

Dmitar Stevanović,
potpukovnik, dipl. inž.
dr Miljko Erić,
pukovnik, dipl. inž.
Vojnotehnički institut,
Beograd
profesor dr Dušan Starčević,
dipl. inž.
Fakultet organizacionih nauka,
Beograd

KONCEPT AD HOC KOMUNIKACIONIH MREŽA ZA POVEZIVANJE SENZORA U OKVIRU KOMANDNO-INFORMACIONIH SISTEMA

UDC: 623.611 : 681.324

Rezime:

U radu je razmatrana mogućnost primene ad hoc mobilnih komunikacionih mreža za povezivanje senzorskih sistema, kao čvornih izvora informacija i kao čvornih elemenata komunikacione mrežne infrastrukture u okviru komandno-informacionog sistema. Korak u evoluciji bežičnih komunikacija predstavljaju ad hoc mreže koje se javljaju u obliku grupa prenosnih računara, mobilnih telefonskih uređaja, personalnih digitalnih asistenta i sličnih korisničkih uređaja, kao i u obliku mreže autonomnih elektronskih senzorskih uređaja. Osnovnu karakteristiku svake ad hoc mreže predstavlja uspostavljanje komunikacije između mrežnih čvorova bez unapred postavljene fiksne mrežne infrastrukture. Umesto mreže fiksni čvorova i baznih stanica, karakterističnih za postojeću bežičnu mrežnu infrastrukturu, nosilac komunikacije postaje mreža čvornih sofisticiranih senzorskih uređaja – stanica. Mogućnost eliminisanja potrebe fiksne komunikacione infrastrukture u sistemima obezbeđenja i kontrole teritorije od izuzetnog je značaja u vojnim primenama, posebno sa aspekta pripreme i vođenja savremenih operacija. Praćenje situacije u vazдушnom prostoru na osnovu vizuelnih osmatračkih i zvukometrijskih stanica, senzorska zaštita objekata i prostora i prikupljanje relevantnih informacionih podataka predstavljaju samo neke od primera praktične primene ad hoc mreža.

Ključne reči: bežične mreže, bežične računarske mreže, ad hoc mreže, senzorske mreže.

A CONCEPT OF AD HOC COMMUNICATION NETWORKS FOR THE SENSORS NETWORKING IN COMMAND CONTROL SYSTEMS

Summary:

The application possibility of ad hoc mobile communication network for connecting sensor systems, as node sources of information and as node elements of communication network's infrastructure, in command information system is presented in this paper. The next step in wireless communication evolution is ad hoc networks, which appear in the form of groups of mobile computers, mobile phone devices, personal digital assistants and in the form of a network of autonomy electronically sensors devices. The basic characteristic of every ad hoc network is establishing communication between network nodes without fixed network infrastructure, established in advance. Instead of fix network nodes and basic stations, that are typical of available wireless networks infrastructure, network of nodes of sophisticated sensors devices (stations) became most important for communication. Possibility of eliminating the need for fixed communication infrastructure in security systems and systems for territory control, is very important in military, especially for the preparation and leading of modern operations. Some of the examples for practical application of ad hoc networks are: air surveillance system based on visual surveillance and acoustic-metric stations, sensor systems for protection of objects and space and collection of relevant information data.

Key words: wireless networks, computer networks, ad hoc networks, sensor networks.

Uvod

Komandno-informacioni sistemi na taktičkom nivou oslanjaju se na korišćenje radio-komunikacija i razvijenu mrežnu infrastrukturu. Pouzdanost sistema je povećana uvođenjem novih tehnika prenosa (prenos u proširenom spektru DS, FH) ali je još uvek zavisna od funkcionisanja mrežne infrastrukture i postaje veoma nesigurna i ranjiva na izviđanje i ometanje u toku priprema i izvođenja operacija. U novije vreme, napretkom novih komunikacionih i informacionih tehnologija pojavljuju se novi koncepti komunikacionih struktura koje su robustnije, pouzdanije i fleksibilnije (samorganizujuće), posebno u taktičkim i operativnim uslovima upotrebe, u kojima posebno mesto dobijaju bežične ad hoc komunikacione mreže.

U protekloj deceniji, jedno od najatraktivnijih poglavlja u računarskoj tehnologiji i komunikacijama predstavljale su bežične tehnologije, koje su za vrlo kratko vreme privukle brojne korisnike, pretrpele brojne modifikacije i transformacije uključujući i implementaciju bežičnog Interneta [1]. Osnovu popularnosti bežičnih mreža donela je pogodnost njihovog korišćenja, mobilnost učesnika i prihvatljiva cena realizacije bežičnih mreža. Osnovno sredstvo, odnosno sve što je potrebno za povezivanje na računarsku mrežu postaje „laptop“ računar, personalni digitalni asistent (PDA), mobilni telefon...

Šta je to što su donele nove tehnologije u pogledu računarskih mreža? Bežične mreže slične su drugim računarskim mrežama – omogućavaju priključenje računara i računarski upravljanih uređaja na raču-

narsku mrežu. Osnovna razlika je u načinu konekcije, nema potrebe za uspostavljanjem fizičke žičane konekcije, nema razvlačenja kablova. Promenjen je prenosni medijum – sve bežične tehnologije koriste radijski deo elektromagnetnog spektra. Izostanak fizičke konekcije omogućio je korisnicima da se kreću u prostoru i da rade kako žele uz pun pristup računarskoj mreži. Naravno, ova pogodnost donela je s druge strane povećane probleme u konceptu sigurnosti i zaštite podataka. Za razliku od žičanih mreža koje mogu biti fizički zaštićene i sa lako izvodljivom kontrolom pristupa, bežične mreže se vrlo teško štite. Prenosni medijum je otvoren za proizvoljan pristup, i paketi podataka su dostupni svima koji raspolažu potrebnom opemom da iz radio-signalu prihvate podatke i dekoduju informaciju. Sva zaštita informacija počiva na kriptovanju što s jedne strane utiče na povećanje cene realizacije mreže, a s druge strane utiče na smanjenje ukupnih performansi mreže [2]. Pokretljivost učesnika prouzrokuje još jedan problem koji nije bio prisutan u žičnim mrežama, a to je problem autonomnog napajanja električnom energijom elemenata mreže, i iznalaženja novih tehnologija konzervisanja energije, „inteligentnih“ algoritama potrošnje i „štedljivih“ potrošača [3].

Klasifikacija bežičnih mreža

Bežične mreže se mogu klasifikovati u dve osnovne kategorije [4]:

- infrastrukturno zasnovane bežične mreže:
 - celularne mobilne mreže (mobilna telefonija),
 - bežične računarske mreže;

– ad hoc bežične mreže kao mreže koje ne zahtevaju bilo kakvu infrastrukturu za rad:

- mobilne ad hoc mreže,
- senzorske ad hoc mreže (mreže autonomnih senzorskih uređaja).

Bežične računarske mreže mogu se podeliti u tri osnovne grupe.

Bežične mreže na daljinu (Wireless Wide Area Network – WWAN), koje pokrivaju relativno velike geografske prostore i koriste radio i satelitske linkove. Obično se koriste za pokrivanje velikih univerzitetskih centara i gradova. U principu su fleksibilnije, jednostavnije za instaliranje i održavanje, i jeftinije po ceni priključka nego tradicionalne žične mreže.

Lokalne bežične mreže (Local Area Network – WLAN) omogućavaju da računari na jednoj geografskoj lokaciji dele informacije i zajedničke uređaje (štampači, baze podataka). Omogućeni su isti servisi kao i u žičnim mrežama. Imaju niz prednosti u odnosu na žični LAN – mobilnost, fleksibilnost, skalabilnost, brzina protoka, jednostavnost i smanjenje troškova instalacije. Neophodne su u situacijama kada, zbog arhitektonskih, geografskih ili drugih razloga, nije moguće ostvariti druge načine formiranja mreže. U osnovi, bežične mreže zahtevaju određenu infrastrukturu: bežične PC kartice u umreženim računarima, pristupnu tačku (Access point), bežični PC adapter i mrežnu konekciju za pristupnu tačku. Potrebna je samo jedna pristupna tačka za jednu WLAN konekciju. Ograničavajući faktor primene je relativno kraći domet veze (30–300 m) i frekvencijski opseg. Ako je potrebno premostiti veća rastojanja koriste se dodatne antene sa pojačivačima za podizanje nivoa signala.

Personalizovane ili lične mreže (Personal Area Network – PAN) su mreže koje omogućavaju komunikaciju prvenstveno elektronskih uređaja unutar prostora od nekoliko metara i razmenu komunikacionih i sinhronizacionih informacija. Tu su pre svega infracrvene mreže (Infrared) za konekciju elektronskih uređaja na vrlo kratkim rastojanjima u okviru ograničene radne prostorije i blutut (Bluetooth) mreže. Blutut tehnologija je zasnovana na principu ugradnje pojedinačnih elektronskih modula (čipova) u elektronske uređaje koji omogućavaju bežičnu komunikaciju između njih, a mogu se i računari sa blutut modulima priključiti na Internet. Blutut koristi frekvencijski opseg 2,402–2,480 GHz, u režimu frekvencijskog skakanja (frequency hopping) do 1600 hop/s, sa standardnom brzinom protoka podataka od 720 kb/s i ograničenim dometom od 10 cm do 10 m [5]. Podržava „point-to-point“ i „point-to-multipoint“ konekciju. Blutut komponente na jednoj mikrolokaciji čine tzv. piconet (pickonet) sa sopstvenom šemom frekvencijskog skakanja, a mreža se formira povezivanjem dva piconeta. Blutut komponente su našle široku primenu u senzorskim mrežama (očekuje se da će blutut tehnologija 2005. biti ugrađena u preko 670 miliona uređaja) [6].

WLAN standardi IEEE 802.11x

Standardizacija u bežičnim lokalnim računarskim mrežama definisana je od strane IEEE.802.11 radne grupe. WLAN je pokriven sa tri varijante standarda: 802.11b, 802.11a i 802.11g [2].

Prvi standard 802.11b pojavio se 1999. godine. Definiše mrežne uređaje za

rad u frekvencijskom opsegu 2,4 do 2,4835 GHz, sa brzinama prenosa do 11 Mb/s (mogućnost rada sa smanjenim brzinama 1, 2 i 5,5 Mb/s pri većim interferencijama i slabljenju signala).

Standard 802.11a (2001) povećao je brzinu prenosa do teorijskog maksimuma od 54 Mb/s i definiše rad u različitim frekvencijskim opsezima 5,15–5,35 GHz i 5,725–5,825 GHz (rad u različitim opsezima nije kompatibilan sa standardom 802.11b).

Standard 802.11g obezbeđuje kompatibilnost sa 802.11b hardverom za rad u frekvencijskom opsegu 2,4 GHz, ali sa brzinama prenosa do 54 Mb/s po standardu 802.11a.

Bežične ad hoc mreže

Bežične ad hoc računarske mreže, za razliku od standardnih bežičnih mreža, ne zahevaju postojanje fiksne infrastrukture za rad, i pogodne su za organizaciju i uspostavu mrežne komunikacije i u uslovima kada je infrastruktura bežičnih mreža oštećena ili uništena (spasilačke akcije, zemljotresi, poplave, ratna razaranja, ratna dejstva, što znači da se komunikacija mora uspostaviti i bez prethodnog organizovanja komunikacione infrastrukture.

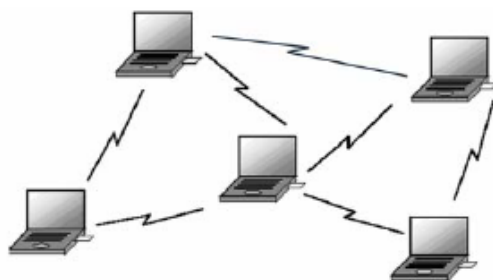
Ad hoc bežične mreže su po definiciji mreže dinamičkih autonomnih mrežnih čvorova koji komuniciraju jedni s drugima formirajući „multihop“ radio-mrežu i održavajući konektivnost u decentralizovanoj strukturi upravljanja. Čvorovi se mogu lako i brzo priključiti ili isključiti iz mreže, mreža je mobilna a prenosni medijum je javni. Čvorovi komuniciraju preko bežičnog linka, u

ambijentu radio-veze uz prisustvo šuma, fedinga i interferencije signala. Pored toga linkovi imaju obično uži propusni opseg nego u fiksnim mrežama [1]. Svaki čvor u bežičnoj ad hoc mreži funkcioniše i kao „host“ i kao ruter, a upravljanje mrežom je distribuirano na mrežne čvorove. Mrežna tehnologija je dinamična zato što povezanost čvorova u mrežu može da se menja sa vremenom – tako što neki čvorovi mogu ispasti iz mreže zbog neispravnosti, gubitka energije ili uništenja, u mrežu se u toku rada mogu povezati novi čvorovi, a tu je i verovatna prisutnost mobilnih (pokretnih) čvorova koji zbog dinamike svog položaja mogu iskakati i vraćati se u mrežu.

U ad hoc mrežama poruka se prenosi (propagira) kroz mrežu koristeći čvorove kroz koje prolazi kao kroz spojnice (svičeve), što zahteva od svakog čvora da mora imati mogućnost rutiranja. Poruka se efektivno prenosi sa jednog mobilnog čvora na drugi, bez potrebe za pristupnim tačkama i drugim mrežnim elementima strukturiranih bežičnih mreža. Time se omogućuje da mrežni čvorovi mogu da komuniciraju na daleko većem rastojanju od svog dometa, zahvaljujući prisustvu drugih mrežnih čvorova koji su u dometu izvorišnog čvora i koji žele ili mogu da pošalju dalje primljeni paket, prosleđujući ga do njegovog odredišta. Dolazi do pojave višestrukih bežičnih skokova, jer paket prelazi sa jednog mobilnog čvora na drugi sve dok ne stigne na odredište pa odatle i ime – multihop po putanjama, odnosno kroz privremeno formiranu ili ad hoc mrežu. Veličina i prostornost ad hoc mreža varira značajno sa karakteristikama prenosnog medijuma i primenjenim protokolom rutira-

nja. Ad hoc mreže su naročito pogodne za aplikacije koje zahtevaju od korisnika da komuniciraju upotrebom mobilnih uređaja (PDA, laptop, mobilni telefon) (slika 1). Osnovne prednosti ovakvog pristupa su jednostavnost instalacije i nadogradnje, skromni zahtevi za servisima postojeće infrastrukture, niska cena, jednostavno održavanje i velika fleksibilnost [1].

Osnovna razlika između opisanih mobilnih i ranije pomenutih senzorskih ad hoc mreža je u tome što je kod senzorskih mreža krajni cilj detekcija–estimacija nekih događaja od interesa, a kod mobilnih ad hoc mreža komunikacija.



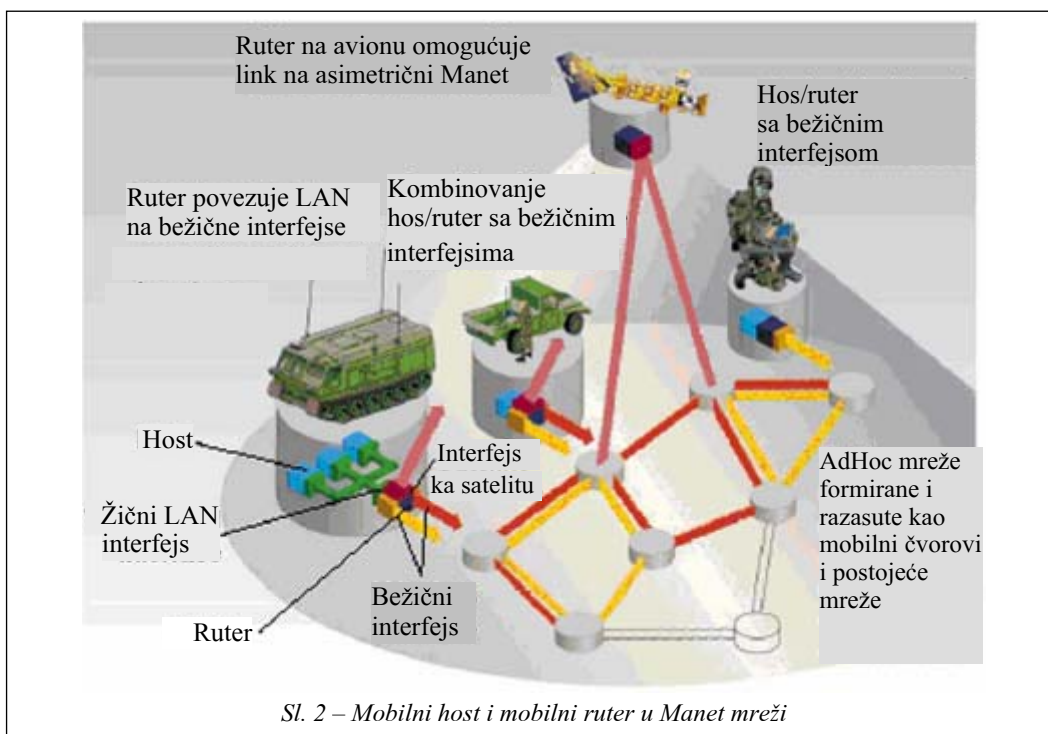
Sl. 1 – Primer mobilne ad hoc mreže

Mobilne ad hoc mreže (Manet)

Mobilne ad hoc mreže (Manet) predstavljaju bežičnu komunikacionu mrežu nezavisnih autonomnih mobilnih korisnika koji obavljaju međusobnu komunikaciju preko bežičnih linkova. Pošto su čvorovi mobilni, mrežna topologija se menja vrlo brzo tokom vremena i može biti potpuno nepredvidiva. Mrežno upravljanje je decentralizovano, sve aktivnosti čvorova, uključujući „otkrivanje“ topologije mreže i isporuka poruka moraju se odvijati u samim čvorovima – što znači da je funkcija rutiranja inkorporirana u

mobilne čvorove. Set aplikacija za Manet je veoma raznolik, počev od malih, statičkih mreža koje su ograničene i u pogledu resursa napajanja, do velikih, mobilnih vrlo dinamičkih mreža. Da bi ovako definisana, nekoegzistentna mreža funkcionisala potrebni su vrlo složeni distributivni algoritmi koji pored ostalog moraju da ostvare determinisanje mrežne organizacije, dostupnost linkova i šeme rutiranja. U ovako fluktuirajućoj mrežnoj topologiji nije moguće jednoznačno unapred da se determiniše problem i moguće relacije pa je neophodno da mreža ima mogućnost samoorganizovanja i prilagođavanja trenutnoj situaciji [9]. Svaki čvor u mreži logički se sastoji iz rutera, procesorskog modula i modula za bežičnu komunikaciju. Čvor može da se sastoji od odvojenih mrežnih uređaja ili su oni integrisani u jedan uređaj kao što je to laptop računar ili PDA uređaj.

Set čvorova koji čini Manet osnova je mobilne rutirajuće infrastrukture („mobile routing infrastructure“) i može da radi izolovano kao zasebna mrežna struktura ili da bude konektovana u veći Internet preko spoljnih rutirajućih funkcija. Dok je u statičkoj mreži putanja od izvora do odredišta optimalna putanja (ruta), ovakva pogodnost nije jednostavno primenljiva kod ad hoc mreža. Faktori, kao što su promenljivi kvalitet bežičnih linkova, slabljenje na propagacionim putanjama, fading, interferencija signala, potrošnja energije, promena topologije postaju relevantni parametri komunikacije. Da bi se ublažilo negativno dejstvo ovih parametara mreža mora biti osposobljena da prilagodi putanje rutiranja pronalazeći optimalni prenosni put. Pored toga, naročito za vojnu primenu, mreža



treba da obezbedi dovoljnu zaštitu informacija, otpornost na izviđanje i ometanje, pouzdan rad i u uslovima namernog ometanja, brzi oporavak mreže u slučaju otkaza čvorova.

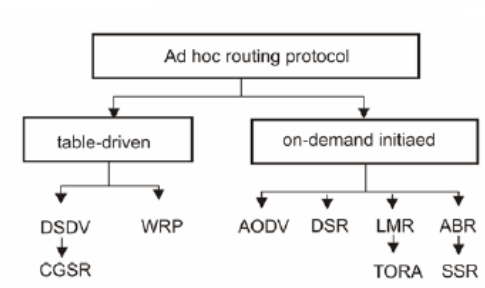
Jedan primer primene Manet mreža u vojnim taktičkim komunikacijama prikazan je na slici 2.

Senzorske ad hoc mreže

Senzorske ad hoc mreže imaju široku primenu u monitorisanju sredine, osetljivih instalacija, daljinskog prikupljanja podataka i analize. Kao i u Manet mreži, čvorovi u mreži se ponašaju i kao hostovi i kao ruteri, a mreža radi u tzv. samoorganizujućoj i adaptivnoj vrsti rada. Radi se uglavnom o mrežama relativno jeftinih višefunkcionalnih senzora, malih di-

menzija i smanjene potrošnje energije. Ovako definisani senzorski čvorovi sastoje se uglavnom od senzorskih elemenata, modula za procesiranje signala, modula za komunikaciju i umrežavanje u senzorske mreže (slika 3). Pored toga čvorovi mogu sadržati i module za pozicioniranje, module za mobilnost, dodatne izvore napajanja i drugo.

Senzorske ad hoc mreže mogu da se sastoje od velikog broja senzorskih čvo-



Sl. 3 – Komponente senzorskog čvora

rova (od nekoliko desetina ili stotina, do više stotina hiljada čvorova) koji su gusto rasuti u prostoru pokrivanja, ali bez unapred određenog raspoređivanja. Senzori se mogu rasejavati izbacivanjem iz letelica, artiljerijskih oruđa, ili ih mogu polagati specijalni roboti, a mogu funkcionisati iz pokreta ili kao stacionarni elementi. Ovo znači da protokoli rutiranja moraju da poseduju sposobnost samoorganizovanja i kooperativnosti između mrežnih senzorskih čvorova i da obezbede funkcionisanje senzorske mreže kako u samoj fazi razvijanja i rasejavanja čvorova, tako i po njihovoj stacionarnosti u određenom reonu upotrebe.

Kod senzorskih mreža osnove razmatranja čine arhitektura, rad, razvoj i lokalizacija komponenti. Senzorski čvorovi imaju izrazito velika ograničenja u napajanju električnom energijom, traju koliko im traje i napajanje, koriste sofisticirane konzervacione tehnike za produženje „životnog veka“, a na potrošnju veliki uticaj imaju i ugrađeni algoritmi rutiranja.

Brojne su aplikacije senzorskih ad hoc bežičnih mreža:

- u vojnim primenama to je, na primer, detekcija kretanja neprijateljskih sredstava, detekcija i praćenje prisustva opasnih materija (otrovni gasovi, radijacija, eksplozivni materijali), kontrola kontaminiranih prostora, kontrola povrede štićenih prostora i sl.,

- kontrola i zaštita potencijalnih terorističkih ciljeva,

- ekološke senzorske mreže za monitorisanja čovekove okoline (ravnicama, planinama, pustinjama, okeanski prostor, atmosfera),

- kontrola saobraćaja na prometnim i magistralnim putevima, raskrscima,

mostovima i sl. sa praćenjem elemenata kretanja i vrste vozila,

- kontrola i upravljanje parkiralištima u velikim gradovima, sa detekcijom i lokalizacijom zauzetih i slobodnih parkiranih mesta,

- kontrola pristupa u i unutar štićenih objekata i prostora,

- kontrola i zaštita u velikim robnim prodavnicama, parking garažama i drugim javnim objektima i sl.

Nove tehnologije i niska cena komponenti utiču na sve širu i masovniju upotrebu bežičnih senzorskih mreža i u drugim oblastima.

Protokoli rutiranja

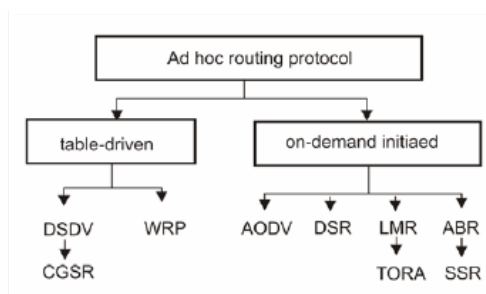
Jedan od glavnih problema koje treba rešiti u ad hoc mrežama, a koji proizilazi iz načina rada mreža, velikog broja čvorova i neophodnog svojstva samoorganizovanja mreže, jeste pitanje rutiranja paketa u mreži u kojoj se svaki čvor mora tretirati kao ruter.

Postojeći protokoli rutiranja, koji se koriste u konvencionalnim mrežama kao što su algoritmi tipa „distant“ vektora ili „link state“, teško su upotrebljivi u ad hoc uslovima. Periodične informacije o ažuriranju topologije mreže šalju se i kada nema nikakve promene što dovodi do povećane potrošnje propusnog opsega; čvorovi se redovno „bude“ za primanje i slanje informacija o rutiranju koje nisu uvek potrebne pa se energetska potencijala čvorova brzo troše; smanjena je skalabilnost mreže jer je velika količina informacija koja putuje kroz mrežu saglasno velikom broju mrežnih čvorova – velika količina informacija o rutiranju koje se redovno emituju i opterećuju mrežu; ve-

liki je broj rutera pa je verovatnoća redundantnih ruta veoma velika; sistem postaje vrlo inertan da odgovori na brze dinamičke promene mrežne topologije. To je dovelo do razvoja tzv. protokola na zahtev (on-demand protocol). Umesto periodičnog oglašavanja ruta, ruta se otkriva samo kada je potrebna, tj. na zahtev što dovodi do smanjenja saobraćaja kroz mrežu. Kada su u pitanju senzorske mreže, ograničenje kapaciteta procesorsko-memorijskih resursa, prioritet u izboru algoritma imaju brzina, pouzdanost i jednostavnost.

Na slici 4 prikazan je pregled najčešće korišćenih algoritama rutiranja u ad hoc mrežama.

Svaki od algoritama prilazi problemu iz različitog ugla i koristi različite pretpo-



Sl. 4 – Algoritmi ad hoc rutiranja:

DSDV – rutiranje sa vektorom rastojanja uz sekvencirane destinacije (Destination Sequenced Distance Vector Routing), WRP – protokol za bežično rutiranje (Wireless Routing Protocol), CGSR – rutiranje sa grupisanim gejevima (Clusterhead Gateway Switch Routing), AODV – ad hoc rutiranje na zahtev sa vektorom rastojanja (Ad Hoc On-Demand Vector Routing), DSR – dinamičko rutiranje sa prikupljanjem adresa (Dynamic Source Routing), LMR – jednostavno mobilno rutiranje (Lightweight Mobile Routing), TORA – vremenski uređeni algoritam za rutiranje (Temporally Ordered Routing Algorithm), ABR – asocijativno rutiranje (Associativity Based Routing), SSR – rutiranje sa stabilnim signalom (Signal Stability Routing)

stavke, pa ni jedan nije univerzalno primenljiv već zavisi od primene. Primera radi, razmotriće se rad DSR algoritma. Ruta se određuje dinamički i samo onda kada je potrebna. Nema periodičnog emitovanja rutera vezano za rutiranje informacije. Kada pošiljalac hoće da pošalje paket, on prvo proverava sadržaj informacije u rutiranju u svojoj memoriji. Ako u njoj postoji validan ulaz za odredište, paket se šalje koristeći sekvencu čvorova koja se nalazi u rutiranje kešu (čuva se skup svih čvorova kroz koje će paket putovati), a ako nema validne rute do odredišta pošiljalac započinje proces otkrivanja rute, što je osnovna ideja svih on-demand algoritama, i potom paket putuje kroz mrežu tražeći odredišni čvor [1].

Ovaj algoritam karakteriše veoma laka implementacija, mogućnost rada sa asimetričnim linkovima, štednja propusnog opsega i energije jer nema oglašavanja, protokol se lako modifikuje i održava. S druge strane, postoji dodatno zauzimanje propusnog opsega zbog prirode rutiranja jer paket rapidno raste u toku propagacije kroz mrežu pošto čuva adrese svih prolaznih čvorova. Kod većih mreža raste veličina poruka i može da dođe do „zagušenja“, odnosno nemogućnosti normalne komunikacije, pa je ovaj protokol pogodan za mreže sa manjim brojem mobilnih čvorova. Pored toga prisutan je i problem sigurnosti u pogledu raspoloživosti, poverljivosti, identifikacije, autentifikacije i neporicanja – posebno u uslovima mogućih spoljnih pretnji ubacivanja pogrešnih informacija u mrežu kao i unutrašnjih pretnji koje dolaze od kompromitovanih čvorova koji mogu da oglašavaju pogrešne rutiranje informacije. Ovo znači da se moraju štititi i podaci i rutiranje informacije.

Specifičnost senzorskih mreža ima dodatna ograničenja u izboru algoritama. Razmotriće se rad AODV algoritma koji definiše tri tipa poruka: zahtev za rutom, odgovor na rutu, grešku na ruti i tri tipa čvorova – master, gateway i slave. Tokom inicijalizacije sistema formiraju se pikonet mreže, svaki čvor kreira tabelu suseda (u pikonetu) i ruting tabelu. Sistem zatim formira pikonet mreže sa master-slave komunikacijom, a čvorovi koji su članovi dva ili više pikoneta su gateway čvorovi. Slave čvorovi, u okviru pikoneta, šalju pakete masteru, a on ih prosleđuje na odgovarajući gateway, sve dok ne stignu u pikonet odredišnog čvora. Server, odnosno čvor na kome se nalazi ekspertski sistem, komunicira sa svim ostalim čvorovima, dok ostali čvorovi šalju svoje podatke samo serveru. Algoritam raspolaže i tehnikom ulaska novog čvora u pikonet i eliminisanja redundantnih pikoneta što doprinosi smanjenju nepotrebnih konekcija tokom otkrivanja rute. I kod ovog algoritma sa povećanjem broja čvorova raste i verovatnoća kolizije na kanalu.

Primena senzorskih ad hoc mreža

Kao što je rečeno, široka je mogućnost primene bežičnih senzorskih ad hoc mreža. Pomoću razvijene infrastrukture moguće je napraviti različite bežične proizvode, a primena može biti od industrijske do kućne i zabavne. U vojnim primenama, na primer, pored navedenih, jedna od bitnih karakteristika funkcionalnosti jeste i saradnja čvorova na procesiranju signala i informacija. Dok je senzorski podatak lokalizovan u svakom čvoru, informacioni sadržaj koji

treba da ekstrahuje mreža je globalan i kao takav mora biti rezultat saradnje i zajedničkog rada čvorova.

Radi ilustracije, posmatraće se jedan hipotetički primer upotrebe ad hoc senzorske mreže, u slučaju ekološke opasnosti (slika 5) [11]. Na delu teritorije blizu velikog grada došlo je do akcidenta na gasnim postrojenjima i do izliva opasne materije u vazduh.



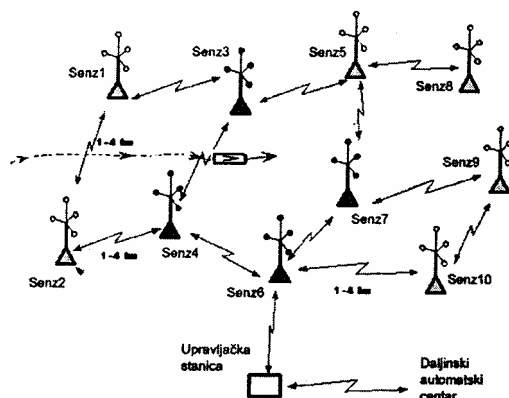
Sl. 5 – Praćenje akcidentnog gasnog oblaka distribuiranom senzorskom ad hoc mrežom

Aktiviraju se jedinice za specijalna dejstva koje pored ostalog treba da evakušu građane i zatvore mostove i saobraćajnice. Sada dolazi na red organizovanje ad hoc mreže. Radi realne procene opasnosti aktiviraju se bespilotne letelice snabdevene velikom količinom minijaturnih hemijskih senzora (reda nekoliko hiljada) i iz letelica se vrši njihovo rasejavanje u akcidentnoj zoni i smeru prema gradskoj zoni. Senzori, odnosno čvorovi se, odmah po izbacivanju, samoorganizuju u ad hoc mrežu sa zadatkom da daju bitne podatke za nastalu situaciju a to su:

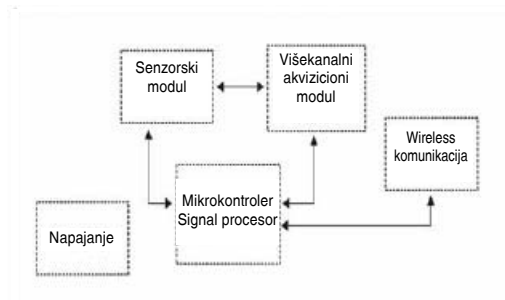
lokacija mesta događaja, vrsta opasnosti, veličina oblaka, smer i brzina kretanja i koncentracija štetnih materija.

Drugi primer je saobraćajnica koju treba pratiti u slučaju nailaska neprijateljskih vozila. U ovom slučaju iz letelice su izbačeni magnetometarski senzori (desetak komada), koji se još u toku leta samoorganizuju u mrežu i odmah po prizemljenju spremni su za rad. Pri nailasku vozila inicira se detekcija i generiše informacija, koja u saradnji sa drugim sensorima može sadržati i podatke o vrsti vozila, brzini pa i smer kretanja.

Sličan ovome je i problem koji nas interesuje. Korišćenjem inteligentnih akustičkih senzora, prostorno razmeštenih, i pasivnog zvukometrijskog izviđanja treba pokriti određenu teritoriju i detekcijom zvučnih izvora otkriti pokretni cilj, odrediti njegove koordinate i praćenjem njegovog kretanja odrediti njegovu trajektoriju. Potrebno je predložiti tehničke elemente mrežne računarske infrastrukture koja bi podržala ovu aplikaciju. Osnovna pretpostavka situacije na terenu data je na slici 6. Sistem treba da bude koncipiran kao distributivna senzorska bežična ad hoc mreža koja se sastoji iz većeg broja



Sl. 6 – Primer senzorske ad hoc mreže na terenu



Sl. 7 – Koncept stanice – senzora za zvukometrijsko izviđanje

identičnih inteligentnih senzorskih stanica, prostorno razmeštenih i komunikacijski povezanih u jedinstvenu ad hoc mrežnu strukturu za pokrivanje posmatrane teritorije. Cilj bi trebalo da istovremeno otkriju i prate bar četiri senzorske stanice tokom čitavog kretanja u zadatom sektoru. Sistem treba da ima mogućnost obrade signala u svakom senzorskom čvoru, međusobnu razmenu podataka i saradnju između čvorova i prenos podataka do glavnog hosta gde se vrši prikupljanje i obrada informacija i donošenje odluka. Koncept tehničkog rešenja senzorske stanice prikazan je na slici 7.

Zaključak

Problematika izložena u ovom radu vezana je za istraživanje tehničkih rešenja bežičnih ad hoc mreža sa senzorskim stanicama kao mrežnim čvorovima i njihovom povezivanju u šire mrežne strukture.

Visoka pouzdanost opažanja, niska cena, brz razvoj karakteristika, tolerancija na pojavu greški i fleksibilnost senzorskih ad hoc mreža omogućuju kreiranje novih i inoviranje postojećih aplikacija u implementacijama daljinskog upravljanja sensorima. Međutim, u realizaciji senzorskih ad hoc

mreža mora se voditi računa i o ograničenjima implementacije koja se tiču skalabilnosti mreže, cene, potrebnog hardvera, zaštite informacija, promene topologije, uslova rada okruženja i potrošnje električne energije. Mogućnost razvoja sistema za kontrolu i zaštitu teritorije bez potrebe izgradnje fiksne infrastrukture od izuzetnog je značaja u vojnim primenama, posebno sa aspekta pripreme i vođenja savremenih operacija.

Literatura:

- [1] Milanović, N.: Senzorske mobilne bežične mreže, ETF, Beograd, 2002.
- [2] Sutton, M.: Hacking the invisible network, Insecurities in 802.11x, iDefense Inc. 2002.
- [3] Crow, B. P. and all.: IEEE 802.11 Wireless local area networks, IEEE Communications Magazine, Sept. 1997.
- [4] Mobile ad hoc and sensor networks – Tutorial, Faculty of engineering, KMINTB (King Mongkut's Institute of Technology North Bangkok), 2003.
- [5] Liddle, D.; Smitton, S.: Wireless networks, Networked service policy, UKOLN, University of Bath.
- [6] Milanović, N.; Malek, M.; Milutinović, V.: Standardization effort for routing and security in ad hoc networks, July 2003.
- [7] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam and Erdal Cayirci, A survey on sensor networks, IEEE Communications Magazine, vol. 40, no. 8, August 20.
- [8] Royer, E. M.; Ton, C.: A review of current routing protocols for ad hoc mobile wireless networks, IEEE Personal Communications, April 1999.
- [9] Corson, M. S. and sar.: Internet based mobile ad hoc networking, IEEE Internet computing, Jul-Avg. 1999.
- [10] Nasipuri, A.: Mobile ad hoc networks, University of North Carolina, Charlotte, 2003.
- [11] Liu J. and sar.: A dual-space approach to tracking and sensor management in wireless sensor networks, Palo Alto Research Center, Report P2002, Mar. 2002.