

Arhitektura bežične LAN mreže IEEE 802.11

Coban, Martina

Undergraduate thesis / Završni rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:119:831754>

Rights / Prava: [In copyright](#)

Download date / Datum preuzimanja: **2020-10-22**



Repository / Repozitorij:

[Faculty of Transport and Traffic Sciences -
Institutional Repository](#)



**SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI**

Martina Coban

ARHITEKTURA BEŽIČNE LAN MREŽE IEEE 802.11

ZAVRŠNI RAD

Zagreb, prosinac 2017.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

ARHITEKTURA BEŽIČNE LAN MREŽE IEEE 802.11

ARCHITECTURE OF WIRELESS LAN NETWORK IEEE 802.11

Mentor: dr. sc. Ivan Forenbacher

Student: Martina Coban, 0135223432

Zagreb, prosinac 2017.

ARHITEKTURA BEŽIČNE LAN MREŽE IEEE 802.11

SAŽETAK

Bežične LAN mreže sve češćom uporabom postale su standard u povezivanju terminalnih uređaja (računala, mobilnih telefona, tableta i sl.) nudeći jednostavnu primjenu uz zadovoljavajuće brzine, veću mobilnost korisnika, a samim time brži i lakši pristup informacijama uz smanjene troškove. Uz mnoge prednosti bežičnih LAN mreža javlja se i glavni nedostatak, a to je sigurnost. Informacije se prenose zrakom, čime mreža postaje dostupna i izvan organizacije u kojoj se koristi. Kako bi se spriječila mogućnost neovlaštenog korištenja i pristupa mreže, jedna od opcija je uvođenje enkripcije (sigurnosni algoritmi). U ovom radu bit će prikazane osnovne značajke bežičnih LAN tehnologija, IEEE 802.11 i OSI referentni model, arhitektura IEEE 802.11 mreže, vrste IEEE 802.11 standarda, zatim sigurnost 802.11 mreže, te budući trendovi bežičnih tehnologija Li-Fi.

KLJUČNE RIJEČI: Bežične LAN mreže, IEEE 802.11, arhitektura, sigurnost, Li-Fi

SUMMARY

Wireless LAN networks have become a standard in access networks offering connection for various user's devices, such as computers, mobile phones, and tablets. They offer easy deployment with satisfactory speed, greater mobility of users, and thus faster and easier access to the sources of information with reduced costs. With many advantages there is also a major disadvantage, security issues. With information being transferred over the air interface, it makes the network accessible outside the organization in which it is used. In order to prevent unauthorized network use or access, one option is to use network encryption. This paper will review basic features of wireless LAN technology, IEEE 802.11 and OSI referent model, architecture of IEEE 802.11 network, types of IEEE 802.11 standards and security of 802.11 networks. The paper concludes by giving preview of future trends of wireless technology – Li-Fi.

KEYWORDS: Wireless LAN network, IEEE 802.11, architecture, security, Li-Fi

SADRŽAJ

1. Uvod	1
2. Osnove bežičnih LAN tehnologija	3
2.1 Povijesni pregled bežičnih LAN tehnologija	3
2.2 Općenito o bežičnoj LAN tehnologiji	4
2.3 Prednosti i nedostaci bežične LAN tehnologije	6
3. IEEE 802.11 i OSI referentni model	9
3.1 Slojevi OSI referentnog modela	9
3.2 Fizički sloj IEEE 802.11 mreže	10
3.2.1 FHSS	12
3.2.2 DSSS	12
3.2.3 Usporedba FHSS i DSSS tehnike	13
3.3 Sloj podatkovne veze IEEE 802.11 mreže	13
3.3.1 CSMA/CA mehanizam	14
3.3.2 RTS/CTS mehanizam	14
4. Arhitektura 802.11 mreže	16
4.1 Temeljni uređaji 802.11 mreže	16
4.2 Konfiguracije/topologije 802.11 mreže	18
4.3 Način rada 802.11 mreže	19
4.4 Sigurnost 802.11 mreže	21
5. Vrste IEEE 802.11 standarda	23
5.1 IEEE 802.11a standard	23
5.2 IEEE 802.11b standard	24
5.3 IEEE 802.11g standard	25
5.4 IEEE 802.11n standard	26
5.5 Novi trendovi IEEE 802.11 standarda	28
6. Budući trendovi Li-Fi tehnologija	31
6.1 Princip rada Li-Fi tehnologije	31
6.2 Prednosti i nedostaci Li-Fi tehnologije	32
7. Zaključak	33
LITERATURA	34
POPIS ILUSTRACIJA	36

Popis slika	36
Popis tablica	36
POPIS KRATICA	37

1.Uvod

U današnje vrijeme gdje tehnologija svakim danom sve više napreduje, teško se ne susresti s uređajima koji nam olakšavaju svakodnevnicu. Svaki čovjek barem jednom je imao priliku koristiti uređaj sa bežičnom tehnologijom. Pametni telefoni omogućuju korisnicima spajanje na internet putem Wi – Fi mreže, bez obzira je li se spajaju na kućne mreže ili javno dostupne mreže. Putem Interneta dostupna im je velika količina informacija, mogu slušati glazbu, gledati filmove, pristupati društvenim mrežama, čitati „online“ knjige, usavršavati svoje znanje putem raznih edukacija i učenja na daljinu (*teleworking*). Dakle, mogućnosti Interneta su neograničene.

Bežična LAN tehnologija i njezina sučelja standardizirani su IEEE 802.11 standardima. Kroz povijest ovo područje pokazalo je veliki interes za istraživanje i unapređenje te se brzo razvijalo. Rezultat toga je pojava nekoliko verzija IEEE 802.11 standarda poput 802.11a, 802.11b, 802.11n, 802.11ac i sl. Svaki od standarda koristi različite modulacije i tehnike prijenosa podataka, može raditi u različitim konfiguracijama ovisno da li korisnik želi napraviti mrežu sa ili bez infrastrukture. U tom pogledu vrlo je važno pitanje budućih tehnologija poput Li-Fi koje donose bitne promjene u brzinama prijenosa podataka, sigurnosti mreže zatim ekonomskim i ekološkim aspektima u odnosu na IEEE 802.11 mreže. Zbog toga glavni cilj rada je pobliže prikazati bežičnu LAN tehnologiju, njezine standarde i karakteristike istih te zašto se sve više ulaže u novu tehnologiju Li-Fi.

Rad je podijeljen u sedam cjelina:

1. Uvod
2. Osnove bežičnih LAN tehnologija
3. IEEE 802.11 i OSI referentni model
4. Arhitektura IEEE 802.11
5. Vrste IEEE 802.11 standarda
6. Budući trendovi – Li-Fi tehnologija
7. Zaključak.

Drugo poglavlje nazivom osnove bežičnih LAN tehnologija opisuje osnovne značajke bežičnih LAN tehnologija te njihov radijus pokrivanja. Prikazan je povijesni pregled bežičnih LAN tehnologija, zatim područje definiranje te prednosti i nedostaci bežičnih LAN tehnologija.

Treće poglavlje opisuje IEEE 802.11 i OSI referentni model. Prikazan je OSI referentni model po slojevima, najviše je bazirano na fizički sloj i sloj podatkovne veze. U fizičkom sloju opisuje se FHSS i DSSS tehnika dok u sloju podatkovne veze prikazan je CSMA/CA i RTS/CTS mehanizam.

Četvrto poglavlje arhitektura IEEE 802.11 standarda opisuje temeljne uređaje, topologiju IEEE 802.11 mreže te načine rada 802.11 mreže. Spomenuta je sigurnost te načini zaštite IEEE 802.11 mreža.

Peto poglavlje opisuje vrste IEEE 802.11 standarda, njihove oznake i godinu standardizacije, frekvencijsko područje u kojem djeluju, širinu prijenosnog pojasa i broj kanala, zatim korištene modulacije i teoretske brzine prijenosa.

Zadnje, šesto poglavlje nazivom budući trendovi Li-Fi tehnologija opisuje tehnologiju koja je u fazi razvijanja te njezine prednosti i nedostatke u odnosu na Wi-Fi tehnologiju.

2.Osnove bežičnih LAN tehnologija

Bežična LAN mreža (*Wireless Local Area Network – WLAN*) je komunikacijska mreža koja omogućava razmjenu podataka između dva ili više povezanih uređaja putem radio valova. Razvijena je kao dodatak žičnoj LAN mrežnoj tehnologiji. LAN (*Local Area Network*) mreža je lokalna mreža koja se najčešće koristi unutar jedne ili više zgrada na ograničenom području. LAN ima mogućnost priključivanja nekoliko stotina terminala, osobnih računala na zajednički komunikacijski kanal. Radijus pokrivanja ovisi o prijenosnom mediju koji se koristi (koaksijalni kabel, upletena parica i optičko vlakno) a iznosi od 100 metara do nekoliko desetaka kilometara, [1]. Bežična LAN mreža ima nešto manji radijus pokrivanja, od 30 do 50 metara u zatvorenom a više od 100 metara u otvorenom prostoru. WLAN se koristi u okviru jedne kuće, zgrade, ustanove, tvornice i sl. te omogućuje veću mobilnost korisnika. Može se primijeniti na mjestima gdje je realizacija ožičenja skupa ili teško izvediva što ga čini ekonomičnim rješenjem umreženja, [1]. Na slici 1 crvenim pravokutnikom označen je središnji uređaj kojim se ostvaruje žična i bežična LAN komunikacija.



Slika 1. Prikaz žične i bežične LAN tehnologije

Preuzeto od [25]

2.1 Povijesni pregled bežičnih LAN tehnologija

Povijest bežičnih mreža i bežičnog umrežavanja seže u davnu 1800-tu godinu pojavom radio valova. Otkrićem radio valova razvila se radio tehnologija bez koje danas bežična tehnologija uopće ne bi postojala. Širenje tehnologije raslo je tijekom godina i proširilo se na ono čime danas komuniciramo, [6].

Godine 1857. u Hamburgu, njemački fizičar Heinrich Rudolf Hertz proizveo je prvi radio val. Telegrafске žice koristio je za primanje radio valova u signalnom obliku, a do 1894. godine komunikacija radio valovima postaje svakodnevica. Heinrich Rudolf Hertz otkrićem elektromagnetskih valova otvorio je put za radio,

televiziju i radar. Nekoliko godina kasnije, talijanski inženjer i fizičar Marchese Guglielmo Marconi proširenjem radijusa odašiljanja radio vala na tri kilometara, postaje "Ocem radija". Do 1899. godine taj oblik komunikacije mogao je putovati prilično daleko u svoje vrijeme. Marconi je mogao poslati signal u radijusu od 15 kilometara preko kanala Bristol, proširenjem radijusa do 50 kilometara mogla se ostvariti komunikacija preko Engleskog kanala u Francusku. Od 1901. godine Marconi je mogao ostvarivati međukontinentalnu komunikaciju radio valovima koja do tog trenutka nije bila moguća, [6].

Drugi svjetski rat predstavlja značajan napredak bežičnih tehnologija. Sjedinjene Države prve su koristile radio valove za prijenos podataka, te im je taj način komunikacije uveliko pomogao tijekom rata. Godine 1971., skupina istraživača pod vodstvom Normana Abranona na Sveučilištu Hawaii, stvorila je prvu radio komunikacijsku mrežu s komutacijom paketa (*packet switching*) pod nazivom „ALOHAnet“. ALOHAnet bila je prva bežična LAN mreža koja nije imala puno mogućnosti ali je bila veliko otkriće. Sastojala se od sedam računala smještenih na četiri otoka koji su komunicirali sa središnjim računalom na otoku Oahu bez uporabe telefonske linije. Sustavu su dodjeljena dva frekvencijska pojasa od 407.350 MHz i 413.475 MHz. Godine 1972, ALOHAnet spaja se na kopnu s WLAN sustavom ARPAnet (*Advanced Research Projects Agency Network*). Arpanet je razvilo američko Ministarstvo obrane za povezivanje sveučilišta i istraživačkih centara, [6].

Prva generacija WLAN tehnologije imala je ograničen kapacitet i vrlo male brzine prijenosa podataka. Druga generacija WLAN tehnologije bila je četiri puta brža od prethodne. Danas, koristi se treća generacija WLAN tehnologije koju je standardizacijsko tijelo IEEE oformilo pod nazivom 802.11. IEEE 802.11 prvi je standard za bežične lokalne mreže objavljen 1997. godine, nakon toga javljaju se inačice, [6].

2.2 Općenito o bežičnoj LAN tehnologiji

Bežične mreže (*Wireless Network*) su računalne mreže koje koriste elektromagnetske valove za komunikaciju. Elektromagnetski valovi nastaju titranjem električnog i magnetskog polja u propusnom mediju na određenoj frekvenciji, prema načinu širenja mogu se podijeliti na longitudinalne i transverzalne valove. Raspon frekvencija određuje koju količinu informacija elektromagnetski signal može prenjeti. Spektar elektromagnetskih valova vrlo je širok te svaki dio spektra ima različita svojstva i frekvenciju. Tako elektromagnetske valove možemo podijeliti na: radio valove, mikrovalove, infracrvene valove, vidljivu svjetlost, ultravioletnu svjetlost te X i Gama zrake. Ovisno o svojstvima neki dijelovi spektra su pogodniji za prijenos informacija od drugih, [23]. Tablica 1 prikazuje raspon frekvencija i valnih duljina

elektromagnetskih valova, crvenom bojom označeno je frekvencijsko područje rada IEEE 802.11 standarda.

Tablica 1. Frekvencijski spektar EM valova

	Raspon frekvencija	Raspon valne duljine
ELF (Extremely low frequency)	3 Hz – 30 Hz	100000 km – 10000 km
SLF (Super low frequency)	30 Hz – 300 Hz	10000 km – 1000 km
ILF (Infra Low frequency)	300 Hz – 3 kHz	1000 km – 100 km
VLF (Very low frequency)	3 kHz – 30 kHz	100 km – 10 km
LF (Low frequency)	30 kHz – 300 kHz	10 km – 1 km
MF (Medium frequency)	300 kHz – 3 MHz	1km – 100 m
HF(High frequency)	3 MHz – 30 MHz	100 m – 10 m
VHF (Very high frequency)	30 MHz – 300 MHz	10 m – 1 m
UHF (Ultra high frequency)	300 MHz – 3 GHz	1 m – 10 cm
SHF (Super high frequency)	3 GHz – 30 GHz	10 cm – 1 cm
EHF (Extremely high frequency)	30 GHz – 300 GHz	1 cm – 1 mm
IR (Infrared) light	300 GHz – 400 THz	1 mm - 750 nm
Visible light	400 THz – 1 PHz	380 – 750 nm
UV (Ultra Violet) light	1 – 30 PHz	10 – 380 nm
X rays	30 PHz – 30 EHz	0.01 – 10 nm
Gamma and cosmic rays	>3 EHz	<0.1 nm

Podatci od [5].

Bežične LAN mreže za prijenos informacija koriste elektromagnetske valove u radijskom ili infracrvenom frekvencijskom području. Osnovna uloga bežičnih LAN mreža je omogućiti mobilnim korisnicima pristup mreži na određenom području. Bežična LAN mreža može biti proširenje žične LAN mreže na mjestima gdje je izgradnja žične LAN mreže neisplativa ili nedopuštena. Može služiti i za povezivanje dvije žične LAN mreže na različitim lokacijama. Korištenje bežičnih LAN mreža raste iz godine u godinu zbog snižavanja cijena opreme i uređaja potrebnih za bežični pristup mreži, te sve veće dostupnosti mobilnih terminalnih uređaja visokih kvaliteta i prihvatljivih cijena, [1], [9].

Proces normizacije imao je veliki utjecaj za razvoj, unaprijeđenje i primjenu bežičnih LAN sustava, tako je u veljači 1980. godine standardizacijsko tijelo IEEE (*Institute of Electrical and Electronic Engineers*) osnovalo radnu grupu 802. Radna grupa 802 radi na principu OSI referentnog modela koji definira dva sloja, fizički sloj (*Physical layer*) i sloj podatkovne veze (*Data link layer*). Kako bi više različitih mreža mogle odašiljati podatke u isto vrijeme, u sloju podatkovne veze potrebno je rabiti postupke upravljanja pristupom prijenosnom mediju. Tako se sloj podatkovne veze dijeli na dva podsloja: podsloj za upravljanje pristupom prijenosnom mediju (*Medium Access Control - MAC*) te podsloj za upravljanje logičkom vezom (*Logical Link Control - LLC*), [1], [9]. U poglavlju 3 biti će detaljnije opisani slojevi OSI referentnog modela i njegove funkcije.

Početak razvoja bežičnih LAN mreža usko je vezan uz postojeće IEEE 802 standarde. Prvo se koristio standard 802.3 poznat pod imenom *Ethernet*, no zbog svojih karakteristika nije zaživio. Zatim se pokušalo sa standardom 802.4 tzv. *token bus* koji također nije zaživio u bežičnim LAN mrežama. Uvidjevši potrebu za nečim

novim, 1990. godine radna grupa IEEE 802 formira radnu podgrupu IEEE 802.11, koja je sedam godina kasnije objavljena kao prvi standard za bežične LAN mreže. U zemljama Europe pa tako i u Republici Hrvatskoj za rad bežičnih LAN mreža koristi se nelicencirano ili ISM (*Industrial, Scientific and Medical*) frekvencijsko područje od 2,4 GHz, dok u zemljama izvan Europe koristi se i ISM područje od 5,8 GHz, [1], [9].

Kao što je već rečeno, bežične LAN mreže za prijenos podataka koriste radio valove koji prenose energiju signala do prijemnika. Podaci koji se prenose se moduliraju, odnosno u prijenosni signal se utiskuje signal informacije. Signal putuje prijenosnim medijem (zrakom) do prijemne strane gdje se vrši demodulacija, kako bi se ponovno dobila informacija. Prilikom prijenosa od izvorišta do odredišta može se javiti izobličenje signala, no javljaju se i specifične smetnje kojih nema u drugim vrstama prijenosa, prema [3],[4], to su:

- *Path loss* - gubitak snage EM zračenja zbog udaljenosti od odašiljača
Snaga EM zračenja može opadati zbog udaljenosti prijemnika od odašiljača te snazi odašiljača.
- *Multipath propagation* - višestazno prostiranje signala
Višestazno prostiranje nastaje kada se dijelovi elektromagnetskog vala iz jednog izvora do odredišta odbijaju od tlo i objekte. Na odredište uz izvorni signal dolaze i njegove zakašnjele varijante.
- Mješanje (interferencija) signala sa drugim izvorima
Radio izvori koji odašilju signal u istom frekvencijskom području međusobno će se pomiješati. Primjer, bežični telefon koji radi na frekvenciji od 2,4 GHz i bežični LAN prijemnik koji također radi na frekvenciji od 2,4 GHz. Tako bežični LAN korisnik koji komunicira putem bežičnog telefona može očekivati smetnje na mreži i telefonu. Također, elektromagnetska buka unutar okoliša (buka motora, mikrovalne pećnice) može dovesti do smetnje.
- *Shadow fading* – prigušenje signala zbog prepreka u prostoru
Shadow fading uzrokuju fizičke prepreke na putu prostiranja EM valova (razni objekti, zgrade). Prigušenje signala može ovisiti o materijalu od kojeg je sastavljena prepreka.

2.3 Prednosti i nedostaci bežične LAN tehnologije

Svaka tehnologija ima svoje prednosti i nedostatke, stoga će u ovom dijelu rada biti navedene prednosti i nedostaci bežične LAN tehnologije u odnosu na žičnu LAN tehnologiju. Danas sve više se koriste bežične LAN tehnologije zbog svoje mobilnosti koje pružaju korisnicima, jednostavnost rukovanja, te manjih troškova

ulaganja, najveći nedostatak predstavlja sigurnost koja se svakim danom sve više usavršava. U nastavku su nabrojene prednosti bežične LAN tehnologije, iz izvora [7], to su:

- Poboljšana produktivnost i usluga. Bežična LAN tehnologija može pružati korisnicima informacije u realnom vremenu bilo kada i bilo gdje. Ova mobilnost podržava produktivnost i mogućnost pružanja usluga koji nije moguć u klasičnim žičnim mrežama.
- Jednostavnost i brza instalacija. Instalacija bežične LAN tehnologije može biti brza i jednostavna bez povlačenja kabela kroz zidove i stropove.
- Fleksibilnost instalacije. Bežična LAN tehnologija omogućuje mreži da putuje gdje žica ne može.
- Smanjeni troškovi vlasništva. Iako su početna ulaganja bežične LAN tehnologije veća od troškova žične LAN tehnologije, ukupni troškovi instalacije i životnog ciklusa mnogu biti znatno niži. Prednosti dugoročnog ulaganja veća su u dinamičnim okruženjima koja zahtijevaju česte selidbe, dodatke i promjene.
- Skalabilnost (prilagodba povećanim zahtjevima). Bežični LAN sustavi mogu se konfigurirati u različitim topologijama kako bi se zadovoljile potrebe specifičnih aplikacija i instalacija. Konfiguracije se lako mijenjaju i kreću se od nezavisnih mreža prikladnih za mali broj korisnika koje omogućuju *roaming* na širem području. Bežični LAN pruža sve funkcionalnosti žičnog LAN-a, ali bez fizičkih prepreka odnosno žica. Konfiguracija bežične LAN mreže obuhvaća neovisne mreže nudeći peer-to-peer povezanost, i infrastrukturne mreže, održavajući potpuno distribuirane podatkovne komunikacije.

Nedostaci bežične LAN tehnologije, iz [11], su:

- Sigurnost. Pitanje sigurnosti jedan je od najvećih prioriteta bežične LAN mreže, stoga važno je informirati se i odabrati jednu od tehnologija enkripcije (šifriranja). Međutim, neke od najčešće korištenih metoda enkripcije pokazuju slabosti i tu nastupaju „hakeri“, koji neovlašteno ulaze u mrežu i koriste privatne podatke u vlastite svrhe.
- Pokrivenost područja. Raspon pokrivanja područja s standardnom opremom iznosi do 30 metara, što je dovoljno u okviru doma, zgrade ali ne i za veće organizacije. Za dobivanje dodatnog raspona kupuju se ponavljači ili dodatne pristupne točke te se troškovi povećavaju.
- Pouzdanost. Signal bežičnog umrežavanja podlozan je smetnjama zbog svog prijenosnog medija, kao i složenim propagacijskim efektima koji su izvan kontrole mrežnog administratora.
- Brzina prijenosa. Ovisno o standardu bežične LAN tehnologije koju koristimo kreće se od 11 Mbps do 54 Mbps, te u novije vrijeme do 100Mbps i više. To su zadovoljavajuće brzine za korisnike koji obavljaju osnovne funkcije, međutim u

većim organizacijama koje zahtjevaju mnogo veće brzine i dalje se koristi žično LAN umrežavanje.

3. IEEE 802.11 i OSI referentni model

OSI (*Open System Interconnection*) referentni model je model za povezivanje otvorenih sustava. Definira funkcije i procese za povezivanje dvaju različitih računalnih sustava. Taj model razvijen je od strane Međunarodne organizacije za normizaciju (ISO – *International Organization for Standardization*) 1977. godine, a službeno je prihvaćen u listopadu 1984. godine kao ISO norma 7928. OSI referentni model sastoji se od sedam slojeva, prvi najniži sloj je fizički sloj (*Physical Layer*), drugi sloj je sloj podatkovne veze (*Data Link Layer*), treći sloj je mrežni sloj (*Network Layer*), četvrti sloj je transportni sloj (*Transport Layer*), peti sloj je sloj sesije (*Session Layer*), šesti sloj je prezentacijski sloj (*Presentation Layer*), a sedmi najviši sloj je aplikacijski sloj (*Application Layer*), [8]. Na OSI-RM temelje se IEEE 802.11 mreže koje su definirane sa samo prva dva sloja: fizičkim slojem i slojem podatkovne veze, prikazano na slici 2.



Slika 2. IEEE 802.11 mreža u odnosu na OSI referentni model

Preuzeto od [9]

3.1 Slojevi OSI referentnog modela

Fizički sloj je najniži sloj OSI-RM i definiran je fizičkim medijem koji omogućava prijenos signala kroz mrežu. Podaci se prijenosnim medijem prenose u obliku signala prema posebno utvrđenim protokolima kako bi se na odredištu ponovno mogao konvertirati u podatke. Ovaj sloj razlikuje se od ostalih po tome što ispod njega postoji samo pasivno okruženje, [8].

Sloj podatkovne veze omogućava prijenos podataka (okvira) do fizičkog sloja. Podaci koji se šalju sadrže oznaku odredišta (MAC adresa), oznaku pošiljatelja te

informacije o tipu okvira, usmjeravanja i segmentaciji. Na ovom sloju obavlja se detekcija i korekcija pogrešaka. Sloj podatkovne veze dijeli se na dva sloja, a to su: kontrola logičke veze (LLC – *Logical Link Layer*) i kontrola pristupa mediju (MAC – *Medium Access Control*), [8].

Mrežni sloj određuje najbolji put za prijenos podataka između dva umrežena računala. Ova sloj prevodi logičke adrese (IP) u fizičke adrese (MAC). Mrežni sloj osigurava putanju paketa u mreži prilikom prijenosa, ukoliko je potrebno može dodatno usitniti pakete u manje pakete, [8].

Transportni sloj omogućava pouzdan prijenos podataka između dva računala. Osigurava da svi podaci koji se šalju budu primljeni i da se mogu koristiti. Protokoli transportnog sloja su: TCP (*Transmission Control Protocol*) i UDP (*User Datagram Protocol*). Transportni sloj osigurava efikasno korištenje mrežnih resursa i usluga ovisno o zahtjevima krajnjih korisnika, [8].

Sloj sesije osigurava komunikaciju između aplikacija na umreženim računalima. Ovaj sloj nadzire prometne puteve, definira početak i kraj komunikacije te obnavlja prekinute veze. Ako u sustavu postoji više mrežnih aplikacija, sloj sesije omogućava nesmetanu komunikaciju između njih te dolazeće podatke usmjerava aplikaciji kojoj su namijenjeni, [8].

Prezentacijski sloj pretvara podatke koje dobiva iz aplikacijskog sloja u oblik pogodan za čitanje. Ovaj sloj je odgovoran za kriptografsku zaštitu te konverzije protokola, [8].

Aplikacijski sloj je najviši sloj OSI-RM koji definira usluge i protokole po kojima aplikacijski programi komuniciraju. Primjeri programa koji koriste aplikacijski sloj su: elektronička pošta, konferencijske aplikacije, WWW (*World Wide Web*), [8].

3.2 Fizički sloj IEEE 802.11 mreže

802.11 standard definira podsloj MAC, MAC servise i protokole te tri četiri fizička sloja. Četiri fizička sloja unutar 802.11 standarda uključuju:

- Infracrveni frekvencijski pojas (IR – *Infra Red*),
- Prošireni spektar skakanja frekvencija (FHSS – *Frequency Hopping Spread Spectrum*),
- Prošireni spektar izravnim širenjem spektra (DSSS – *Direct Sequence Spread Spectrum*),
- Tehniku frekvencijskog multipleksa ortogonalnih podnositelja (OFDM – *Orthogonal Frequency Division Multiplexing*), [16].

802.11 Logical Link Control				2. Data Link Layer
802.11 Medium Access Control				
IR	FHSS	DSSS	OFDM	1. Physical Layer

Slika 3. 802.11 područje definiranja

Podatci od [16]

U razvoj infracrvenog fizičkog sloja vrlo je malo ulagano (zbog prirode tehnologije-nužnosti direktne optičke vidljivosti između uređaja), FHSS i DSSS spadaju u tehniku proširenog spektra, a OFDM se koristi za uskopojasne mikrovalne LAN-ove.

TEHNIKA PROŠIRENOG SPEKTRA

Spread Spectrum tehnika ostvaruje se sa korištenjem pseudoslučajnog binarnog niza (PN – *pseudo noise*) koji ima valni oblik sličan šumu. Ako se korisni signal pomnoži sa pseudoslučajnim binarnim nizom, prema [16], dolazi do:

- Spektar snage signala proširuje osnovni pojas na šire frekvencijsko područje,
- Signal poprima valni oblik šuma.

Korisni signal prilikom prijenosa skriva se unutar šuma komunikacijskog kanala. Prošireni korisni signal vraća se na prijašnju širinu pojasa, dok se ostale smetnje proširuju. Na ovaj način smanjuje se gustoća spektra šuma u osnovnom pojasu te poslije filtriranja od njega ostaje samo mali šum. Na prijemnoj strani signal se sažima te dekodira pomoću PN signala. Zbog male gustoće snage, signal proširenog spektra omogućuje korisnicima nesmetano korištenje istog medija za slanje podataka, prilikom čega se međusobno neće ometati, [16].

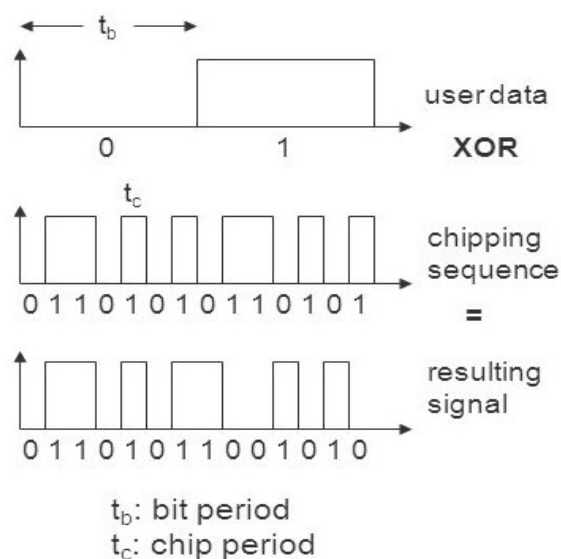
Prošireni spektar definira tri tehnike, FHSS i DSSS tehniku te *Hybrid System* koji je kombinacija prve dvije tehnike. Kod FHSS-a proširenje spektra se provodi zajedno s postupkom modulacije, dok se kod DSSS-a proširenje spektra provodi prije primjene postupka modulacije,[16].

3.2.1 FHSS

Kod FHSS tehnike unutar spektra se definiraju frekvencijski skokovi. Skokovi su promjene frekvencija na kojima se prenose podaci. Promjenama frekvencije upravlja PN-slijed. Kod načina rada FHSS-a, predajnik neko vrijeme šalje kratke nizove podataka na jednoj frekvenciji, a zatim se prebacuje na drugu frekvenciju. Predajnik i prijatelj moraju biti sinkronizirani prema slijedu preskakanja da nebi došlo do gubitka podataka. Kod IEEE 802.11b standarda, frekvencije se mijenjaju 1600 puta u sekundi. Cijeli frekvencijski pojas od 2,4 GHz dijeli se na 79 neprekrivajućih podkanala a širina svakog kanala iznosi 1 MHz. *Time slot* označava vremenski interval za vrijeme kojeg se u određenom kanalu nalazi podatak, i traje minimalno 625 mikrosekundi. Prilikom pojave interferencije na jednoj frekvenciji, podaci se ponovno šalju drugom frekvencijom. FHSS postiže visoki stupanj sigurnosti prijenosa zbog stalnog mijenjanja frekvencije, stalno mijenjanje frekvencije omogućava rad više različitih radijskih mreža unutar istog područja, ali bez međusobnih ometanja. FHSS omogućava brzine prijenosa podataka od 1-2 Mbps, [16].

3.2.2 DSSS

Kod DSSS-a, na signalu koji se prenosi prvo se vrši XOR operacija (operacija množenja) s pseudo slučajnim signalom (PN) veće frekvencije i na taj način signalu se proširuje spektar snage na šire frekvencijsko područje. Na slici 4 prikazan je postupak izvođenja XOR operacije.



Slika 4. Prikaz XOR operacije

Preuzeto od [10].

Nakon proširenja, signal se modulira modulacijskom tehnikom (npr. BPSK, FSK) i prenosi kroz bežični prijenosni medij. Kada stigne do odredišta, na prijemnoj strani, modulirani signal se demodulira. Na izlazu iz demodulatora prošireni signal se množi s lokalno generiranim pseudo slučajnim signalom koji je u koleraciji sa PN signalom korištenim kod predajnika. Zatim se signal ponovo sužava te se dobiva originalni oblik. Kod IEEE 802.11 standarda pseudo slučajni kod još se naziva *chip* ili *chipping code* (on omogućuje prijamniku da profiltrira šumove i smetnje). DSSS tehnika omogućava brzine prijenosa podataka od 1, 2, 5.5 i 11 Mbps, [16].

3.2.3 Usporedba FHSS i DSSS tehnike

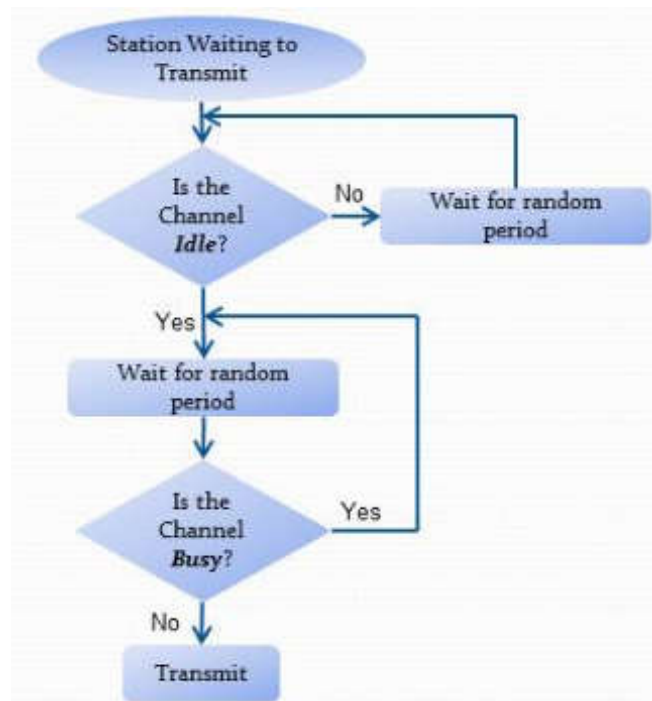
Usporedbom FHSS i DSSS tehnike, već na prvi pogled možemo vidjeti prednosti DSSS tehnike. Iako je DSSS tehnika mnogo robusnija, ima veći doseg pokrivenosti čak i kada radi s pola izlazne snage u odnosu na FHSS tehniku. FHSS nudi više iskoristivih frekvencija zbog skakanja po kanalima, no postoji povećana mogućnost smetnji ukoliko se koristi više uređaja na određenom prostoru. Kako FHSS modulacija nije toliko raširena, možemo ju koristiti kada u komunikacijskom kanala postoji puno smetnji. Kod FHSS tehnike mogućnost kolizije je manja. Ipak, sve te prednosti nisu dovoljne da se usporede s DSSS tehnikom koja može raditi na puno većim udaljenostima. Kod DSSS-a, s manjim brojem bežičnih točaka možemo dobiti bolju iskoristivost, no opet DSSS omogućuje korištenje većeg broja pristupnih točaka za potpuno iskorištenje kapaciteta bez generiranja smetnji. Dakle, DSSS tehnika ima veću efikasnost u odnosu na FHSS, [20].

3.3 Sloj podatkovne veze IEEE 802.11 mreže

Sloj podatkovne veze IEEE 802.11 sastoji se od dva podsloja: podsloja MAC (*Medium Access Control*) i kontrole logičke veze (LLC – *Logic Link Control*). 802.11 koristi isti 802.2 LLC i 48-bitno adresiranje kao i drugi 802 LAN-ovi, što omogućuje vrlo jednostavno premošćivanje s bežične na žičnu mrežu, ali MAC je jedinstven za bežične LAN mreže. 802.11 MAC vrlo je sličan konceptu 802.3, jer je osmišljen kako bi podržao više korisnika koji koriste zajednički medij. 802.3 Ethernet LAN-ovi koriste CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) mehanizam, dok u 802.11 bežičnim LAN-ovima koristi se nešto izmijenjeni mehanizam CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*). U 802.11 mrežama još se koristi RTS/CTS mehanizam koji spriječava koliziju, [19].

3.3.1 CSMA/CA mehanizam

CSMA/CA je osnovni pristupni mehanizam za IEEE 802.11 mreže. Vrlo je sličan CSMA/CD mehanizmu koji se koristi u žičnim LAN mrežama (IEEE 802.3) ali s nekoliko razlika. Za razliku od IEEE 802.3 mreža koje šalju signale dok god ne detektira neki drugi paket, CSMA/CA neće početi s odašiljanjem dok bilo koja druga stanica emitira signal i dok se ne dobije povratna informacija da određena stanica sluša. Prije emitiranja signala, bežični uređaj osluškava komunikacijski kanal kako bi ustanovio emitira li ga neki drugi uređaj. Ukoliko postoji neki drugi uređaj pričekat će slučajno generirani vremenski odsječak i ponovo slušati komunikacijski kanal, ako nitko drugi ne koristi kanal, uređaj počinje s emitiranjem, [20]. Slika 5 opisuje princip rada CSMA/CA mehanizma.



Slika 5. CSMA/CA mehanizam

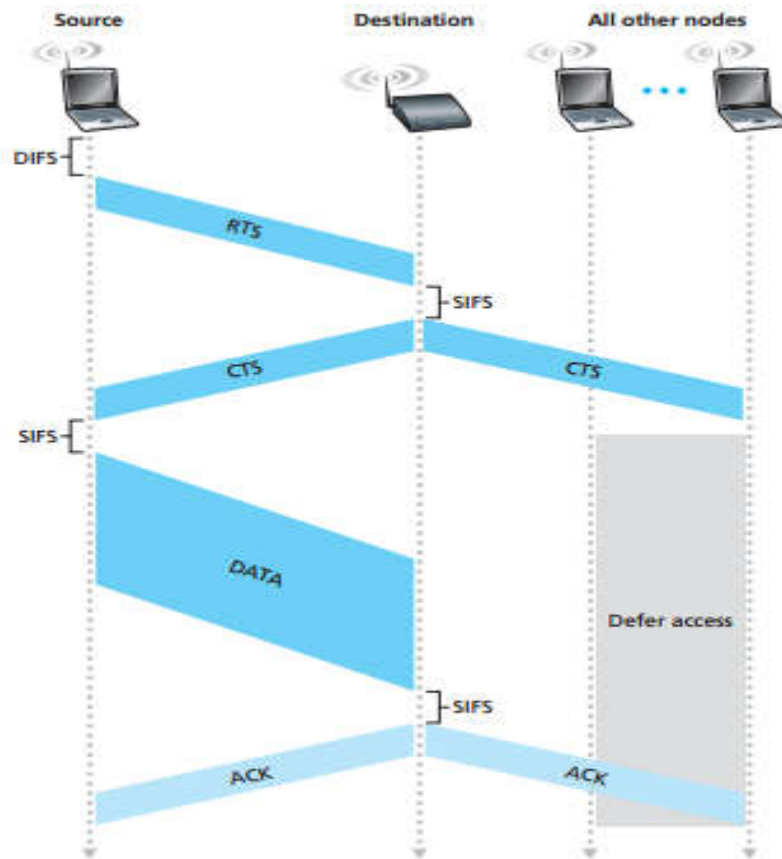
Preuzeto od [17].

3.3.2 RTS/CTS mehanizam

Kako bi se spriječila kolizija koja nastaje istovremenim emitiranjem dvaju uređaja, u IEEE 802.11 standard se uklopio još jedan mehanizam, RTS/CTS (Request to Send/Clear to Send).

Primjer RTS/CTS komunikacije je slijedeći, ukoliko je neki bežični klijent poslao adresirani podatak na neku pristupnu točku (AP), AP će poslati RTS okvir tom klijentu

te tražiti vrijeme predajte tog podatka. Bežični klijent odgovara CTS okvirom, u kojem govori AP-u da je spreman primiti njegovu transmisiju i da neće održavati komunikaciju ni s kim drugim dok AP ne završi prijenos, [20]. Slika 6 opisuje primjer RTS/CTS komunikacije.



Slika 6. Primjer RTS/CTS komunikacije

Preuzeto od [3].

U isto vrijeme i drugi bežični klijenti mogu "vidjeti" ovaj dogovor ali se ne priključuju komunikaciji. Ovaj način omogućava prijenos podataka s minimalnom mogućnošću dolaska kolizije, te rješava problem „skrivenog klijenta“. Skriveni klijent javlja se kada imamo dva ili više klijenata koji su u doseg AP-a ali ne i međusobno. Za razliku od žičnih LAN mreža gdje svaki klijent direktno "vidi" svakog drugog klijenta, udaljenost kod bežičnih LAN mreža uzrokuje pojavu skrivenog klijenta, tako da klijenti mogu komunicirati isključivo posredstvom AP-a, [20].

4.Arhitektura 802.11 mreže

Arhitekturu 802.11 mreže možemo opisati kao skup međusobno povezanih komponenti koje zajedno funkcioniraju u cjelini. Prema [5], sastoji se od sljedećeg:

- Transceiver (transmitter/receiver)-klijenti
- Antena (omnidirekcionalna)-antena za prijem signala
- Pristupna točka (AP – *Access Point*)
- Bežični medij

Prilikom izrade bežične LAN mreže potrebno je imati vanjsku antenu, pristupnu točku (AP) koja se nalazi u bežinom usmjerivaču, bežični adapter (mrežna kartica uređaja) te jednog ili više klijenata. Bežični usmjerivač (*Wireless Router*) je mrežni uređaj čija je osnovna funkcija prosljeđivanje paketa iz vanjske (WAN – *Wide Area Network*) u lokalnu mrežu (LAN – *Local Area Network*) te određivanje najboljih ruta paketa kroz mrežu. Većina bežičnih usmjerivača imaju ugrađen prospojnik (*switch*) koji služi za spajanje više računala u LAN mrežu, [8].

4.1 Temeljni uređaji 802.11 mreže

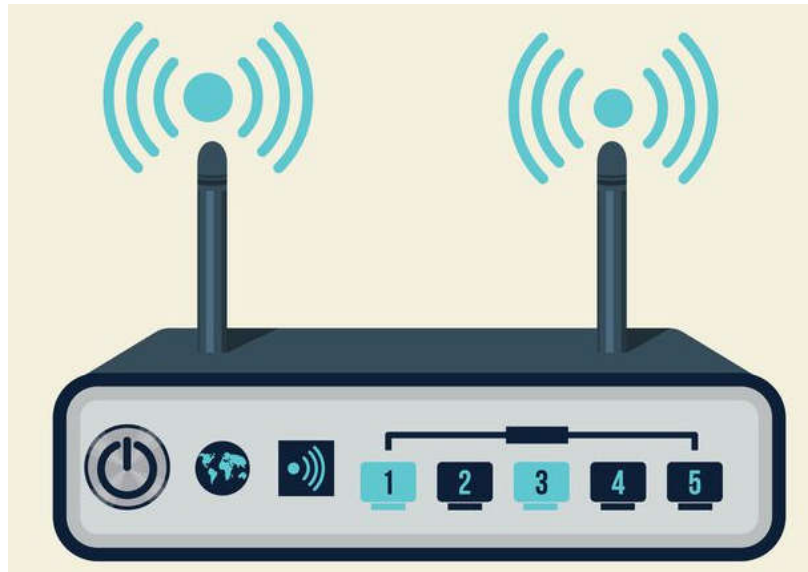
PRISTUPNA TOČKA

Pristupna točka je uređaj koji omogućuje bežičnim uređajima pristupa žičnoj mreži. Bežični uređaji koji se spajaju na pristupnu točku bilo da je otvorenog ili zatvorenog tipa mogu pristupiti Internetu te pretraživati sadržaj koji se nudi. Otvorene pristupne točke nudi sve veći broj restorana, kafića, hotela, zračnih luka i sl., te ne zahtjevaju unos identifikacijskih podataka (lozinke) za uređaje koji se spajaju na nju. Glavni nedostatak otvorenih bežičnih mreža je sigurnost, jer je mrežni promet vidljiv svima. Zbog toga *Hackeri* imaju mogućnost pristupiti povjerljivim informacijama te u konačnici ih zloupotrijebiti. Zatvorene pristupne točke najčešće se koriste u okviru tvrtke, organizacije, stambenih prostora te su zaštićene određenim tipom zaštite (WEP, WPA, WPA2). Prilikom spajanja na zatvorenu bežičnu mrežu mora se unjeti lozinka, [16]. Slika 7 prikazuje uređaj za bežičnu komunikaciju.

Postoje četiri načina rada pristupne točke, prema [24], to su:

1. *Root Mode* – AP uređaj spojen je na žičnu mrežu, i radi kao središnja pristupna točka na koju se spajaju bežični klijenti.
2. *Client Mode* – AP uređaj radi kao klijent te se spaja na drugi AP uređaj. Kada AP uređaj radi u ovom modu ne može primati ostaje klijente, isključivo se ponaša kao klijent.

3. *Bridge Mode* – AP uređaj radi kao bežični most i koristi se za spajanje dvaju ili više mreža. Mostovi se mogu nalaziti u različitim djelovima iste zgrade ili zasebnim zgradama.
4. *Repeater Mode* – AP uređaj radi kao *repeater*, odnosno ponavlja signal neke druge AP na svom području. Može povezivati klijente sa svog područja u mrežu i njihov promet prosljeđivati prvoj AP. U ovom načinu rada propusnost je smanjena te se preporučuje samo ako je neprohodna.



Slika 7. Primjer uređaja AP za bežični LAN

Preuzeto od [23]

ANTENA

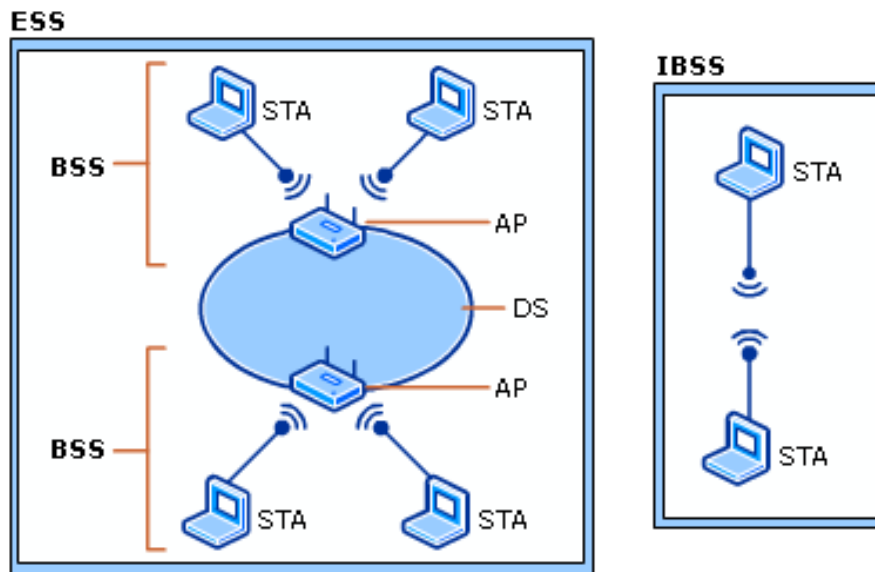
Svaka bežična pristupna točka i bežična kartica imaju ugrađene omnidirekionalne antene. Ove vrste antena signal odašilju u svim smjerovima, a zbog svoje veličine imaju ograničeni domet djelovanja. Za bolji domet signala potrebna je direkionalna antena (vanjska) koja djeluje na većim udaljenostima a koristi se sa klijentske strane prema pristupnoj točki, [16].

KLIJENTI

Prilikom spajanja terminalnih uređaja (prijenosnih računala, stolnih računala i sl.) na AP potrebno je imati bežičnu mrežnu karticu koja već može biti ugrađena u uređaj ili se može koristiti USB kartica, koja je vrlo praktična jer ju mogu koristiti sva računala s USB portom, [16].

4.2 Konfiguracije/topologije 802.11 mreže

Topologija 802.11 mreže sastoji se od osnovnog skupa usluga (BSS – *Basic Service Set*), neovisnog skupa usluga (IBSS – *Independent Basic Service Set*), proširenog skupa usluga (ESS – *Extended Service Set*) te distribucijskog sustava (DS – *Distribution System*) i klijenata (STA – *Station*), [15].



Slika 8. Arhitektura 802.11 mreže

Preuzeto od [15].

IBSS je bežična mreža, koja se sastoji od najmanje dvije STA, te se koristi kada pristup DS-u nije moguć. IBSS se ponekad naziva Ad-hoc bežičnom mrežom, [15].

BSS predstavlja bežičnu mrežu koja se sastoji od jednog bežičnog AP-a koji podržava jednog ili više bežičnih klijenata. BSS se još naziva infrastrukturnom bežičnom mrežom. Svi bežični klijenti u BSS-u komuniciraju preko AP-a. AP osigurava povezanost sa žičnim LAN-om i pruža funkcionalnost premošćivanja kada jedan STA potiče komunikaciju s drugim STA ili čvorom na DS-u, [15]. Primjer BSS-a: u okviru jednog stana, kuće.

ESS je skup dvije ili više pristupne točke koje su povezane s istom žičnom mrežom, a definira pojedinačni lokalni mrežni segment ograničen na jedan usmjernik (poznat kao podmreža), [15]. Primjer ESS-a: u okviru jedne organizacije, tvrtke, ustanove.

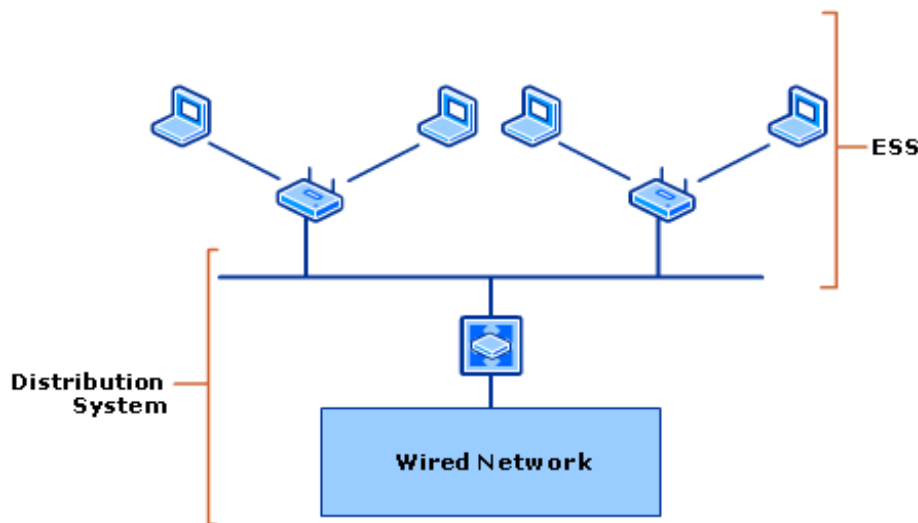
DS je logička komponenta koja se koristi za povezivanje BSS-ova. Pruža distribucijske usluge kako bi omogućio *roaming* klijenata između BSS-ova, [15].

4.3 Način rada 802.11 mreže

IEEE 802.11 standard definira dva načina rada bežičnih LAN mreža, prema [16], to su:

- *Infrastructure Mode* – infrastrukturni način rada,
- *Ad-hoc Mode* – *Ad-hoc* način rada.

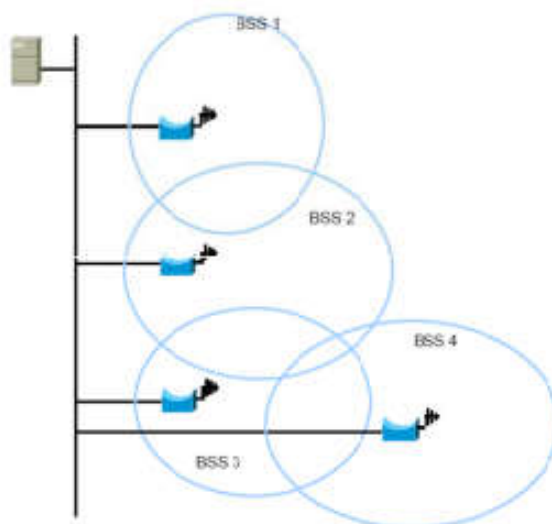
Kod infrastrukturnog načina rada BSS stanice komuniciraju putem pristupne točke te je najvažnije da stanice budu u njenom dosegu. Kako bi stanica mogla komunicirati prvo se mora spojiti na pristupnu točku. Optimalan broj stanica koji se može spojiti na pristupnu točku ovisi o raznim parametrima, poput konfiguraciji mreže, udaljenosti i korištenom standardu. Važno je napomenuti da performanse mreže (npr. propusnost) opadaju s većim brojem od optimalnog broja spojenih stanica na pristupnu točku. BSS-om moguće je pokriti ograničeno područje, 10-30m u zatvorenom te 100m na otvorenom području. Ako se želi pokriti veće područje, potrebno je povezati više BSS-ova odnosno pristupnih točaka, [16].



Slika 9. Infrastrukturni način rada 802.11 mreže

Preuzeto od [15].

Veći broj povezanih BSS-ova naziva se ESS. Ako stanice unutar ESS-a žele komunicirati, njihove pristupne točke moraju razmjenjivati podatke o spojenim stanicama. Na slici 8 prikazan je primjer ESS-a sa četiri spojena BSS-a, [16].

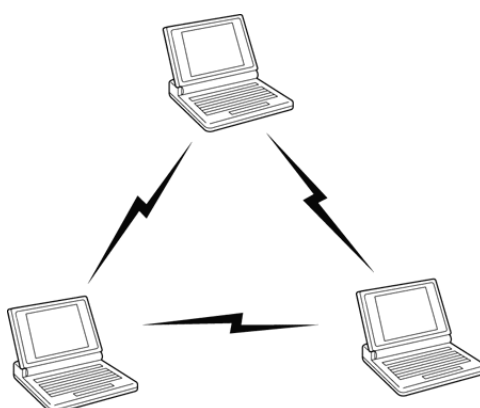


Slika 10. Prikaz *Extended Service Set* (ESS)

Preuzeto od [15].

Primjer: ako neka stanica koja je spojena na AP1 želi komunicirati sa stanicom koja je spojena na AP4, AP1 mora znati da je odredišna stanica spojena na AP4. Kada AP1 primi paket od izvorišne stanice mora ga putem žične mreže proslijediti do AP4 koja zatim taj paket prosljeđuje odredišnoj stanici, [16].

Ad-hoc način rada omogućuje da svaki čvor može izravno komunicirati sa svim drugim čvorovima, tako da pristupne točke nisu potrebne. Korisnici će koristiti Ad-hoc način kada žele napraviti mrežu bez infrastrukture. Zbog nedostatka infrastrukture čvorovi sami osiguravaju usluge kao što su usmjeravanje, dodjeljivanje, prijevod adresa i dr. Još jedan nedostatak je taj što svi korisnici moraju biti u dometu radio signala. Ako se želi povećati domet radio signala tada se koristi infrastrukturni način rada, [15].



Slika 11. Ad-hoc način rada 802.11 mreže

Preuzeto od [25].

4.4 Sigurnost 802.11 mreže

Zbog prirode medija, 802.11 mreže mnogo više su izloženi napadima i neovlaštenim upadima u mrežu. Kako bi se korisnici zaštitili od njih, uvodi se kriptografija. Njome se onemogućuje otkrivanje i mijenjanje podataka, lažiranje identiteta i slično. Stoga, važno je na vrijeme se informirati o mogućim metodama zaštite 802.11 mreže te ih u konačnici primjenjivati. U zaštiti 802.11 mreža mogu se koristiti djelomične metode zaštite, a to su: IP filtriranje i filtriranje po MAC adresi. Oba načina zaštite nisu potpuna jer se IP i MAC adresa mogu lažirati. Prava i potpuna zaštita 802.11 mreže postiže se uporabom enkripcijskih ključeva tj posebno oblikovanih protokola kao što su : WEP, WPA i WPA2, [21].

WEP

WEP (*Wireless Encryption Protocol*) protokol je protokol za zaštitu bežičnih mreža, opisan IEEE 802.11b standardom. WEP zaštita temelji se na enkripciji podataka između krajnjih točaka, a odnosi se na fizički sloj i sloj podatkovne veze. WEP protokol koristi kriptografske ključeve duljina 64, 128 i 256 bita. Optimalna duljina ključa mora biti što veća, a istovremeno što manja da se enkripcija može obaviti što brže. Kriptiranje i dekriptiranje podataka obavlja se tajnim ključem, a protokol uključuje metode utvrđivanja mijenjanja sadržaja poruke između izvorišta i odredišta, [21].

WEP enkripcija koristi RC4 sustav za kriptiranje podataka, koji na temelju ključa stvaraju pseudo nasumični niz kojim se pomoću XOR funkcije kriptira ulazna poruka. Poznavanjem ključa moguće je niz dekriptirati na odredištu uporabom iste funkcije, [21].

Slaba točka WEP protokola je enkripcija podataka, zbog toga što WEP kriptira bit po bit ulaznog niza, te se ne smije dopustiti da se niz bitova kojima se kriptira tekst ponavlja. Ukoliko napadač ima mogućnost prisluškivanja mreže, te zna kako se stvara niz u RC4 algoritmu, kriptanalizom može otkriti tajni ključ. Da bi se izbjeglo ponavljanje nizova kojima se kriptira tekst uz ključ se u RC4 poruci šalje i proizvoljni inicijalizacijski vektor. U mrežama kroz koje prolazi velika količina podataka 24-bitnih inicijalizacijskih vektora postoji velika vjerojatnost ponavljanja niza, [21].

WPA

WPA (*Wi-Fi Protected Access*) protokol je protokol za zaštitu bežičnih mreža, opisan u IEEE 802.11i standardu, te omogućava enkripciju podataka i provjeru identiteta korisnika. WPA kao i WEP koristi RC4 sustav za kriptiranje podataka i to sa 128-bitnim ključem i 48-bitnim inicijalizacijskim vektorom. Uz RC4 sustav, WPA

koristi TKIP protokol (*Temporal Key Integrity Protocop*), koji dinamički mijenja ključeve za vrijeme korištenja sustava. Kombinacijom inicijalizacijskog vektora i TKIP protokola sustav se može lagano obraniti od napada koji se koriste za otkrivanje ključa kod WEP protokola, [21].

Prednost WPA protokola u odnosu na WEP je uvođenje TKIP protokola. Osim što osigurava sigurniju provjeru besprijekornosti poruke, TKIP za kriptiranje teksta koristi složenije funkcije za stvaranje niza bitova. Napadaču se na taj način otežava otkrivanje tajnog ključa prisluškivanjem mreže. TKIP protokol jamči da je svaki paket u mreži kriptiran drugim ključem, [21].

WPA2

WPA2 (Wi-Fi Protected Access 2) protokol se kao i WPA temelji na IEEE 802.11i standardu i uključuje sve mehanizme koje koristi WPA s tim da se uvode i dodatna poboljšanja od koji je najvažnija CCMP enkripcija. CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) enkripcija temelji se na AES algoritmu i ulančanom kriptiranju blokova. AES (*Advanced Encryption Standard*) je simetrični kriptografski algoritam koji kriptira blokove podataka veličine 128 bita, a ključ kojim se kriptira može bit veličine 128, 192 ili 256 bita. Uz AES, CCMP uvodi ulančano kriptiranje blokova za izradu autentifikacijske oznake podataka, [21].

CCMP enkripcija može se opisati kao: prvo se treba podijeliti sadržaj na blokove zatim prepisati zaglavlje i broj paketa u izlaznu poruku, pomoću AES algoritma i brojača kriptirati blokove i zapisati ih u izlaznu poruku. Pomoću AES algoritma i inicijalizacijskog vektora izračunati MIC i zapisati ga iza podataka u izlaznu poruku te izračunati niz za provjeru okvira (FCS) i zapisati ga na kraj poruke, [21].

CCMP dekripcija može se opisati kao: u primljenom paketu pročitati zaglavlje, broj paketa i FCS broj. Provjeriti FCS paketa i podijeliti sadržaj na blokove. Pomoću brojača i AES-a dekriptirati blokove te pomoću AES-a i inicijalizacijskog vektora izračunati MIC i usporediti s onim zapisanim u paketu. Nesigurnosti WPA zaštite proizašle su iz ograničenja nametnutih prilikom oblikovanja WPA protokola, [21].

5.Vrste IEEE 802.11 standarda

Standardizacijsko tijelo IEEE (*Institute of Electrical and Eletronic Engineers*), 1990. godine osnovalo je radnu grupu 802.11, koja je sedam godina kasnije objavljena kao prvi standard za bežične LAN mreže. IEEE 802.11 standard poznat je pod nazivom Wi – Fi (*Wireless Fidelity*), a radi u frekvencijskom području od 2,4 GHz i postiže dvije brzine prijenosa podataka, 1Mbps i 2Mbps. Ovaj standard definira tri tehnike prijenosa podataka na fizičkom sloju, a to su: tehnika izravnog slijeda u proširenom spektru (DSSS – *Direct Sequence Spread Spectrum*), tehnika frekvencijskog skakanja u proširenom spektru (FHSS – *Frequency Hopping Spread Spectrum*) i tehnika difuznog infracrvenog zračenja (DIFR – *Diffuse Infrared*). Ubrzo nakon IEEE 802.11 standarda pojavila se potreba za nadogradnjom, tako su osnovane nove radne podgrupe s ciljem poboljšanja i ubrzanja bežičnih LAN mreža. Najčešće korištene inačice ali i one koje su u fazi razvijanja i predstavljaju budućnost, čije glavne značajke opisane su u nastavku rada, prema [1] trenutno su:

- IEEE 802.11a,
- IEEE 802.11b,
- IEEE 802.11g,
- IEEE 802.11n,
- IEEE 802.11 ad/ac,
- Li-Fi

5.1 IEEE 802.11a standard

Godine 1999. odobren je standard IEEE 802.11a, drugim nazivom Wi – Fi 5 (*Wireless Fidelity5*) zato jer se koristi u frekvencijskom području U – NII (*Unlicensed – National Information Infrastructure*) od 5 GHz. Ovaj standard koristi tehniku frekvencijskog multipleksa ortogonalnih podnositelja OFDM (*Orthogonal Frequecy Division Multiplexing*) koja omogućava brzine prijenosa podataka do 54 Mbps, realna brzina je dva puta manja. Ako je potrebno, brzina prijenosa podataka može se smanjiti na 48, 36, 24, 18, 12, 9 ili 6 Mbps, [12].

OFDM dijeli signal kroz 52 različita podnositelja (*subcarrier*) podataka. Četiri podnositelja sustav koristi kao referencu kojom se služi kako bi izbjegao pomake u frekvenciji ili u fazi tijekom prijenosa, dok njih 48 pružaju odvojene puteve kroz koje se šalju informacije u paralelnom načinu rada. Rezultirajuća frekvencija podnosećeg signala iznosi 0,3125 MHz, ako širina pojasa iznosi 20MHz i podijeljena je na 64 podnositeljska kanala. Iako se koristi samo 52 podnositeljska kanala zauzimajući 16,6 MHz, preostali prostor služi kao zaštitni pojas između kanala, [12].

Za svaku brzinu prijenosa podataka kod 802.11a podnositelja koristi se odgovarajući oblik modulacija, a to su: BPSK (*Binary Phase Shift Keying*), QPSK (*Quadrature Phase Shift Keying*), 16 QAM (*16-level Quadrature Amplitude Modulation*) i 64 QAM (*64-level QAM*), [1].¹

Tablica 2. Karakteristike 802.11a standarda

Datum realizacije	1999.godina
Brzine prijenosa (Mbps)	54 Mbps
Modulacija	BPSK, QPSK, QAM
Frekvencijsko područje (GHz)	5 GHz
Širina kanala (MHz)	20 MHz

Podatci od [12].

5.2 IEEE 802.11b standard

IEEE 802.11b standard prvi je bežični LAN standard koji se široko prihvaćao i ugrađivao u mnoga prijenosna računala i ostalu opremu. U srpnju 1999. godine, IEEE je ratificirao standard 802.11b, a ideja za bežično umrežavanje brzo je prihvaćena te se Wi – Fi hotspot mjesta postavljaju u mnoge urede, hotele, zračne luke kako bi ljudi mogli pristupati Internetom, svojim e-mail-ovima i drugim sadržajima ili "surfati" tijekom putovanja, [1].

IEEE 802.11b standard od strane WECA (*Wireless Ethernet Compatibility Alliance*) organizacije nazvan je Wi-Fi (*Wireless Fidelity - bežična vjernost*). Radi na frekvencijskom području od 2,4 GHz i postiže brzine prijenosa podataka do 11 Mbps, realna brzina je dva puta manja. Pri prijenosu podataka IEEE 802.11b standard koristi CSMA/CA tehniku koja je definirana u izvornom IEEE 802.11 standardu i zadržana u IEEE 802.11b, [1].

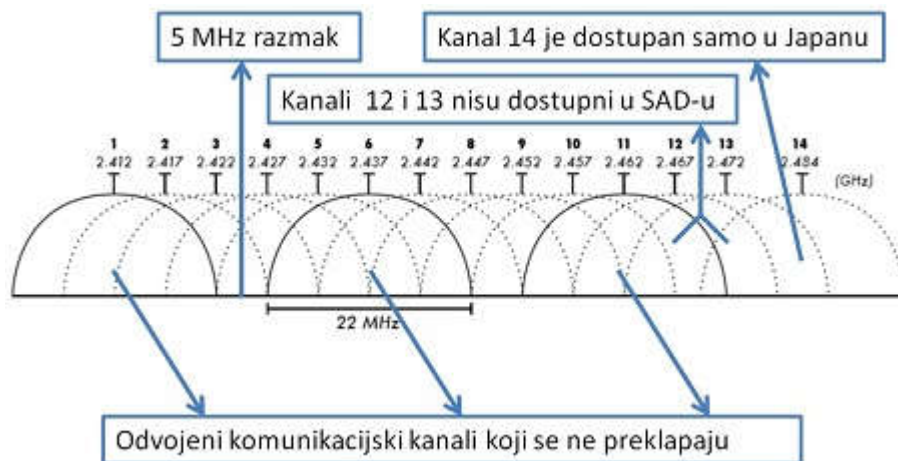
Kod CSMA/CA tehnike, stanica koja želi napraviti prijenos paketa preko komunikacijskog kanala, prvo čeka da se kanal oslobodi zatim ga odašilje. Odnosno, ako ga kanal ne primi, paket se odmakne od slučajno generiranog vremenskog odsječka uz pretpostavku da je drugi prijenos izazvao smetnje, zatim opet čeka slobodan kanal te ponovno prenosi podatke. Ako je kanal slobodan, stanica ne započinje odmah odašiljati paket, već prvo šalje RTS okvir. RTS okvir sadrži adresu

¹ Detaljniji opis na [1] i [12].

primatelja i vrijeme trajanja prijenosa. Na ovaj način se ostale stanice obavještavaju koliko će dugo trebati čekati na svoj prijenos. Stanica koja je označena kao primatelj u RTS okviru, po primitku salje CTS okvir. Poslije toga započinje prijenos paketa koji se mora potvrditi sa ACK-om, [1].

IEEE 802.11b koristi DSSS modulaciju, koja uključuje prijenos informacijskih bitova stvaranjem odgovarajuće kodne riječi.²

Nadalje, 802.11b dijeli raspoloživi spektar u 14 kanala od kojih svaki ima širinu od 22 MHz. U Sjedinjenim Američkim Državama, FCC omogućava korištenje 11 kanala. Četiri kanala dostupna su u Francuskoj, 13 u Europi a samo 1 u Japanu. Također, postoji i preklapanje susjednih kanala jer svaki ima širinu od 22 MHz i svi dijele pojas koji je samo 83 MHz u frekvencijskom području od 2.4 do 2.483 GHz, što dodatno utječe na performanse. Stoga, svaki zadani sustav mora održavati maksimalnu odvojenost kanala i fizičku odvojenost od ostalih sustava u blizini, [1].



Slika 12. Prikaz frekvencijskog spektra 802.11b standarda

Preuzeto od [22].

5.3 IEEE 802.11g standard

U lipnju 2003. godine odobren je standard IEEE 802.11g koji je kompatibilan sa prethodna dva standarda. Omogućava spoj prednosti IEEE 802.11a i IEEE 802.11b standarda koristeći frekvencijsko područje od 2,4 GHz, a ostvarena brzina prijenosa je do 54 Mbps, [1].

² Za detaljniji način rada DSSS tehnike, vidjeti [1].

Kao i IEEE 802.11a standard, IEEE 802.11g koristi OFDM tehniku multipleksiranja na brzinama prijenosa od 6, 9, 12, 18, 24, 36, 48, i 54 Mbps, pri čemu brzina koja se postiže vrlo je osjetljiva na udaljenost i gubitak signala. Modulacijska tehnika ista je kao i kod IEEE 802.11b standarda, CCK, dok su QPSK, BPSK i QAM opet u skladu sa 802.11a standardom.³ Dual-band komponente široko su dostupne, tako da računala opremljena s 802.11a lako komuniciraju s 802.11g pristupnom točkom i obrnuto. Kada pristupna točka podržava IEEE 802.11g i IEEE 802.11b standard istodobno, performanse se gube, posebno od IEEE 802.11b standarda, [1].

Tablica 3. Karakteristike 802.11g standarda

Datum realizacije	2003.godina
Brzina prijenosa (Mbps)	54
Modulacija	CCK, BPSK, QPSK, QAM
Frekvencijsko područje (GHz)	2,4
Širina kanala (MHz)	22

Podatci od [9].

5.4 IEEE 802.11n standard

Nakon IEEE 802.11a, IEEE 802.11b, IEEE 802.11g standarda počelo se sve više razmišljati kako i na koji način povećati brzine prijenosa podataka. U siječnju 2004. godine IEEE objavio je da se formirao novi standard za razvoj većih brzina, IEEE 802.11n. Formalno je objavljen u srpnju 2009. godine. IEEE 802.11n standard ima impresivnu izvedbu, radi na frekvencijskom području od 2,4 GHz i 5 GHz, te brzina prijenosa kreće se do 600 Mbps. IEEE 802.11n standard koristi BPSK, QPSK te QAM modulacijsku tehniku. Kako bi se omogućile veće performanse 802.11n standarda ugrađene su nove značajke, prema [13], to su:

- Promjena u provedbi OFDM multipleksiranja
- Uvođenje MIMO sustava
- MIMO ušteda energije
- Širi propusni kanal
- Antenska tehnologija
- Smanjena podrška za prijašnje kompatibilnosti u posebnim uvjetima za poboljšanje propusnosti

³ Detaljnije na [1].

MIMO

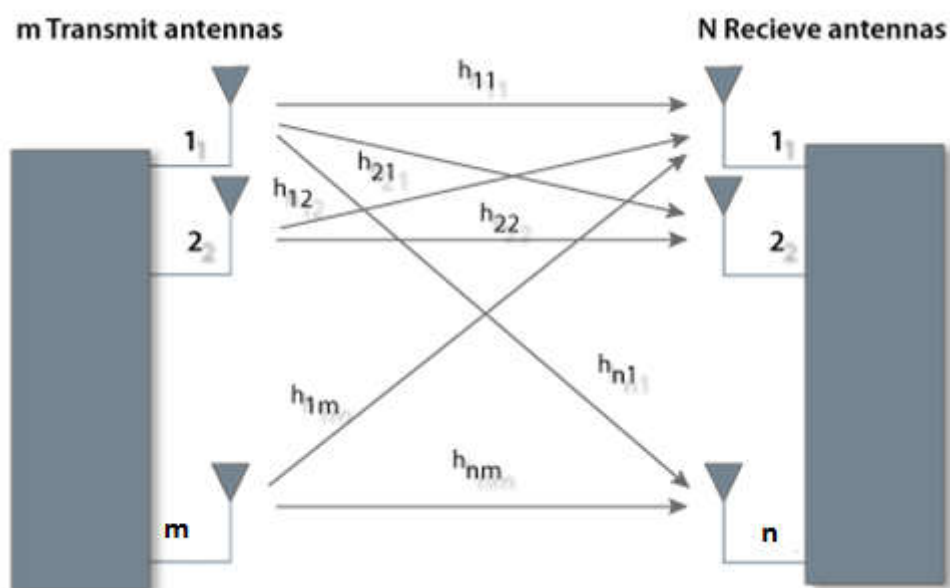
IEEE 802.11n standard koristi MIMO (Multiple Input Multiple Output) sustav poznat kao višestruki ulaz, višestruki izlaz. Sustav koristi višestruke antene za odašiljanje i višestruke antene za primanje koje rade na istoj frekvenciji, [13].

Kako bi se prikazala sposobnost određenog sustava ili radija koristi je jednostavni oblik $a \times b : c$, gdje je a najveći broj odašiljačkih antena; b je najveći broj antena za prijem; i c najveći broj prostornih strujanja podataka, [13].

Primjer: $2 \times 4 : 2$, bio bi za radio sučelje koji može prenositi dvije antene i primati četiri, ali može samo slati i primati dva strujanja podataka. IEEE 802.11n standard omogućuje sustave s oblikom do $4 \times 4 : 4$, [13].

Međutim, uobičajene konfiguracije koje se upotrebljavaju su: $2 \times 2 : 2$, $2 \times 3 : 2$, $3 \times 2 : 2$. Ove konfiguracije imaju istu sposobnost prijenosa podataka, a razlikuju se samo po mogućnosti koje pružaju antene. Konfiguracija $3 \times 3 : 3$ postaje sve raširenija jer ima veću propusnost zbog dodatnog strujanja podataka, [13].

Na slici 18 prikazan je MIMO sustav sa M odašiljačkih antena i N prijemnih antena. Sa svake M odašiljačke antene odašilje se drugačiji podatkovni niz, a na N prijemnim antenama prima se superpozicija svih odaslanih signala, [13].



Slika 13. MIMO sustav

Preuzeto od [24]

Za smanjenje interferencije koristi se MIMO tehnologija u kombinaciji sa OFDM modulacijom, odnosno MIMO-OFDM.

ANTENSKA TEHNOLOGIJA

Za 802.11n standard, antenska tehnologija znatno je poboljšana uvođenjem mogućnosti usmjeravanja snopa i raznolikosti, [13].

Usmjeravanje snopa fokusira radio signale izravno na putu prostiranja za prijemne antene radi poboljšavanja raspona i ukupnih performansi. Viša razina signala i bolji omjer signal/šum značit će da se može iskoristiti cijeli kanal, [13].

Raznolikost koristi dostupne antene i odabire najbolji podskup od većeg broja antena kako bi se dobili optimalni uvjeti signala. To se može postići jer u MIMO sustavima često postoji višak antena. Budući da 802.11n standard podržava bilo koji broj antena između jedne i četiri, moguće je da jedan uređaj ima tri antene, a drugi s kojim komunicira samo dvije. Višak antene može se koristiti za pružanje raznolikosti prijema ili prijenosa prema potrebi, [13].

KOMPATIBILNOST

802.11n pruža kompatibilnost sa uređajima u mreži koji koriste prijašnje verzije standarda, no samo u modu 802.11n nudi znatne prednosti. Postoje tri načina rada na kojima 802.11n pristupna točka može raditi, prema [13], to su:

- Legacy mode (samo 802.11a, b i g),
- Mixed mode (mješovito 802.11a, b, g i n),
- Greenfield mode (samo 802.11n).

5.5 Novi trendovi IEEE 802.11 standarda

Zbog sve većih zahtjeva korisnika, svakim danom razvijaju se novi standardi čiji je cilj omogućiti veće propusnosti, proširenje dometa signala te veću jednostavnost korištenja usluge. Sve to omogućuju slijedeći standardi: IEEE 802.11ad, IEEE 802.11ac, IEEE 802.11ax, IEEE 802.11af, IEEE 802.11ah, IEEE 802.11ai, IEEE 802.11aq.

VELIKA PROPUSNOST

IEEE 802.11ad standard prvi je objavljen te veliku propusnost ostvaruje pomoću *beamforming-a* odnosno usmjeravanja snopa. Radi na frekvencijskom području od

60 GHz što omogućava veće širine kanala, nedostatak je taj što dolazi do prigušenja vala i gubitka propagacije. Drugi standard je IEEE 802.11ac koji donosi značajne promjene jer omogućuje DL-MU-MIMO što je veliki napredak. Za razliku od IEEE 802.11ad koji koristi 64-QAM, IEEE 802.11ac koristi 256-QAM. Najnoviji standard IEEE 802.11ax obećava poboljšanje u odnosu na prethodni standard. Također novost je korištenje STR tehnike odnosno full duplex-a, [14].

PROŠIRENJE DOMETA

IEEE 802.11af i IEEE 802.11ah standardi posebno su izgrađena s ciljem proširenja dometa Wi-Fi signala čak do jednog kilometra u ruralnim područjima i otvorenim poljima. Prvi objavljeni standard IEEE 802.11af donosi značajke koje se odnose na *channel acquisition* i geolokacijske baze podataka, dok IEEE 802.11ah standard ima bolju energetska učinkovitost. Oba standarda rade na frekvencijskom području od 1 GHz, [14].

JEDNOSTAVNOST KORIŠTENJA USLUGE

Za postizanje veće jednostavnosti korištenja Wi-Fi usluga zaduženi su IEEE 802.11ai i IEEE 802.11aq standard. IEEE 802.11ai standard kao rješenje nudi način da se ubrza početno uspostavljanje veze, a IEEE 802.11aq standard nudi PAD (*Preassociation discovery*). Iako su oba standarda u fazi razvijanja, ne može se točno razlučiti koji koristi bolje metode i tehnologije za ostvarivanje jednostavnosti korištenja usluge, [14]. Za jednostavniju usporedbu, u tablici 4. sažete su glavne karakteristike navedenih IEEE 802.11 standarda.

Tablica 4. Usporedba IEEE 802.11 standarda

IEEE 802.11 standard	Godina	Frekvencijsko područje	Bandwidth	Modulacija	Transmisijska shema	Brzine
802.11	1997	2.4 GHz	22 MHz	DBPSK, DQPSK	DSSS/FHSS	≤ 2 Mbps
802.11a	1999	5 GHz	20 MHz	BPSK, QPSK, QAM	OFDM	≤ 54 Mbps
802.11b	1999	2.4 GHz	22 MHz	CCK, DBPSK, DQPSK	DSSS	≤ 11 Mbps
802.11g	2003	2.4 GHz	22 MHz	CCK, BPSK, QPSK, QAM	DSSS/OFDM	≤ 54 Mbps
802.11n	2009	2.4/5 GHz	20/40 MHz	BPSK, QPSK, QAM	OFDM, MIMO	≤ 600 Mbps

802.11ad	2012	60 GHz	2160 MHz	BPSK, QPSK, QAM	OFDM, MIMO	≤ 6.76 Gbps
802.11ac	2013	5 GHz	40/80/160 MHz	BPSK, QPSK, QAM	OFDM, MIMO	≤ 6.93 Gbps

Podatci od [5]

6. Budući trendovi Li-Fi tehnologija

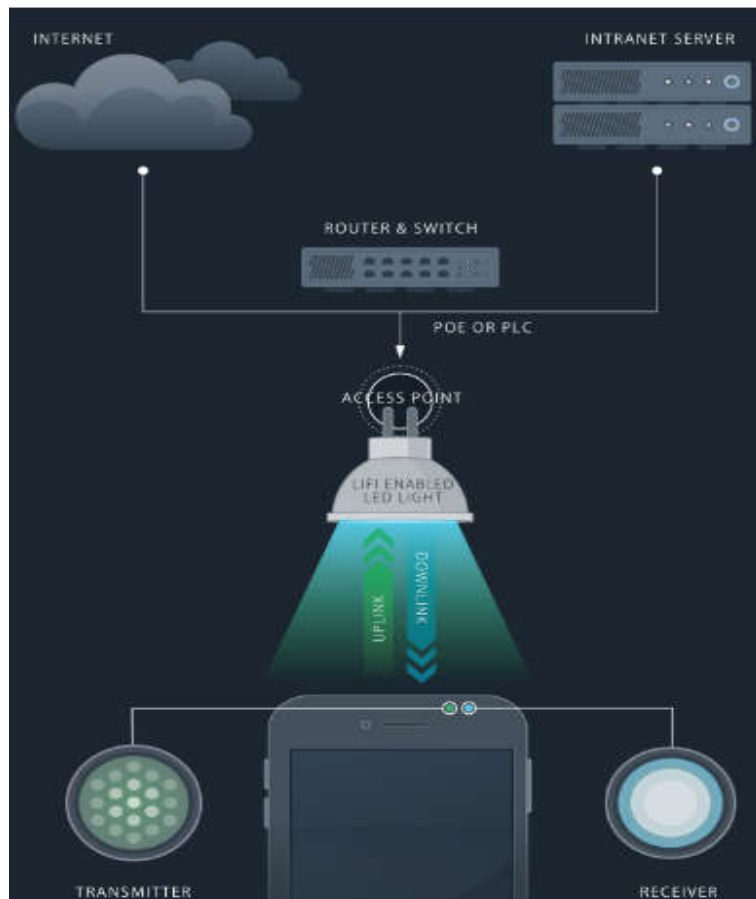
Li-Fi (*Light Fidelity*) je komunikacijska tehnologija koja za prijenos podataka koristi spektar vidljivog svjetla. Li-Fi tehnologija svijetu je predstavljena još 2011. godine od strane profesora Harald Hassa. Njegova ideja je bila pretvoriti obične žarulje u bežične rutere, tako je 2012. godine pokrenuo tvrtku Pure Li-Fi koja se bavi razvojem Li-Fi uređaja: „Sve što je potrebno učiniti jest ugraditi mikročip na bilo koji rasvjetni uređaj te tako spojiti dvije funkcije: osvjetljenje i bežični prijenos podataka. U budućnosti nećemo imati 14 milijuna žarulja, već isto toliko Li-Fi uređaja, a to bi značilo čišću, zeleniju i svjetliju budućnost“, rekao je Hass 2011. godine, [22].

6.1 Princip rada Li-Fi tehnologije

Li-Fi tehnologija uključuje infracrvenu i ultra-ljubičastu komunikaciju kao i vidljivu svjetlost. Posebna je po tome što se ista svjetlosna energija koja se koristi za osvjetljenje također koristi za komunikaciju. Li-Fi omogućuje prijenos podataka modeliranjem intenziteta svjetlosti, koji zatim prima foto-osjetljiv detektor. Svjetlosni signal se zatim demodulira u električki oblik. Ovaj oblik modulacije se provodi na takav način da se ne percipira na ljudsko oko. Li-Fi može raditi u zatvorenom i otvorenom prostoru sa zatamnjenim svjetlima i nije strogo vidljiva tehnologija. Pure Li-Fi tehnologija je također LED agnostika, što znači da radi s mnogo LED svjetala, [23].

Način rada Li-Fi tehnologije je vrlo jednostavan ali učinkovit. Kada se na LED žarulju primijeni konstantna struja, iz žarulje se emitira konstantna struja fotona koju vidimo kao osvjetljenje. LED žarulje su poluvodički uređaji, pa se osvjetljenje može modulirati pri iznimno velikim brzinama koje se mogu detektirati pomoću foto-detektora. Uporaba ove tehnike omogućava velike brzine prijenosa podataka. U laboratorijskim uvjetima postignuta je brzina prijenosa od 224Gbps, pri takvoj brzini prijenosa moguće je preuzeti 18 filmova ili nekog drugog sadržaja veličine 1,5 Gb u samo jednoj sekundi, [22], [23]. Na slici 14 može se vidjeti princip rada Li-Fi tehnologije.

Radiofrekvencijska komunikacija zahtijeva radijske sklopove, antene i složene prijemnike, dok Li-Fi je mnogo jednostavniji i koristi izravne modulacijske tehnike slične onima koji se koriste u *low-cost* infracrvenim komunikacijskim uređajima (daljinski upravljač), [23].



Slika 14. Princip rada Pure Li-Fi tehnologije

Preuzeto od [23]

6.2 Prednosti i nedostaci Li-Fi tehnologije

Prednost ove tehnologije je kapacitet koji nudi u odnosu na trenutno postojeće tehnologije. Elektromagnetski spektar vidljive svjetlosti je oko 10000 puta veći od elektromagnetskog spektra radio valova i zato otvara veće mogućnosti istraživanja nove tehnologije. Implementacija Li-Fi bežičnog prijenosa podataka ne bi trebala predstavljati problem jer se već sad u svijetu koristi veliki broj LED žarulja. Samim time ova tehnologija postaje energetska učinkovita s obzirom da je prijenos podataka putem svjetla besplatan. Dakle, LED svjetla bi mogla imati dvostruku funkciju, osim osvjetljenja prostorija pomoći će i u kreiranju mreže koja će spajati sve uređaje u kući ili stanu, [22].

Glavni nedostatak Li-Fi tehnologije u odnosu na Wi-Fi tehnologiju je taj što svjetlo ne prolazi kroz zidove pa ima ograničen domet, ujedno to je i prednost jer je sigurnija od neovlaštenog upada u mrežu.

7. Zaključak

Bežične LAN mreže postaju sastavni dio života, jer funkcionalnosti koje pružaju uvelike pospješuju kvalitetu života. Sve veći broj korisnika odlučilo se na taj način komunikacije jer pruža veću slobodu kretanja i brzu implementaciju. Već prvi standard IEEE 802.11 došao je kao zamjena za žične LAN mreže, a rastom tehnologije i funkcije stvoreni su novi standardi. Zahtjevi korisnika postajali su sve veći, posebno po pitanju brzine prijenosa podataka, područja pokrivanja, sigurnosti te ostalih performansi, a realizacija istih odvijala se kroz razvoj i nastanak novih IEEE 802.11 standarda. Uz sve to, pitanje sigurnosti i dalje je predstavljalo najveći problem, jer signal koji se prenosio zrakom mogao se presresti i korisnici su se suočili s gubitkom, krađom ili krivotorenjem osobnih podataka. Stoga izuzetno je važno iskoristiti sve mogućnosti zaštite koje pružaju IEEE 802.11 standardi.

Analizom rezultata istraživanja vidljivo je da bežična LAN tehnologija postaje jedna od vodećih tehnologija na telekomunikacijskom tržištu. Svojim trendom širenja omogućila je korisnicima nesmetano korištenje Interneta u privatne ili poslovne svrhe u bilo kojem trenutku. Jednostavnost korištenja i brza implementacija najvažnija su obilježja tehnologije dok kasnije dolazi brzina prijenosa i ostale performanse. Ove karakteristike postižu se uporabom posebno oblikovanih mehanizma i modulacija koji su svakim novim IEEE 802.11 standardom razvijeniji. Budućnosti bežičnih LAN mreža nalazi se u standardima kao što su IEEE 802.11ah, IEEE 802.11ai i IEEE 802.11ax i tehnologijama koje ti standardi donose. Iako su trenutno bežične LAN mreže u ekspanziji, nova tehnologija kao što je Li-Fi pokazuje veliki interes za istraživanje. Svojim pilot-projektima pokazala je i više nego zadovoljavajuće brzine prijenosa podataka, bolji način zaštite mreže, ekonomski i ekološki je prihvatljivija no jedina mana joj je ograničeni domet signala zato što svijetlo ne prolazi kroz zidove.

Na kraju svega može se zaključiti da su bežične LAN mreže budućnost u svijetu računalnih mreža. Teško je reći kako će bežične LAN mreže preuzeti žične, ali kada je potrebna mobilnost i brza i jeftina implementacija, bežične LAN mreže su u većoj prednosti.

LITERATURA

- [1] Ray Horak: *Telecommunications and Data Communications Handbook, The Context Corporation*, 2007.
- [2] Jyrki T. J. Penttinen: *The Telecommunications Handbook, Engineering Guidelines for Fixed, Mobile and Satellite System*, 2015.
- [3] James F. Kurose, Keith W. Ross: *Computer Networking, A Top-Down Approach*, 2013.
- [4] Bažant, A., Gledec, G.: *Osnove arhitekture mreže*, Element, Zagreb, 2009.
- [5] Forenbacher, I.: *Auditorna predavanja iz Arhitekture telekomunikacijske mreže*, Fakultet Prometnih Znanosti, Zagreb, 2015.
- [6] Techiesupports: *Povijest bežičnog umrežavanja*, 2011
<http://techiesupports.blogspot.hr/2011/11/brief-history-of-wireless-networking.html>
(lipanj, 2017)
- [7] Gary S. Rogers, John Edwards: *An Introduction to Wireless Technology*, 2003.
- [8] Mrvelj, Š.: *Auditorna predavanja iz Tehnologije telekomunikacijske mreže*, Fakultet prometnih znanosti, Zagreb, 2014.
- [9] HAKOM: *Radijske tehnologije za širokopolasni nepokretni pristup i mjerenja*, Fakultet elektrotehnike i računarstva, Zagreb, 2008.
<https://www.hakom.hr/UserDocsImages/2010.g/Zeno/Studije/Radijske%20tehnologije%20za%20sirokopolasni%20nepokretni%20pristup%20i%20mjerenja.pdf> (kolovoz, 2017)
- [10] Universität Karlsruhe: *Mobile Communications Chapter 2: Wireless Transmission*, Njemačka, 1998.
<http://slideplayer.com/slide/5663226/> (kolovoz 2017.)
- [11] Techwalla: *Nedostaci bežičnih mreža*
<https://www.techwalla.com/articles/disadvantages-of-wireless-networks> (lipanj, 2017)
- [12] Ian Poole: *Radio-electronics, IEEE 802.11a*
<http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11a.php> (lipanj, 2017)
- [13] Ian Poole: *Radio-electronics, IEEE 802.11n*
<http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11n.php> (lipanj, 2017)

[14] I. Škorić: *Budući razvoj IEEE 802.11 (Wi-Fi) standarda bežičnih mreža*, Osijek, 2016.

[15] Technet.microsoft

[https://technet.microsoft.com/en-us/library/cc757419\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx) (lipanj, 2017)

[16] Jeren, B., Pale, P.: *Sustavi za vođenje i praćenje procesa*

http://spvp.zesoi.fer.hr/predavanja%202008/WE_skripta.pdf (lipanj, 2017)

[17] URL: [http://1.bp.blogspot.com/-](http://1.bp.blogspot.com/-zFrNpnFc9mA/T0dG9udNgtI/AAAAAAAAAGMo/7eMTrSYnjs/s1600/Slide3.JPG)

[zFrNpnFc9mA/T0dG9udNgtI/AAAAAAAAAGMo/7eMTrSYnjs/s1600/Slide3.JPG](http://1.bp.blogspot.com/-zFrNpnFc9mA/T0dG9udNgtI/AAAAAAAAAGMo/7eMTrSYnjs/s1600/Slide3.JPG)
(srpanj, 2017)

[18] Ben Joan

<http://www.differencebetween.net/technology/difference-between-fhss-and-dsss/>
(lipanj, 2017)

[19] URL:

<http://www3.nd.edu/~mhaenggi/NET/wireless/802.11b/Data%20Link%20Layer.htm>
(lipanj, 2017)

[20] S. Šopar: *Lokalne bežične mreže po IEEE 802.11 standardu*, Varaždin, 2004.

[21] CARNet: *WPA2 zaštita*

<http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-267.pdf> (srpanj, 2017)

[22] URL: <http://www.mygadgets.my/li-fi/> (srpanj, 2017)

[23] Pure Li-Fi

<http://purelifi.com/technology/> (kolovoz, 2017)

[24] Aries Institute of Technology, Inc.

http://www.aries.net/demos/Wireless/chapter04/chapter04_1.html (kolovoz, 2017)

[25] URL: <https://www.techsgig.com/wireless-ad-hoc-network-windows-7-share-internet/> (lipanj, 2017)

[26] A.Madirazza: *802.11n Draft2.0 u teoriji*, 2009.

<http://www.pcekspert.com/clanak/802-11n-draft2-0-u-teoriji/> (lipanj, 2017)

[27] SILVUS technology

<http://silvustechnologies.com/technology/introduction-to-mimo> (lipanj, 2017)

POPIS ILUSTRACIJA

Popis slika

Slika 1. Prikaz žične i bežične LAN tehnologije	3
Slika 2. IEEE 802.11 mreža u odnosu na OSI referentni model	9
Slika 3. 802.11 područje definiranja.....	11
Slika 4. Prikaz XOR operacije.....	12
Slika 5. CSMA/CA mehanizam	14
Slika 6. Primjer RTS/CTS komunikacije.....	15
Slika 7. Primjer uređaja AP za bežični LAN.....	17
Slika 8. Arhitektura 802.11 mreže.....	18
Slika 9. Infrastrukturni način rada 802.11 mreže	19
Slika 10. Prikaz <i>Extended Service Set</i> (ESS).....	20
Slika 11. Ad-hoc način rada 802.11 mreže.....	20
Slika 12. Prikaz frekvencijskog spektra 802.11b standarda.....	25
Slika 13. MIMO sustav.....	27
Slika 14. Princip rada Pure Li-Fi tehnologije	32

Popis tablica

Tablica 1. Frekvencijski spektar EM valova	5
Tablica 2. Karakteristike 802.11a standarda.....	24
Tablica 3. Karakteristike 802.11g standarda.....	26
Tablica 4. Usporedba IEEE 802.11 standarda.....	29

POPIS KRATICA

16QAM - 16-level Quadrature Amplitude Modulation

64QAM - 64-level Quadrature Amplitude Modulation

AES - Advanced Encryption Standard

AP - Access Point

BPSK - Binary Phase Shift Keying

BSS - Basic Service Set

CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

CTS - Clear to Send

DIFR - Diffuse Infrared

DS - Distribution System

DSSS - Direct Sequence Spread Spectrum

ESS - Extended Service Set

FCS - Frame Check Sequence

FHSS - Frequency Hopping Spread Spectrum

IBSS - Independent Basic Service Set

IEEE - Institute of Electrical and Electronic Engineers

IR - Infra Red

LAN - Local Area Network

Li-Fi - Light Fidelity

LLC - Logical Link Control

MAC - Medium Access Control

MAN – Metropolitan Area Network

MIMO - Multiple Input Multiple Output

OFDM - Orthogonal Frequency Division Multiplexing

PAD - Preassociation discovery

PHY - Physical Layer

PN - Pseudo Noise

QPSK - Quadrature Phase Shift Keying

RTS - Request to Send

STA - Station

TKIP - Temporal Key Integrity Protocol

U – UNII - Unlicensed National Information Infrastructure

WECA - Wireless Ethernet Compatibility Alliance

WEP - Wireless Encryption Protocol

Wi-Fi - Wireless Fidelity

WLAN - Wireless LAN

WPA - Wi-Fi Protected Access

WPA2 - Wi-Fi Protected Access 2

METAPODACI

Naslov rada: Arhitektura bežične LAN mreže IEEE 802.11

Student: Martina Coban

Mentor: dr. sc. Ivan Forenbacher

Naslov na drugom jeziku (engleski): Architecture of wireless LAN network IEEE 802.11

Povjerenstvo za obranu:

- prof. dr. sc. Slavko Šarić, predsjednik
- dr. sc. Ivan Forenbacher, mentor
- doc. dr. sc. Marko Periša, član
- prof. dr. sc. Zvonko Kavran, zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: **Zavod za informacijsko-komunikacijski promet**

Vrsta studija: Preddiplomski

Studij: Promet

Akademski naziv: univ. bacc. ing. traff.

Datum obrane završnog rada: 05. Prosinca, 2017.



Sveučilište u Zagrebu
Fakultet prometnih
znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj _____ završni rad

isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu _____ završnog rada

pod naslovom **Arhitektura bežične LAN mreže IEEE 802.11** _____

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, _____ 22.11.2017. _____

(potpis)