

WLAN – brezžična lokalna omrežja

*Klemen Albreht, Rudolf Sušnik, Jaka Sodnik in Sašo Tomažič,
Fakulteta za elektrotehniko, Univerza v Ljubljani*

Povzetek — Namen članka je pregled osnovnih značilnosti brezžičnih lokalnih omrežij in prevladujočih standardov na tem področju. Posebna pozornost je posvečena načinom zagotavljanja varnosti v teh omrežjih. Opisane so osnovne značilnosti javnih WLAN omrežij in njihova primerjava z omrežji tretje generacije mobilne telefonije.

Ključne besede — WLAN, PWLAN, IEEE 802.11, BRAN, HIPERLAN, varnost, WEP, WPA

Abstract — This paper explains some basic characteristics of wireless local area networks and prevalent standards in this area. It emphasizes some security methods in wireless networks. It also describes basic characteristics of public WLAN networks and compares them with third generation mobile networks.

Keywords — WLAN, PWLAN, IEEE 802.11, BRAN, HIPERLAN, security, WEP, WPA

I. UVOD

Velika porast uporabe osebnih računalnikov po letu 1980 je porodila idejo o združevanju le-teh v lokalna omrežja. Ta so omogočala pretok in izmenjavo informacij med posameznimi uporabniki znotraj podjetij in ustanov. Nastali so t.i. informacijski otoki ali lokalna omrežja (LAN - local Area Network). Približno desetletje kasneje je Internet posamezne otoke povezal v enotno telekomunikacijsko omrežje, izmenjava različnih vrst informacij je postala preprosta in hitra.

Današnja alternativa omenjenim omrežjem LAN, ki za prenos uporabljajo prepletene dvovode in koaksialne kable ter optična vlakna, so brezžična lokalna omrežja WLAN (Wireless LAN). Služijo istemu namenu kot žična omrežja, le da za prenos informacij uporabljajo radijsko valovanje in tako omogočajo mobilnost uporabnikov. Komunikacija ni več omejena z infrastrukturo vodnikov in kablov in je zato precej fleksibilnejša.

Današnja brezžična lokalna omrežja delujejo v t.i. nelicenčnih frekvenčnih področjih, za uporabo katerih ni potrebno posebno dovoljenje (frekvenčni pas od 2.40GHz – 2.484 GHz in od 5.725 GHz – 5.850GHz).

Osnovne prednosti WLAN omrežij so:

- mobilnost uporabnikov,
- preprosta in hitra namestitve sistema,
- popolna združljivost z žičnimi omrežji,
- nizka cena in
- zmožljivost glede na ostala mobilna omrežja

Šibki točki sistema, ki ju velja izpostaviti sta:

- nizka varnost komunikacije (zračni medij) in
- potreba po varčevanju z energijo pri mobilnih postajah zunanjega napajanja.

II. ARHITEKTURA WLAN OMREŽIJ

Osnovna gradnika brezžičnih lokalnih omrežij sta dostopovna točka (angl. Access Point) in brezžični odjemalec oziroma postaja (angl. WLAN client). Dostopovna točka je krmilna enota, ki skrbi za dodeljevanje zmogljivosti posameznim postajam in hkrati nadzoruje dostop do dostopovnega omrežja. WLAN postaje so računalniki, dlančniki in ostale naprave, ki so opremljene z brezžično mrežno kartico.

Glede na uporabljene osnovne gradnike brezžičnih lokalnih omrežij poznamo tri topologije teh omrežij. Najenostavnejša so priložnostna ali "ad hoc" omrežja, kjer postaje med seboj neposredno komunicirajo brez potrebe po dostopovni točki. Druga topologija je osnovna postavitev omrežja, kjer imamo eno dostopovno točko in poljubno število postaj. Pri taki postavitvi omrežja poteka vsa komunikacija med postajami preko dostopovne točke. Kadar uporabimo večje število dostopovnih točk, povezanih med seboj z dostopovnim omrežjem, pa govorimo o razširjeni postavitvi omrežja.



Slika 1: »Ad hoc« in osnovna postavitev omrežja WLAN

III. STANDARDI NA PODROČJU WLAN OMREŽIJ

Na področju brezžičnih lokalnih omrežij prevladujeta dve družini standardov. Prva je družina standardov IEEE 802.11, druga pa ETSI BRAN (Broadband Radio Access Networks).

Tabela 1: Protokolni sklad 802.11

Aplikacijski sloj
L3
LLC (802.2)
MAC (802.11)
Fizični sloj (802.11)

Osnovna razlika med obema družinama standardov je ta, da se delavne skupine IEEE 802.11 ukvarjajo predvsem s prenosom IP prometa, družina BRAN pa je bolj osredotočena na prenos ATM prometa preko brezžičnih lokalnih omrežij.

Prvi standard iz družine IEEE 802.11 je bil izdan leta 1997, nastajal pa je približno sedem let. V osnovi definira tri različne fizične sloje:

- IR (Infrared),
- razpršeni spekter s frekvenčnim skakanjem – FHSS (Frequency Hopping Spread Spectrum),
- razpršeni spekter z neposrednim zaporedjem – DSSS (Direct Sequence Spread Spectrum)

Hitrosti prenosa na fizičnem sloju, ki jih standard zagotavlja, sta 1 in 2 Mbit/s.

Standard definira tudi kontrolo dostopa do fizičnega medija – MAC (Medium Access Control). Glavna naloga tega sloja je dodeljevanje prenosnega medija postajam, ki zanj na nek način tekmujejo. Skrbi tudi za avtentikacijo in priključevanje postaj na dostopovne točke in nadzoruje porabo energije v mobilnih postajah. Tu velja poudariti, da je MAC sloj praktično enak v vseh verzijah standarda 802.11x, do ključnih razlik pride v fizičnem sloju.

Tabela 2: Pregled WLAN standardov

Standard	Frekvenčno področje [GHz]	Max. hitrost prenosa [Mbit/s]
IEEE 802.11	2.4-2.4835	2
IEEE 802.11a	5.150-5.350 5.725-5.825	54
IEEE 802.11b	2.4-2.4835	11
IEEE 802.11g	2.4-2.4835	54
HIPERLAN/2	5.150-5.350 5.470-5.725	54

Standard vsebuje tudi algoritem za šifriranje in zagotavljanje integritete sporočil imenovan WEP (Wired Equivalent Privacy).

Dve leti pozneje sta bila sprejeta še dva standarda iz te družine in sicer 802.11a in 802.11b.

Standard IEEE 802.11b uporablja na fizičnem sloju CCK (Complementary Code Keying) modulacijski postopek, ki omogoča še dve dodatni hitrosti prenosa in sicer 5.5 in 11 Mbit/s. Deluje v 2.4 GHz frekvenčnem področju, kjer lahko uporabljamo le tri neodvisne uporabniške kanale. Večina današnjih naprav deluje po tem standardu.

Standard IEEE 802.11a uporablja OFDM (Orthogonal Frequency Division Multiplexing) modulacijski postopek in deluje v 5 GHz frekvenčnem področju. Omogoča hitrosti prenosa do 54 Mbit/s na vsakem od dvanajstih neodvisnih kanalih. Naprav narejenih po standardu IEEE 802.11a ni dovoljeno uporabljati v Evropi, saj standard ne omogoča dinamične izbire kanala in kontrole oddajne moči. Trenutno se s tem problemom ukvarja delovna skupina pod oznako IEEE 802.11h.

Letos je bil sprejet standard IEEE 802.11g, ki vključuje dobre lastnosti prej omenjenih standardov. Deluje v 2.4 GHz frekvenčnem območju, uporablja OFDM in CCK modulacijski postopek in je združljiv z 802.11b. Omogoča hitrosti prenosa do 54 Mbit/s. Prednost tega standarda pred IEEE 802.11a je v večjem dometu, slabost pa je možnost uporabe največ treh neodvisnih kanalov.

Standardi znotraj družine IEEE 802.11 še vedno nastajajo. Delovna skupina z oznako IEEE 802.11e se ukvarja z zagotavljanjem prioritet časovno občutljivemu prometu. To je predvsem pomembno za prenos govora in gibljivih slik.

Delovna skupina IEEE 802.11f se ukvarja s problemom komunikacije med dostopovnimi točkami, da bi omogočili gostovanja med različnimi dostopovnimi točkami.

Učinkovite varnostne rešitve nastajajo pod okriljem IEEE 802.11i.

Zaradi velike borbe po prevladi na trgu, se je pojavilo veliko naprav, ki delujejo po osnutkih standardov. Posledica je nezdržljivost naprav različnih proizvajalcev. V ta namen je bilo ustanovljeno neprofitno mednarodno združenje Wi-Fi, ki izdaja certifikate o skladnosti naprav s standardi IEEE 802.11a, b in g.

Družina standardov BRAN vključuje štiri standarde in sicer HIPERLAN/1 (High Performance Radio Local Area Network), HIPERLAN/2, HIPERACCESS in HIPERLINK.

HIPERLAN/1 je uporaben kot širokopasovno in prilagodljivo neodvisno lokalno omrežje. Uporablja do pet kanalov, pri čemer vsak od njih omogoča hitrosti prenosa 10 od 20 Mbit/s pri dometu do 50 metrov.

HIPERLAN/2, za razliko od standardov IEEE 802.11, ne omogoča le prenosa IP prometa ampak tudi

ATM in UMTS prometa. Torej je povezavno orientiran in omogoča tudi zagotavljanje kvalitete storitev. Na fizičnem sloju je najbolj podoben standardu IEEE 802.11a. Deluje v 5 GHz frekvenčnem področju in uporablja OFDM modulacijski postopek. Omogoča hitrosti prenosa do 54 Mbit/s.

Naprav narejenih po teh standardih zaenkrat še ni na tržišču.

IV. ZAGOTAVLJANJE VARNOSTI V BREŽIČNIH LOKALNIH OMREŽJIH

Kot je bilo nakazano že v uvodu, je pri WLAN omrežjih potrebno posebno pozornost posvetiti zagotavljanju varnosti. WLAN omrežja trpijo vse nevarnosti žičnih omrežjih in še dodatne nevarnosti zaradi uporabe brezžičnega medija. V nadaljevanju se bomo omejili predvsem na slednje.

Signal WLAN omrežij se lahko širi tudi po prostorih, kjer si tega ne želimo. Tako lahko pride do prisluškovanja ali pa tudi do nepooblaščenega dostopa do omrežja. Zato je potrebno poskrbeti za ustrezno avtentikacijo, v posameznih primerih pa tudi za šifriranje podatkov.

Pri vstopu v WLAN omrežje se mora uporabnik identificirati, da mu ponudnik omogoči storitev. Seveda tudi uporabnik želi zanesljivo vedeti kam se je priključil. Ker uporabniki v WLAN omrežjih nimajo fizičnega dostopa do omrežne opreme, se morajo prepričati, da se povezujejo na pravo dostopovno točko. V zvezi z varnostjo v WLAN omrežjih moramo upoštevati tudi ostale varnostne parametre, kot npr. zagotavljanje integritete sporočil, varovanje pred napadi ipd. Če so brezžična omrežja pravilno konfigurirana, lahko zagotavljajo primerno varnost. Njihova slabost je prav gotovo ta, da niso samostojno upravljana, poleg tega pa ne omogočajo zaščite pred napadi z zavrnitvijo storitve DOS (Denial of Service).

V nadaljevanju bomo opisali nekaj standardov, ki se nanašajo na zagotavljanje varnosti v WLAN omrežjih.

A. WEP

Standard IEEE 802.11 v osnovni različici predpisuje za zagotavljanje varnosti uporabo protokola WEP (Wired Equivalent Privacy). Osnovna značilnost protokola je statičen ključ, ki se uporablja za avtentikacijo in šifriranje podatkov. Glavni problem ključa je, da ga je s pasivnim opazovanjem radijskega prometa možno relativno hitro ugotoviti. Kljub podaljšanju ključa iz 40 na 128 bitov te velike pomanjkljivosti ni možno odpraviti, saj se čas, potreben za napad, povečuje linearno in ne eksponentno.

Ker standard ne zagotavlja ustrezne varnosti, so se začele uporabljati nekatere varnostne rešitve znane iz žičnih omrežij. Med najbolj razširjenimi velja omeniti

princip navideznih zasebnih omrežij (VPN, Virtual Private Network).

B. WPA

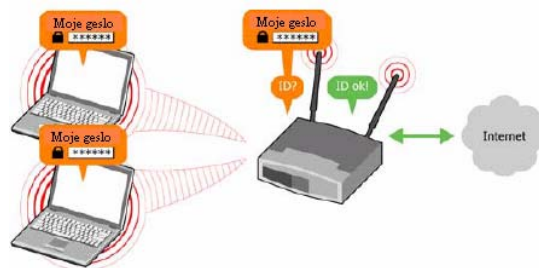
Namen protokola WPA (Wi-Fi Protected Access) naj bi bilo odpravljanje slabosti protokola WEP. Protokol WPA je bil predstavljen letos, nastal pa je v domeni združenja Wi-Fi. WPA bo tudi del standarda IEEE 802.11i, ki naj bi bil sprejet v letu 2004.

Protokol WPA omogoča relativno visoko stopnjo zaščite uporabniških podatkov in omogoča dostop do omrežja le avtoriziranim uporabnikom. WPA temelji na šifrnem algoritmu TKIP (Temporal Key Integrity Protocol) in avtentikaciji po standardu 802.1X. Dolžina ključa v algoritmu TKIP je 128 bitov, pri čemer gre za dinamične ključe, ki se jih distribuira s pomočjo avtentikacijskega strežnika. Z dodatno uporabo protokola EAP (Extensible Authentication Protocol) je omogočena uporaba digitalnih potrdil, unikatnih uporabniških imen, gesel, pametnih kartic ipd.

Šifrirni algoritem TKIP zelo poveča moč in kompleksnost šifriranja, zato je napad na tak sistem zelo zapleten, če ne celo nemogoč. TKIP je predalagan tudi za standard WPA2.

B.1 Zagotavljanje varnosti za domače uporabnike in majhne pisarne

Majhni uporabniki si težko privoščijo namestitve in vzdrževanje avtentikacijskih strežnikov RADIUS (Remote Authentication Dial-In User Service). Protokol WPA takim uporabnikom omogoča uporabo vnaprej razdeljenih ključev ali gesel (slika 2). Ta način omogoča enako močno šifriranje kot v običajni izvedbi z dinamičnimi ključi, razlika je le v tem, da je tu geslo vnaprej vpisano v uporabnikovo napravo in v dostopovno točko. To seveda pomeni, da je sistem bolj ranljiv, vendar kljub temu omogoča relativno visok nivo varnosti za majhne uporabnike.



Slika 2: WPA za domače uporabnike in majhne pisarne

C. WPA2

TKIP šifriranje, 802.1X/EAP avtentikacija in tehnologija vnaprej razdeljenih ključev so lastnosti protokola WPA, ki jih bo vključeval tudi protokol WPA2. WPA2 bo vseboval šifrirni algoritem AES (Advanced Encryption Standard).

Algoritem AES uporablja ključne spremenljive dolžine (128, 192 in 256 bitov). Protokol WPA2 bo, tako kot WPA, namenjen zagotavljanju varnosti v napravah IEEE 802.11, vključujoč 802.11a, 802.11b in 802.11g.

Za prehod na standard WPA bo potrebna programska nadgradnja dostopovnih točk in WLAN postaj, za prehod na WPA2 pa bo potrebna tudi zamenjava strojne opreme.

D. Avtentikacija na osnovi standarda TLS

Standard 802.1X je bil prvotno razvit za avtentikacijo uporabnikov v žičnih lokalnih omrežjih. Prisluškovanje je seveda možno tudi v žičnih omrežjih, vendar za to potrebujemo dostop do omrežne opreme, kar je precej težje kot v brezžičnih omrežjih, kjer se signali širijo tudi izven prostorov, kjer naj bi delovalo omrežje. V brezžičnih omrežjih moramo zato pomisliti tudi na šifriranje radijskega prometa.

Šifriranje in vzajemno avtentikacijo lahko npr. zagotovimo s pomočjo standarda Transport Layer Security (TLS). Na osnovi TLS so bili razviti trije protokoli, ki so primerni za uporabo v brezžičnih lokalnih omrežjih:

- EAP – TLS (Transport Layer Security),
- TTLS (Tunneled Transport Layer Security),
- PEAP (Protected EAP).

Protokol EAP – TLS predpisuje uporabo digitalnih potrdil v smeri od odjemalca in v smeri proti odjemalcu. Tak način zahteva uporabo odjemalčevih certifikatov, kar pa je včasih lahko moteča zahteva.

TTLS in PEAP sta bila razvita zaradi omenjene slabosti EAP – TLS, oba uporabljata starejše mehanizme za avtentikacijo uporabnika. Protokola TTLS in PEAP sta si precej podobna, sta dvo-stopenjska protokola, ki v prvi stopnji zagotavljata zaščito povezave, v drugi pa avtentikacijo. V prvi stopnji se vzpostavi TLS tunel, pri čemer se avtentikacijski strežnik predstavi odjemalcu z digitalnim potrdilom. Po vzpostavitvi varnega kanala se izvede še avtentikacija odjemalca.

E. EAP-SIM avtentikacija

Standardi vrste EAP – SIM bodo izvajali avtentikacijo v brezžičnih lokalnih omrežjih s

pomočjo SIM kartice. Ta vrsta avtentikacije je uporabna predvsem v javnih WLAN omrežjih, še posebej pa bo prišla do pomena, ko bo omogočeno prehajanje med WLAN omrežji in omrežji mobilne telefonije.

V. JAVNA BREŽŽIČNA LOKALNA OMREŽJA

WLAN omrežja so bila prvotno mišljena predvsem za zasebno uporabo, zlasti kot zamenjava in dopolnitev žičnim lokalnim omrežjem. Preprosta uporaba in dostopna cena tehnologije sta dva izmed dejavnikov, ki sta vodila v javno uporabo WLAN omrežij.

Storitve WLAN omrežij za javno rabo ponujajo operaterji mobilne telefonije in ponudniki dostopa do interneta - ISP (Internet Service Provider). Ponudniki javnih brezžičnih lokalnih omrežij PWLAN (Public Wireless Local Area Network) omogočajo uporabo storitev iz dostopovnih točk, ki so običajno nameščene na krajih, kjer se zadržuje veliko ljudi. Ta mesta, t. i. vroče točke (angl. hot spots), so npr. letališča, hoteli, večji prireditveni prostori ipd. Storitve javnih WLAN omrežij pridejo prav zlasti med potovanji.

V prvi fazi razvoja javnih WLAN omrežij govorimo predvsem o vročih točkah, kjer so uporabniki bolj ali manj stacionarni, medtem ko druga faza razvoja vključuje poljubno mobilnost uporabnika. V prvi fazi gre torej za gostovanje pri različnih operaterjih, v drugi fazi pa tudi za prehajanje med različnimi dostopovnimi tehnologijami.

Pri uporabi WLAN omrežij za javno rabo je potrebno upoštevati več dejavnikov:

- avtentikacija uporabnika in avtorizacija storitev,
- varen prenos podatkov,
- vzdrževanje neprekinjene povezave,
- gostovanje in
- zaračunavanje.

V nasprotju z zasebno rabo WLAN omrežij, kjer lahko npr. sistemski administrator poskrbi za prednastavitve podatkov, potrebnih za avtentikacijo, je v primeru javnega omrežja potreben čim bolj preprost način priklopa v omrežje in avtentikacija uporabnika.

Uporabnik ne želi posegati v nastavitve računalnika, pač pa zgolj vtipkati svoje uporabniško ime in geslo. Opisani način avtentikacije imenujemo WEB dostop. Drug način avtentikacije, ki temelji na SIM kartici (EAP – SIM, prejšnje poglavje), pa od uporabnika zahteva, da si na svojem računalniku naloži poseben program.

O varnem prenosu podatkov smo obširno spregovorili v prejšnjih poglavjih, medtem ko o neprekinjeni povezavi, v primeru prehajanja med različnimi dostopovnimi tehnologijami, v prvi fazi razvoja javnih WLAN omrežij še ne moremo govoriti.

Obstajajo določene rešitve za gostovanje, ko se npr. uporabnik, ki ima sklenjeno razmerje z operaterjem A poskuša prijaviti na vstopni točki operaterja B. Če operaterja omogočata gostovanje, operater B posreduje zahtevo operaterju A, ki uporabnika avtentificira in mu omogoči uporabo storitve.

Zaračunavanje, ki je v primeru javnih WLAN omrežij glavni motiv operaterjev, lahko temelji na različnih principih:

- dejanski čas uporabe storitve,
- količina prenesenih podatkov,
- pavšalno zaračunavanje (angl. flat rate),
- storitve brez zaračunavanja

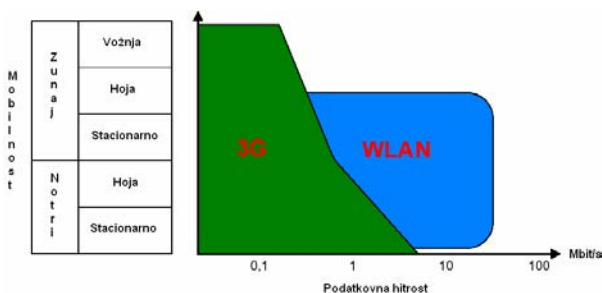
VI. 3G IN BREZŽIČNA LOKALNA OMREŽJA

Ob pojavu WLAN omrežij so nastajale polemike, da bi ta vrsta omrežij utegnili biti velika konkurenca prihajajočim mobilnim omrežjem 3. generacije UMTS (Universal Mobile Telecommunications Service). Danes velja, da se omrežji 3G in WLAN dopolnjujeta, kar se odraža tudi v tem, da je večina operaterjev WLAN omrežij mobilnih operaterjev.

Tudi v okviru UMTS foruma je bilo izdano poročilo [3] o pomembnosti vključevanja javnih WLAN omrežij v sklopu omrežij 3G. Poročilo govori o dveh bistvenih razlikah med omenjenimi omrežji:

- nivo mobilnosti,
- hitrost prenosa podatkov.

Nivo mobilnosti v 3G omogoča globalno pokrivanje in zadostno hitrost prenosa podatkov tudi v primeru gibanja. V nasprotju s tem, je hitrost prenosa podatkov v omrežjih WLAN večja, vendar je mobilnost pri tem močno omejena. Slika 3 prikazuje primerjavo mobilnosti in hitrosti prenosa podatkov v omrežjih 3G in WLAN.



Slika 3: Primerjava hitrost/mobilnost v omrežjih 3G in WLAN [2], [3]

VII. ZAKLJUČEK

Današnja brezžična lokalna omrežja predstavljajo zanimivo in hkrati zelo priročno možnost dostopa do

interneta. Tako za končne uporabnike kot lastnike omrežij velja, da so brezžična omrežja poceni in preprosta za uporabo. Ker gre za relativno novo tehnologijo, imamo opravka s precej nedorečenimi oziroma nestandardiziranimi tehnološkimi in konceptualnimi faktorji, ki pa jih bomo z nadaljnjim razvojem zagotovo rešili.

Za nekatere storitve bi vsekakor želeli prenosne hitrosti, ki bi bile večje od sedaj dosegljivih 22 Mbit/s, zato npr. delovna skupina pod oznako IEEE 802.11n razvija rešitve, ki bodo omogočale hitrosti prenosa 108 Mbit/s oziroma 320 Mbit/s. V mislih imamo tudi povečevanje izkoristka hitrosti prenosa koristnih podatkov v primerjavi s hitrostjo prenosa na fizičnem sloju. Na področju varnosti v brezžičnih omrežjih se naslednje leto obeta standard IEEE 802.11i, ki naj bi varnost reševal na celovit način.

V prihodnosti si na fizičnem sloju veliko obetamo od sistemov t.i. ultra širokega spektra (UWB – Ultra Wide Band). V ZDA je za ta način že predpisan frekvenčni pas med 3.1 in 10.6 GHz, v Evropi pa ta pas še ni definiran. Po predvidevanjih je v tem frekvenčnem pasu s tehnologijo UWB moč doseči hitrosti prenosa nad 10 Gbit/s.

Na trgu so se pojavili tudi prvi telefoni VoWIP (Voice over Wireless IP) za prenos govora z internetnim protokolom IP preko brezžičnih omrežij. Taki sistemi bi bili lahko zelo uporabni za poceni interno brezžično telefonijo v podjetjih.

Opisane aktivnosti in perspektive na področju brezžičnih lokalnih omrežij navajamo kot protitež pomislekom, ki jih zasledimo na različnih koncih. Prav gotovo bo minilo še nekaj časa, preden bomo lahko govorili o zares hitrih, varnih, zanesljivih in mobilnih brezžičnih lokalnih omrežjih, vendar smo glede na atraktivnost predstavljene tehnologije prepričani, da se bo to zgodilo.

LITERATURA

- [1] K. Albrecht, Brezžična lokalna omrežja in njihova varnost, diplomsko delo, Fakulteta za elektrotehniko, Ljubljana, 2003
- [2] B. Šergon, Brezžična lokalna omrežja, diplomsko delo, Fakulteta za elektrotehniko, Ljubljana 2003
- [3] Report No. 22, UMTS Forum, julij 2002
- [4] Public Wireless WLAN for Mobile Operators: WLAN beyond the enterprise!, White Paper, Alcatel, marec 2003
- [5] Sasken Communication Technologies Ltd.: White paper on WLAN, oktober 2003
- [6] AirDefense, Knowledge center, Wireless LAN Overview, oktober 2003 (<http://www.airdefense.net/wlans/overview.shtml>)



Klemen Albreht (klemen@klub-nsk.si) je diplomiral leta 2003 na Fakulteti za elektrotehniko Univerze v Ljubljani iz področja brezžičnih lokalnih omrežij. Je študent podiplomskega študija elektrotehnike.



Rudolf Sušnik (rudolf.susnik@fe.uni-lj.si) je diplomiral leta 2001 na Fakulteti za elektrotehniko v Ljubljani. Je mladi raziskovalec v Laboratoriju za komunikacijske naprave na Fakulteti za elektrotehniko v Ljubljani in študent podiplomskega študija elektrotehnike. Njegovo raziskovalno in razvojno delo je osredotočeno na komunikacijska

omrežja, obdelavo signalov in akustiko.



Jaka Sodnik (jaka.sodnik@fe.uni-lj.si) je diplomiral leta 2002 na Fakulteti za elektrotehniko v Ljubljani. Je mladi raziskovalec v Laboratoriju za komunikacijske naprave na Fakulteti za elektrotehniko v Ljubljani in študent podiplomskega študija elektrotehnike. Njegovo raziskovalno in razvojno področje obsega obdelavo signalov,

komunikacijska omrežja in akustiko.



Sašo Tomažič (saso.tomazic@fe.uni-lj.si) je doktoriral leta 1991 na Univerzi v Ljubljani s področja telekomunikacij. Je profesor na Fakulteti za Elektrotehniko v Ljubljani, predstojnik Laboratorija za komunikacijske naprave in predstojnik Katedre za telekomunikacije. Bil je nacionalni koordinator za področje

telekomunikacij na Ministrstvu za šolstvo, znanost in šport in svetovalec za področje telekomunikacij na Ministrstvu za obrambo. Njegovo sedanje delo obsega raziskave na področju obdelave signalov, varnosti v telekomunikacijah, elektronskega poslovanja in porazdeljenih informacijskih sistemov.