PREDLOG AD HOC RAČUNARSKE MREŽE NA KATEDRI VOJNIH ELEKTRONSKIH SISTEMA VA PRIMENOM BLUETOOTH TEHNOLOGIJE

Terzić R. *Miroslav,* Vojna akademija, Katedra vojnih elektronskih sistema, Beograd

UDK: 621.39:654.16]:004.7

Sažetak:

U profesionalnim organizacijama gde ne postoji mrežna infrastruktura za povezivanje računara u lokalne mreže (LAN) prelazi se na druga (alternativna) rešenja. Ukoliko je organizacija razmeštena u jednom objektu i razmak između najudaljenijih tačaka (računara) nije veći od 100 m povezivanje je moguće realizovati u ad hoc mrežama primenom bluetooth modula. U radu je predložena ad hoc računarska mreža Katedre vojnih elektronskih sistema primenom bluetooth tehnologije.

Ključne reči: *bluetooth, ad hoc, računarska mreža, Katedra vojnih elektronskih sistema, bezbednost.*

Uvod

Početak novog milenijuma predstavlja prekretnicu u razvoju bluetooth modula. Bluetooth je otvoren standard za digitalni radio malog dometa. Odlikuje se niskim troškovima, malom snagom i tehnologijom niskog profila, koja obezbeđuje mehanizme za stvaranje malih bežičnih mreža zasnovanih na trenutnim potrebama. Pored toga, nudi brz i pouzdan prenos i glasa i podataka. Zbog navedenih odlika bluetooth moduli postaju standardne komponente većine elektronskih sistema od mobilnih telefona, ličnih digitalnih asistenata (PDA), preko jedinica za industrijsku kontrolu do kućnih uređaja. Bluetooth je prvobitno bio zamišljen kao zamena za kablove u bežičnim komunikacijama. Međutim, članovi SIG (zajednica sa posebnim interesovanjima za specifična područja tehnike) planiraju razvoj širokog spektra korisničkih uređaja i poboljšanje bežičnog povezivanja. Danas je bluetooth standardizovan unutar IEEE 802.11 PAN radne grupe formirane početkom 1999. godine. Današnje ad hoc mreže su primarno bazirane na bluetooth tehnologiji. Tokom realizacije ad hoc mreža primenom bluetooth modula posebnu pažnju treba posvetiti aspektu bezbednosti.

terzicmiroslav@yahoo.com

U radu je opisana lokalna računarska mreža primenom bluetooth tehnologije koja bi se mogla koristiti na Katedri vojnih elektronskih sistema Vojne akademije. Predložena računarska mreža doprinosi povećanju efikasnosti organizacije i rada katedre. Zbog određenih nedostataka koji se javljaju kod komunikacija primenom bluetooth modula, deo rada opisuje i bezbednosni aspekt predložene mreže.

Organizacija katedre vojnih elektronskih sistema vojne akademije

Katedra Vojnih elektronskih sistema (VES) Vojne akademije obavlja sve poslove koji se odnose na: organizaciju i rad katedre, planiranje, organizaciju i realizaciju nastave, vežbi i posebnih oblika nastave iz matičnih predmeta; kontrolu i praćenje realizacije nastave, ispita i ostalih zadataka; planiranje i realizaciju vojnostručne obuke pripadnika katedre; planiranje i realizaciju naučnoistraživačkih projekata iz matičnih oblasti od interesa za Vojsku Srbije; održavanje i unapređenje nastavne materijalne baze; vođenje propisane nastavne dokumentacije i dr.

Na Katedri vojnih elektronskih sistema obrazuju se sledeće uže unutrašnje jedinice:

1. Odsek za radarske i elektronske sisteme,
2. Odsek za raketne sisteme i sisteme upravljanja vatrom,
3. Odsek za elektroopremu vazduhoplova,
4. Odsek vojnih telekomunikacionih sistema i elektronskih dejstava, i
5. Grupa nastavnika za zaštitu informacija (slika 1).

Slika 1 – Organizacija Katedre VES

Pripadnici Katedre vojnih elektronskih sistema razmešteni su u 19 kancelarija u jednoj zgradi na dva nivoa. Načelnik Katedre i šefovi odseka nalaze se u zasebnim kancelarijama, dok su u ostalim kancelarijama jedan do dva pripadnika Katedre VES. Svaka kancelarija opremljena je računarima. Razmak između dve najudaljenije kancelarije nije veći od 30 m linijom optičke vidljivosti. U zgradi ne postoji adekvatna mrežna struktura, pa bi lokalno umrežavanje računara primenom LAN tehnologije iziskivalo, pored ostalog, i određene građevinske radove, što u ovom trenutku nije izvodljivo. Otežavajuću okolnost predstavlja i reorganizacija Katedre VES, koja se odvija u skladu sa akreditacijom Vojne akademije.

Imajući u vidu navedena ograničenja jedno od rešenja za povezivanje računara na Katedri VES predstavlja *ad hoc računarska mreža primenom bluetooth tehnologije*.

Koncept ad hoc računarske mreže na katedri vojnih elektronskih sistema primenom bluetooth tehnologije

Bluetooth je bežična tehnologija povezivanja uređaja na kratkim rastojanjima koja primenjuje male snage zračenja. Dizajnirana je kao zamena za kablovske sisteme povezivanja, kao i druge tehnologije kratkog dometa (kao što je infracrveno zračenje IrDA). Bluetooth se primenjuje u personalnom okruženju koje se proteže u radijusu do 100 m.

Bluetooth obezbeđuje tri različite klase upravljanja snagom. Uređaji prve klase (najveće snage) imaju izlaznu snagu od 100 mW i domet do 100 m. Uređaji druge klase imaju izlaznu snagu 2,5 mW i domet do 10 m. Uređaji treće klase (najmanje snage) imaju izlaznu snagu od 1 mW i domet od 10 cm do 10 m. To je sažeto prikazano u tabeli 1.

Tabela 1

Klase uređaja prema snazi

Tip	**Snaga**	**Nivo snage**	**Operativni domet**
Klasa 1	visoka	100 mW (20 dBm)	do 100 m
Klasa 2	srednja	2.5 mW (4 dBm)	do 10 m
Klasa 3	niska	1 mW (0 dBm)	10 cm – 10 m

Osnovne karakteristike bluetooth tehnologije prikazane su u tabeli 2.

Tabela 2

Osnovne karakteristike bluetooth tehnologije

Karakteristika	**Opis**
Fizički sloj	Prošireni spektar sa frekventnim skakanjem (FHSS)
Frekventni opseg	2,4–2,4835 GHz (ISM opseg)
Frekvencija skakanja	1600 hops/s
Brzina prenosa	do 3 Mbps
Bezbednost mreže i podataka	Tri režima bezbednosti (bez, nivo linka i nivo servisa), dva nivoa poverenja u uređaj, tri nivoa bezbednosti servisa. Sekvencijalno šifrovanje za poverljivost, pitanje–odgovor za autentikaciju. Ključevi na osnovu PIN–a i ograničeno upravljanje.
Operativni domet	Oko 10 m do 100 m
Prednosti	Nisu potrebne žice i kablovi. Moguć prolaz kroz zidove i druge prepreke. Troškovi u opadanju. Mala snaga i minimalni hardver.
Nedostaci	Mogućnost preplitanja sa drugim korisnicima ISM opsega. Relativno niska brzina prenosa. Oticanje signala izvan željenih granica.

Najznačajniji detalji tehničkih specifikacija za povezivanje korišćenjem bluetooth tehnologije su:

– bluetooth uređaji formiraju pikomreže (bežične ad hoc mreže za mobilne uređaje) i dele zajednički komutacioni kanal. Ukupni kapacitet kanala je 723,2 kb/s, odnosno 2,1 Mbps kod novijih uređaja. Zaglavlja i informacije o pregovaranju (handshaking) troše oko 20% kapaciteta;

– pikomreža se sastoji od upravne stanice (master) i do 7 potčinjenih stanica - klijenata (slave). Master može istovremeno biti klijent u drugoj pikomreži, ali ne može istovremeno biti master u dve pikomreže;

– više pikomreža može paralelno biti u funkciji sve dok uzajamno ometanje ne poništi koristi paralelnog rada;

– master vrši prenos u parnim vremenskim odsečcima, a klijent u neparnim. Takav prenos naziva se „duplex sa podelom vremena“ (Time Division Duplex – TDD);

– direktna komunikacija je moguća samo između master i slave ili obrnuto. Komunikacija između klijenata se usmerava preko mastera;

– svi uređaji imaju mogućnost da budu ili master ili klijent. U opštem slučaju uloga mastera dodeljuje se uređaju koji inicira komunikaciju;

– između uređaja postoje dva načina prenosa podataka: SCO (sinhrona konekcija) za prenos zvuka ili glasa i ACL (asinhrono) za prenos podataka;

– u pikomreži mogu biti do 3 SCO linka (sa jednim, dva ili tri slave) gde svaki koristi 64000 b/s;

– SCO linkovi od tačke do tačke koriste odsečke koje rezerviše master, kako bi se izbegli problemi kolizije;

– ACL klijenti mogu vršiti prenos samo po zahtevu mastera;

– ACL je ili link od tačke do tačke ili od tačke do više tačaka (broadcast), odnosno do svih klijenata u pikomreži;

– U Evropi i SAD bluetooth koristi frekventni opseg od 2400 do 2483,5 MHz u slobodnom ISM radio-opsegu, sa 79 kanala radio-frekvencija (RF) širine 1 MHz. U praksi taj opseg iznosi od 2402 do 2480 MHz. U Japanu se koristi frekventni opseg od 2472 do 2497 MHz sa 23 RF kanala od 1 MHz;

– kanal za podatke vrši skok na slučajan način 1600 puta u sekundi sa jednog na drugi od 79 (23) RF kanala. To je frekvencijsko skakanje (frequency hopping) i smanjuje interferenciju sa drugim uređajima u ISM opsegu;

– svaki kanal je podeljen na odsečke u trajanju od 625 μs;

– paketi mogu biti dužine do 5 odsečaka;

– maksimalna snaga prenosa ograničena je na 100 mW, čime se postiže domet do oko 100 m. Uređaji male snage koriste 2,5 mW i imaju domet do 10 m;

– nivo osetljivosti definisan je tako da je u odnosu na broj pogrešnih bitova (BER – Bit Error Rate) 10^{-3}, čime se ograničava prosečna verovatnoća prijema pogrešnog bita;

– pri prenosu podataka koristi se provera redundantnosti (CRC), dok su kodovi za ispravke grešaka opcioni. Zbog toga se u slučaju detekcije greške vrši retransmisija.

Topologija mreže

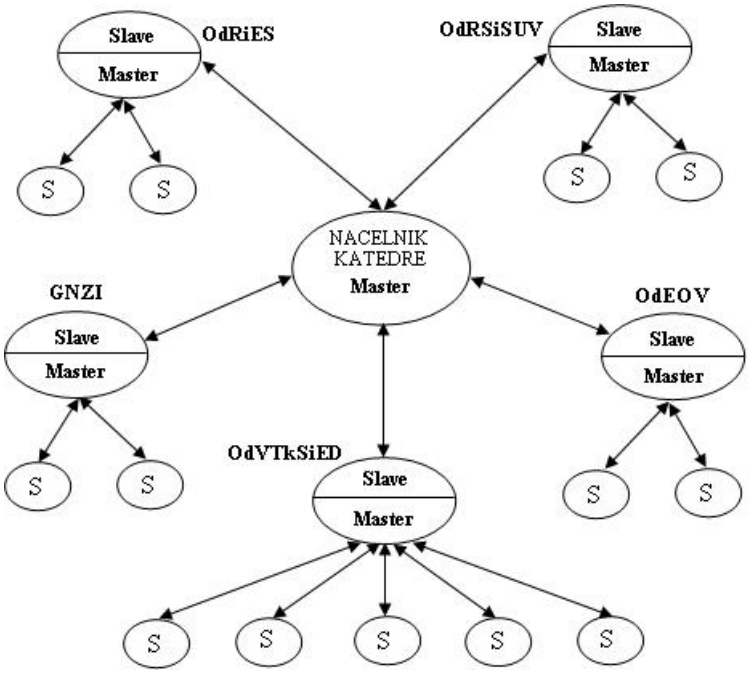
Mobilni usmerivači u bluetooth mreži kontrolišu promenjivu topologiju i tok podataka između uređaja (kompjutera) koji mogu da uspostave direktnu vezu. Uređaji se mogu pomerati (kretati) na slučajan način i mreže se moraju prekonfigurisati u hodu da bi održale topologiju. Bluetooth koristi kombinaciju tehnologije prenosa paketa i tehnologije circuit–switching.[1]

Prednost prenosa paketa je u tome što dozvoljava uređajima da šalju više paketa informacija istim putem. Pošto taj metod ne troši sve resurse, olakšava udaljenim uređajima održavanje toka podataka širom rasprostranjene mreže.

[1] Circuit-switching tehnologija odnosi se na komutaciju veze u decentralizovanim mrežama sa postojanjem redundantnih puteva za prenos podataka između dve tačke – dva korisnika. Circuit-switching obezbeđuje: podelu poruka koje se razmenjuju u blokove ili pakete i prenos paketa između čvorova metodom store and forvard – sačuvaj i prosledi.

Kada bluetooth uređaji komuniciraju međusobno formiraju takozvanu pikomrežu, koja može imati do 8 aktivnih uređaja i tri kanala za prenos glasa.

U bluetooth komunikaciji koristi se specifičan uzorak frekvencijskog skakanja, a sve pristupe kanalima kontroliše i sinhronizuje upravni uređaj. Uzimajući u obzir organizaciju Katedre vojnih elektronskih sistema, u njoj je moguće formirati 6 pikomreža. Jedna pikomreža odnosi se na vezu između načelnika katedre i šefova odseka, dok su ostalih 5 pikomreža mreže odseka. Više pikomreža formira scatternet (slika 2).



Slika 2 – Raspršena mreža Katedre VES sa pikomrežama, upravnim uređajima i klijentima

Upravni uređaj u jednoj pikomreži može biti klijent u drugoj pikomreži, a uređaji mogu istovremeno biti klijenti u više pikomreža. Za prebacivanje između pikomreža koristi se vremensko multipleksiranje. Topologija scatterneta obezbeđuje fleksibilan metod kojim uređaji održavaju višestruke veze. To može biti od velike koristi za mobilne uređaje koji često ulaze i izlaze iz okruženja drugih uređaja. Uloga uređaja (master ili slave), nakon uspostave veze od tačke do tačke sa drugim uređajem, često nema značaj za protokole višeg nivoa i korisnike.

Režimi rada

U bluetooth specifikaciji, osim normalnog aktivnog režima, postoje i osnovni režimi koji omogućavaju uštedu energije, omogućavanjem da radio-čipovi na klijentima uđu u režim parkiranja (park), osluškivanja (sniff) ili zadržavanja (hold) bluetooth konekcije (ali ne i celog uređaja). Kada uređaj nije u vezi nalazi se u stanju pripravnosti (standby).

Aktivni režim

Kada je slave u aktivnom režimu uvek „sluša“ transmisiju od mastera. Master šalje pakete aktivnim klijentima da bi očuvao sinhronizaciju i da bi im javio kada mogu da šalju povratne pakete. Klijenti u aktivnom stanju slušaju sve pakete od mastera. Ako se zna da u tom trenutku neki drugi slave komunicira sa masterom, dovoljno je da se slušaju samo zaglavlja paketa, a ne celi paketi. Aktivno stanje obezbeđuje kraće vreme odgovora ali i troši najviše energije pošto slave sve vreme prima pakete i spreman je za slanje paketa.

Režim osluškvanja

U režimu osluškivanja klijent može smanjiti potrošnju energije tako što je aktivan samo povremeno. Master može određenom klijentu slati pakete u određenim redovnim intervalima (mada ne mora to uraditi u svakom interalu). Klijent treba da sluša pakete od mastera samo na početku takvog intervala (uz određenu vremensku toleranciju). Ukoliko se paketi šalju, klijent mora da ih primi, ako ne, može biti na stand by (da „spava“) do narednog intervala. Snaga i odzivnost zavise od dužine intervala osluškivanja i biće manji u odnosu na aktivan režim.

Režim zadržavanja

U režimu zadržavanja klijent se dogovori sa masterom o trajanju zadržavanja i u tom intervalu potpuno obustavi slušanje paketa. Za to vreme slave može realizovati druge aktivnosti, poput povezivanja sa drugim uređajima, ili jednostavno „spavati“. Kada vreme zadržavanja istekne klijent nastavlja da sluša masterov paket. U režimu zadržavanja odzivnost može biti slabija od odzivnosti u režimu osluškivanja. Ušteda energije zavisi od trajanja perioda zadržavanja i od aktivnosti klijenata u tom periodu.

Terzić, M., Predlog ad hoc računarske mreže na katedri vojnih elektronskih sistema VA primenom bluetooth tehnologije, str. 111–120

Režim parkiranja

U režimu parkiranja klijenti održavaju sinhronizaciju sa masterom, ali se više ne smatraju aktivnim članovima pikomreže. Taj režim omogućava masteru da organizuje komunikaciju sa više od sedam klijenata, koliko je dozvoljeno u pikomreži, menjanjem aktivnih i parkiranih klijenata. Parkirani klijenti ostaju u sinhronizaciji periodičnim slušanjem mastera. Režim parkiranja je najmanje odzivan pošto klijent mora izvršiti tranziciju da bi postao aktivan član pikomreže, pre nego što se nastavi komunikacija. Režim parkiranja omogućava veću uštedu energije nego ostali režimi.

Bezbednosni aspekt predložene mreže

Ad hoc računarska mreža primenom bluetooth tehnologije, pored prednosti koje nudi, ima i određenih slabosti. Posebnu pažnju treba obratiti na tajnost, integritet podataka i raspoloživost mreže. Neželjenim bezbednosnim propustima korisnka uređaja, koji su manje svesni opasnosti nego administratori bezbednosti, olakšavaju se napadi na sigurnost mreže.

U osnovi, napadi su akcije koje su usmerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža. Postoje različite vrste napada, ali se oni generalno mogu klasifikovati u četiri osnovne kategorije: presecanje, tj. prekidanje (engl. interruption) – napad na raspoloživost; presretanje (engl. interception) – napad na poverljivost; izmena (engl. modification) – napad na integritet; fabrikovanje (engl. fabrication) – napad na autentičnost.

Metode zaštite

Za metode zaštite postoji nekoliko pristupa i podela. S vremenom ove klasifikacije evoluiraju i menjaju se s razvojem tehnologije i primene računarskih sistema i mreža. Prema nekim autorima postoje četiri grupe metoda zaštite: kriptografske metode, programske metode, organizacione metode i fizičke metode.

Aspekti zaštite

Aspekti zaštite često se definišu u odnosu na položaj mehanizama zaštite u računarskom ili informacionom sistemu ili računarskoj mreži. Oni često podrazumevaju sledeće nivoe:

– zaštitu na nivou aplikacije. Ona može da obuhvati, na primer, sledeće elemente: softversku zaštitu aplikacije (recimo, zaštitu od prekora-

čenja bafera), razvijanje sopstvene aplikacije za komunikaciju bluetoothom, upotrebu promenljivih i što dužih PIN-ova, izradu programa koji zahteva autentifikaciju lozinkom, izolovanje bitnih aplikacija na umreženim računarima (na primer, aplikacija koje se odnose na povezivanje sa mobilnim telefonima i PDA uređajima, aplikacija koja se odnose na internet konekciju), primenu specifičnih protokola (na primer, kriptografski zaštićenog protokola SSH, korišćenje sopstvenog šifarskog algoritma[2]);

– zaštitu na nivou operativnog sistema. Ona obuhvata i vezu operativni sistem-aplikacija za komunikaciju bluetoothom, kao i odnos prema vezama sa drugim sistemima (na primer, blokiranje nepotrebnih servisa, obezbeđivanje sveobuhvatne i obavezne kontrole na nivou korisnika, obezbeđivanje integriteta softvera koji čini operativni sistem);

– zaštitu na nivou mrežne infrastrukture. Ona se, uglavnom, odnosi na primenu mrežnih barijera (engl. firewalls), blokiranje nepotrebnih portova, šifrovanje putanje..;

– proceduralnu i operacionu zaštitu. Ovaj nivo zaštite obuhvata sledeće elemente: definisanje i sprovođenje pravila zaštite, politike i procedure, detekciju napada, sprovođenje preventivnih mera radi zaštite i smanjivanja ranjivosti sistema, upravljanje konfiguracijom sistema, podizanje svesti o sigurnosnim problemima i obrazovanje pripadnika katedre.

Zaključak

Predložena lokalna ad hoc računarska mreža može da se koristi u manjim organizacijama ili zasebnim organizacionim celinama veće organizacije. Katedra vojnih elektronskih sistema je manja organizaciona celina Vojne akademije Vojske Srbije i funkcioniše na principima jednostarešinstva i subordinacije. Nalazi se u objektu u kojem ne postoji mrežna infrastruktura za povezivanje računara u LAN. Jedno od rešenja za povezivanje računara u lokalnu mrežu, koje bi zadovoljilo ekonomski i bezbednosni aspekt, kao i principe funkcionisanja katedre, predstavlja ad hoc računarska mreža primenom bluethoot tehnologije.

Rešenje predstavljeno u ovom radu zasnovano je na iskustvima u realnom profesionalnom mobilnom okruženju, gde postoji potreba za umrežavanjem računara na kratkim odstojanjima, i može biti primenjeno na takvo i slično okruženje.

[2] Pojedini autori [7] razvili su sopstveni šifarski algoritam, nazvan MGAe2. Ovaj šifarski algoritam integrisan je u jezgro Linuks operativnog sistema, a njegova upotreba se vrši putem Ipsec bezbedosnog sistema. To znači da je sadržaj celokupne komunikacije šifrovan na IP (mrežnom) nivou OSI i TCP/IP modela i da ne postoji potreba za izmenom nosećeg bežičnog hardvera i protokola na sloju veze.

Literatura

[1] Bluetooth SIG Security Expert Group: Bluetooth™ Security White Paper (2002).

[2] Bluetooth SIG Security Expert Group: Specification of the Bluetooth system (Vol. 0–4), Covered Core Package version: 2.1 + EDR (2007).

[3] Bluetooth Technology (), 15.10. 2009.

[4] Bluetooth Tutorial (*www.palowi*reless*. com/bluetooth/infotooth/tutorial. asp*), 15. 10. 2009.

[5] Dave Singel´ee and Bart Preneel: Improved Pairing Protocol for Bluetooth (2005).

[6] Zavodnik, G.: Bezbednost bluetooth komunikacija – magistarski rad, Univerzitet Singidunum, Beograd, 2008.

[7] Vejnović, M., Jevremović, A., Šimić, G.: Primena sopstvenog šifarskog algoritma za zaštitu ajax poziva kod WEB aplikacija, ETRAN, Palić, 2008.

[8] Vejnović, M., Jevremović, A.: Uvod u računarske mreže, Univerzitet Singidunum, Beograd, 2007.

PROPOSAL FOR AN AD HOC COMPUTER NETWORK IN THE MILITARY ELECTRONIC SYSTEMS DEPARTMENT AT THE MILITARY ACADEMY APPLYING BLUETOOTH TECHNOLOGY

Summary:

The historical development of the Bluetooth module is given in the introduction of this paper. The importance of the Bluetooth standard for wireless connection on small distances is shown as well.

The organization of the Department of Military Electronic Systems is presented with its area of duties, subordinate sections and deployment.

The concept of a local area network for this Department, using Bluetooth technology, includes network topology and working regimes based on the main characteristics and technical specifications for the connection with Bluetooth technology. The Department's disperse computer network is proposed as a scatter net where one piconetwork includes the Head of Department and the Heads of Sections while other piconetworks are formed from the Heads of Sections and their subordinates.

The security aspect of the presented network deals with basic computer network attack categories, protection methods and aspects.

The paper concludes with some recommendations for the local area network using Bluetooth technology with respect to its economical and security aspects as well as to the managing principles of the Department.

Key words: *Bluetooth, ad hoc, computer network, Military Electronic Systems Department, security.*

Datum prijema članka: 25. 11. 2009.

Datum dostavljanja ispravki rukopisa: 27. 11. 2009.

Datum konačnog prihvatanja članka za objavljivanje: 28. 11. 2009.