omogućile su razvoj senzorskih stanica male potrošnje energije i komunikacije malog dometa. Senzorske stanice su jednostavne strukture i sastoje se od senzora, mikroprocesora za obradu podataka i komunikacionog dela. Primena senzorskih mreža je najviše zastupljena u proizvodnim procesima, kao što su industrijsko upravljanje i nadzor. U vojsci je primena uglavnom ograničena na nadzor i kontrolu ulaska u određene prostorije radi sigurnosti, kao i nadzor područja radi mogućeg ugrožavanja zdravlja zaposlenog ljudstva.

Algoritmi rutiranja u MANET mrežama

Efikasno rutiranje jedno je od glavnih pitanja koje treba rešiti u *ad hoc* mrežnoj arhitekturi (Tipper, et al, 2002), (Trivedi, 2001). U mobilnim mrežama izdvajaju se tri grupe protokola rutiranja: proaktivni ili tablični (*table-driven*), reaktivni ili protokoli na zahtev (*on-demand*) i hibridni protokoli, čije su osnovne karakteristike prikazane u tabeli 1.

Tabela 1

Osnovne karakteristike proaktivnih, reaktivnih i hibridnih protokola rutiranja

Table 1

Basic characteristics of proactive, reactive and hybrid routing protocols

Algoritam / Karakteristika	Proaktivni	Reaktivni	Mešoviti
Topološka zavisnost	Periodično	Po zahtevu	Oba
Organizacija mreže	Jednonivovska/ hijerarhijska	Jednonivovska	Hijerarhijska
Upravljanje mobilnošću	Periodično ažuriranje	Održavanje putanje	Oba
Pristup putanji	Uvek dostupan	Dostupan po potrebi	Oba
Komunikaciono opterećenje	Visoko	Nisko	Srednje

U proaktivnim protokolima rutiranja put prema odredištu određuje se čim se čvor uključi u mrežu i održava se tokom rada povremenim obnavljanjem puta (tabela rutiranja je u svakom trenutku ažurna). U reaktivnim protokolima rutiranje se odvija prema potrebi slanja podataka. Kada čvor želi poslati podatke odredištu, ako ne postoji dostupan put, protokol pokrene proces nalaženja puta prema odredištu. Hibridni protokoli rutiranja kombinuju prethodno navedene načine rada.

Proaktivni protokoli rutiranja

U konvencionalnim mrežama za rutiranje se najčešće koriste algoritmi najkraćeg rastojanja (*distance vector*) i stanja linka (*link state*) koji podrazumevaju periodično ažuriranje tabela rutiranja (Das, et al, 2000), (Haas, Pearlman, 2000). U nekim slučajevima izvršena je adaptacija algoritama za upotrebu u *ad hoc* mrežama, gde se svaki mobilni čvor posmatra kao ruter. Ovakvi algoritmi pripadaju klasi proaktivnih, odnosno *table-driven* algoritama, čiji su predstavnici DSDV (*Destination-Sequen-*

ced Distance Vector), WRP (*Wireless Routing Protocol*), FSR (*Fisheye State Routing*), OLSR (*Optimized Link State Routing*) i GSR (*Global State Routing*) protokol.

DSDV (Destination-Sequenced Distance Vector)

Tabela rutiranja kod DSDV algoritma sadrži sledeći skok (*hop*), cenu putanje i odredišni broj sekvence (Perkins, Bhagwat, 1994), (Guoyou, 2007). Dodeljivanje brojeva sekvenci ima zadatak da napravi razliku između neaktivnih i najnovijih putanja, kao i da se izbegne formiranje petlji. Tabele rutiranja ažuriraju se na dva načina: potpuni prenos (*full dump*), pri čemu se prenose sve dostupne informacije, dok drugi način podrazumeva samo prenos promena (*incremental dump*) u odnosu na prethodni sadržaj tabele rutiranja.

WRP (Wireless Routing Protocol)

WRP algoritam formira tabele rutiranja koje sadrže rastojanje do odredišnog čvora, cenu linka i liste prenetih poruka – MRL (*Message Retransmission List*). MRL sadrži informacije o susednim čvorovima koji nemaju ažurne poruke. Pri prijemu poruke ažuriranja, čvor modifikuje tabelu rutiranja i traži nove, poboljšane putanje u skladu sa informacijama. Ukoliko nema promene u tabeli rutiranja, vrši se prenos *Hello* poruke kojom se obezbeđuje održanje povezanosti. Nakon detekcije bilo kakve promene na linku, čvor proverava prisutnost svojih suseda, čime se eliminišu petlje i povećava brzina konvergencije. Nedostatak WRP algoritma je potreba za velikom količinom resursa pri obradi podataka i ograničena skalabilnost.

FSR (Fisheye State Routing)

FSR algoritam karakteriše smanjenje veličine poruke ažuriranja (tehnika ribljeg oka – *fisheye*) u zavisnosti od udaljenosti mobilnog čvora. Time se vrši pravovremeno ažuriranje poruka sa bliskih čorova, ali se formira i veliko kašnjenje sa udaljenih. Međutim, manje precizni podaci o najboljoj putanji ka udaljenom odredištu postaju detaljniji kako se paket približava odredištu. FSR obezbeđuje bolju skalabilnost u odnosu na veličinu mreže, jer ne čuva informacije o svim mrežnim čvorovima na istom nivou. Umesto toga, preciznost informacija o stanju linka je obrnuto proporcionalna rastojanju, čime se smanjuje preopterećenje, jer se informacije razmenjuju češće kod bliskih, nego u slučaju udaljenih čvorova.

OLSR (Optimized Link State Routing)

OLSR algoritam karakteriše optimalno rutiranje u zavisnosti od stanja veza. Svaki čvor odabira među svojim susedima onoga koji je zadužen za prosleđivanje kontrolnih paketa. Svaki čvor prati koji su ga čvorovi odabrali za dalje prosleđivanje kontrolnih paketa i stanje veza samo prema njima. Samo te veze dužan je da objavi mreži. Optimizacija dolazi do izražaja sa većom gustinom čvorova u mreži.

GSR (Global State Routing)

GSR algoritam temelji se na razmeni informacija o stanju svih veza, pomoću kojih čvorovi održavaju globalnu sliku mrežne topologije i lokalno odlučuju o rutiranju. Za razliku od protokola DSDV, paketi stanja veza se ne šalju svima u mreži, već samo susednim čvorovima.

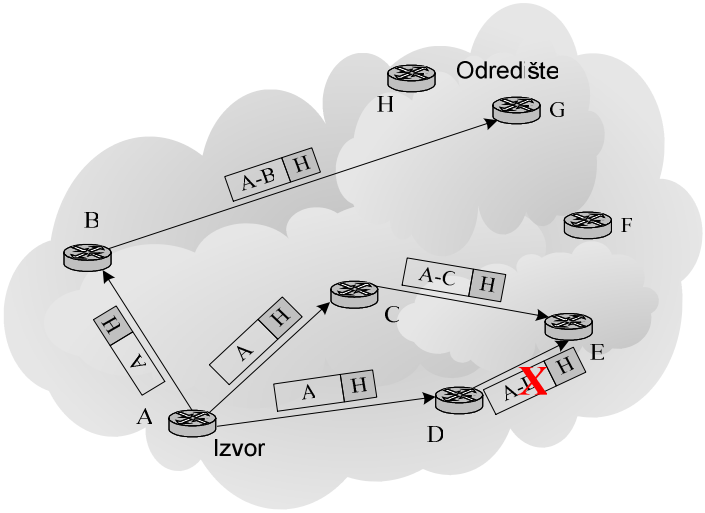
Proaktivni algoritmi rutiranja kod konvencionalnih mreža obrađuju veoma retko promene mrežne topologije. Proaktivno rutiranje bazira se na tabelama rutiranja (*table-driven*) za koje je karakteristično dodatno opterećenje kontrolnim paketima. Čvorovi u kontinuitetu određuju putanje ka svim dostupnim čvorovima i pokušavaju da održe najažurnije informacije, tako da izvorni čvor može trenutno dobiti željenu putanju rutiranja. Međutim, nedostaci ovih algoritama mnogo su veći od prednosti. Prvo, veliko je dodatno zauzimanje propusnog opsega (periodične informacije o ažuriranju topologije šalju se uvek, bez obzira na to da li se dogodila promena). Zatim, brže je iskorišćenje kapaciteta baterija, jer se čvorovi aktiviraju za prijem/predaju informacija o rutiranju koje nisu uvek potrebne. Sledeći nedostatak je slabija skalabilnost mreže (velika količina informacija u mreži je direktno srazmerna broju mrežnih čvorova), kao i postojanje redundatnih putanja usled velikog broja rutera (mobilni čvor-ruter) i nemogućnost brzog odgovora na dinamičke promene u mrežnoj topologiji. U slučaju MANET mreža, primena navedenih algoritama zahteva mehanizme koji će dinamički sakupljati informacije o promenama i slati ažurne podatke na bazi promena.

Reaktivni protokoli rutiranja

Zbog prethodnih razloga pojavljuju se *on-demand* protokoli za rutiranje, odnosno protokoli po zahtevu (reaktivni). Osnovna ideja podrazumeva da se ne koristi periodično oglašavanje putanja, već se putanja otkriva samo kada je potrebna, tj. na zahtev. Na taj način smanjuje se mrežni saobraćaj, ali se postavlja pitanje efikasnosti protokola, kao i kašnjenje pri određivanju putanje. Najpoznatiji *on-demand* algoritmi rutiranja u MANET mrežama su DSR (*Dynamic Source Routing)*, AODV (*Ad hoc On-demand Distance Vector*), TORA (*Temporally Oriented Routing Algorithm*), LAR (*Location-Aided Routing*) i ABR (*Associatively-Based Routing*).

DSR (Dynamic Source Routing)

DSR algoritam rutiranja baziran je na konceptu izvornog (*source*) rutiranja u kojem pošiljalac definiše sekvencu čvorova kroz koje će paket biti poslat (Johnson, Maltz, Hu, Jetcheva, 2009). Sekvenca se nalazi u keš memoriji (tabela rutiranja) na svakom čvoru. Proces rutiranja sastoji se od dve faze: otkrivanja i održavanja rute.

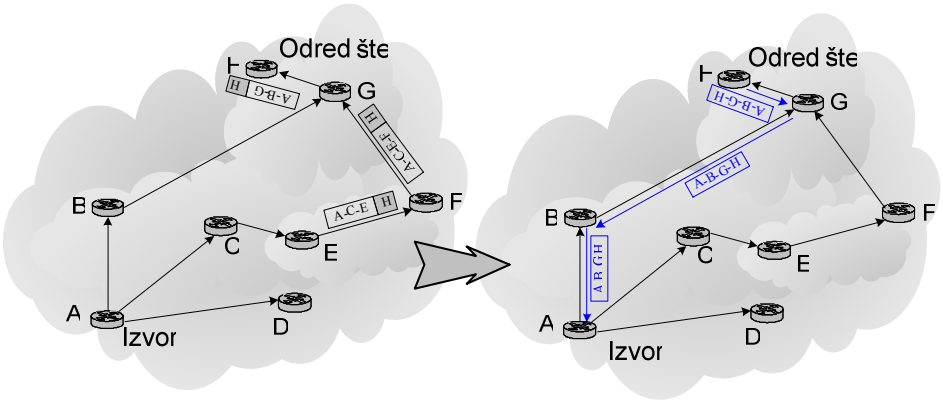


Slika 1 – Proces otkrivanja rute kod DSR algoritma rutiranja
Figure 1 – Process of route discovery in the DSR routing algorithm

Putanja se otkriva dinamički i to samo onda kada je potrebna. Ukoliko pošiljalac namerava da pošalje paket, proverava svoju tabelu rutiranja i, ukoliko postoji sekvenca ka odredištu, putanja je određena i paket će prelaziti preko poznatih čvorova. Ako u keš memoriji ne postoji odgovarajuća sekvenca, pošiljalac inicira otkrivanje rute slanjem paketa zahteva za rutom, RREQ (*Route REQuest*) preko svojih suseda kroz mrežu. RREQ paket mora da sadrži adresu pošiljaoca, odredišta, kao i memoriju za skladištenje adresa prikupljenih na putu u polju snimanje rute (*route record*). Sadržaj polja *route record* stalno raste, tj. ažurira se dok paket ne stigne do odredišta. Odredišni čvor generiše paket RREP (*Route REPly*) odgovor na rutu radi obaveštavanja pošiljaoca o otkrivenoj ruti.

Postoje dve mogućnosti slanja RREP paketa. Prvo, RREP se može vratiti inverznom rutom prema polju *route record* iz RREQ paketa. Međutim, to je moguće samo ako je kvalitet prenosa isti u oba smera, odnosno ako su bežični linkovi apsolutno simetrični, što najčešće nije slučaj. Drugi način je uključivanje originalnog paketa RREQ u RREP koji odredišni čvor šalje izvorišnom. Kada izvorišni čvor dobije inverzni RREQ, on tada zna gde da pošalje RREP. Ovaj metod zove se *piggybacking*.

U fazi održavanja rute definisani su mehanizmi potvrđivanja (*acknowledgement*) i obaveštavanja o grešci na putanji RERR (*Route ERRor*). Potvrde mogu biti *hop-to-hop* (provera grešaka pri svakom hopu, odnosno prenosu preko bežičnog linka) ili *end-to-end* (provera grešaka samo na predaji i prijemu). Kod provere na svakom hopu, nakon prijema paketa, svaki čvor šalje potvrdu čvoru od kojeg je primio paket u definisanom intervalu (*timeout*). Čvor koji nije primio potvrdu šalje izvorišnom čvoru RERR poruku kojom ga obaveštava koji bežični link više nije funkcionalan. Zatim se može koristiti alternativna putanja (ako postoji) ili se ponovo može pokrenuti proces otkrivanja putanje. U slučaju *end-to-end* kontrole, ne postoji informacija o tome na kom čvoru je došlo do prekida, pa izvorišni čvor može da pretpostavi da je došlo do prekida na poslednjem linku, što nije uvek tačno. Međutim, implementacija ovakve kontrole je mnogo jednostavnija i ne uvodi dodatno opterećenje u mrežu (slika 2).



Slika 2 – Proces održavanja putanje
Figure 2 – Process of maintaining the path

Prednosti DSR algoritma rutiranja:

- veoma laka implementacija,
- mogućnost rada sa asimetričnim linkovima,
- ušteda propusnog opsega i energije (ruteri se ne oglašavaju periodično, već po zahtevu),
- nema dodatnog saobraćajnog opterećenja u mreži kada nema promene mrežne topologije,
- protokol podržava višestruke putanje ka odredištu, tako da nije potrebno otkrivati nove putanje uvek kada dođe do prestanka rada nekog čvora.

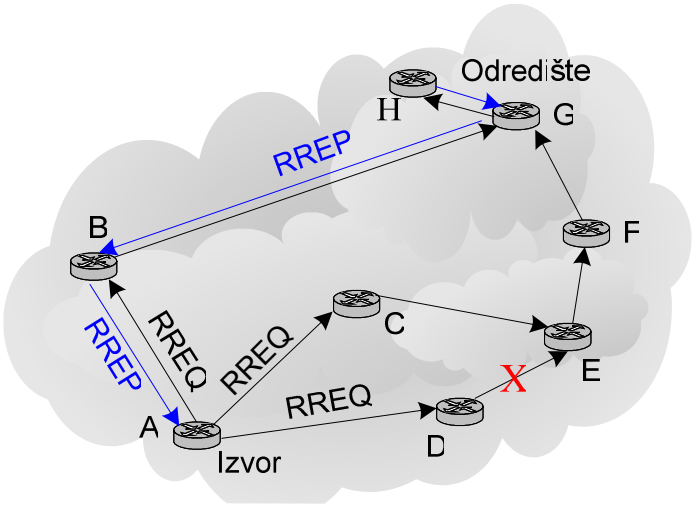
Nedostaci DSR algoritma rutiranja:

- dodatno zauzimanje propusnog opsega (sadržaj RREQ paketa brzo raste prolaskom kroz mrežu, jer čuva adrese svih čvorova kroz koje paket prolazi, usled slanja čitave sekvence čvorova, moguće je da informacija o rutiranju bude znatno veća od korisne poruke),
- skalabilnost (što je mreža veća, potrebno je više bežičnih hopova, tako da će porast veličine poruka u jednom trenutku postati neprihvatljiv za normalnu komunikaciju).

Konačno, DSR protokol je pogodan za primenu u MANET mrežama sa manjim brojem mobilnih čvorova koji se kreću srednjim brzinama.

AODV (Ad hoc On-demand Distance Vector)

Izvorišni čvor emituje RREQ paket svim susedima radi otkrivanja putanje do odredišta i čeka na odgovor, što je slično DSR algoritmu, kako je prikazano na slici 3. Razlika je, pre svega, u strukturi RREQ paketa (Perkins, Das, 2009), (Perkins, Royer, Das, 2003). Broj sekvence SN (*Sequence Number*) jeste broj koji generiše svaki čvor i koji se uvećava svaki put kada se u njegovom dometu dogodi neka promena (izlazak iz dometa komunikacije ili prestanak funkcionisanja čvora). Odredišni broj sekvence, DSN (*Destination Sequence Number*) jedinstveni je broj koji se čuva u tabeli rutiranja i povezan je sa svakom poznatom putanjom na čvoru. Prema tome, minimalni format RREQ paketa je: RREQ (scr, dest, srcSN, dstSN) – adresa izvorišnog čvora, adresa odredišnog čvora, izvorišni broj sekvence i odredišni broj sekvence. RREQ paket više ne sadrži polje *route record*, odnosno nema više informacija o čvorovima kroz koje prolazi, što je možda najbitnija prednost ovog pristupa – paket je manji i propusni opseg se čuva. Osnovna razlika je u tome što DSR čuva celu putanju (sekvencu čvorova), dok AODV pamti samo naredni skok u celoj putanji. Kada RREQ paket stigne do čvora koji ima putanju do odredišnog čvora, vrši se poređenje vrednosti DSN polja i tabele rutiranja tekućeg čvora. Ako je vrednost DSN iz RREQ veća, putanja tekućeg čvora nije dovoljno „sveža" i tada šalje RREQ paket dalje i ažurira DSN vrednost u svojoj tabeli rutiranja. U suprotnom, čvor generiše RREP paket koji šalje izvornom čvoru zajedno sa informacijom o otkrivenoj putanji. Iz prethodnog se može zaključiti da je osnovna namena DSN koncepta odgovor na dinamičke promene mrežne topologije. RREP paket vraća se izvorišnom čvoru preko inverzne putanje koja je formirana prilikom propagacije RREQ paketa. Za svaku putanju u tabeli rutiranja čvor održava listu susednih čvorova koji koriste tu putanju kako bi ih obavestio u slučaju prekida linka na toj putanji. Prekid linka otkriva se odsustvom *hello* poruka koju svaki čvor mora da emituje nakon isteka unapred definisanog intervala.



Slika 3 – Princip određivanja putanje kod AODV algoritma rutiranja
Figure 3 – Principle of determining the path of the AODV routing algorithm

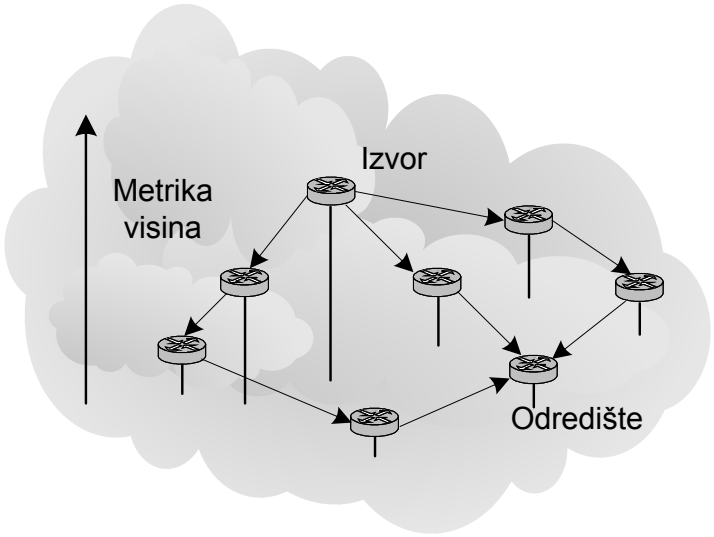
Prednosti AODV u odnosu na DSR algoritam rutiranja:

- znatno manje dodatno mrežno opterećenje, jer su kontrolni paketi i poruke manji,
- pri rutiranju koriste se samo dve adrese, umesto cele putanje. Na ovaj način postiže se dobra skalabilnost, jer veličina paketa ne zavisi od veličine mreže,
- AODV podržava rutiranje ka više definisanih čvorova istovremeno (eng. *multicast*).

Međutim, AODV se može primeniti samo u slučaju simetričnih linkova. Zatim, svaki čvor mora da emituje *hello* poruke, čime se dodatno uvećava opterećenje mreže i smanjuje mogućnost uštede energije u tzv. *sleep* režimu. Takođe, AODV ne omogućava višestruke putanje do istog odredišta, tako da u slučaju kada neki čvor izađe iz dometa ili prestane da funkcioniše, mora se otkriti potpuno nova putanja.

TORA (Temporally Oriented Routing Algorithm)

Ovaj algoritam predstavlja *link-reversal* algoritam, gde se mrežna topologija definiše upotrebom usmerenog acikličnog grafa, u kojem su čvorovi u mreži prikazani kao čvorovi grafa sa usmerenim granama koje predstavljaju linkove. Link je uvek usmeren od čvora sa većom visinom ka čvoru sa manjom visinom. Odredišni čvor ima najmanju visinu u grafu, dok se ostalim čvorovima dodeljuju veće visine u skladu sa porastom rastojanja od odredišta (Park, Corson, 2009).



Slika 4 – Uslovi definisanja TORA algoritma
Figure 4 – Conditions for the TORA algorithm

Formiranje grafa započinje kada svi čvorovi u mreži u grafu imaju neodređenu visinu (NULL), izuzev odredišnog koji ima visinu nula (ZERO), manju od vrednosti NULL. Izvorišni čvor emituje paket QRY (*Query*) susedima, pri čemu se prenosi kroz mrežu i markira sve potencijalne čvorove za otkrivanje putanje postavljanjem *route request flag* na svakom čvoru. Kada QRY paket stigne do čvora sa bar jednim silaznim linkom, čvor emituje paket UPD (*Update*) koji se vraća unazad kroz mrežu i postavlja visine svih čvorova čiji je *route request flag* setovan. Sada svak čvor dobija veću visinu od prethodnog, pri čemu se formira jedna silazna putanja između izvorišnog i odredišnog čvora. Uslovi definisanja TORA algoritma prikazani su na slici 4.

Navedenim mehanizmom omogućava se formiranje više silaznih putanja do svakog odredišnog čvora, odnosno podržava se *multipath* rutiranje. U slučaju prekida linka, ako čvor ima bar jednu silaznu putanju, ne ponavlja se proces otkrivanja putanje, već se emituje UPD paket i oporavlja mrežni graf.

Prednosti TORA algoritma:

- proces otkrivanja putanje je veoma brz,
- mogućnost rutiranja po više putanja (eng. *multipath*),
- oporavak grafa u slučaju otkaza linka je na lokalnom nivou,
- algoritam podržava rutiranje u više skokova (eng. *multicast)*.

Osnovni nedostatak algoritma je zahtev za spoljašnjim mehanizmom sinhronizacije merenja vremena, kao što je GPS (*Global Positioning*

System), usled čega znatno poskupljuje konfiguracija algoritma. Takođe, sa porastom vremena, mrežni graf postaje sve manje optimalan. Problem se može rešiti slanjem *refresh* paketa za osveženje grafa, što unosi dodatno opterećenje za mrežu.

Osnovna primena TORA algoritma je kod velikih mreža sa gusto raspoređenim čvorovima, gde prethodni algoritmi ne daju dobre rezultate. Za ovakav mrežni scenario potrebno je opremiti svaki mrežni čvor GPS prijemnikom i implementirati TORA algoritam.

LAR (Location-Aided Routing)

LAR za rutiranje koristi podatke o lokaciji radi povećavanja efikasnosti smanjenjem kontrolnih paketa. Kao i prethodni algoritam, zahteva stalnu dostupnost globalnog sistema za pozicioniranje (GPS).

ABR (Associatively-Based Routing)

ABR je usmereni protokol, koji novu putanju uspostavlja prema kriterijumu stabilnosti bežične veze. Stabilnost određuje na osnovu poznavanja karakteristika uspostavljene veze u nekom intervalu.

Hibridni (Mešoviti) protokoli rutiranja

Može se zaključiti da su prethodno navedeni protokoli rutiranja korisni i primenljivi u određenim slučajevima i situacijama. Ali, kako neke od situacija često nisu jednostavno određene, to se kombinacijom svojstava gornjih protokola može postići bolja efikasnost. Tada za komunikaciju u jednom delu mreže upotrebljavaju proaktivne protokole rutiranja, a u ostalom delu reaktivne protokole rutiranja. Najpoznatiji algoritmi hibridnih protokola rutiranja su zonski protokol rutiranja ZRP (*Zone Routing Protocol*), ADV (*Adaptive Distance Vector*) i CEDAR (*Core Extraction Distributed Ad hoc Routing*).

ZRP (Zone Routing Protocol)

ZRP protokol primenjuje reaktivni ili proaktivni protokol rutiranja u zavisnosti od toga da li je odredište unutra ili van zone područja određene udaljenosti. Unutar zone komunikacija se obavlja proaktivnim, a van zone reaktivnim protokolom rutiranja.

ADV (Adaptive Distance Vector)

ADV protokol karakterističan je po adaptivnom mehanizmu, kojim se smanjuje broj kontrolnih paketa ako se opterećenje mreže povećava.

CEDAR (Core Extraction Distributed Ad hoc Routing)

CEDAR protokol zasniva se na izboru jezgrenih čvorova, koji čine najmanji dominirajući skup čvorova, sa osobinom da se svaki čvor nalazi u dominantnom skupu ili je bar susedan čvoru iz dominantnog skupa. Jezgreni čvorovi nalaze rutu i usmeravaju saobraćaj za čvorove koji su sa njima povezani, kao njihovi članovi.

Sigurnost rutiranja u ad hoc mrežama

Pod pojmom sigurnost prenosa informacija uglavnom se podrazumeva ispunjavanje tri najbitnija sigurnosna zahteva. To su tajnost (*confidentiality*), integritet (*integrity*) i raspoloživost (*availability*).

- Tajnost podrazumeva zaštitu podataka od neovlašćenog pristupa i korišćenja. Do podataka treba da dođe samo onaj kome su oni i namenjeni. U vojsci se tajnost gotovo uvek obezbeđuje šifrovanjem (Terzić, 2011), a ključevi se neprestano menjaju. Ako neovlašćena osoba čak i dođe do podataka, bez poznavanja kriptografskog ključa ne može ih upotrebiti.
- Integritet štiti podatke od neovlašćene promene. Autentičnost podataka postiže se primenom kodova (*message authentication code*) ili digitalnim potpisima.
- Raspoloživost predstavlja zahtev da željena usluga bude uvek dostupna. Nedostupna usluga može biti štetna, kao i krađa (povreda tajnosti) i lažno predstavljanje (povreda inegriteta). Uskraćivanje pristupa usluzi (*denial of service*) teško se otkriva, jer se ne zna da li je nedostupnost podacima posledica napada ili nekog spoljnjeg uticaja.

Napadi u ad hoc mrežama

Zbog načina prenosa otvorenim medijem, bežična mreža je podložna raznim napadima, a među najvažnije se ubrajaju:

- preplavljivanje – napad kojim neprijatelj opterećuje mrežu lažnim zahtevima za traženje puta ili neprekidno šalje pakete sa ciljem da preoptereti rutiranje u čvorovima;
- lišavanje sna – radnja kada napadač kontinuirano šalje kontrolne pakete i ne dozvoljava uštedu energije i gašenje delova koji ne moraju biti aktivni;
- crna rupa – napad kada lažnim odgovorima neprijatelj tvrdi da je preko njegovog čvora najkraći put do odredišta. Takvim postupkom uspeva da pridobije da većina puteva vodi preko njegovog čvora, a zatim odbacuje sve pakete koji dođu do njega;

- podela mreže – postiže se lažnim rutiranjem paketa, tako da je između nekih čvorova komunikacija potpuno onemogućena, pa se deli na dva odvojena dela. Izolacija jednog čvora je specijalni slučaj podele, a primenjuje se na nekom od bitnih čvorova;
- crvni put –napad koji zahteva saradnju dva zlonamerna čvora. Komunicirajući međusobno stvaraju privid najkraće udaljenosti, čime mogu postići da većina puteva prolazi njima;
- navala – napad koji je primenljiv kod protokola koji određuju puteve na osnovu zahteva koji je prvi stigao. Neprijatelj neprestano šalje svoje zahteve za uspostavljanjem puta prema odredištu, sa težnjom da dođu do čvorova koji su najbliži odredištu pre legitimnih zahteva. Time napadač postiže da se nalazi na većini puteva i kontroliše saobraćaj;
- otkrivanje lokacije – napad kojim neprijatelj dolazi do informacije o poziciji čvorova, a samim tim i o topologiji mreže;
- nevidljivi čvor – napad kojim neprijatelj sakriva identitet svog čvora. Napadač učestvuje u komunikaciji jednostavno ponavljajući primljene pakete.

Da bi neki protokol zadržao željenu efikasnost (Jevtović, Pavlović, 2011) i u uslovima napada, mora imati mogućnost da pronađe ispravne puteve i da otkrije kvarove na njima. Drugim rečima, mora osigurati otkrivanje puta i uspešno prosleđivanje podataka.

Ispitivanje sigurnosnih svojstava komunikacijskih protokola provodi se da bi se odredila tačnost i pouzdanost uz prisustvo napada na mrežu. Postoji veći broj metoda za ispitivanje, ali autori najčešće objavljuju rezultate upoređujući postojeće protokole pod određenim napadima, simulacijom mreže. Mrežna simulacija koristan je alat u ispitivanju efikasnosti i može pokazati kako se protokol ponaša u uslovima definisanog napada. S obzirom na to da se u simulaciji neprijateljske akcije moraju definisati da bi se mogao sagledati njihov uticaj na mrežu, simulacija ne može odgovoriti na pitanje kako će se mreža ponašati u slučaju do sada nepoznatog napada. Ako se simulacijom pokaže da je napad malo verovatan, to ne znači da ne postoji, odnosno da je protokol siguran od tog napada. Mrežna simulacija uglavnom se ne koristi u fazi ispitivanja puta, već češće u fazi prosleđivanja paketa, kako bi se predvidelo ponašanje mreže u datim okolnostima.

Zaključak

Uspostava mrežne konekcije i uspešno prosleđivanje podataka je važna funkcija svake komunikacijske mreže. Za razliku od žičnih i infrastrukturnih bežičnih mreža, *ad hoc* mreže karakteriše veća mobilnost, višeskokovitost i samoorganizovanost. Zbog specifičnosti pojavila se potreba za razvojem protokola dizajniranih specijalno za *ad hoc* mreže. Za posebne namene, kao što su vojne potrebe, kod dizajniranja protokola uzi-

ma se u obzir sigurnost kao jedan od najvažnijih zahteva. U vojnim aviosistemima, po pitanju sigurnosti moraju se koristiti sistemi sa nultom tolerancijom na pogreške. Postoji više metoda za ispitivanje sigurnosti protokola za rutiranje, a često primenjivana je mrežna simulacija. Kombinacija više različitih metoda povećava uspešnost ispitivanja.

Literatura

Corson, S., Macker, J., 2009, *RFC 2501: Mobile Ad Hoc NETworking (MANET): routing protocol performance issues and evaluation consideration*, available at http://www.ietf.org/internet-drafts/ draft-ietf-manet-issues-01.txt (visited: 10. 05. 2009).

Das, S., Perkins, C., Royer, E., 2000, *Performance Comparison of two on-demand routing protocols for ad hoc networks*, INFOCOM 2000, IEEE, pp.3-12.

Guoyou, H., 2007, *Destination-sequenced distance vector (DSDV) protocol*, Technical report, Helsinki University of Technology, Finland.

Haas, Z.J., Pearlman, M. R., 2000, *The Zone Routing Protocol (ZRP) for Ad Hoc Networks*, internet draft, March.

Jevtović, V.M., Pavlović, Z.B., 2011, *Topološka analiza telekomunikacionih mreža,* Vojnotehnički glasnik/Military Technical Courier, Vol.59, No.1, pp 96-110.

Johnson, D.B., Maltz, D.A., Hu, Y.C., Jetcheva, J.G., 2009, *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*, IETF Manet Working Group INTERNET-DRAFT available at http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-07.txt, (visited: 12. 05. 2009).

Omidyar, C.G., 2000, *Survivability analysis of Ad Hoc wireless network architecture*, volume 1818 of Lecture Notes in Computer Science.

Park, V.D., *Corson,* M.S.*,* 2009, *Temporally-Ordered Routing Algorithm (TORA) version 1: functional specifications*, internet draft, available at http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec-01.txt (visited 24. 06. 2009).

Perkins, C., Bhagwat, P., 1994, *Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers*, Proceedings of SIGCOMM, pp. 234-244.

Perkins, C., Das, S.R., 2009, *Ad-hoc On-Demand Distance Vector (AODV) Routing*, IETF Manet Working Group INTERNET-DRAFT available at http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-11.txt, (visited: 19. 05. 2009).

Perkins, C., Royer, E.B., Das, S., 2003, *Ad hoc On-Demand Distance Vector (AODV) Routing*, RFC 3561, July.

Snow, A.P., Varshney, U., Malloy, A. D*.,* 2000, *Reliability and survivability of wireless and mobile networks*, IEEE Computer.

Terzić, R.M., 2011, *Predlog ad hoc računarske mreže na Katedri vojnih elektronskih sistema VA primenom bluetooth tehnologije,* Vojnotehnički glasnik/Military Technical Courier, Vol.59, No.1, pp 111-120.

Tipper, D., Dahlberg, T., Shin, H., Charnsripinyo, C., 2002, *Providing fault tolerance in wireless access networks*, IEEE Communications Magazine, pp. 40-58.

Trivedi, K.S., 2001, *Probability and Statistics with Reliability, queuing, and Computer Science Applications*, John Wiley & Sons, Second edition.

SAFETY OF ROUTING PROTOCOLS IN AD HOC NETWORKS AND POSSIBLE ATTACKS IN THE NETWORK

FIELD: Telecommunications
ARTICLE TYPE: Professional Paper

Summary:

This paper describes an ad hoc network, specific for its mobility, more abruptness and self-organization. Because of their properties, routing protocols in ad hoc networks must be adapted to applications and satisfy safety requirements - confidentiality, integrity and availability. These are the characteristics and challenges for the development of protocols to counter attacks, especially in military applications. Some of the known attacks are described and one of the methods for safety testing routing protocols is listed.

Introduction

Ad hoc networks are temporary networks established for some particular purpose. Participants in the network – stations, entities (entrances and exits) from the network- move, create new and terminate the old connection. Without the infrastructure and central management, they need to find information about the neighboring nodes and to manage communication. Due to the growing need for communication in areas where there is no infrastructure, such as site accidents, fires, floods, agricultural land, and certainly for the army, the number of wireless devices is increasing. Communication based on the principle anywhere and anytime is in demand. In this paper, the focus will be on ad hoc networks for military purposes. This network must be able to transmit tactical information in the presence of enemy attack, which requires an answer to the question of security protocols in ad hoc networks. Certainly, the development of the Internet and wireless communications has led to rapid development of malicious procedures intended to unauthorized access to information, communications jamming and disabling or changing data in the personal interest.

Specifics of ad hoc networks

Wireless ad hoc networks are dynamic self-organizing networks of peer nodes (Omidyar, 2000). They are formed without planning, without any infrastructure and each node is equally involved in traffic forwarding. In addition to sending information, they act as a host which has to transmit the control data from/to other nodes. the routing process dynamically adapts to the network status as it changes, in accordance with changing position or termination/arrival of new nodes. Since the communication is based on wireless connection, there is a problem of noise attenuation and interference. As it is previously mentioned, all this requires the selected protocols that can cope with these challenges.

Ad hoc networks are characterized by: mobility, abruptness, decentralization and self-organization. Regarding their application, these networks are divided into mobile ad hoc networks MANET, access networks (mesh) and sensor networks.

MANET routing algorithm in networks

*Efficient routing is one of the main issues that has to be resolved in an ad hoc network architecture (*Tipper, et al, 2002)*, and (*Trivedi, 2001).

Mobile networks are divided into three groups of routing protocols: proactive or table-driven, reactive or protocols on request (on-demand) and hybrid protocols, whose main characteristics are given in Table 1.

In proactive routing protocols, the route to a destination is determined as soon as the node joins the network and will be held during the times of periodic renewal (routing table is updated each time). In reactive protocols, routing is done by sending the appropriate data. When a node wants to send data to the destination, if there is no available link, the protocol starts the process of finding a path towards the destination. Hybrid routing protocols combine the above modes.

Routing security in ad hoc networks

Security of information transfer generally requires fulfilling the three most important security requirements. These are: confidentiality, integrity and availability.

The attacks in ad hoc networks

Because of the open medium transmission, the wireless network is vulnerable to various attacks, the most important including:

- *Flooding*
- *Sleep deprivation*
- *Black Holes*
- *Distribution network*
- *Wormhole*
- *The rush*
- *Detection of the location*
- *The invisible node*

To maintain a desired efficiency in terms of attack, routing protocol must be able to find the correct paths and failures to disclose them. In other words, protocols must provide path detection and successful submission of data.

Conclusion

Establishing a network connection and a successful data transmission is an important feature of any communication network. Unlike wired and wireless infrastructure networks, ad hoc networks are characterized by greater mobility, abruptness and self-organization. Because of the specificity, the need for the development of protocols designed particularly for ad hoc networks has developed. For special purpo-

ses, as military requirements are, designing the protocol takes into account safety as one of the most important requirements. In military air systems, security systems with zero tolerance for error must be used. There are several methods for safety testing of routing protocols, and the network simulation is often applied. The combination of different methods increases the success of test performances.

Key words: *protocols, ad hoc networks, security.*

Datum prijema članka/Paper received on: 17. 04. 2012.
Datum dostavljanja ispravki rukopisa/Manuscript corrections submitted on: 25. 05. 2012.
Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 27. 05. 2012.