Online ISSN 1848-3380 , Print ISSN 0005-1144
ATKAFF 52(3), 269–278(2011)

Lovro Seder, Željko Ilić, Mladen Kos

Sigurno usmjeravanje u *ad hoc* mrežama

Pozvani osvrt

Ad hoc mreže specifične su po svojim karakteristikama (necentraliziranost, samoorganiziranje i višeskokovnost). Zbog toga usmjerni protokoli u *ad hoc* mrežama moraju biti prilagođeni pojedinim primjenama mreže i zadovoljavati glavne zahtjeve — propusnosti, skalabilnost i sigurnost.

U radu je prikazan pregled sigurnosti usmjeravanja u *ad hoc* mrežama. Navedena su svojstva *ad hoc* mreža i izazovi razvoja protokola usmjeravanja u njima. Opisani su glavni sigurnosni problemi u usmjeravanju i metode ispitivanja sigurnosti usmjernih protokola.

Ključne riječi: usmjeravanje, ad hoc mreže, sigurnost

1 UVOD

Razvoj Interneta i bežičnih komunikacija u posljednjem desetljeću doveo je do pojave sveprisutnosti bežičnih uređaja. Pristup bilo gdje i bilo kad traženiji je no ikad. Iz potrebe za komunikacijom i na mjestima gdje nema postavljene infrastrukture, kao što su poljoprivredne površine, mjesta nesreća i bojno polje, razvilo se načelo *ad hoc* komunikacije.

Ad hoc mreže privremene su mreže uspostavljene za neku određenu svrhu. Članovi mreže, stanice, ulaze i izlaze iz mreže, dolaze i odlaze, pomiču se stvarajući nove i raskidajući stare veze. Bez infrastrukture i središnjeg upravljanja, moraju same nalaziti informacije o svojem susjedstvu i upravljati komunikacijom.

Zbog samoorganiziranosti, pokretnosti i nedostatka infrastrukture niču novi zahtjevi u razvoju komunikacijskih protokola. Koncept *ad hoc* znači prilagođenost svakoj pojedinoj primjeni. Mreža vozila mora moći obavještavati o nesreći i pri velikim brzinama, senzorska mreža mora moći javiti o šumskom požaru i kod kvara određenog broja senzora, a vojna mreža mora prenositi taktičke informacije i u prisutnosti protivnika.

Posljednji primjer dovodi do glavnog pitanja o kojem će biti riječi u ovom radu — sigurnosti usmjernih protokola u *ad hoc* mrežama. Razvoj bežičnih mreža doveo je do usporednog razvoja zlonamjernih postupaka kojima je cilj pristup neovlaštenim informacijama, onemogućavanje komunikacije ili promjena podataka u svoju korist.

Stoga razvoj protokola, a naročito protokola za usmjeravanje u *ad hoc* mrežama, mora voditi računa o svim parametrima potrebnim za ispravno djelovanje mreže.

1.1 *Ad hoc* mreže

Bežične *ad hoc* mreže višeskokovne su dinamičke samoorganizirajuće mreže ravnopravnih čvorova. Formiraju se bez prethodnog planiranja, bez postavljanja infrastrukture, a u njima svaki čvor ravnopravno sudjeluje u prosljeđivanju prometa. Osim što igra ulogu domaćina (engl. *host*) i šalje svoje podatke ili podatke svojih korisnika, mora se ponašati i kao usmjernik (engl. *router*) i sudjelovati u razmjenjivanju kontrolnih podataka usmjernih protokola i prosljeđivati podatke drugih čvorova. Usmjeravanje je distribuirano po svim čvorovima mreže. Dinamički se prilagođava stanju mreže kako se ona mijenja promjenom položaja, prestankom rada ili dolaskom novih čvorova.

Ad hoc mreže omogućavaju brzo postavljanje neovisnih više ili manje mobilnih stanica u održivu, robusnu i efikasnu mrežu koja omogućava komunikaciju u raznim prilikama — od običnog pristupa Internetu, preko vojnih operacija i operacija spašavanja, do komuniciranja u slučaju elementarnih nepogoda i prirodnih i drugih katastrofa.

Budući da komuniciraju preko bežične veze, *ad hoc* mreže pate od problema inherentnih radiokomunikaciji, kao što su šum, gušenje i interferencija. Osim što imaju manju pojasnu širinu i propusnost od žičanih mreža, promjenjiva topologija mreže uslijed pomicanja čvorova, njihovih kvarova, dolaska novih čvorova i vanjskih utjecaja zahtijeva učinkovite usmjerne protokole koji će se nositi s tim izazovima [1].

1.2 Svojstva *ad hoc* mreža

U nedostatku pristupnih točaka koje u infrastrukturnom načinu povezuju udaljene BSS-ove, komunikacija stanica koje su izvan međusobnog dosega mora se odvijati preko

stanica koje se nalaze između njih. Tako svaka stanica osim svojeg prometa mora prosljeđivati promet susjednih stanica.

Sljedeća svojstva opisuju sve vrste *ad hoc* mreža [2].

Mobilnost. Glavni razlog postojanja mobilnih *ad hoc* mreža njihova je mobilnost. Ona omogućava brzo postavljanje mreže u područjima bez infrastrukture. Vrsta mobilnosti (individualna, grupna, planirana) utječe na odabir usmjeravanja.

Višeskokovnost. U višeskokovnoj mreži put od izvorišta do odredišta prolazi drugim čvorovima. Višeskokovnost pomaže u obilaženju prepreka i očuvanju energije.

Decentraliziranost i samoorganiziranost. *Ad hoc* mreža mora sama određivati parametre komunikacije (adresiranje, usmjeravanje, grupiranje, pozicioniranje). U nekim slučajevima mogu postojati čvorovi s većim ovlastima koji čine logičku mrežu unutar mreže i koordiniraju i upravljaju nekim dijelovima komunikacije.

Ad hoc mreže prema najčešćim se primjenama dijele na mobilne *ad hoc* mreže (engl. *mobile* ad hoc *networks*, skr. MANET), *mesh*-mreže i senzorske mreže.

1.3 Vrste *ad hoc* mreža

1.3.1 Mobilne *ad hoc* mreže

Mobilna *ad hoc* mreža (engl. *mobile* ad hoc *network*, skr. MANET) autonomni je skup mobilnih uređaja koje komuniciraju putem bežičnih veza relativno male propusnosti [1]. Oni uspostavljaju kratkotrajnu ili privremenu komunikaciju bez podrške infrastrukture. Glavno je svojstvo MANET-a pokretljivost čvorova koja može obuhvaćati raspon od male (npr. prijenosna računala u učionici) do velike (npr. automobili na autocesti). Budući da *ad hoc* mreža nema postavljenu infrastrukturu, mobilnost stanica uzrokuje dinamičnu strukturu mreže. Topologija mreže promjenjiva je u vremenu kako stanice mijenjaju svoj položaj i izlaze iz dometa jednih i ulaze u domet drugih stanica.

Mobilne *ad hoc* mreže predstavljaju općeniti oblik *ad hoc* mreža. Ostale vrste *ad hoc* mreža specifičnije su po svojim svojstvima.

Zbog promjenjivosti mreže stanice moraju moći prepoznati prekid veze prema susjednoj stanici i pronaći novi, okolni put prema odredištu.

Primjeri su mobilnih *ad hoc* mreža

- mreže vozila (vehicular networks)
- mreže u vojnim operacijama
- mreže u kriznim situacijama — spašavanje, požari, potresi.

1.3.2 *Mesh*-mreže

Bežične pristupne mreže (engl. *wireless mesh networks*, skr. WMN) razvijene su u cilju pružanja telekomunikacijskih usluga na područjima gdje se ulaganje u infrastrukturu ne isplati ili je neizvedivo. Svaki čvor (nepokretna ili slabo pokretna bežična stanica) omogućava komunikaciju svojim bežičnim klijentima i uz to prosljeđuje promet s drugih čvorova.

Sastoje se od čvorova-usmjernika (engl. *mesh router*, skr. MR) koji omogućavaju bežičnim stanicama preko poveznika (engl. *gateway*) pristup vanjskoj mreži, najčešće Internetu.

Temelje se na nekom postojećem standardu za fizički sloj i podsloj MAC, npr. 802.11, što im daje isplativost zbog sveprisutnosti opreme. No, zbog slabe skalabilnosti standardnog protokola kod primjene u višeskokovnim mrežama, potrebno je razviti optimirane protokole i u sloju podatkovne veze (pristup mediju) i u mrežnom sloju (usmjeravanje).

U [3] su navedene sljedeća svojstva *mesh*-mreža:

- višeskokovna bežična mreža — cilj je razvoja WMNa proširiti područje pokrivanja postojećih bežičnih mreža bez žrtvovanja kapaciteta i pružiti stanicama bez izravne optičke vidljivosti pristup mreži
- ad hoc mreža sa sposobnošću samoformiranja, samoreformiranja i samoorganiziranja
- integracija s postojećim tipovima bežičnih mreža — 802.11, 802.15, 802.16, mobilna mreža, senzorske mreže

Kao i ostale vrste bežičnih *ad hoc* mreža, i *mesh*-mreže odlikuje necentraliziranost (nema središnje koordinacije među čvorovima) i višeskokovna (engl. *multihop*) komunikacija. Međutim, postoje sljedeća obilježja po kojima se u bitnome razlikuju [4]:

Nemaju energetskih ograničenja. Za razliku od mobilnih *ad hoc* i senzorskih mreža, kojima se u radu nastoji optimirati potrošnja električne energije, čvorovi *mesh*-mreže imaju pristup dovoljnim količinama električne energije.

Statičnost. *Mesh*-mreža je statična, za razliku od MANET-a koji su mobilni i senzorskih mreža u kojima senzori sami po sebi ne moraju biti mobilni, no uslijed prestanka rada pojedinih senzora (iscrpljen izvor energije, kvar) mreža mijenja topologiju.

Više primopredajnika. Padom cijena bežičnih sustava postalo je isplativo ugraditi višestruke primopredajnike u čvorove-usmjernike, što kod mreža s uređajima s ograničenim pristupom energiji i veličinom nije prikladno.

Prometni model. U *mesh*-mrežama promet je uglavnom usmjeren od poveznika i prema njemu; čvorovi-usmjernici prvenstveno će usmjeravati promet na putu od krajnje točke (korisnika) do poveznika; zbog toga dolazi do većeg opterećenja čvorova blizu poveznika kroz koje prolazi veći broj putova.

Propusnost. *Mesh*-mreža mora biti skalabilna za više tisuća korisnika, jer joj je prvenstvena namjena pristup internetu.

1.3.3 Senzorske mreže

Razvoj i dostupnost bežične tehnologije doveo je do razvoja jeftinih malenih senzorskih stanica male potrošnje energije i bežične komunikacije malog dometa. Senzorske stanice sastoje se od senzora, procesora podataka i komunikacijskog dijela [5, 6].

Razlika senzorskih mreža od mobilnih ad hoc mreža:

- broj senzora mnogo je veći, čak i nekoliko redova veličine
- velika gustoća senzora u postavljenoj mreži
- visoka stopa kvarova (mehaničkih kvarova, iscrpljivanja izvora el. energije)
- premda su senzori uglavnom nepokretni, njihovi česti kvarovi uzrokuju česte promjene topologije
- senzorske stanice ograničene su energije, procesne snage i memorije

Primjena senzorskih mreža područja su kao industrijsko upravljanje i nadzor, automatizacija kućanstva i potrošačka elektronika, praćenje inventara i upravljanje nabavom, pametna poljoprivreda, sigurnost i vojska, praćenje zdravlja i nadzor područja pod prirodnim i drugim katastrofama.

2 USMJERAVANJE U *AD HOC* MREŽAMA

Važnost usmjeravanja u dinamičnim višeskokovnim mrežama u posljednje je vrijeme poticala znanstvenike na istraživanje novih usmjernih protokola za *ad hoc* mreže. No značajke *ad hoc* mreža otežavaju tu zadaću. U mobilnim *ad hoc* mrežama pokretnost čvorova uzrokuje česte promjene mrežne topologije i podjelu mreže. Zbog nepredvidive promjenjivosti kapaciteta bežičnih veza gubici paketa sve su češći. Priroda bežične komunikacije dovodi do već spomenutih problema skrivenog i izloženog terminala (stanice). A pokretne stanice imaju ograničene energetske i računalne resurse pa zahtijevaju da se pri razvijanju protokola pazi na efikasnost.

Valja uzeti u obzir neke bitne činjenice pri projektiranju usmjernih protokola u *ad hoc* mreži. To je prvo arhitektura koja može biti hijerarhijska ili nehijerarhijska; zatim jednosmjernost ili dvosmjernost veza; učinkovitost potrošnje energije; sigurnost; postojanje čvorova većih sposobnosti (računskih, energetskih ili većeg dometa), (engl. *superhosts*); kvaliteta usluge (engl. *Quality of Service*, skr. QoS); i konačno potreba za slanjem paketa prema grupi čvorova (*multicast*) [7, 8].

Arhitektura. Može biti hijerarhijska i nehijerarhijska (plosnata). U samoorganizirajućim mrežama gdje svaki čvor neovisno o drugima odlučuje o usmjeravanju najčešće je arhitektura nehijerarhijska. Svi su čvorovi vidljivi svim čvorovima, kao u protokolima vektora udaljenosti sa sekvenciranjem po odredištu (engl. *Destination-Sequenced Distance Vector*, skr. DSDB) i Bežičnom usmjernom protokolu (engl. *Wireless Routing Protocol*, skr. WRP). Međutim, nehijerarhijski protokoli ne ponašaju se dobro kod povećavanja broja čvorova u mreži (nisu skalabilni), jer količina prenesenih podataka za potrebe usmjeravanja (engl. *routing overhead*) brzo raste s veličinom mreže. Hijerarhijska arhitektura organizira mrežu u više hijerarhijskih slojeva gdje čvorovi višeg ranga komuniciraju međusobno i sa svojim „podređenim“ čvorovima. Jedan je od načina grupiranje u grozdove (engl. *clustering*). Vođa svake grupe mora pratiti koji su čvorovi članovi njegove grupe. Primjeri su *Clusterhead Gateway Switch Routing* (CGSR) i *Cluster-Based Routing Protocol* (CBRP).

Jednosmjerne veze. U bežičnim mrežama veze se između čvorova zbog karakteristika bežične komunikacije ne mogu općenito smatrati dvosmjernima. Razlozi su za to razlike u snazi radioodašiljača kod primjerice pokretnih stanica, gdje su oni zbog ograničene energije slabiji, i nepokretnih stanica, ili pak satelita, gdje su jači; zatim interferencija koja ometa prijam kod jedne stanice; radijska tišina u taktičkim mrežama (vojna ili policijska primjena) s otvorenom potrebom prijma. Mobilnost čini veze vremenski promjenjivima pa tako i njihovu jednosmjernost i dvosmjernost.

Energetska učinkovitost. Protokol bi trebao biti učinkovit u potrošnji električne energije. Prigodom razvoja usmjernog protokola morali bi se uzeti u obzir ograničenost izvora energije malih uređaja kao što su primjerice senzori u senzorskim mrežama. Zato bi se proces usmjeravanja trebao rasporediti po čvorovima sudionicima.

Sigurnost. Zbog bežične komunikacije *ad hoc* mreže podložnije su napadima. Sigurnost valja imati na umu u dizajniranju svih aspekata usmjernih protokola.

Superčvorovi. Usmjerni protokoli uglavnom pretpostavljaju jednakost svih stanica u *ad hoc* mreži. U nekim slučajevima postoji čvor s većim mogućnostima (npr. većom pojasnom širinom ili stalnim napajanjem) koji služe kao potpora (u vojnim scenarijima), kao mreža okosnica (engl. *backbone*) ili kao ponor za senzorsku mrežu.

Kvaliteta usluge. Odabir parametra cijene u mreži utječe na učinak mreže — iskorištenost veza, zagušenje i efikasnost. Neke su od metrika koje se mogu uzeti u obzir pouzdanost puta, stabilnost puta, preostala energija i preostala pojasna širina.

Multicast. Slanje paketa grupi odredišta (engl. *multicast*) šalje jednu kopiju podataka istodobno prema više primatelja. Time se ekonomičnije iskorištavaju veze i štedi energija. Upotrebljava se kod distribuiranja multimedijskih sadržaja, kod obavještavanja i u kritičnim situacijama, gdje su ograničeni u sudionicima komunikacije. Zbog promjenjivosti mrežne topologije projektiranje višeodredišnih protokola također je izazov.

2.1 Klasifikacija *ad hoc* usmjernih protokola

Konstrukcija usmjernih protokola projektiranih za žičane mreže ne čini ih optimalnima za bežične *ad hoc* mreže. Povećavanjem broja čvorova, razmjena informacija vezanih uz usmjerni protokol nesrazmjerno raste i opterećuje bežične veze. Zato su razvijeni protokoli baš za *ad hoc* mreže. Dijele se na proaktivne ili tablične, reaktivne ili protokole na zahtjev i hibridne. U proaktivnim usmjernim protokolima put prema odredištu određuje se čim se čvor uključi u mrežu i održava se tijekom rada povremenim obnavljanjem putova; usmjerna tablica je u svakom trenutku ažurna (koliko može biti). U reaktivnim protokolima usmjeravanje se odvija prema potrebi slanja podataka; kad čvor želi poslati podatke odredištu, ako ne postoji (ažurni) put, protokol pokrene proces nalaženja puta prema odredištu. Hibridni usmjerni protokoli kombiniraju proaktivni i reaktivni način rada.

U [9] i [10] usmjeravanje se dijeli i prema broju faza u radu protokola, ovisno o tome uspostavlja li se put kroz mrežu prije slanja podataka ili zajedno sa slanje. Jednofazni protokoli objedinjuju proces usmjeranja i slanje podataka, a dvofazni razdvajaju fazu traženja puta i fazu slanja podataka.

Jednofazni protokoli, u koje spadaju usmjeravanje plavljenjem (engl. *flooding*), usmjeravanje metodom glasina (engl. *gossiping*) i lokacijski potpomognuto usmjeravanje (engl. *location aided routing*, skr. LAR).

Plavljenje šalje paket svim susjedima, što jamči da će stići do svih spojenih čvorova, pa i odredišta. Međutim, neefikasno, jer stvara suvišni promet u mreži. Metoda glasina pokušava povećati efikasnost smanjujući broj čvorova kojima se prosljeđuju paketi. Lokacijski protokoli također nastoje smanjiti promet nastao plavljenjem oslanjajući se na lokaciju pošiljatelja i primatelja kod odlučivanja dobivenu nekim mehanizmom lociranja (kao što je npr. globalni sustav za pozicioniranje, GPS). Jednofazni protokoli često se upotrebljavaju u fazi određivanja puta kod dvofaznih protokola.

U dvofaznim protokolima otkrivanje puta kroz mrežu i slanje podataka razdvojeni su u dvije faze. U prvoj fazi, fazi otkrivanja puta, protokol pronalazi put kroz mrežu. Nakon toga podaci se šalju tim putom sve dok je aktivan (nije istekao ili se prekinuo zbog kvara ili pomicanja čvorova). Posebno traženje puta smanjuje pretek kontrolnog prometa u mreži, jer samo čvorovi na putu prosljeđuju pakete.

Među dvofazne protokole mogu se svrstati reaktivni i proaktivni protokoli. Reaktivni iniciraju fazu traženja puta samo kad je to potrebno (moraju poslati podatke odredištu, a nemaju put prema njemu). Proaktivni protokoli kontinuirano traže i obnavljaju putove kroz mrežu (prva faza) pa uvijek imaju (relativno) ažurne usmjerne tablice pomoću kojih usmjeravaju podatke (druga faza).

Prednost dvofaznih protokola — smanjenje kontrolnog prometa u mreži, jer samo čvorovi na putu moraju prosljeđivati pakete — istovremeno je i nedostatak. U slučaju kvara i na jednom elementu (čvoru ili vezi) puta, put postaje nevažeći.

Osim ove, postoje i druge klasifikacije *ad hoc* usmjernih protokola.

Prema vrsti čvorova dijele se na uniformne i neuniformne. U uniformnim protokolima svi čvorovi imaju jednaku ulogu u mreži; ti su protokoli najčešće nehijerarhijski. Neuniformni protokoli razlikuju više vrsta čvorova prema ulozi koju imaju u procesu usmjeravanja; uloge se čvorovima obično dodjeljuju nekim distribuiranim algoritmima. Prema organizaciji čvorova neuniformni protokoli dalje se dijele na zonske hijerarhijske (*zone-based*), nakupinske hijerarhijske (*cluster-based*) i jezgrene (*core-node-based*).

U zonskim usmjernim protokolima čvorovi se organiziraju konstruirajući zone prema nekom odabranom algoritmu (npr. prema zemljopisnom položaju). Čvorovi moraju određivati putove samo prema čvorovima unutar zone, a posebni čvorovi zaduženi su za međuzonsku komunikaciju.

Nakupinski usmjerni protokoli grupiraju čvorove u nakupine i pomoću nekog algoritma bira se vođa svake nakupine. Vođe prate čvorove koji su članovi nakupine i vode brigu o usmjeravanju. Nakupine mogu biti organizirane i u više razina. Primjer je takvog protokola *Clusterhead Gateway Switch Routing* (CGSR).

U jezgrenim usmjernim protokolima tzv. jezgreni čvorovi (*core nodes*) čine okosnicu (*backbone*) mreže. Odabrani su dinamički i obavljaju usmjerne funkcije u mreži. Takav je prokol *Core-Extraction Distirbuted Ad Hoc Routing* (CEDAR).

Protokoli se razlikuju i prema odabranoj metrici (cijeni) upotrebljavanoj za usmjeravanje. Najčešće protokoli određuju put prema broju skokova. U tom slučaju kraći putovi imaju veću stabilnost, što vrijedi ako se pretpostavi

jednaka vjerojatnost kvara za sve bežične veze. Međutim, to često nije slučaj pa neki protokoli kao što su *Associatively Based Routing* (ABR) i *Signal Stability-Based Routing* (SSR) rabe stabilnost veze i jakost signala kao cijenu. Osim njih, rabe se i metrike upotrebljavane u usmjernim protokolima s kvalitetom usluge iz žičanih mreža, kao što su kašnjenje, kolebanje kašnjenja, propusnost i brzina gubljenja paketa.

Usmjeravanje se može temeljiti osim na topologiji i na takvim parametrima kao što je odredište i lokacija. Protokoli temeljeni na topologiji skupljaju informacije o mrežnoj topologiji od drugih članova mreže i na temelju tih informacija donose usmjerne odluke, dok protokoli temeljeni na odredištu prate samo sljedeći skok prema odredištu. Lokacijski protokoli usmjeravaju rabeći informacije o svojem položaju (npr. pomoću GPS-a) i položaju odredišta.

2.1.1 Proaktivni usmjerni protokoli

Proaktivni ili tablični (engl. *table-driven*) protokoli kontinuirano obnavljaju usmjernu tablicu prema svim čvorovima u mreži pokušavajući održati usmjerne informacije ažurnima. Svi čvorovi nastoje imati ispravnu i konzistentnu sliku mrežne topologije proaktivno dopunjavajući i osvježavajući njeno stanje, bez obzira na postojanje podatkovnog prometa u mreži. Time je pretek (engl. *overhead*) velik.

Većina proaktivnih protokola preuzeta je iz žičanih mreža, uz prilagodbu zahtjevima *ad hoc* mreža.

Slijedi kratki popis najpoznatijih proaktivnih protokola. Više se informacija može naći u [8, 11, 12]

WRP. Bežični usmjerni protokol (engl. *Wireless Routing Protocol*, skr. WRP) temeljen je na protokolu vektora udaljenosti. Svaki čvor vodi tablicu udaljenosti, usmjernu tablicu, tablicu cijena veza i listu retransmisije poruka (*Mesage Retransmission List*, MRL). Čvorovi razmjenjuju usmjerne tablice sa susjedima putem poruka koje mogu slati periodički ili kod promjene stanja veze.

DSDV. Vektor udaljenosti sa sekvenciranjem po odredištu engl. *Destination-Sequenced Distance Vector*, skr. DSDV, također temeljen na algoritmu vektora udaljenosti, razlikuje se od protokola WRP po tome što čvor zapisuje, uz sljedeći skok prema odredištu i udaljenost do odredišta, i redni broj (*sequence number*) koji generira odredište. Pomoću rednog broja razlikuje se važeći put od zastarjeloga i sprječava se nastanak petlji, nedostatak karakterističan za algoritam vektora udaljenosti.

OLSR. Optimirano usmjeravanje pomoću stanja veza [13] (engl. *Optimized Link State Routing*, skr. OLSR) proaktivan je usmjerni protokol usmjeravanja pomoću stanja veza. Svaki čvor odabire među svojim susjedima s kojima ima simetričnu vezu višespojne sklopnike (engl. *multipoint relay*, skr. MPR) koji su zaduženi za prosljeđivanje kontrolnih paketa. Svaki čvor prati koji su ga čvorovi odabrali kao MPR i stanje veza samo prema njima. Samo te veze dužan je objaviti mreži.

OLSR je optimirana varijanta protokola stanja veza. Optimizacija se sastoji u tome što svaki čvor prosljeđuje usmjerne informacije samo MPR-ovima. Time se smanjuje količina kontrolnog prometa prisutnog kod plavljenja prema svim susjedima. Osim toga, samo se za dio veza mora pratiti stanje, čime se smanjuje i količina informacija u usmjernim paketima.

Zbog toga što OLSR kao proaktivni protokol održava usmjernu tablicu prema svim čvorovima u mreži, pogodan je u prometnim modelima sa mnogo komunicirajućih parova izvorište–odredište, i gdje se ti parovi često mijenjaju. Tada kontinuirano održavanje slike mrežne topologije pokazuje prednosti pred reaktivnim protokolima. Optimizacije pak dolaze do izražaja što je veća gustoća čvorova u mreži. Veća gustoća čvorova znači veću optimizaciju u donosu na neoptimirane protokole stanja veza.

GSR. *Global State Routing* protokol je temeljen razmjeni informacija o stanju svojih veza, pomoću kojih čvorovi održavaju globalnu sliku mrežne topologije i lokalno odlučuju o usmjeravanju. Za razliku od protokola DSDV paketi stanja veza ne šalju se svima u mreži, nego samo susjedima.

FSR. Usmjeravanje pomoću stanja tehnikom „ribljeg oka“ (engl. *Fisheye State Routing*, skr. FSR, FSR) hijerarhijski je usmjerni protokol temeljen na protokolu GSR a služi se tehnikom „ribljeg oka“. Pomoću posebne strukture mreže smanjuje se količina kontrolnog prometa namijenjena ažuriranju usmjernih informacija. Informacije o bližim čvorovima ažuriraju se češće nego one o daljim čvorovima. Kao riblje oko koje sliku u centru vidi s više detalja nego dio slike na rubovima, čvor ima najtočniju informaciju o čvorovima koji su mu blizu. Ako čvor i nema ažurne podatke o odredištu, kako mu se paket približava, više informacija postaje dostupno.

2.1.2 Reaktivni usmjerni protokoli

Reaktivni protokoli funkcioniraju „na zahtjev“ (engl. *on-demand*). Traže put samo kad postoji potreba za slanjem podataka kroz mrežu. Traženje uglavnom počinje tako da izvorište (čvor koji želi slati podatke) pošalje zahtjev za putom kroz mrežu. Zatim čeka da mu netko pošalje ili cijeli put skok po skok do odredišta (kod protokola s izvorišnim usmjeravanjem), ili da mu susjedi pošalju svoje udaljenosti do odredišta na temelju kojih će odrediti svoju najkraću udaljenost (tako se ponašaju primjerice protokoli vektora udaljenosti). Zbog potrebe za traženjem puta prije

slanja korisničkog prometa reaktivni protokoli imaju veće kašnjenje ili zadršku od pokušaja slanja do trenutka kad se paket može poslati. Zato su reaktivni protokoli primjenjiviji u visoko pokretljivoj mreži s manjim prometom.

Reaktivni protokoli koje valja spomenuti navedeni su u sljedećim retcima [8, 11, 12].

DSR. Dinamično izvorišno usmjeravanje (engl. *Dynamic Source Routing*, skr. DSR) [14] reaktivni je protokol s izvorišnim usmjeravanjem. Zamišljen je tako da smanjuje količinu kontrolnih paketa. Ne zahtijeva periodično javljanje susjedima. Samo usmjeravanje sastoji se od dva dijela — traženje puta i održavanje puta.

AODV. Protokol Ad hoc on-demand distance vector [15] (AODV) sličan je protokolu DSR, s tom razlikom da implementira i redni broj odredišta pomoću kojeg se određuje aktualni put prema odredištu.

TORA. Vremenski uređeni usmjerni algoritam (engl. *Temporally-Ordered Routing Algorithm*, skr. TORA) reaktivni je protokol s elementima proaktivnosti. Putovi su određeni usmjerenim acikličnim grafom (engl. *Directional Acyclic Graph*, skr. DAG). U traženju puta upotrebljava preokretanje veza (engl. *link reversal*).

LAR. Lokacijski potpomognuto usmjeravanje (engl. *Location-Aided Routing*, skr. LAR) za usmjeravanje rabi podatke o lokaciji radi povećanja efikasnosti smanjenjem preteka kontrolnih paketa. Zahtijeva dostupnost globalnog sustava za pozicioniranje (GPS).

ABR. *Associatively-Based Routing* distribuirani je usmjerni protokol. Bira putove s obzirom na stabilnost bežične veze. Stabilnost određuje promatranjem veze u nekom vremenskom intervalu.

2.1.3 Hibridni usmjerni protokoli

Reaktivnost, odn. proaktivnost protokola korisna je i primjenjiva u određenim slučajevima i situacijama. Često te situacije nisu jednostavno određene pa se kombinacijom svojstava može postići bolja učinkovitost. Hibridni usmjerni protokoli sadrže karakteristike i proaktivnih i reaktivnih protokola. U komunikaciji s nekim dijelovim mreže upotrebljavaju proaktivno usmjeravanje, a s ostalim dijelovima reaktivno. Neki su hibridni protokoli [8, 11]:

ZRP. Zonski usmjerni protokol (engl. *Zone Routing Protocol*, skr. ZRP) primjenjuje reaktivnost i proaktivnost u ovisnosti o tome je li odredište unutar ili izvan zone, područja određenom udaljenosti. Unutar zone komunicira nekim proaktivnim protokolom, a izvan zone reaktivnim.

ADV. *Adaptive Distance Vector* protokol je vektora udaljenosti s adaptivnim mehanizmom pomoću kojeg smanjuje učestalost slanja kontrolnih paketa u ovisnosti o opterećenju mreže.

CEDAR. *Core Extraction Distributed Ad hoc Routing* [16] hijerarhijski je protokol temeljen na odabiru jezgrenih čvorova, koji čine najmanji dominirajući skup. Dominirajući skup pojam je iz teorije grafova definiran kao skup vrhova (čvorova) sa svojstvom da je svaki vrh iz grafa ili u dominirajućem skupu, ili je susjed nekog vrha iz dominirajućeg skupa. Jezgreni čvorovi usmjeravaju promet za svoje članove.

3 SIGURNOST USMJERAVANJA U *AD HOC* MREŽAMA

Priroda komunikacijskog kanala u bežičnim mrežama otežava primjenu sigurnosnih rješenja. *Ad hoc* struktura zbog nedostatka središnjeg upravljanja dodatno komplicira taj problem.

3.1 Sigurnosni zahtjevi

Sigurnost u informacijskoj tehnologiji mora zadovoljiti tri sigurnosna zahtjeva [17]. To su tajnost (engl. *confidentiality*), integritet (engl. *integrity*) i raspoloživost (engl. *availability*) — obično skraćeno nazivani *CIA* prema engleskom nazivlju.

Tajnost označava zaštitu podataka od neovlaštenog pristupa. Osigurava da do podataka može doći samo onaj kome su namijenjeni. Najčešće se implementira kriptografskim metodama, šifriranjem podataka pomoću simetričnih šifri ili nesimetričnih sustava javnih i privatnih ključeva. Tako treća osoba bez poznavanja kriptografskog ključa ne može pročitati podatke čak ako do njih i dođe.

Integritet se odnosi na vjerodostojnost podataka ili izvora. Štiti podatke od neovlaštene promjene, u kojem je slučaju riječ o integritetu podataka. Integritet izvora, zvan i autentikacija, štiti vjerodostojnost izvora podataka. Integritet se postiže primjenom kodova za autentikaciju poruke (engl. *message authentication code*, MAC[1]), jednosmjenih funkcija sažetaka (engl. *one-way hash function*) ili digitalnim potpisima.

Raspoloživost se odnosi na podatke ili resurse. Jedan je od sigurnosnih zadataka osigurati da usluga bude uvijek dostupna. Nedostupna usluga barem je tako loša kao ona koja ne postoji. Nedostupnost važne usluge može biti barem toliko štetna kao i krađa (kršenje tajnosti) i lažno predstavljanje (povreda integriteta). Napadi na raspoloživost (uskraćivanje pristupa usluzi, engl. engl. *denial of service*, skr. DoS) teško se otkrivaju, jer je potrebno otkriti je li nedostupnost posljedica napada ili vanjskog utjecaja.

Neki autori tim trima stupovima dodaju i autentikaciju (engl. *authentication*) i neporecivost (engl. *nonrepudiation*). Autentikacija jamči identitet (pošiljatelja),

[1] *message authentication code* naziva se i *message integrity code* (MIC) da bi se razlikovao od podsloja kontrole pristupa mediju (engl. *medium access control*) u tekstovima gdje se zajedno spominju

a neporecivost jamči da je podatak uistinu poslao navedeni pošiljatelj, odn. da ga je primatelj primio [11, 18].

Sigurnost u *ad hoc* mrežama može se promatrati na bilo kojem sloju protokolnog složaja (zbog toga što se napadi na mrežu mogu odvijati na bilo kojem sloju). Na primjer, tajnost se komunikacije može ostvariti s kraja na kraj na aplikacijskom ili na transportnom sloju. S druge strane, sloj podatkovne veze može zaštititi komunikaciju od prisluškivanja na razini veze, od čvora do čvora. Budući da se usmjeravanje odvija uglavnom na mrežnom sloju, zadaća je dizajnera usmjernog protokola osim razvoja i zaštita procesa usmjeravanja (otkrivanja puta kroz mrežu) i procesa prosljeđivanja prometa (na otkrivenom putu).

3.2 Napadi u *ad hoc* mrežama

Zbog same prirode komunikacije preko otvorenog zajedničkog medija, bežična mreža podložna je napadima, a nedostatak centralizirane koordinacije u *ad hoc* mrežama povećava njihov broj i raznolikost.

Napadi mogu biti pasivni i aktivni. Pasivni napadi služe napadačima da dođu do neovlaštenih informacija. Ne ometaju rad mreže, zbog čega ih je gotovo nemoguće otkriti. Informacije do kojih pasivni napadač nastoji doći mogu biti identitet i pozicija čvorova, kriptografski materijal i sl. Aktivni napadi iznutra ili izvana pokušavaju onemogućiti komunikaciju ili izmijeniti podatke u komunikaciji.

Nadalje, napadi mogu biti usmjereni na mehanizme *ad hoc* mreže, kao što je usmjeravanje, a mogu napadati i sigurnosne mehanizme kao što je primjerice mehanizam razmjene ključeva.

Napadi na sigurno usmjeravanje dijeli se na vanjske i unutrašnje. Vanjski napadači nisu dio mreže, nemaju sigurnosne vjerodajnice kao što su simetrični ili nesimetrični ključevi.

Unutrašnji napadači (nazivaju se i bizantskim napadačima[2]) kompromitirani su članovi mreže koji se ne ponašaju prema zadanim pravilima protokola. Njihove su ruke odriješene činiti bilo kakve zlonamjerne stvari pa predstavljaju veliki izazov za rješavanje.

Ne mora svaka nepravilna aktivnost u *ad hoc* mreži biti zlonamjerna. Sebičnost čvorova radi očuvanja energije i racionalnije uporabe računalnih resursa također je problem. Sebičan čvor odlučuje iz navedenih razloga odbaciti paket, dok za to vrijeme iskorištava susjedne čvorove za prosljeđivanje vlastitih paketa. Sebičnost smanjuje kvalitetu usluge i ugrožava jedan osnovni sigurnosti zahtjev — raspoloživost [18].

Pregled napada u *ad hoc* mrežama može se naći na više mjesta u literaturi [11, 12, 20], a najvažniji slijede.

[2]Bizantski je napadač onaj koji ima potpunu kontrolu nad autenticiranim čvorom. Takvom se čvoru ne može vjerovati i njegovi postupci ne moraju biti u skladu s protokolom. Naziv potiče od problema bizantskih generala opisanog u [19].

Preplavljivanje. Napadač preplavljuje mrežu lažnim zahtjevima za traženje puta ili neprekidno šalje pakete oglašavanja puta s ciljem da preoptereti implementacije usmjeravanja u čvorovima.

Lišavanje sna. Napadač pokušava iscrpiti ili potrošiti resurse. Radi uštede električne energije, čvorovi kad ne moraju slati ugase neke sustave (spavaju). Ovaj napad kontinuirano šalje upite i ne dopušta prijelaz čvorova u režim sna.

Crna rupa. U ovome napadu lažnim odgovorima napadač tvrdi da je najkraći put do odredišta. Pridobeći takvim postupkom većinu putova da prolazi njime, odbacuje sve pakete koji dođu do njega.

Podjela mreže. Lažnim usmjernim paketima napadač pokušava onemogućiti komunikaciju između nekih čvorova, dijeleći mrežu na dva odvojena dijela. Specifični je slučaj podjele izolacija jednog čvora.

Crvotočina. Napad crvotočine (engl. *wormhole*) uključuje suradnju dva zlonamjerna čvora. Dva napadača komuniciraju zasebnim kanalom ili tuneliranjem prometa stvarajući time privid kraće međusobne udaljenosti. Time mogu pridobiti da većina putova prolazi njima.

Navala. Napad navale (engl. *rushing attack*) primjenjiv je kod protokola koji određuju putove na temelju zahtjeva koji prvi stigne. Napadač „navaljuje“ svojim zahtjevima za uspostavu puta prema odredištima. Ako njegovi zahtjevi dođu do susjeda odredišta prije legitimnih zahtjeva, put će prolaziti napadačem, a susjedi će legitimne zahtjeve odbaciti. Time napadač postiže to da se nalazi na većini putova.

Otkrivanje lokacije. Napad otkrivanja lokacije (engl. *location disclosure*) daje napadaču informacije o poziciji čvorova a time i strukturi i topologiji mreže.

Nevidljivi čvor. Napad nevidljivog čvora sastoji se u napadačevom neotkrivanju svojeg identiteta u protokolima koji se temelje na identifikaciji čvorova. Napadač sudjeluje u komunikaciji jednostavnim ponavljanjem primljenih paketa.

3.3 Sigurnosni problemi u *ad hoc* mrežama

U literaturi se može naći više pregleda sigurnosti i sigurnosnih problema u *ad hoc* mrežama, bilo mobilnih (MANET), bilo statičnih (*mesh*) [10, 11, 18, 20]. Najveći je problem to što nema dogovorene unificirane definicije sigurnosti usmjeravanja u *ad hoc* mrežama. Jedan je razlog tomu, prema [10], neuklapanje svojstava sigurnog usmjeravanja u koncept sigurnosti *CIA* (tajnost, integritet, raspoloživost). Napadač napadom na prosljeđivanje paketa ugrožava raspoloživost, no to čine napadi i na proces pronalaženja puta kroz mrežu. Sposobnost protokola da pronalazi (najkraće) putove kroz mrežu predstavlja integritet

tog njegovog procesa. Ubacivanje lažnih usmjernih poruka ugrožava integritet. Njihovo zlonamjerno prosljeđivanje nije pitanje integriteta, no svejedno se smatra napadom ako sprječava normalno funkcioniranje protokola [10].

Drugi je problem (a potječe iz prvog) nedosljednost pretpostavki o sigurnosti i napadima prilikom projektiranja protokola, što uzrokuje pogreške u dizajnu sigurnih usmjernih protokola. S jedne su strane „nesigurni“ protokoli koji su dizajnirani bez vođenja računa o sigurnosti. Naknadno poboljšavanje sigurnosnih karakteristika težak je i neisplativ posao. S druge strane, nedostatak zajedničke predodžbe o sigurnosti i karakteristikama napadača onemogućavaju usporedbu različitih protokola.

Kao rješenje tih problema, u [10] se predlaže promatranje sigurnosti iz kuta zadovoljavanja ciljeva protokola. Postavlja da je protokol siguran ako u prisutnosti zlonamjernih čvorova i pod napadom izvršava svoje ciljeve prema specifikacijama. Budući da je osnovni cilj usmjernog protokola određivanje optimalnih putova kroz mrežu i usmjeravanje prometa pronađenim putovima, daje sljedeća svojstva:

Točnost. Usmjerni je protokol točan ako pronađeni putovi postoje u mreži.

Pouzdanost. Usmjerni je protokol pouzdan ako su putovi koje pronalazi uvijek točni, čak i u slučaju (nezlonamjernih) kvarova.

Sigurnost. Usmjerni je protokol siguran ako održava točnost i pouzdanost i pod (zlonamjernim) napadima.

Da bi protokol zadržao efikasnost i u zlonamjernom okružju, mora moći pronaći ispravne putove i otklanjati kvarove na njima. Drugim riječima, mora osigurati ispravno izvođenje obje faze — i otkrivanje puta, i prosljeđivanje podataka.

3.4 Metode ispitivanja sigurnosnih svojstava protokola

Ispitivanje sigurnosnih svojstava komunikacijskih protokola mora formalno odrediti i točnost i pouzdanost u prisutnosti napadača. U članku [10] tvrdi se da u literaturi nedostaje sustavna analiza sigurnosti te da se uglavnom upotrebljavaju neiscrpne i neformalne metode ispitivanja sigurnosti.

U tablici 1 navedene su metode ispitivanja sigurnosti navedene u članku. Dijele se na neiscrpne i iscrpne. Neiscrpne metode nemaju definirani proces ispitivanja koji prate kod analize. Zbog toga nisu ponovljive ili im rezultati nisu uvijek dosljedni. Iscrpne metode sustavno prate razrađeni proces ispitivanja, što daje pouzdanije rezultate, no teže se implementiraju [10].

Tablica 1. Pristupi ocjenjivanju sigurnosti komunikacijskog sustava. Preuzeto iz [10].

		Obilježja pristupa		
	Analitički pristup	Nepoznati napadi	Zajamčenost svojstva	Bezuvjetna sigurnost
neiscrpni	vizualni pregled	da	ne	ne
	simulacija mreže	ne	ne	ne
iscrpni	analitički dokazi	da	da	ne
	modeli simulirljivosti	da	da	ne
	formalne metode	da	da	ne

Obilježja dana u tablici određuju što može pojedina metoda ustanoviti pod kojim uvjetima. Prvo obilježje, nepoznati napadi, opisuje može li promatrana tehnika ispitivanja pronaći nepoznate napade, ili samo potvrditi već poznate. Sljedeće obilježje određuje može li ispitivanje jamčiti zadovoljavanje traženih sigurnosnih svojstava. Posljednje obilježje govori o bezuvjetnoj sigurnosti. Nijedna ispitna metoda ne može potvrditi bezuvjetnu sigurnost. Nije moguće osigurati protokol od još neotkrivenih napada i nepoznatih sigurnosnih svojstava u okolini s neograničenim mogućnostima napadača [10].

Slijedi kratki pregled metoda, a detaljan opis može se naći u [10].

3.4.1 Neiscrpni postupci provjere

Pod neiscrpne metode spadaju vizualni pregled i simulacija mreže. Iako ne mogu jamčiti da zadano sigurnosno svojstvo vrijedi ili ne, ipak su važan korak u određivanju sigurnosnih karakteristika [10].

Vizualni pregled Vizualni pregled najvjerojatnije je najstarija metoda određivanja sigurnosti. Temelji se na ljudskoj analizi i intuiciji i najzastupljenija je analiza *ad hoc* mrežnih protokola i njihove sigurnosti.

Upotrebljava se najčešće za nalaženje napada na protokole objavljene u znanstvenoj literaturi. Analiza se svodi na kružni iterativni proces objavljivanja i poboljšavanja. Po objavljenom napadu, autor protokola unaprijedi ga i objavi promjene, što za sobom povlači novu analizu napada.

Primjer jednog takvog razvoja može se proučiti u slijedu protokola DSR→SRP→Ariadne. Protokol DSR [14]

nije imao nikakvih sigurnosnih svojstava pa je bio podložan bilo kakvim napadima. Razvoj protokola SRP [21] uveo je provjeru integriteta s kraja na kraj između izvorišta i odredišta. Premda su autori tvrdili da je protokol siguran od napada jednog napadača, u [22] je opisan napad u kojem zlonamjerni čvor za vrijeme traženja puta proslijedi paket ne dodajući se u listu akumuliranih čvorova koja opisuje put prema odredištu (tzv. napad nevidljivog čvora). Protokol Ariadne [23] za razliku od protokola SRP autenticira svaki zasebni skok. U [24] otkriveno je više napada na protokol Ariadne.

Više je protokola razvijeno pomoću vizualnog pregleda što ga čini odista važnim načinom ispitivanja sigurnosti. Međutim, rezultate vizualnog pregleda ne treba uzeti kao jedini pokazatelj sigurnosti, jer ne mogu niti otkriti sve moguće napade na promatrani protokol, niti dokazati da napadi ne postoje.

Mrežna simulacija Simulacija mreže važan je alat za procjenu učinka mrežnog protokola. No ne može otkriti nepostojeće napade niti iscrpno ispitati zadovoljavanje zadanog sigurnosnog svojstva [10]. Napadi moraju biti unaprijed poznati da bi se mogli ugraditi u simulaciju. Budući da daju statističku projekciju mrežnog učinka pod određenim uvjetima (napadima), ne mogu odgovoriti na pitanje postoji li ili ne postoji napad. Ako se simulacijom pokaže da je napad malo vjerojatan, to ne znači da ne postoji, odn. da je protokol u tom slučaju siguran od tog napada.

Mrežna simulacija uglavnom se ne upotrebljava za ispitivanje sigurnosnih karakteristika protokola u fazi otkrivanja puta. Češće se rabi u fazi prosljeđivanja paketa kako bi se predvidjelo ponašanje mreže u danim okolnostima.

Budući da se u simulaciji napadači i njihove akcije moraju definirati da bi se mogli proučavati njihovi učinci na mrežu, simulacija ne može odgovoriti na to kako će se mreža ponašati u slučaju dosad nepoznatog napada.

Jedan je primjer ocjenjivanja sigurnosti protokola protokol ODSBR [25]. U [25] i [26] autori su simulacijom uspoređivali protokole ODSBR i AODV [15], utvrdili da se protokol OSDBR ponaša bolje pod bizantskim napadima i tvrde da je zato sigurniji. Međutim, u [10] se tvrdi da zbog fiksnih pretpostavki simulacije nije uzeto u obzir da se takav napadač može ponašati promjenjivo (primjerice u skladu s protokolom za vrijeme ispitivanja, a zlonamjerno za vrijeme prosljeđivanja).

Mrežna simulacija koristan je alat u ispitivanju efikasnosti i optimalnog ponašanja protokola i može pokazati kako se protokol nosi s napadima. No budući da ne može analizirati je li protokol siguran ili nije, uporaba simulacije mora se kombinirati s drugim metodama ispitivanja, kao što je primjerice vizualni pregled [9].

3.4.2 Iscrpni postupci provjere

Iscrpne metode, u koje spadaju analitički dokazi, modeli simulirljivosti i formalne metode, mogu potvrditi ili opovrgnuti sigurnosne pretpostavke koje su pridijeljene sustavu [9].

Analitički dokazi Analitički dokazi matematički su dokazi temeljeni na pretpostavkama, lemama i teoremima pomoću kojih se dokazuju zadani sigurnosni ciljevi [9]. Upotrebljavaju se i za vrednovanje formalnih metoda opisanih u nastavku.

Matematički dokazi imaju svojih nedostataka. Dokazivanje ovisi o pretpostavkama o sustavu i može postati veoma kompleksno kako se sustav povećava. Dokazi se teško uspoređuju. Budući da se ne mogu jednostavno generalizirati, svaki se mora prilagoditi pojedinom slučaju. To povećava razlike između pojedinih primjena, a potreba za ručnim prilagodbama povećava vjerojatnost pogreške.

Modeli simulirljivosti Pomoću modela simulirljivosti dokazuje se da je protokol siguran ako se može apstrahirati idealnim modelom tako da napadač nema veće sposobnosti u stvarnom protokolu nego u idealnom. U idealnom protokolu postoji i svevideći prorok (engl. *oracle*) zbog koga je napadač protiv idealnog protokola nemoćan [9]. Primjer primjene ove metode može se naći u [27].

Formalne metode Formalne metode razvijane su radi povećavanja pouzdanosti kritičnih sustava, kao što su kontrola leta i operacije u nuklearnoj elektrani. Premda ne mogu osigurati potpunu ispravnost sustava, vrlo su korisne zbog boljeg upoznavanja sustava i povećavanja njegove pouzdanosti.

Sustav i njegove karakteristike precizno se definiraju formalnim matematičkim ili semantičkim opisom. Nakon toga se provjeravaju kontrolom modela, dokazivanjem teorema ili provjerom ekvivalencije [28].

4 ZAKLJUČAK

Usmjeravanje je važna funkcija svake komunikacijske mreže. Višeskokovnost, necentraliziranost i potreba za samoorganiziranošću svojstva su koja *ad hoc* mreže razlikuje od žičanih i infrastrukturnih bežičnih mreža. Zbog toga se pojavila potreba za istraživanjem i razvojem protokola dizajniranih baš za *ad hoc* mreže, pa čak i posebno za pojedinu namjenu. Pri dizajnu, nažalost, često se ne uzima u obzir jedan od najvažnijih zahtjeva, sigurnost, a naknadna ispitivanja i dorade već gotovog protokola mogu biti neučinkoviti. Nedostatak jedinstvene i unificirane definicije

sigurnosti *ad hoc* mreža u literaturi dodatno otežava problem.

Dobro definirani formalni postupci ispitivanja sigurnosti i ispravnosti već se dulje vrijeme upotrebljavaju u sustavima s nultom tolerancijom na pogreške, kao što su nuklearne elektrane, zrakoplovi i svemirske letjelice. U novije se doba primjenjuju i za razvoj i analizu distribuiranih sustava kao što su operacijski sustavi te kriptografski i komunikacijski protokoli. Njihova primjena na ispitivanje sigurnosti usmjernih protokola pokazuje dobre rezultate, a kombiniranje više raznovrsnih metoda povećava uspješnost ispitivanja.

LITERATURA

[1] XiangYang Li, *Wireless ad hoc and sensor networks*. Cambridge University Press, 2008.

[2] M. Gerla, *Ad hoc networks*, ch. 1, pp. 1–22. Springer, 2005.

[3] I. F. Akyildiz, Xudong Wang, and Weilin Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, pp. 445–487, Mar. 2005.

[4] N. Nandiraju, D. Nandiraju, L. Santhanam, Bing He, Junfang Wang, and D. Agrawal, "Wireless Mesh Networks: Current Challenges and Future Directions of Web-In-The-Sky," *IEEE Wireless Communications*, vol. 14, pp. 79–89, Aug. 2007.

[5] E. H. Callaway, *Wireless sensor networks: architectures and protocols*. Auerbach Publications, 2004.

[6] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, pp. 102–114, Aug. 2002.

[7] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, *Ad hoc mobile wireless networks: Principles, protocols and applications*. Auerbach Publications, 2007.

[8] A.-S. Pathan and Choong Seon Hong, *Routing in mobile ad hoc networks*, ch. 4, pp. 59–96. Springer, 2009.

[9] T. R. Andel, *Formal security evaluation of ad hoc routing protocols*. Ph. d., The Florida State University, 2007.

[10] T. R. Andel and A. Yasinsac, "Surveying security analysis techniques in MANET routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 4, pp. 70–84, 2007.

[11] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile Ad Hoc routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.

[12] S. Agrawal, S. Jain, and S. Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks," *Journal of Computing*, vol. 3, pp. 41–48, May 2011.

[13] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)." RFC 3626 (Experimental), Oct. 2003.

[14] D. B. Johnson, Yih-Chun Hu, and D. A. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4." RFC 4728 (Experimental), Feb. 2007.

[15] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing." RFC 3561 (Experimental), July 2003.

[16] P. Sinha, R. Sivakumar, and V. Bharghavan, "CEDAR: a core-extraction distributed ad hoc routing algorithm," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1454–1465, 1999.

[17] M. Bishop, *Computer security: art and science*. Addison-Wesley Professional, 2003.

[18] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 7, pp. 2–28, Jan. 2005.

[19] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[20] P. G. Argyroudis and D. O'Mahony, "Secure routing for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 3, pp. 2–21, 2005.

[21] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, vol. 31, pp. 193–204, Jan. 2002.

[22] J. D. Marshall, *An Analysis of the Secure Routing Protocol for mobile ad hoc network route discovery: using intuitive reasoning and formal verification to identify flaws*. Msc, Florida State University, 2003.

[23] Yih-Chun Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," in *Proceedings of the 8th annual international conference on Mobile computing and networking - MobiCom '02*, vol. 11, (Atlanta, GA, USA), pp. 12–23, ACM Press, Jan. 2002.

[24] L. Buttyán and I. Vajda, "Towards provable security for ad hoc routing protocols," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks - SASN '04*, (New York, New York, USA), pp. 94–105, ACM Press, 2004.

[25] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on-demand secure routing protocol resilient to byzantine failures," in *Proceedings of the 1st ACM workshop on Wireless security (WiSe '02)*, (Atlanta, Georgia, USA), pp. 21–30, ACM, 2002.

[26] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "Mitigating byzantine attacks in ad hoc wireless networks," tech. rep., Johns Hopkins University, Baltimore, MD, 2004.

[27] G. Ács, L. Buttyán, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 5, pp. 1533–1546, Nov. 2006.

[28] D. Câmara, A. A. F. Loureiro, and F. Filali, "Formal Verification of Routing Protocols for Wireless Ad Hoc Networks," in *Guide to Wireless Ad Hoc Networks* (S. Misra, I. Woungang, and S. C. Misra, eds.), Computer Communications and Networks, ch. 8, pp. 189–210, Springer, 2009.