Ranka Grubešić

Bežična lokalna mreža

Ranka Grubešić
Ericsson Nikola Tesla d.d., Zagreb, Hrvatska
Ericsson Nikola Tesla d.d., Zagreb, Croatia

Ključne riječi
WLAN, Bežična lokalna mreža
Pristup bežičnoj lokalnoj mreži
WDAS, Rješenje za istovremenu pokrivenost GSM i WLAN mreže
UMTS, Univerzalni sustav pokretnih telekomunikacija
MO WLAN, Ericssonovo rješenje za bežičnu lokalnu mrežu
U(SIM) potvrda vjerodostojnosti
Ericssonov WLAN poslužitelj za potvrdu vjerodostojnosti

Key Words
WLAN, Wireless Local Area Network
Public WLAN Access
WDAS, WLAN Distributed Antenna System
UMTS, Universal Mobile Telecommunications System
MO WLAN, Mobile Operator WLAN
U(SIM) Authentication
Ericsson WLAN Authentication Server

Sažetak

Tijekom proteklih nekoliko godina mobilnost sve više obilježava suvremeni životni stil. GSM, GPRS i nadolazeći EDGE i UMTS promijenili su svijest i očekivanja korisnika. Tradicionalni, žični načini komunikacije više nisu dovoljni ni u govornim, ni u podatkovnim komunikacijama. Bežična lokalna mreža (WLAN - *Wireless Local Area Network*), možda više poznata kao bežični LAN ili Wi-Fi, stoga sve više ulazi u telekomunikacijsku svakodnevnicu. Za mobilne operatore, WLAN je usluga komplementarna njihovim GSM/GPRS i UMTS sustavima, jednostavna za implementaciju i održavanje. WLAN tehnologija predstavlja i odličan način širokopojasnoga pristupa Internetu. Standardiziranost, nelicencirane frekvencije rada i visoke brzine prijenosa čine WLAN izuzetno zanimljivom i traženom tehnologijom. Ericsson je jedan od inicijatora WLAN standardizacije pod krovom 3GPP organizacije. U ovom članku prikazani su ključni segmenti WLAN tehnologije, a detaljnije se predstavlja Ericssonovo rješenje *Mobile Operator* WLAN i njegova integracija s mobilnim mrežama te Ericssonovo rješenje za distribuciju WLAN mrežnih elemenata – WDAS (WLAN *Distributed Antenna System*).

WIRELESS LOCAL AREA NETWORK

Abstract

During past few years the world has been getting increasingly mobile: GSM, GPRS and upcoming EDGE and UMTS, have changed the world and end users' expectations. Traditional wired ways of communicating are neither sufficient in voice, nor in data communications any more. Wireless Local Area Network (WLAN), also known as Wireless LAN or Wi-Fi, is therefore becoming increasingly present in the telecom industry. For mobile operators WLAN is a service complementary to their GSM/GPRS and UMTS systems, easy to implement and maintain. WLAN technology also enables excellent broadband access to the Internet. Standardization, non-licensed operating frequencies and high transfer speeds make WLAN extremely interesting technology in demand. Ericsson is one of initiators of the WLAN standardization under the umbrella of the 3GPP organization. This paper introduces key segments within WLAN technology and Ericsson's solution. It also presents Mobile Operator WLAN and its integration into the mobile networks in detail, as well as Ericsson's solution for network elements distribution, WLAN Distributed Antenna System (WDAS).

1. Uvod

Tržište bežičnih lokalnih mreža (WLAN - *Wireless Local Area Network*) je trenutačno u velikoj i brzoj ekspanziji. Ako uzmemo u obzir javni, poslovni ili kućni WLAN, sve je poželjnije bežično povezivanje, nauštrb fiksnih mreža, tim više što su cijene bežičnog pristupa Internetu i intranetu sve niže i konkuriraju tradicionalnom fiksnom pristupu. Mobilni operatori, i ne samo oni, istražuju mogućnosti proširivanja svoje ponude usluga osiguranjem WLAN pristupa podatkovnim mrežama. U zadnje vrijeme se dosta govori i o prijenosu govora preko bežičnih lokalnih mreža.

Postoji mnogo prednosti bežičnoga povezivanja od kojih je najvažnija mobilnost. Nakon godina korištenja GSM-a i u očekivanju 3G mobilnih mreža, korisnici su sve zahtjevniji i nisu zadovoljni samo s uslugom dobivanja pristupa podatkovnoj mreži ili s mogućnošću primanja ili slanja poziva sa svog telefona. Korisnici traže fleksibilnost, veće brzine prijenosa, pouzdanost, sigurnost, jednostavnost upotrebe mobilnih uređaja, potvrde vjerodostojnosti (*authentication*) i plaćanja usluge te dostupnost. WLAN nije prilika samo za vlasnike mreža na veoma prometnim javnim mjestima (*hotspots),* kao što su aerodromi, hoteli, konferencijski centri, kafići, restorani, knjižnice, i sl., gdje postoje velike potrebe potencijalnih korisnika za propusnošću i velikim brzinama prijenosa. Na takvim mjestima je relativno jednostavno ugraditi WLAN sustav, prodavati *pre-paid* kartice za WLAN i omogućiti jednostavan i brz pristup Internetu svakom korisniku koji to želi. Dugoročno gledajući, WLAN tehnologija je prirodni korak dalje u evoluciji bežičnih komunikacijskih sustava. Uz integraciju s 3G mobilnim mrežama ona omogućava optimalno zadovoljenje potreba korisnika i korištenje resursa objedinjene operatorove mreže.

2.5G i 3G komunikacije omogućavaju mobilnost i potpunu pokrivenost korisnika kojemu je u svakom dijelu mreže (a i šire, uz mogućnost neograničenoga kretanja - *roaming*) i u bilo koje doba omogućen pristup govornim i podatkovnim komunikacijama, dok je u područjima s visokim kapacitetom korištenja i velikim zahtjevima kupaca prirodno koristiti WLAN rješenja. Na određenim javnim prometnim mjestima, gdje postoje zahtjevi za visokim brzinama prijenosa i gdje se stalno ili povremeno pojavljuje veliki broj istovremenih korisnika, što operator mobilne mreže može zadovoljiti samo uz veća ulaganja, WLAN je jeftina alternativa koja zadovoljava povećane potrebe za opsegom prijenosa na kraćim udaljenostima (do 100 m). K tome, mobilnim operatorima je posebno zanimljiva činjenica da se podatkovne usluge mogu ponuditi bez diskontinuiteta (*seamlessly)* – korisnik ne mora niti primijetiti da je sa svoje GPRS/UMTS mreže prešao na WLAN mrežu. Naglasak je na komplementarnosti – WLAN mreža i 3G mreža ne mogu zamijeniti jedna drugu, ali zajedno mogu postići sinergiju i pružiti još više mogućnosti korisnicima.

2. WLAN standardizacija

Što je bežična lokalna mreža? Riječ je podatkovnoj mreži, dosega do nekoliko stotina metara, koja se može koristiti na tri načina: kao korporacijski intranet, kod kuće ili kao javna mreža ograničenoga dosega za pristup Internetu (PWLAN – *Public WLAN*). Osnovni elementi mreže su pristupne točke (AP - *Access Points*) s pripadajućim antenama i pristupni poslužitelji za mreže s nekoliko pristupnih točaka, koji dalje komuniciraju s elementima na višim razinama (čvorovi za upravljanje, potvrdu vjerodostojnosti, naplaćivanje i sl.). Za pristup bežičnoj lokalnoj mreži su potrebne WLAN kartice, koje se umetnu u WLAN terminal (najčešće je to prijenosno računalo ili PDA uređaj (*Personal Digital Assistant*). Promet između korisnika, pristupnih točaka i pristupnih poslužitelja se odvija putem radio sučelja. Elementi međusobno komuniciraju putem Etherneta, kao i u svakoj drugoj lokalnoj mreži (LAN - *Local Area Network*).

Do sada najuspješniji WLAN standardi su iz IEEE 802.11 porodice. Danas postoji nekoliko 802.1 standarda koji se međusobno razlikuju prema korištenim tehnologijama i karakteristikama. *Tablica 1.* prikazuje osnovnu usporedbu tih standarda. 1997. godine su izašli prvi 802.11 standardi, ograničeni na 2 Mbit/s, koji su radili na 2,4 GHz. Ti standardi su koristili tri različite vrste fizičkog sloja: infracrveni (nikad razvijen), *Frequency Hopping* (FH) i *Direct Sequence* (DS). 1999. su standardizirani 802.11a i 802.1b, danas svjetski najuspješniji WLAN standard, poznatiji kao Wi-Fi (*Wireless Fidelity*). Produkti bazirani na 802.11b imaju brzine do 11 Mbit/s i koriste nasljednika DS-a, *Direct-sequence Spread Spectrum* (DSSS) modulaciju, također poznatu i kao *High-Rate* DSSS (HR/DS ili HR/DSSS). 802.11a koristi treću tehniku radio modulacije, *Orthogonal Frequency Division Multiplexing* (OFDM) i postiže brzine prijenosa do 54 Mbit/s. Standard 802.11a radi na drugačijem frekvencijskom pojasu (5 GHz) i za sada je ograničen samo na Sjedinjene Američke Države. Postoji i standard 802.11g, koji je još uvijek u procesu standardizacije i koji radi na 2,4 GHz, ali koristi OFDM i dostiže 54 bit/s kao i standard 802.11a.

Osim IEEE standarda, ponegdje u Americi, Japanu i Europi se koristi ETSI standard HiperLAN/2 (5 GHz, OFDM, do 54 Mbit/s), koji nikad nije dostigao toliku popularnost na tržištu kao 802.11 standardi, a ne očekuje se niti da će to postići u budućnosti.

802.11 standardi imaju radne frekvencije u nelicenciranim područjima – 2,4 GHz i 5 GHz. To ih čini izuzetno

IEEE Standard	Brzina	Frekvencijski pojas	Modulacijska tehnika	Opis standarda
802.11	1 Mbit/s 2 Mbit/s	2,4 GHz	IR, FH, DS	Prvi standard (1997). Radio dio – i FH i DS modulacijska tehnika.
802.11a	do 54 Mbit/s	5 GHz	OFDM	Drugi standard (1999), iako produkti izašli tek krajem 2000. Koristi se u SAD.
802.11b	5,5 Mbit/s 11 Mbit/s	2,4 GHz	HR/DSSS	Treći standard, ali drugi val produkata. Poznat i kao Wi-Fi. Trenutačno najzastupljeniji WLAN standard u svijetu.
802.11g	Do 54 Mbit/s	2,4 GHz	OFDM	Nije još standardiziran.

Tablica 1. Usporedba WLAN standarda

primamljivim tehnologijama jer značajno smanjuju cijenu implementacije. Očekuje se da će frekvencija od 2,4 GHz biti najkorištenija u svjetskim razmjerima. U zadnjih nekoliko godina gotovo svi komercijalni IEEE standardi i razvoji temeljeni su upravo na toj frekvenciji. Međutim, u području nelicenciranih frekvencija postoji granica snage za odašiljač, kako bi spektar mogao biti korišten bez interferencije već na vrlo bliskim frekvencijama.

3. Prednosti bežične lokalne mreže

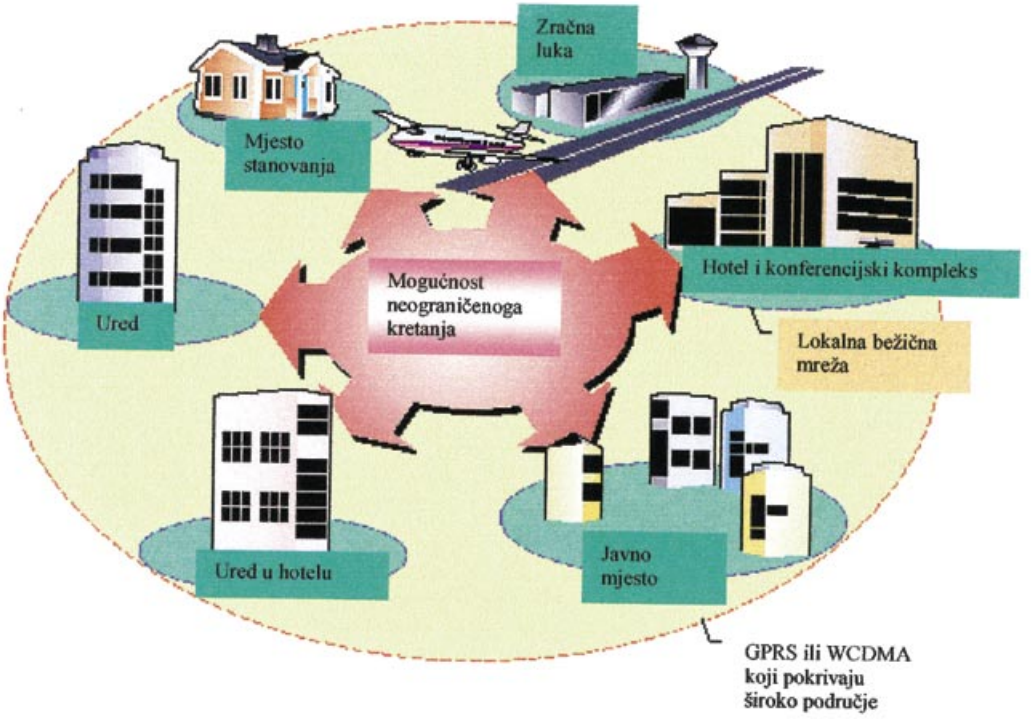
Kao što je već odavno pokazano u razvoju bežičnih usluga, pokrivenost područja (*coverage)* je najvažniji faktor za uspjeh bežične tehnologije. Ericssonovo uvjerenje je da upravo na tom području mobilni operatori mogu ponuditi najviše: oni već imaju infrastrukturu koja pokriva velika područja, u većini slučajeva imaju gotovo potpunu pokrivenost zemlje u kojoj nude usluge. Uz male dodatne troškove mobilni operatori mogu na jednostavan način dodati *indoor* WLAN pristup korisnicima. Također, mobilni operatori raspolažu već razvijenim i postavljenim sustavima za nadzor, naplaćivanje usluga, potvrdu vjerodostojnosti te komunikaciju s korisnicima, a imaju i veliku bazu podataka o mobilnim pretplatnicima, uglavnom poslovnim profesionalcima za koje se smatra da će biti prva važna grupa korisnika kombinirane celularne/WLAN mreže. Poslovni profesionalci često putuju, često im je potreban brzi pristup Internetu ili kompanijskom intranetu, koriste mobilne telefone i prijenosna računala te su otvoreni prema novim tehnologijama koje im omogućavaju jednostavnije i efikasnije obavljanje posla. Ericssonovo je stanovište, koje se potvrđuje u svijetu, da su mobilni operatori među prvima u ciljnoj grupi pružatelja WLAN usluga.

WLAN je postigao znatnu pažnju telekomunikacijske javnosti proteklih nekoliko godina. U većim gradovima SAD-a i Europe postoje javne WLAN mreže. Zašto je onda broj WLAN korisnika u svijetu ipak još uvijek relativno malen? Za to postoji nekoliko razloga:

- Slaba pokrivenost – npr. pokriveno je područje aerodroma, ali ne i prilaza aerodromu, tako da korisnici još uvijek nemaju uvijek i svugdje pristup Internetu;
- Nedostatak brand prepoznavanja – u slučaju kad su WLAN pružatelji usluga novi i nepoznati, korisnici su neskloni korištenju usluge;
- Nepostojanje mogućnosti neograničenoga kretanja (*roaming*) – korisnici moraju koristiti usluge različitih operatora na različitim mjestima.

Možemo zaključiti da se ti problemi mogu prevladati ako već postojeći mobilni operatori počnu koristiti WLAN mreže i tehnologije. Naime, GPRS/UMTS operatori su već etablirani na tržištu, većinom imaju odličnu pokrivenost svojom mobilnom mrežom, a imaju i sklopljene ugovore o mogućnosti neograničenoga kretanja s drugim mobilnim operatorima.

WLAN, kao i svaka dolazeća tehnologija, ima i "dječjih bolesti". Problemi o kojima se najviše priča na skupovima o WLAN tehnologijama su pitanja sigurnosti te potvrde vjerodostojnosti, autorizacije i naplaćivanja usluge (AAA



Slika 1. Vizija Ericssonovoga rješenja MO WLAN – premošćivanje LAN-a i WAN-a

– *Authentication, Authorization and Accounting*). Kao i kod svake lokalne mreže sigurnost (upadanje u mrežu, prisluškivanje, neovlašteno korištenje mrežnih resursa) je osjetljivo pitanje na koje treba obratiti posebnu pozornost, a zbog bežičnosti je rješavanje toga problema još više otežano. Korisnicima je važno da potvrda vjerodostojnosti, autorizacija i naplaćivanje usluge bude što jednostavnije i brže. Standardizacija je najbolji odgovor na oba problema. Ericsson, osim što je aktivno uključen u rad standardizacijske grupe 3GPP, ima rješenje i za zadovoljavajuću sigurnost i jednostavnu i efikasnu potvrdu vjerodostojnosti, koje omogućuje zajedničku potvrdu vjerodostojnosti za WLAN i GPRS/UMTS mrežu te jednaku razinu sigurnosti za WLAN i za pripadajuću GPRS/UMTS mrežu: Ericssonov WLAN poslužitelj za potvrdu vjerodostojnosti (EWAS - *Ericsson WLAN Authentication Server*), mrežni WLAN element, prvi te vrste u svijetu, o kojemu će u daljnjem tekstu biti više riječi.

4. Mobile Operator WLAN (MO WLAN)

Ericssonovo rješenje za bežičnu lokalnu mrežu - Mobile Operator WLAN (MO WLAN) je WAN-WLAN *interworking* sustav (Slika 1.). Trenutačno aktualna inačica je 2.0. Podržani IEEE standardi su 802.11b, 802.11a i IEEE 802.11g, a buduće inačice MO WLAN-a će ići u korak s evolucijom IEEE standarda.

4.1. Arhitektura MO WLAN sustava

U skladu sa zahtjevima 3GPP standardizacijskoga modela, MO WLAN ima minimalan utjecaj na opremu i rad WLAN mreže, kao i na promjene i adaptaciju operatorove mreže. Poseban je naglasak stavljen na što manje promjene u registru vlastitih pretplatnika (HLR - *Home Location Register*) i centru za potvrdu vjerodostojnosti (AuC - *Authentication Centre*). U operatorovoj mreži tako nikakvih promjena uobičajenih funkcionalnosti neće biti u elementima SGSN (*Serving GPRS Support Node*), GGSN (*Gateway GPRS Support Node*), HLR, AuC, NTP (*Network Time Protocol*) i DNS (*Domain Name Server*), dok EMA (*Ericsson Multi Activation*) i BGw (*Billing Gateway*) moraju biti rekonfigurirani. Na Slici 2. su prikazani MO WLAN elementi.

Pristupna točka djeluje kao radio sučelje prema WLAN terminalima i komunicira s pristupnim poslužiteljem (ASN - *Access Serving Node*) preko WLAN Ethernet mreže. ASN potvrđuje vjerodostojnost pristupa te djeluje kao DHCP poslužitelj i obračunava korisničke usluge, a kada je spojen na IP temeljnu mrežu i na sustav upravljanja pristupom (AMS - *Access Management System*), on obavlja (neke) funkcije kontrole, potvrde vjerodostojnosti, statistike, administracije i naplaćivanja u suradnji s

pristupnikom za naplaćivanje (*Billing Gateway*) u mobilnoj mreži, a sastoji se od nekoliko odvojenih čvorova:

• Sustav za nadzor usluga (SCS - *Service Control System*) – redundantni čvor koji služi za potvrdu vjerodostojnosti, kontrolu usluga, a sadrži i bazu podataka s korisničkim računima i profilima;

• Sustav za statistiku i naplaćivanje (SAS - *Statistics and Accounting System*) obavlja statističke funkcije i funkcije naplaćivanja;

• Poslužitelj za administrativnu obradu korisnika i naplatu usluga (CABS - *Customer Administration and Billing Server*) – obavlja administraciju korisničkih profila;

• Poslužitelj sučelja za programiranje aplikacija (APIS - *Application Program Interface Server*) – odgovoran je za kreiranje korisničkih računa i profila – podatke šalje u SCS;

• SUS poslužitelj (SUS - *Sign-up and User self-administration Server*) – omogućava korisniku stvaranje voucher računa ili, primjerice, promjenu zaporke.

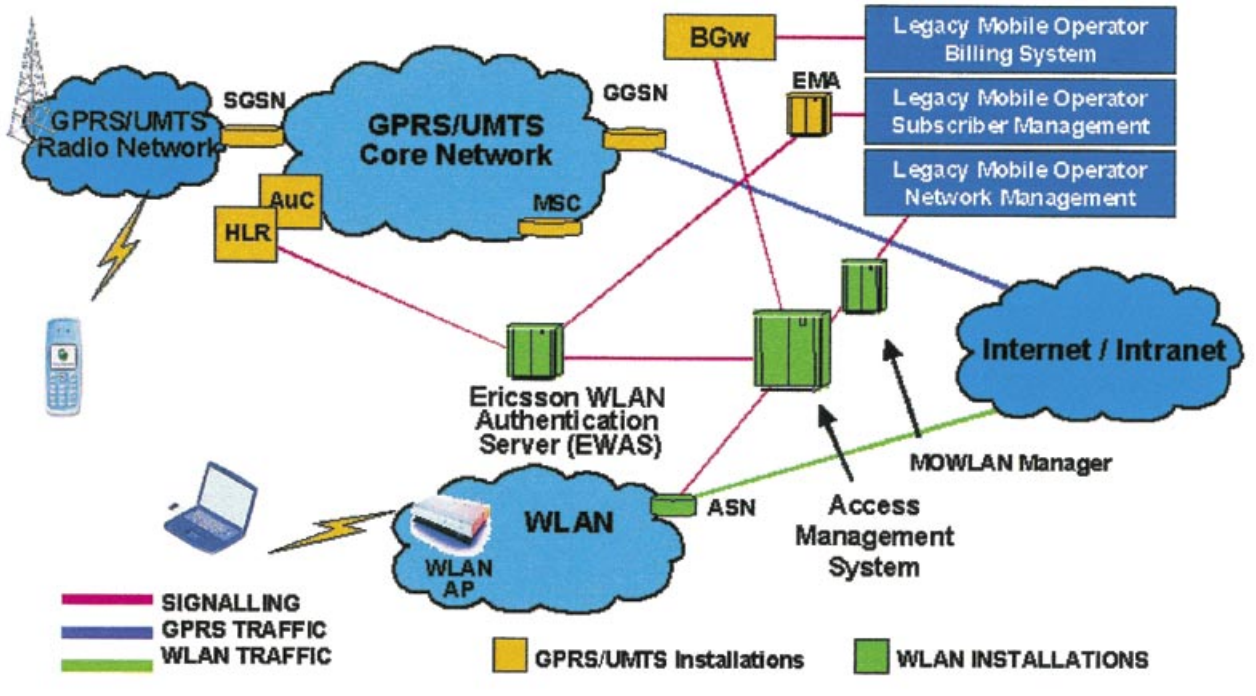
MO WLAN *Manager* je čvor zadužen za centralizirani nadzor MO WLAN sustava i obuhvaća upravljanje elementima sustava, mrežom i cijelim sustavom (*element, network & system management).*

Potvrda vjerodostojnosti u MO WLAN-u se odvija pomoću RADIUS protokola. Postoje tri vrste potvrde vjerodostojnosti u MO WLAN mreži:

• Pomoću U(SIM) kartice – ovaj način potvrđivanja vjerodostojnosti je Ericssonov adut na WLAN tržištu te objedinjuje potvrdu vjerodostojnosti u operatorovim GPRS/UMTS i WLAN mrežama. Ericssonovo rješenje za istovremenu pokrivenost GSM i WLAN mreže (EWAS - *Ericsson WLAN Authentication Server*) je čvor koji to omogućava, a komunicira s HLR-om i AuC-om i EMA-om u mobilnoj mreži. U(SIM) se odnosi na UMTS SIM kartice. Ericssonov U(SIM) sustav potvrde vjerodostojnosti temelji se na dva protokola – EAP SIM (*Extensible Authentication Protocol Subscriber Identification Module*) protokolu i EAP AKA (*Extensible Authentication Protocol Authentication and Key Agreement*) protokolu. EAP SIM protokol se koristi kod GSM/GPRS mreža, a EAP AKA protokol se koristi kod GSM/ GPRS i UMTS mreža.

• Pomoću jednokratne zaporke (OTP - *One Time Password*) koja se šalje SMS-om do korisnikovog mobilnog telefona. Taj pristup temelji se na Internet tehnologiji. Takva potvrda vjerodostojnosti se realizira pomoću poslužitelja za potvrdu vjerodostojnosti koji djeluje na principu jednokratne zaporke (OTP AS - *One Time Pass-*

Slika 2. Arhitektura sustava MO WLAN R2.0



word Authentication Server) koji se također spaja na AMS.

• Pomoću statičkog korisničkog imena – to je također pristup utemeljen na Internet tehnologiji. Čvor koji omogućava tu vrstu potvrde vjerodostojnosti nalazi se u AMS grupi čvorova. Ovaj način potvrde vjerodostojnost dozvoljava i plaćanje unaprijed pomoću *voucher* kartice.

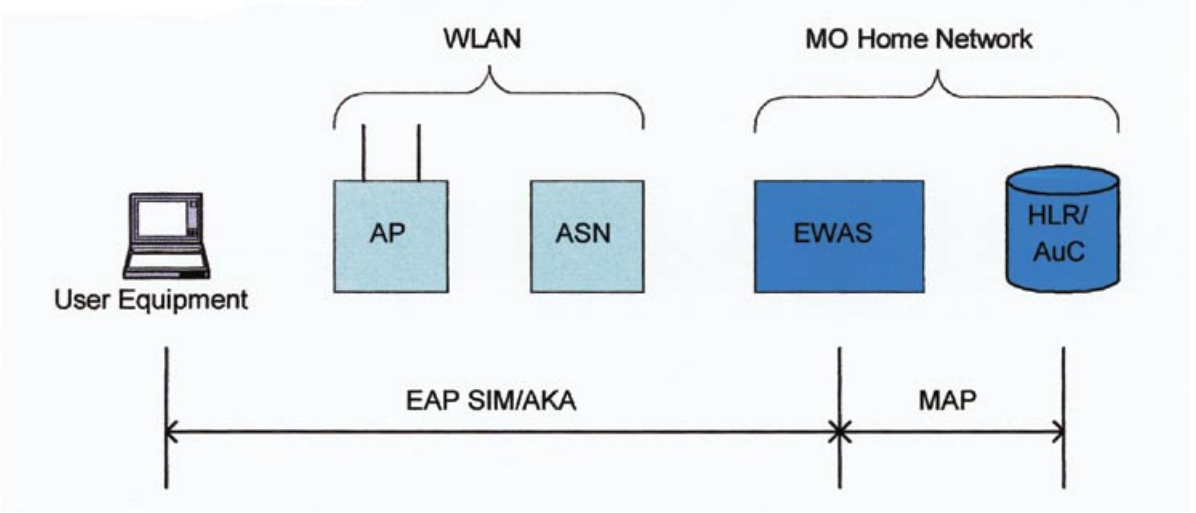
4.2. Potvrda vjerodostojnosti u MO WLAN – EWAS sustavu

Na *Slici 3.* je prikazan (U)SIM-bazirani model potvrde vjerodostojnosti. Ključni element je EWAS. EWAS (RADIUS poslužitelj) komunicira s ASN-om (RADIUS poslužitelj i klijent istovremeno) i AP-om (RADIUS klijent) preko EAP SIM ili EAP AKA protokola koji se prenosi RADIUS-om, a s druge strane u mobilnoj mreži s HLR-om pomoću MAP protokola.

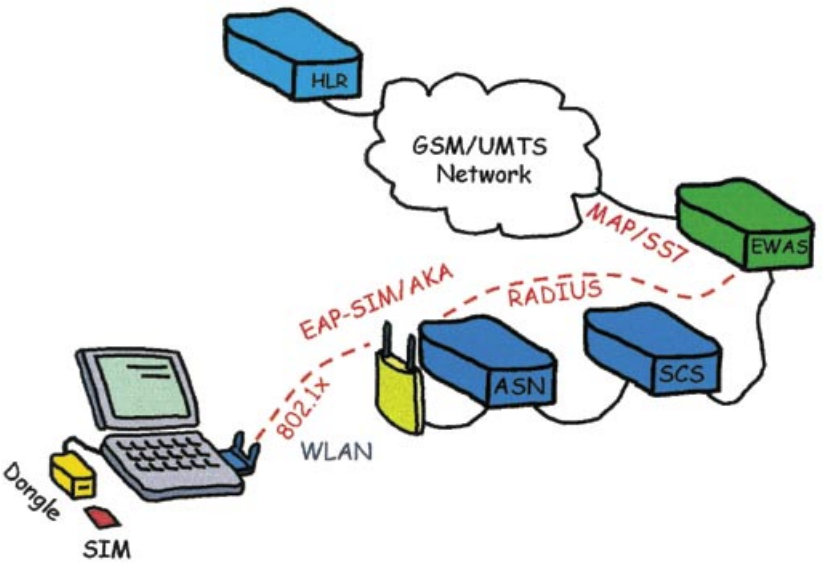
EWAS nije samo poslužitelj za potvrdu vjerodostojnosti, nego omogućava i sigurnost korisnicima. Naime, moguće je ponuditi WLAN korisnicima jednaku sigurnost prometa kao i u matičnoj GPRS/UMTS mreži. U budućnosti EWAS će evoluirati u HSS (*Home Subscriber Server*) poslužitelj.

Na sljedećim slikama prikazani su različiti načini potvrde vjerodostojnosti u MO WLAN rješenju.

Slika 4. prikazuje potvrdu vjerodostojnosti korisnika pomoću U(SIM) kartice. Terminal pristupnoj točki šalje informacije o identitetu pomoću 802.1x protokola. Pristupna točka šalje informaciju pomoću RADIUS-a preko ASN-a i SCS-a (*Service Control System* – dio AMS-a) do EWAS-a, koji određuje vrstu potvrde vjerodostojnosti i šalje informaciju o identitetu do mobilne mreže, gdje se

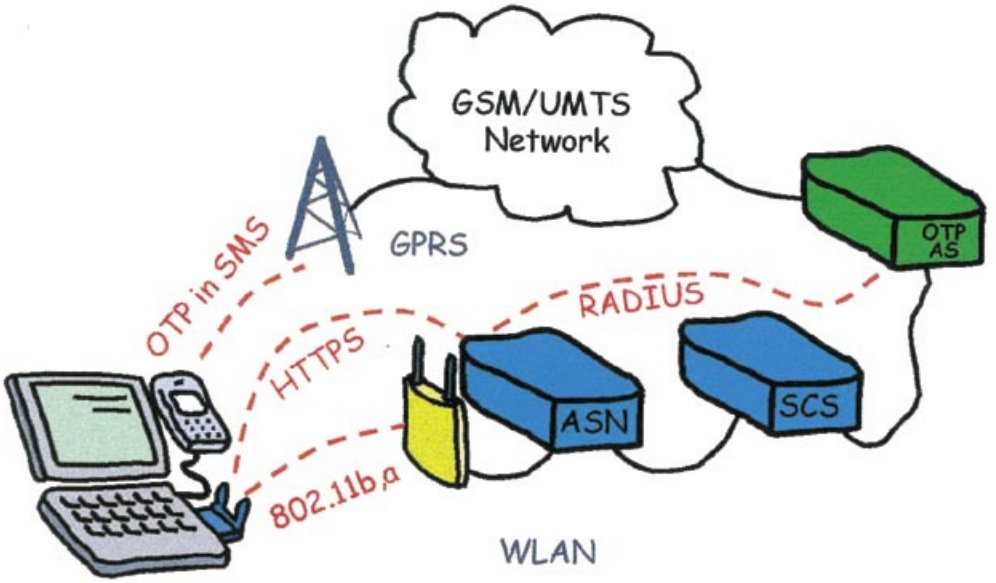


Slika 3. U(SIM) potvrda vjerodostojnosti u WLAN mreži pomoću EWAS-a



Slika 4. Signalizacija pri U(SIM) potvrdi vjerodostojnosti u MO WLAN-u

Slika 5. Potvrda vjerodostojnosti putem OTP-a u MO WLAN-u



provjerava u HLR-u. HLR provjerava korisnikov identitet i određuje hoće li se konekcija prihvatiti. Ako se konekcija prihvaća, uspostavlja se komunikacijski kanal između terminala i pristupne točke, zaštićen putem WPA sustava (Wi-Fi *Protected Access*).

Na Slici 5. prikazana je web-bazirana potvrda vjerodostojnosti u MO WLAN-u. Prije provjere identiteta, uspostavlja se 802.11b konekcija između terminala i pristupne točke. ASN dodjeljuje IP adresu i korisnik upisuje svoju prijavu (*login*). ASN ga prosljeđuje do OTP AS-a pomoću RADIUS-a, a OTP AS šalje jednokratnu zaporku preko mobilne mreže do zaslona korisnikovog mobilnog telefona. Korisnik ga upisuje i nova poruka ide do OTP AS-a, koji uspoređuje zaporke i odobrava konekciju. Za *voucher* pristup i pristup sa statičkom prijavom i zaporkom SCS služi kao poslužitelj za potvrdu vjerodostojnosti i odlučuje o uspostavljanju veze.

4.3. Sigurnost

Sigurnost je izrazito važan čimbenik kada je u pitanju lokalna mreža, posebice bežična. Osim zaštite korisnika od prisluškivanja i krađe korisnikovog akreditiva (*credentials),* potrebno je zaštititi i samu mrežu od pasivnih i aktivnih neovlaštenih upada i osigurati da korištenje mreže bude korisniku adekvatno naplaćeno.

Za enkripciju podataka standardi porodice 802.11 definiraju WEP (*Wired Equivalent Privacy*) protokol koji štiti od prisluškivanja i pasivnih napada na mrežu, a radi pomoću kodiranih ključeva. U praksi se WEP protokol, nažalost, pokazao prilično nezadovoljavajućim rješenjem. Većina korporacijskih i javnih bežičnih mreža uopće ga ne koristi zbog ograničene upotrebljivosti i vrlo nespretne uporabe ključeva.

Korporacijske bežične mreže su u pravilu dobro osigurane korištenjem virtualne privatne mreže (VPN - *Virtual Private Network*). VPN protokoli nalaze se iznad WLAN protokola na mrežnom složaju i osiguravaju potvrdu vjerodostojnosti i enkripciju s kraja na kraj mreže, npr., između prijenosnog računala i korporacijskog vatrozida (*firewall).*

Međutim, operatori javne bežične mreže se suočavaju s većim problemom sigurnosti. Zasad se uglavnom koristi kombinacija 802.1x link sloja i EAP i RADIUS protokola, kao što je prikazano na slikama u poglavlju 4.2.

EAP protokol (*Extensible Authentication Protocol*) je ekstenzija PPP protokola (*Point-to-point Protocol*) i koristi se za sigurnu potvrdu vjerodostojnosti na zračnom sučelju između korisnika i AP-a. Standard 802.1x predstavlja link sloj IEEE 802.11 porodice standarda. Osim što se može koristiti samo u kombinaciji s EAP-om, 802.1x definira kako će se koristiti EAP potvrda vjerodostojnosti. Sigurnost je garantirana samo za vrijeme potvrde vjerodostojnosti, ali ne i za vrijeme prijenosa podataka.

Gledano sa stajališta vrste potvrde vjerodostojnosti, korisnici koji koriste web-baziranu prijavu (OTP, stati-

čka zaporka, *voucher*) neće imati siguran prijenos podataka. Kod te vrste potvrde vjerodostojnosti nema enkripcije, niti zaštite integriteta podataka na zračnom sučelju, već korisnik mora sam zaštititi svoje podatke, npr., korištenjem virtualne privatne mreže. S druge strane, korištenjem U(SIM) potvrde vjerodostojnosti zračno sučelje kojim se prenose podaci između WLAN terminala i pristupne točke zaštićeno je TKIP protokolom (*Temporal-key Integrity Protocol*) koji je definiran u WPA (Wi-Fi *Protected Access*) sustavu zaštite podataka za WLAN. Na taj način korisnici GPRS/UMTS mreže imaju istu razinu sigurnosti korištenjem WLAN-a kao i u svojoj matičnoj mreži.

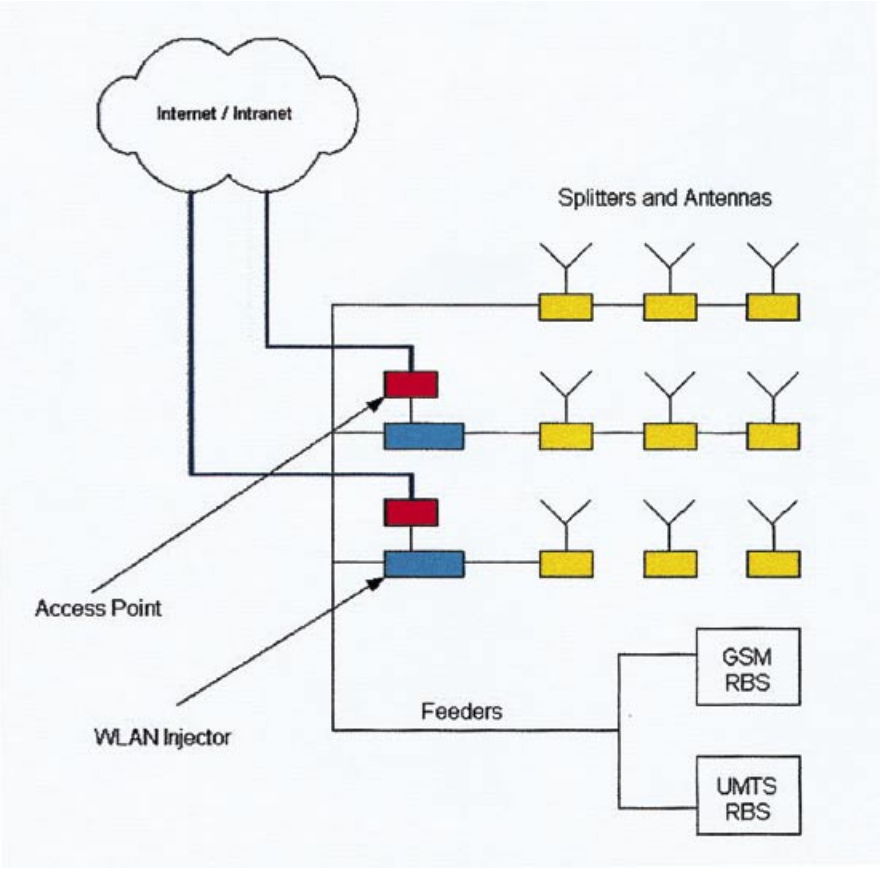
IEEE organizacija trenutačno radi na specifikaciji 802.11i standarda. Taj standard bi trebao popuniti još uvijek prazno mjesto protokola za sigurnost bežične mreže, jednostavnog za uporabu, jedinstvenog i efikasnog. 802.11i će biti izgrađen na temelju dva protokola: TKIP i AES (*Advanced Encryption Standard*). Enkripcijski algoritam AES je temeljen na EAP protokolu. Pomoću dinamičkog pregovaranja o potvrdi vjerodostojnosti i enkripcijskom algoritmu između pristupnog terminala i pristupne točke, osigurana je znatno veća razina sigurnosti od one postojeće. Međutim, nije još poznato kada će prva inačica 802.11i protokola izaći na tržište.

4.4. Profil elemenata mreže

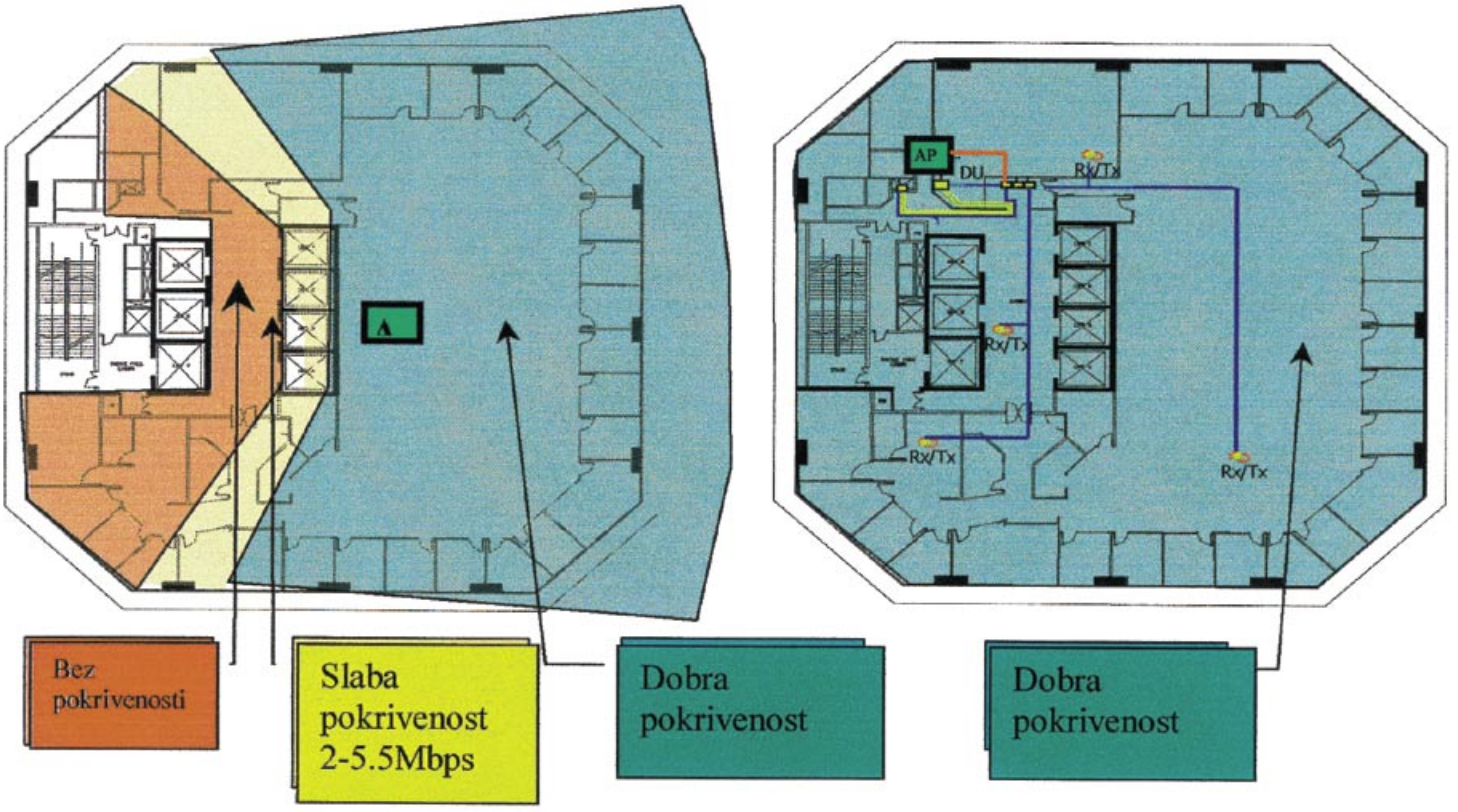
MO WLAN sustav nudi različite usluge različitim korisnicima – postoje *Gold, Silver* i *Bronze* pretplate. Diferencijacija se provodi prema geografskom faktoru i vrsti željenih aplikacija. Npr., povremeni korisnici (*Bronze*) imaju ograničeni pristup Internetu, dok redovni korisnici (*Silver*) nemaju ograničenja. Korisnici s posebnim pogodnostima (*Gold*) dobivaju dodatne usluge. Također, postoje i *voucher* kartice koje se prodaju u hotelima, aerodromima i sl.

4.5. Mogućnost neograničenoga kretanja

MO WLAN omogućuje neograničeno kretanje i na područjima koja pokrivaju drugi operatori u čijoj se ponudi nalaze WLAN usluge podržane RADIUS protokolom. Neograničeno kretanje uvjetuje da partneri koji tu mogućnost podržavaju definiraju profil elemenata mreže tako da oni budu kompatibilni.



Slika 6. Ericssonovo rješenje za WDAS - WLAN Distributed Antenna System



Slika 7. Usporedba samostojećega (Stand-alone) i WDAS rješenja za pokrivenost WLAN područja

5. Rješenje za istovremenu pokrivenost GSM i WLAN mreže (WDAS)

Trenutačni standard za WLAN pokrivenost je distribucija odvojenih pristupnih točaka u željenom području – to je tzv. samostojeći (»*Stand alone*«) način. Broj pristupnih točaka potrebnih za tu vrstu pokrivenosti je značajan. Na primjer, do 1000 pristupnih točaka je potrebno za pokrivanje područja aerodroma. Ericssonovo rješenje WLAN *Distributed Antenna System* (WDAS) je rješenje za istovremenu pokrivenost GSM i WLAN mreže, čime je broj pristupnih točaka smanjen za 30-70%. Naravno, pri tome nisu smanjene mogućnosti niti WLAN niti GSM odašiljača. Na Slici 6. prikazano je WDAS rješenje.

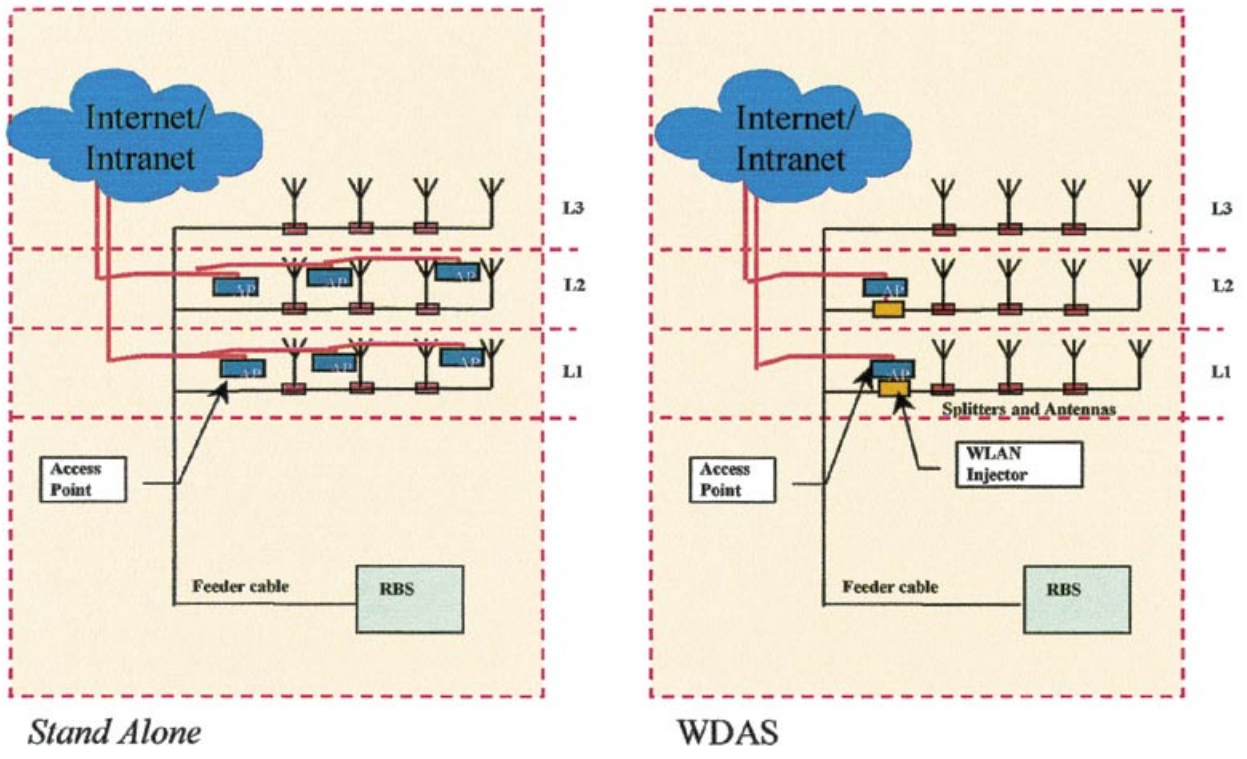
5.1. Prednosti WDAS rješenja

Prva prednost WDAS rješenja koju treba istaknuti je značajno smanjenje troškova implementacije, zbog smanjenja broja pristupnih točaka, odnosno smanjenja ulaganja u instalacijske usluge, održavanje, hardverske komponente i sl. Osim financijske, daljnje prednosti WDAS-a su: poboljšana RF propagacija, poboljšana kontrola osipanja signala i jednostavnost dobivanja dozvole.

Teoretski, jedna samostojeća pristupna točka (*Stand-alone* AP) ima pokrivenost od nekoliko stotina metara (na otvorenom). Međutim, u realnim uvjetima u zgradi, zbog prepreka kao što su zidovi, dizala i sl., pokrivenost se drastično smanjuje. Kao što je prikazano na Slici 7., kod standardnog načina bit će potrebno ponekad i znatno više pristupnih točaka nego kod WDAS rješenja. Što ima više prepreka, razlika je očiglednija.

Nekontrolirano osipanje signala je čest popratni efekt kod samostojećih implementacija. Kako je kod WLAN-a pitanje sigurnosti posebno istaknuto, posebnu pažnju treba obratiti tom problemu, naročito kod korporacijskih mreža gdje je sigurnost podataka prioritet. Koristeći WDAS, postiže se bolja kontrola područja pokrivenosti (*footprint)* i praktički se ne može detektirati signal izvan željenog područja.

Također, postoji još jedna prednost WDAS-a, ne toliko očigledna. Naime, kad se koristi samostojeći sustav,



Slika 8. WDAS implementacija

primjerice u trgovačkim centrima ili u zračnim lukama, pružatelj usluge mora pregovarati sa svakim pojedinim vlasnikom prostora u koji se planira postaviti pristupna točka ili antena. To je, naravno, vremenski zahtjevan i skup proces. Kod WDAS implementacije dovoljno je dogovoriti postavljanje antena s vlasnikom zgrade, kao što je obično slučaj i kod implementacije GSM antena.

5.2. Komponente WDAS sustava

WDAS implementacija se postiže korištenjem istih komponenata kao kod samostojećih verzija, s dodatkom WLAN Injectora koji omogućuje integraciju s GSM DAS (*Dual Attached Station*) elementom. Ericssonov WLAN Injector, ključna komponenta WDAS rješenja, smanjuje gubitke i za WLAN i za GSM/WCDMA signale, a također omogućuje i visoku izolaciju između WLAN pristupnih točaka i GSM/WCDMA osnovnih primopredajnih postaja (BTS - *Base Transceiver Station*) te djelotvorno eliminira rizik interferencije. Ako se, npr., WDAS postavlja na nekoliko katova zgrade, na svaki kat će se vjerojatno postaviti po jedan Injector i određeni broj pristupnih točaka (Slika 8.). Pristupne točke su umrežene u DAS na »*floor-by-floor*« bazi. Jedna pristupna točka podržava otprilike četiri antene.

6. Zaključak

Nelicencirane frekvencije i visoke brzine prijenosa podataka WLAN sustava čine ih zanimljivima i celularnim i ISP operatorima. Povezivanjem WLAN mreže na matičnu GPRS/UMTS mrežu, mobilni operatori mogu postići potpunu pokrivenost svoje mreže i ponuditi dodatni širokopojasni pristup na određenim javnim mjestima na kojima je to potrebno. WLAN je korak dalje u evoluciji bežičnih komunikacijskih sustava i jedna od komponenti buduće sveobuhvatne bežične širokopojasne mreže.

IEEE standardi 802.11a, 802.11b i 802.11g su trenutačno vodeći u svijetu. Ericssonovo MO WLAN rješenje podržava sva tri standarda, s naglaskom na 802.11b, poznatiji kao Wi-Fi, i u potpunosti je sagrađen na zahtjevima standardizacijske grupacije 3GPP. Bitna prednost MO WLAN rješenja je U(SIM) potvrda vjerodostojnosti pomoću EWAS-a (Ericsson WLAN *Authentication Server*), koji objedinjuje potvrdu vjerodostojnosti korisnika GPRS/UMTS i WLAN mreže.

Ericssonovo rješenje za pokrivenost WLAN mrežom je rješenje koje omogućuje istovremenu pokrivenost GSM i WLAN mreže, čime se postižu značajne direktne i indirektne uštede, dok performanse oba sustava ostaju ne-

promijenjene. Ključna komponenta WDAS rješenja je WLAN Injector, Ericssonov proizvod koji omogućuje integraciju WLAN DAS-a s GSM DAS-om.

7. Popis kratica

3GPP - Third-generation Partnership Project
AES - Advanced Encryption Standard
AKA - Authentication and Key Agreement
AP - Access Point
APIS - Application Program Interface Server
AS - Authentication Server
ASN - Access Serving Node
AUC - Authentication Center
BGw - Billing Gateway
CABS - Customer Administration and Billing Server
DAS - Distributed Antenna System
DHCP - Dynamic Host Configuration Protocol
DNS - Domain Name System
DS - Direct Sequence
DSSS - Direct-sequence Spread-spectrum
EAP - Extensible Authentication Protocol
EMA - Ericsson Multi Activation
ETSI - European Telecommunication Standard Institute
EWAS - Ericsson WLAN Authentication Server
FH - Frequency Hopping
GPRS - Global Packet Radio Service
GSM - Global System for Telecommunication
HLR - Home Location Register
HSS - Home Subscriber Server
IR - Infrared Light
LAN - Local Area Network
MAP - Mobile Application Part
MO WLAN - Mobile Operator WLAN
NTP - Network Time Protocol
OFDM - Orthogonal Frequency Division Multiplexing
OTP - One-Time Password
PDA - Personal Digital Assistant
PWLAN - Public Wireless Area Network
RADIUS - Remote Authentication Dial In User Service
SAS - Statistics and Accounting System
SCS - Service Control System
SIM - Subscriber Identification Module
SMS - Short Message Service
SUS - Sign-up and User self-administration Server
TKIP - Temporal-key Integrity protocol
UMTS - Universal Mobile Telecommunications System
U(SIM) - UMTS SIM
VPN - Virtual Private Network
WAN - Wide Area Network
WDAS - WLAN Distributed Antenna System
WEP - Wired Equivalent Privacy
WLAN - Wireless Local Area Network
WPA - WiFi Protected Access

Literatura

[1] Ranka Grubešić, Boris Drilo, Ana Janković, Lana Šindler: Public WLAN Access Service within 3G Network Evolution Scenario - An Ericsson View, WLAN Conference, Ljubljana, June 2003

[2] Tomas Boström, Tomas Goldbeck-Löwe and Ralf Keller: Ericsson Mobile Operator WLAN Solution, Ericsson Review, January 2002, pp. 36-43

[3] Tomas Göransson, Johan Ebenhard: Mobile Operator WLAN Release 2.0 - System Description, Ericsson-wide Internal Description, January 2003

ADRESA AUTORA:
Ranka Grubešić
e-mail: ranka.grubesic@ericsson.com
Ericsson Nikola Tesla d.d.
Krapinska 45
p.p. 93
HR-10 002 Zagreb
Hrvatska

Uredništvo je primilo rukopis 15. studenoga 2003.