Analiza karakteristika bežičnih mreža i WiFi mesh tehnologije u zatvorenim prostorima

Vrdoljak, Marko

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

ANALIZA KARAKTERISTIKA BEŽIČNIH MREŽA I WIFI MESH TEHNOLOGIJE U ZATVORENIM PROSTORIMA

ANALYSIS OF THE CHARACTERISTICS OF WIRELESS NETWORKS AND WIFI MESH TECHNOLOGY IN INDOOR ENVIRONMENT

Mentor: izv. prof. dr. sc. Marko Periša

Student: Marko Vrdoljak

JMBAG: 0135261836

Zagreb, kolovoz 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 25. svibnja 2024.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Arhitektura telekomunikacijske mreže**

ZAVRŠNI ZADATAK br. 7493

Pristupnik: **Marko Vrdoljak (0135261836)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza karakteristika bežičnih mreža i WiFi mesh tehnologije u zatvorenim prostorima**

Opis zadatka:

U radu je potrebno analizirati karakteristike bežičnih mreža te opisati njihovu klasifikaciju. Istodobno, važno je navesti arhitekturu WiFi mesh tehnologije i njezinu primjenu u zatvorenim prostorima.

Mentor:

izv. prof. dr. sc. Marko Periša

Predsjednik povjerenstva za završni ispit:

SAŽETAK

Digitalna komunikacija prevladava u današnjem svijetu zahvaljujući bežičnim tehnologijama. Pokrivajući velike površine, bežične mreže omogućavaju krajnjim korisnicima mobilnost i pristup Internetu bez potrebe za kabelima. WiFi mesh tehnologija, korištenjem više čvorova za stvaranje mreže, pruža veću pokrivenost signala i veće brzine prijenosa uz jednostavnu instalaciju. U tom kontekstu, to je čini pogodnijom za implementaciju u zatvorenim prostorima od tradicionalnog WiFi-a. Zbog načina komunikacije u bežičnim mrežama, one su često meta kibernetičkih napada. To izaziva stvaranje naprednih sigurnosnih protokola i tehnologija, kako bi se zaštitili osjetljivi podaci i resursi korisnika mreže.

KLJUČNE RIJEČI: bežična mreža; mesh; tehnologija; ruter

SUMMARY

Digital communication prevails in today's world thanks to wireless technologies. By covering large areas, wireless networks allow users mobility and access to the Internet without the need for cables. WiFi mesh technology, by using multiple nodes to create a network, provides greater signal coverage and higher transmission speeds with easy installation. In that context, it makes it more suitable for implementation in indoor environments compared to traditional WiFi. Due to the way of communication in wireless networks, they are often the target of cyber attacks. This causes the creation of advanced security protocols and technologies, in order to protect sensitive data and resources of network users.

KEYWORDS: wireless network; mesh; technology; router

SADRŽAJ

1. UVOD

Dosadašnjim razvojem bežičnih tehnologija sve je manja potreba fizičkih kabela za povezivanje uređaja i pristup Internetu. Njihovim razvojem dolazi do sveprisutnosti bežičnih mreža u otvorenim i zatvorenim prostorima. Također, promijenili su se zahtjevi krajnjih korisnika koji žele pristup Internetu bilo gdje i bilo kada. WiFi je postao globalni simbol bežičnih tehnologija, no uviđajući njegove mane inženjeri su razvili WiFi mesh. Rješenje koje nudi šire pokrivanje signala što je svakako jedna od glavnih mana tradicionalnog WiFi-a, jednostavnost instalacije i bolje performanse bežične mreže samo se neke od prednosti te tehnologije.

Rad analizira karakteristike bežičnih mreža, s posebnim osvrtom na WiFi mesh tehnologiju i njezinu primjenu u zatvorenim prostorima. Pored toga, cilj je istaknuti prednosti implementacije WiFi mesh-a u stambenim i sveučilišnim prostorima navodeći postojeće sigurnosne prijetnje.

Ovaj rad je organiziran u šest ključnih poglavlja:

1. Uvod
2. Pregled karakteristika bežičnih mreža
3. Vrste i značajke bežičnih tehnologija
4. Analiza WiFi mesh tehnologije u zatvorenim prostorima
5. Sigurnosni aspekti WiFi mesh tehnologije
6. Zaključak

U poglavlju „Pregled karakteristika bežičnih mreža“ navedene su temeljne karakteristike bežičnih mreža koje su potkrijepljene tehničkim opisom. Isto tako, objašnjen je princip rada bežičnih mreža, uz njezinu klasifikaciju na PAN, LAN, MAN i WAN.

Treće poglavlje koje glasi „Vrste i značajke bežičnih tehnologija“, obrađuje WiFi mrežu, Bluetooth i Zigbee mrežu. Prikazujući evoluciju 802.11 standarda i njegov način rada, osnovnu podjelu Bluetooth-a predviđenu za različite načine komunikacije te topologije Zigbee mreže.

Sljedeće četvrto poglavlje, naziva „Analiza WiFi mesh tehnologije u zatvorenim prostorima“ uključuje tri tipa arhitekture bežične mesh mreže, predočavajući rezultate implementacije mesh sustava u sveučilišnom prostoru s pomoću simulacijskog alata i proučavajući eksperiment implementacije kućnog mesh-a.

Poglavlje „Sigurnosni aspekti WiFi mesh tehnologije“ pruža kritički pogled na potencijalne sigurnosne prijetnje u mrežnim slojevima bežične mesh mreže. Istodobno identificirajući sigurnosne zaštite mrežnih slojeva mreže koji su segmentirani po OSI modelu. I na samom kraju, rad je zaključen te su donesene glavne spoznaje rada.

2. PREGLED KARAKTERISTIKA BEŽIČNIH MREŽA

Prijenos podataka u kontekstu telekomunikacija je ključan i najznačajniji proces. Bežične mreže (eng. *Wireless network*) su sustavi za prijenos podataka koji omogućuju komunikaciju između terminalnih uređaja putem elektromagnetskih valova. Nastavno, mreža se odnosi na mrežu gdje je povezanost ostvarena bez fizičkog povezivanja kabela [1].

U informacijsko-komunikacijskim sustavima, elektromagnetski val definira se kao pojava kojom objašnjavamo širenje elektromagnetske energije u prostoru. Sastoji se od električnog i magnetskog polja koje su međusobno povezane komponente. Radiovalovi, mikrovalovi i infracrveni valovi koriste se za bežični prijenos informacija [1].

Bežičnim mrežama mrežni operatori (eng. *Network operator*) proširuju svoje mreže izvan dometa žičnih veza. Implementacija zahtjeva manje vremena u odnosu na žične mreže uz osjetno niži trošak. Jednostavno, zbog manjeg broja komponenti potrebnih za funkcioniranje mreže. Pri čemu ne zahtijevaju dodatne resurse u vidu provlačenja kabela i bušenja rupa u zidovima (smanjenje strukturnog kabliranja). Što čini bežične mreže vrlo fleksibilnim [1].

Mobilnost se smatra glavna prednost bežičnih mreža. Korisnici mreže mogu se kretati i ostati povezani bilo gdje i bilo kad dok god su unutar zone pokrivenosti. Postupak koji omogućava prijelaz s jedne pristupne točke (eng. *Access Point* - AP) na najbliži drugi AP naziva se *roaming*. Terminalni uređaj identificira slab signal i počinje skenirati okolinu za prekapčanje na bežičnu mrežu jačeg signala [1].

Propagacija elektromagnetskog vala kroz betonske zidove, staklo, plastiku, drvo i ostale materijale zaslužna je za korištenje bežičnih mreža na lokacijama gdje nije moguća implementacija i korištenje infrastrukture žične mreže. Primjeri su izolirane lokacije ekstremnih temperatura (pustinje, planine), zračni promet, vodni promet.

Skalabilnost je karakteristika bežične mreže koja olakšava konfiguraciju mreže prilikom promijene broja korisnika. Pogotovo u sklopu poslovnih ureda, javnih mjesta gdje je potrebno brzo prilagođavanje novim zahtjevima mreže. Mnogi današnji objekti kako privatni, poslovni tako i javni imaju veliki broj pametnih uređaja koji se mogu brzo i jednostavno povezati zahvaljujući bežičnoj mreži.

Posebnost bežičnih mreža nosi sa sobom i problematične karakteristike koji ne postoje u drugim mrežama. Interferencija je jedna od njih. Definira se kao pojava degradiranja signala uzrokovana komunikacijom drugih uređaja (mikrovalna pećnica, računalo, radar) u istom frekvencijskom području. Osnovne dvije vrste interferencije [2]:

- Interferencija po istom kanalu nastaje kada više uređaja koriste isti kanal za prijenos podataka. Komunikacija između terminalnih uređaja je po načelu „slušaj dok drugi govore“.

- Interferencija po susjednom kanalu nastaje kada više uređaja koristi susjedne kanale. Susjedni kanali su frekvencijski kanali koji se nalaze jedan pored drugog. Naime, terminalni uređaji komuniciraju istovremeno „bez čekanja na svoj red“.

Spomenuta propagacija elektromagnetskog vala u prostoru posljedično rezultira gubitkom snage signala. Signalu je svaka prepreka smetajuća. Različiti objekti, predmeti čak i ljudi osjetno će smanjiti jačinu signala. Ovisno o prepreci elektromagnetski val će se uslijed propagacije reflektirati, difraktirati ili raspršiti. Unutar zatvorenih prostora signal će promijeniti put i transformirati se mnogo puta do odredišta. Jasno, cilj je održati snagu jakog signala što je udaljenije moguće. Kako bi se omogućila velika zona pokrivenosti signala [2].

Savršeni scenariji je jasna linija vidljivost (eng. *Line of sight* - LOS) između odašiljača i prijemnika kojom se ostvaruju velike snage signala i visoka pouzdanost. Tipično korišteno za komunikacije infracrvenim valovima ili mikrovalovima. Opisanim scenarijem se podrazumijeva nepostojanje fizičkih prepreka (drveća, zgrade) između prijemnika i odašiljača koje znatno skraćuju udaljenost propagacije signala i mogu blokirati signal [2].

2.1 Princip rada bežičnih mreža

Infrastruktura bežičnih mreža se sastoji od komponenti od kojih se neke preklapaju s infrastrukturom žičnih mreža. Elementi bežične infrastrukture predstavljaju samo dio ukupne mrežne infrastrukture koja je većinom povezana i umrežena s pomoću raznih vrsta kabela na velikim udaljenostima. Ona omogućuje uspostavljanje i funkcioniranje bežičnih komunikacija. Pri tome, rad bežičnih mreža zasniva se na pretvaranju informacijskih signala u oblik pogodan za prijenos putem zraka [3].

Krajnji korisnici mogu biti ljudi, roboti ili drugi subjekti koji se koriste prednostima bežične mreže. U najvećem postotku krajnji korisnik je osoba koja inicira i prekida korištenje bežične mreže s pomoću terminalnog uređaja. Roboti, na primjer, mogu primati naredbe putem bežične mreže odnosno centralnog računala za izvršavanje radnji u automatiziranoj proizvodnji. Najsofisticiraniji mobilni terminalni uređaj današnjice je pametni telefon (eng. *Smartphone*) čiji broj se procjenjuje na preko 6 milijardi uređaja u svijetu. Zbog njegovih karakteristika kao što su male dimenzije i težina, kamera visoke kvalitete, mnogobrojni senzori, brzi procesor i ostalo, savršeno se uklapa u koncept bežičnih mreža [3].

Mrežna kartica (eng. *Network interface card* - NIC) može biti integrirana u terminalni uređaj ili se priključuje kao mrežni adapter. Predstavlja *hardver* koji omogućava povezivanje terminalnog uređaja na mrežu. Mreža je uobičajeno Internet ili lokalna računalna mreža (eng. *Local Area Network* – LAN) [3]. Postoje dva tipa mrežnih kartica koje karakteriziraju dva načina povezivanja na mrežu. Prvi tip, *Ethernet* NIC koristi se za žično povezivanje, potrebno je povezati jedan kraj mrežnog kabela s konektorom

kartice a, drugi s *ruterom*. Standardni konektor je RJ45 (oklopljeni i neoklopljeni) različite vrste *Ethernet* kabela podržavaju različite brzine prijenosa. Drugi tip, bežični NIC (eng. *Wireless* NIC) omogućava povezivanje na mrežu bežičnim putem. Osim po dizajnu razlikuje se po WiFi (eng. *Wireless Fidelity*) standardima koje podržava, sigurnosnim protokolima i modulacijskim postupcima. Sadrži antenu koja se koristi za odašiljanje i prijem elektromagnetskog vala. Također, može imati funkciju zamijene antene što nije slučaj kod integriranih kartica. Jedan od glavnih benefita mrežnih kartica je dodjeljivanje jedinstvene (eng. *Media Access Control* - MAC) adrese terminalnom uređaju [4].

Slika 1. Bežična mrežna kratica, [4]

Ključni elementi infrastrukture bežične mreže su bazne stanice (eng. *Base station*), kontrolori pristupa (eng. *Access controllers*), aplikacijski *softver* za povezivanje (eng. *Application connectivity software*) i distribucijski sustav (eng. *Distribution system*) [3].

Bazna stanica je uobičajena infrastrukturna komponenta koja povezuje bežične komunikacijske signale koji putuju zrakom do žičane mreže koja se često naziva distribucijski sustav. Omogućuje korisnicima pristup širokom rasponu mrežnih usluga. Zrak služi kao medij za prijenos elektromagnetskih valova, što je temelj bežičnog umrežavanja, a kvaliteta prijenosa signala ovisi o preprekama između odašiljača i prijemnika, korištenim modulacijskim postupcima, atmosferskim uvjetima, interferenciji, vrsti polarizacije antene i tako dalje [3].

Nerijetko, bazne stanice sadržavaju bežični NIC koji implementira istu tehnologiju kao i bežični NIC na korisničkim uređajima kako bi omogućila kompatibilnu komunikaciju. Dakle, u tom slučaju korisnikov uređaj iskorištava svoj pun potencijal u smislu korištenja kvalitetnijih WiFi standarda, sigurnosnih mehanizama i energetske učinkovitosti. Ovisno o njihovoj namjeni, bazne stanice imaju različite nazive. Na primjer, AP predstavlja tipičnu baznu stanicu za bežične LAN mreže (eng. *Wireless Local Area Network* - WLAN). Postojanje više od jednog AP-a unutar zatvorenog

prostora omogućava se *roaming* odnosno korisnikovo kretanje kroz objekt. Kako se korisnik kreće po određenom dijelu objekta i kako se približava drugim AP-ovima, NIC se automatski ponovno povezuje s najbližim AP-om za održavanje pouzdane i stalne komunikacije [3].

Najnapredniji oblici baznih stanica su *ruteri* i poveznik (eng. *Gateway*) koji pružaju dodatne mrežne funkcije. Poveznici su čvorovi u komunikacijskoj mreži koji se koriste za povezivanje dvije raznorodne mreže. Mogu imati funkciju kontrole pristupa mreži i resursima unutar nje, potom stvoriti uvjete za povezanost aplikacija koje koriste različite protokole za izvršavanje. S druge strane, *ruter* jamči povezanost mnogo uređaja na jednoj širokopojasnoj mreži. Primljene IP (eng. *Internet Protokol* - IP) pakete mrežne razine usmjerava određenim algoritmima prema odredištu. Bazna stanica može podržavati komunikaciju od točke do točke (eng. *Point to Point*) ili od točke do više točaka (eng. *Point to Multipoint*). Komunikacija od točke do točke dozvoljava izravan prijenos podataka od jedne bazne stanice ili terminalnog uređaja do drugog. Ovakva konfiguracija je uobičajena za bežičnu komunikaciju na velikim udaljenostima. Komunikacija od točke do više točaka označava mogućnost komunikacije bazne stanice s više terminalnih uređaja i baznih stanica istovremeno. Takav scenariji čest je u WLAN mrežama gdje AP omogućava tu funkciju [3].

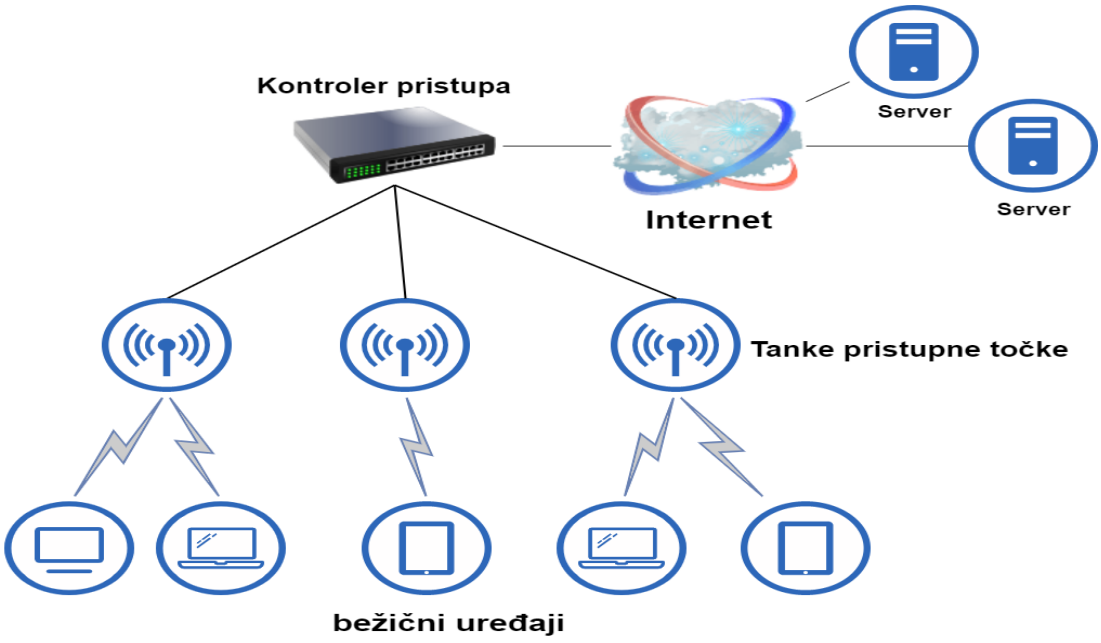
Poznati problem u bežičnim mrežama je pitanje mrežne sigurnosti. *Hardver* koji pomaže u tome nalazi se u žičnom dijelu mreže između AP-ova i zaštićenog dijela bežične mreže te se naziva kontroler pristupa. On centralizirano upravlja AP-ovima i kontrolira mrežni promet. Većina kontrolera pristupa sadrži ugrađenu bazu podataka koje se koristi za autentifikaciju korisnika pri spajanju na mrežu. Naime, manjim privatnim mrežama zbog manjeg broja korisnika i AP-ova autentifikacija ugrađenom bazom podataka je prihvatljivo rješenje. Međutim, u mrežama s velikim brojem korisnika i AP-ova, to može uzrokovati ograničenje skalabilnosti, otežano upravljanje i održavanje mreže. Shodno tome, koristi se drugačiji način autentifikacije, odnosno vanjska sučelja prema poslužiteljima (eng. *Server*) za autentifikaciju. Između ostalog, kontroleri pristupa mogu pružiti enkripciju prometa od strane klijenta (eng. *Client*) do *server-a* i nazad. Podmrežni *roaming* je funkcija kontrolera pristupa koja dopušta održavanje povezanosti i prelaska terminalnog uređaja s jedne podmreže na drugu podmrežu iste mreže bez potrebe za ponovnom autentifikacijom. Kontroler pristupa može kategorizirati korisnike s obzirom na mogućnosti korištenja različitih usluga. Dakle, korisnici višeg prioriteta dobit će veću propusnost (eng. *Bandwidth*) za korištenje zahtjevnijih usluga [3].

U radu s kontrolerom pristupa najbolje performanse postiže tanki AP (eng. *Thin AP*). Poznata je pod nazivom „inteligentna antena“ namijenjena je za smanjene kompleksnosti AP. Generalno, njezina glavna funkcija je primanje i odašiljanje mrežnog prometa kontroleru pristupa koji obrađuje okvire (eng. *Frame*) te ih prosljeđuje u žični LAN. Protokol korišten za komunikaciju tankog AP-a i kontrolera pristupa je vlasnički (eng. *Proprietary*) [5].

Prednosti implementacije kontrolera pristupa s tankim AP-om [3]:

- Niži trošak pogotovo u mrežama s velikim brojem AP-ova kao što su mreže kampusa, poduzeća, bolnica. Veći broj potrebnih AP-ova prati veću uštedu.
- Otvorenost sustava, svaki bežični NIC korisničkog uređaja će proći kroz sve funkcionalnosti kontrolera pristupa neovisno o proizvođaču tankih AP-ova, što nije slučaj kod drugih vrsta AP-a.
- Centralizirana podrška je značajna prednost, jer se većina konfiguriranja, nadzora i rješavanja problema unutar mreže izvršava na kontroleru pristupa zahvaljujući jednostavnim tankim AP-ovima koji su ograničenih funkcija.

Slika 2. prezentira pojednostavljenu arhitekturu mreže kojom su bežični uređaji spojeni na tri prostorno raspoređene tanke AP-e. Kontroler pristupa je spojen sa svim AP-ovima žično i osigurava centralizirano upravljanje i konfiguraciju mreže. Također je povezan s Internetom i *server-ima*, omogućujući uređajima unutar mreže pristup uslugama globalne mreže i vanjskim resursima [5].



Slika 2. Arhitektura mreže s kontrolerom pristupa i tankim pristupnim točkama

Izvor: [5]

Aplikacijski *softver* za povezivanje je vrsta *softvera* koji kreira i kontrolira vezu između komunikacije klijenta i *server-a*. Za jednostavne radnje poput web pretraživanja i slanja elektroničke pošte nije potreban. Doduše, ako dođe do pucanja veze protokoli su obično dovoljno otporni da mogu ponovno uspostaviti vezu. Premda, za složenije aplikacije potrebno je sučelje koje će osigurati klijentu korištenje resursa smještenih na udaljenim krajnjim sustavima [3].

Softver emulatora terminala replicira funkcionalnosti i ponašanje starijih terminala na modernim računalima pružajući jednostavno korisničko sučelje za aplikacijski *softver* koji se izvršava na drugom računalu. Korisnikovo sučelje emulira izgled, veličinu slova

i prikaz ekrana koji su karakteristični za odabrani tip terminala. Također, korisnik može upisivati naredbe i interaktivno raditi sa aplikacijskim *softver-om* preko ulaznih jedinica računala. U bežičnim sustavima korištenje *softver-a* emulatora terminala ima problem održavanja kontinuirane veze s starijim aplikacija. Zbog postojanja perioda nakon kojih se automatski prekida veza ako se ne zabilježe nikakve aktivnosti na strani klijenta [3].

Izravno povezivanje s bazom podataka je među najpopularnijim načinom aplikacijskog povezivanja. Korisniku pruža izravnu vezu sa *server-om* baze podataka za dohvaćanje podataka, izmjenu podataka, generiranje analitičkih izvještaja i slično. Slanjem upita strukturiranog jezika (eng. *Structured Query Language* - SQL) ili naredbe izravno bazi podataka, *server* baze podataka obavlja naredbu ili vraća dohvaćeni upit korisniku aplikacije. Izravno povezivanje daje razvojnim programerima potpunu kontrolu nad strukturom baze podataka jer ne postoje posredničkih slojevi. Uz to, mogu brzo implementirati promjene bez potrebe konfiguracije podataka na drugim mjestima [3].

Distribucijski sustav je sastavan i temeljan dio bežičnih mreža za njihovo funkcioniranje. Uključuje različite vrste kabela, mrežne uređaje za međusobno umrežavanje i osiguravanje kontinuirane usluge. Višestruki pristup s osjetilom nositelja (eng. *Carrier Sense Multiple Access* - CSMA) je protokol upotrebljavan u žičnim i bežičnim mrežama. Osmišljen je za dijeljenje zajedničkog medija od strane više NIC-eva za prijenos informacija. Kako bi se smanjila kolizija kada dva ili više NIC-a žele poslati informacije u isto vrijeme, oni rade na principu osluškivanja komunikacijskog kanala prije slanja. Dakle, kada je komunikacijski kanal slobodan, terminalni uređaj šalje informacije. Ako dođe do kolizije, odnosno takozvanog sudara informacija dvaju uređaja, događa se detekcija kolizije i ponovni pokušaj slanja [3].

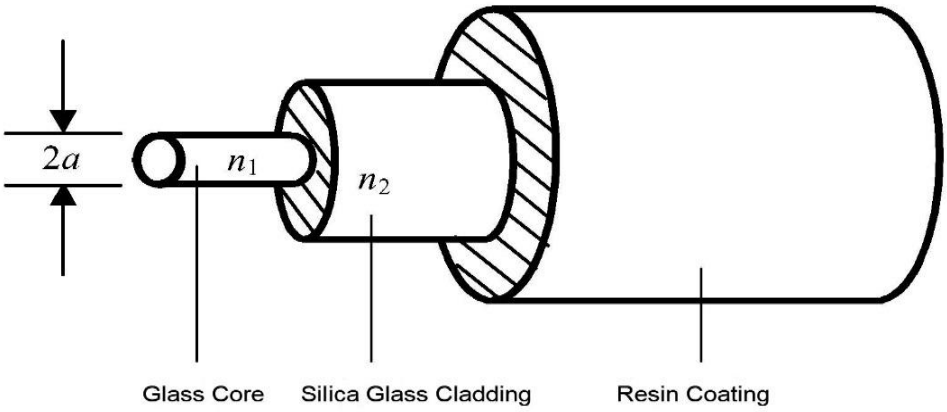
Golem broj računala u zatvorenim prostorima je kompleksnije okruženje za postavljanje bežične mreže u odnosu na uobičajene stambene prostore. Koncentrator (eng. *Hub*) se smatra pasivnim mrežnim uređajem za umrežavanje višestrukog broja računala. Radi na principu primanja mrežnog prometa i prosljeđivanja istog na sve svoje priključke (eng. *Port*). Glede nepotrebnog prosljeđivanja prometa svim računalima, u mnogim slučajevima zamjenjuje ga aktivni mrežni uređaj prospojnik (eng. *Switch*). Prospojnik omogućuje više kolizijskih domena ovisno o broju spojenih računala čime povećava performanse mreže. Smanjuje mrežno zagušenje prosljeđujući primljene okvire prema zadanom odredištu. U zatvorenim prostorima može doći do pojave mrtvih zona (eng. *Dead spots*) koje definiraju mjesto sa slabim i nedovoljnim signalom za korištenje telekomunikacijskih usluga. Jedno od rješenja je instalacija pojačivača signala (eng. *Reapeter*). On pojačava snagu primljenog signala kako bi povećao domet signala u bežičnoj mreži [3].

Najbolji mediji koji se koriste za umrežavanje AP-a i drugih elemenata arhitekture bežične mreže su optički kabel i kabel s uparenim paricama (eng. *Twisted pair*). Postoje dvije verzije kabela s uparenim paricama: nezaštićene uparene parice (eng. *Unshielded Twisted Pair* - UTP) i zaštićene uparene parice (eng. *Shielded Twisted Pair* - STP). Cat 5 (eng. *Category 5*) je UTP kabel pete kategorije te je jedan od

najpopularnijih među njima. Sastoji se od četiri para (po dvije žice) upletenih bakrenih žica. Maksimalne je dužine 100 metara. Poboljšana kategorija Cat 5 kabla je Cat 5e (eng. *Enhanced Category 5*) koja se koristi u modernim mrežnim sustavima jer podržava brzine prijenosa do 1 Gbit/s [3].

Optički kabel je mediji zadužen za prijenos svjetlosnih signala koji su oblik elektromagnetskog zračenja iznad frekvencije vidljive svjetlosti. Spomenuti mediji ima prednosti zbog podržavanja vrlo visokih brzina prijenosa većih od 1 Gbit/s, dugog životnog vijeka i neosjetljivosti na elektromagnetske interferencije. Sačinjen je od obično 8 optičkih vlakana koji prenose svjetlosne signale. Iz slike 3 prikazuje se strukturna podjela vlakna na tri temeljna dijela: staklena jezgra, obloga od silicijskog stakla i premaz od smole koji ima djelovanje zaštitnog sloja. Gdje „$2a$“ predstavlja promjer jezgre optičkog vlakna, uglavnom iznosa 50 ili 62.5 µm. Nadalje, „n_1“ označava indeks loma jezgre koji mora biti veći od indeksa loma obloge „n_2“ [6].

Jednomodno i višemodno vlakno imaju različite načine prijenosa svjetlosti. Višemodno vlakno ima veći promjer staklene jezgre, skuplje je i koristi se na kraćim udaljenostima kao što su instalacije u zgradama ili kampusima. Jednomodno je komercijalnije u upotrebi, koristi se na većim udaljenostima, ima mogućnost prijenosa samo jednog moda svjetlosti te je stabilnije u odnosu na višemodno vlakno [6].



Slika 3. Struktura optičkog vlakna, [6]

2.2 Klasifikacija bežičnih mreža

Računalne mreže teško je klasificirati po jednom kriteriju. Svakako, kompleksnosti doprinosi kontinuirani razvoj tehnologije. Granice između mreža postaju kompliciranije za definiranje, no pretežito su određene udaljenostima odnosno područjima koje pokrivaju.

Uz parametar područja pokrivenosti važan je i način prijenosa paketa putem komunikacijskog kanala. Nadalje, specificira se način komunikacije od klijentske strane do primatelja.

Primitivno gledajući postoje tri načina prijenosa koji su u širokoj upotrebi [8]:

1. Emitiranje (eng. *Broadcast*) je način komunikacije gdje klijent šalje informaciju (tekst, video, zvuk, slika) koju će primiti svi korisnici dijeljenog komunikacijskog kanala. Koristi se specijalna *broadcast* adresa kako bi se osiguralo da svi korisnici u mreži prime istu informaciju istovremeno.
2. Jednostruki prijenos (eng. *Unicast*) je metoda prijenosa gdje se informacija šalje samo jednom određenom primatelju. Koristi se odredišna adresa primatelja kako bi se osiguralo da samo taj primatelj primi informaciju.
3. Višesmjerno slanje (eng. *Multicast*) je način slanja informacije prema većem broju primatelja odnosno grupi primatelja koji su zainteresirani za isti sadržaj ili resurs. Koristi se *multicast* adresa kako bi samo članovi određene grupe primili informaciju.

Primarno, klasifikaciju bežičnih mreža možemo podijeliti na osobnu računalnu mrežu (eng. *Personal Area Network* - PAN), LAN, metropolijsku računalnu mrežu (eng. *Metropolitan Area Network* – MAN) i računalnu mrežu širokog područja (eng. *Wide Area Network* – WAN) [7].

1 m	Kvadratni metar	PAN
10 m	Ured	LAN
100 m	Zgrada	
1 km	Kampus	
10 km	Grad	MAN
100 km	Država	WAN
1000 km	Kontinent	

Slika 4. Primjeri udaljenosti i područja po klasifikaciji mreže

Izvor : [7]

PAN mreža pokriva iznimno malu površinu od nekoliko metara (slika 4), primjeri upotrebe uključuje povezivanje pametnog telefona s nosivim uređajima korištenjem *Bluetooth* tehnologije. LAN mreža obuhvaća područje od nekoliko desetaka metara do jednog kilometra. Primjer LAN mreže je povezivanje računala unutar jedne zgrade korištenjem WiFi tehnologije. MAN mreža, kao što joj ime ukazuje, pokriva područje cijelog jednog grada. WAN je najveća mreža, pokriva više država ili čak kontinent. Najpoznatiji primjer WAN mreže je Internet [7].

2.2.1 Osobna računalna mreža – PAN

Gotovo svako računalo ima priključenu tipkovnicu, miš i printer. Bez korištenja bežične veze, ova veza se mora uspostaviti s kabelima. Ovo predstavlja dvije vrste PAN mreža: žični PAN (eng. *Wired* PAN), koji može biti ostvaren povezivanjem miša s računalom putem USB (eng. *Universal Serial Bus* - USB) kabla, i bežični PAN (eng. *Wireless* PAN - WPAN), ostvaren korištenjem jedne od bežičnih tehnologija kratkog dometa, na primjer *Bluetooth-om* [7].

Pojava sve većeg broja bežičnih uređaja (pametni sat, slušalice...) povećava zastupljenost WPAN mreža. *Bluetooth* je bežična tehnologija koja omogućuje brzo uparivanje uređaja. Ta činjenica implicira da uređaji ne mogu međusobno komunicirati osim ako prethodno nisu otkrili jedan drugog. Tehnologija je temeljena na skokovitoj promjeni nosive frekvencije (eng. *Frequency hopping spread spectrum* - FHSS), koja pruža prijenosnim uređajima formiranje WPAN mreže u korisnikovoj blizini. PAN mreža jednostavnije je arhitekture i dizajnirana je za osobnu upotrebu, pružajući korisnicima mobilnost i praktičnost. Ne zahtijeva učestalo održavanje i poprilično ju je lagano postaviti [7].

Radiofrekventna identifikacija (eng. *Radio Frequency Identification* - RFID) je tehnologija koja koristi niskofrekventne, visokofrekventne i ultra visokofrekventne radiovalove za komunikaciju između čitača (eng. *Reader*) i RFID oznaka (eng. *Tag*). Oznaka je malih dimenzija, sadrži mikročip i antenu za primanje radiovalova. Čitač emitira radiovalove putem svoje antene. Kada oznaka u svojoj blizini detektira emitirani signal, čeka slučajno odabrano vrijeme prije nego li odgovori sa svojim identifikacijskim podacima. Radi izbjegavanja situacije gdje više oznaka u malom prostoru, odgovara na jedan signal u isto vrijeme.

Nakon primanja podataka, čitač prenosi podatke do računala na kojem će se isti obraditi. Zahvaljujući WPAN mreži implementacija RFID tehnologije je moguća kod praćenje inventara i životinja, beskontaktnog plaćanja, kontrole pristupa objektu i ostalih primjena [7].

2.2.2 Lokalna računalna mreža – LAN

Danas gotovo svaka zgrada, kampus, kafić, dom ima svoju privatnu mrežu. Kada je korištena od strane tvrtke, naziva se poslovna mreža. LAN se naširoko koristi za povezivanje osobnih računala i elektroničkih uređaja kako bi im se omogućilo dijeljenje resursa i razmjena informacija [7].

Bežični LAN (eng. *Wireless* LAN - WLAN) realiziran je na mjestima gdje nije presudna brzina i pouzdanost veze (performanse) nego, mobilnost i pružanje usluge što većem broju korisnika. Standard za WLAN je 802.11 dat je od instituta inženjera elektrotehnike i elektronike (eng. *Institute of Electrical and Electronics Engineers* - IEEE) odnosno

popularnije zvan WiFi. WLAN mreže koegzistiraju u nelicenciranom frekvencijskom spektru. Nezaobilazan je frekvencijski pojas od 2.4 GHz, on je jedan od najrasprostranjenijih za WLAN mreže. Zbog prirode spektra često je podložan zagušenjem i interferencijom. Osim toga, postoje i drugi frekvencijski pojasevi koji se koriste, poput 5 GHz, koji ima veći broj kanala i doprinosi većoj propusnosti i brzini prijenosa. WLAN mreže zahvalne su i u izvanrednim situacijama (npr. prirodne nepogode) zahtijevajući samo nekoliko elemenata fizičke infrastrukture za davanje usluge. *Broadcast* način prijenosa paketa zastupljen je u WLAN mrežama, jer signal nije usmjeren samo jednom uređaju koji prima podatke. Zlonamjerni uređaji u dometu signala mogu presresti pakete koji nisu namijenjeni njima. Glede mnogih prednosti i uvjerljivo najkorištenije mreže, WLAN donosi sa sobom sigurnosne rizike čija se rješenja i dalje usavršavaju [7].

Žični LAN (eng. *Wired* LAN) obilježava malo kašnjenje i niska vjerojatnost pogreške, ali je ograničen duljinom kabla. Brzine prijenosa obično se kreću od 100 Mbit/s do 1 Gbit/s. Naravno, postoji više topologija žičnog LAN-a, a među dominantnijim je zvijezdasta topologija. U zvijezdastoj topologiji sva su računala povezana vezom od točke do točke s mrežnim uređajem, što podsjeća na izgled zvijezde. Također, međusobnim spajanjem prospojnika može se iz nekoliko manjih LAN mreža kreirati jedna velika mreža. Fizička mreža može se dodatno dijeliti u logičke virtualne LAN mreže (eng. *Virtual* LAN - VLAN). Prospojnik razdvaja dolazni mrežni promet između različitih grupa *port-ova*. Svaka grupa čini jednu VLAN mrežu koja djeluje kao zaseban LAN, iako su računala spojena na isti prospojnik. Administrator mreže vodi računa o kreiranju VLAN mreža, njihovom broj računala, te odabiru imena mreža koje je često povezano s bojom kabla kojim su računala povezana s mrežnim uređajima [7].

2.2.3 Metropolijska računalna mreža – MAN

U ranijim sustavima, antena velike snage bila bi postavljena na vrhu obližnjeg brda i televizijski signal bi se zatim prenosio do kuća pretplatnika televizijskog sadržaja. Kasnije su davatelji usluge potpisivali ugovore s lokalnim vlastima za kabelsko povezivanje cijelih gradova. Kabelske televizijske mreže najpoznatiji su primjer žične MAN mreže (eng. *Wired* MAN). Kada je Internet počeo privlačiti širu publiku, operatori kabelskih TV mreža shvatili su da s nekim promjenama u sustavu mogu pružiti dvosmjernu internetsku uslugu u neiskorištenim dijelovima spektra. Upravo takva promjena na tržištu povećala je njihovu ponudu usluga, a posljedično potom stvorila veće prihode i proširila bazu korisnika [7].

Svjetska interoperabilnost za mikrovalni pristup (eng. *Worldwide Interoperability for Microwave Access* - WiMAX) referira se na IEEE 802.16 standard. WiMAX tehnologija pruža bežični širokopojasni pristup na velikim udaljenostima i često se smatra alternativom kabelskom povezivanju za pristup Internetu. Prijenos podataka bazira se na frekvencijskom multipleksu ortogonalnih podnosilaca (eng. *Orthogonal frequency-division multiplexing* - OFDM). Umjesto da se sadržaj poruke modulira na jedan

prijenosi signal, on se modulira na više podnosilaca, čime se povećava otpornost na pogreške prilikom prijenosa, posebno u urbanim sredinama. WiMAX bazne stanice visoke su snage, procijenjena udaljenost odašiljanja je 10 puta veća u odnosu na WiFi bazne stanice. Bežična MAN mreža (eng. *Wireless* MAN - WMAN) često je sinonim za WiMAX. Brojne implementacije WiMAX-a koriste licencirani spektar koji međusobno dijele korisnici, što može uzrokovati smanjenju kvalitete usluge [7].

2.2.4 Računalna mreža širokog područja – WAN

Poduzeća, podatkovni centri, obrazovne institucije povezuju svoje mreže koje su geografski razmještene na velikim udaljenostima. Stvarajući najskuplju i najveću WAN mrežu koja se sastoji od mnogobrojnih LAN mreža. Za povezivanje LAN mreža različitih lokacija uobičajena praksa je iznajmljivanje prijenosnog medija od telekomunikacijskih tvrtki. Umjesto iznajmljivanja prijenosnog medija, tvrtke mogu koristiti Internet za povezivanje svojih lokacija putem virtualne privatne mreže (eng. *Virtual Private Network* - VPN) [7]. No, postoje i drugi načini povezivanja, a svaka metoda ima svoje prednosti i nedostatke te izbor najčešće ovisi o specifičnim potrebama i resursima organizacije. Poduzeća često koriste VPN za povezivanje svojih poslovnih mreža smještenim u različitim državama ili kontinentima. Između ostalog, mnogi zaposlenici područja informacijsko-komunikacijskih tehnologija rade na udaljeni način, stoga postavljanje vatrozida (eng. *Firewall*) omogućava kreiranje takozvanog „tunela“ između njihove lokacije i poslovne mreže. Kriptiranjem podataka, VPN osigurava pouzdanost rada s osjetljivim podacima poduzeća [7].

Mrežni operatori su okosnica Interneta, međusobno povezuju svoje autonomne sustave za razmjenjivanje prometa i pružanje usluge pristupa Internetu krajnjim korisnicima. Protokolima usmjeravanja *ruteri* razmjenjuju informacije o usmjeravanju i donose odluke o prosljeđivanju paketa.

WAN definira umrežavanje žičnih i bežičnih mreža diljem svijeta. Međutim, bežična računalna mreža širokog područja (eng. *Wireless Wide Area Network* – WWAN) označava sustave ćelijske građe. Povezivanje je ostvareno bežičnim putem, isto tako pokriva veliko geografsko područje, pružajući veće brzine prijenosa i mobilnost. Istaknuti su mobilni sustavi koji daju veći broj usporednih komunikacija u istom frekvencijskom opsegu i ponovno korištenje frekvencija. Nudeći multimedijske usluge, govor preko IP-a, (eng. *Voice over* IP - VoIP), širokopojasni pristup internetu i tako dalje [9].

3. VRSTE I ZNAČAJKE BEŽIČNIH TEHNOLOGIJA

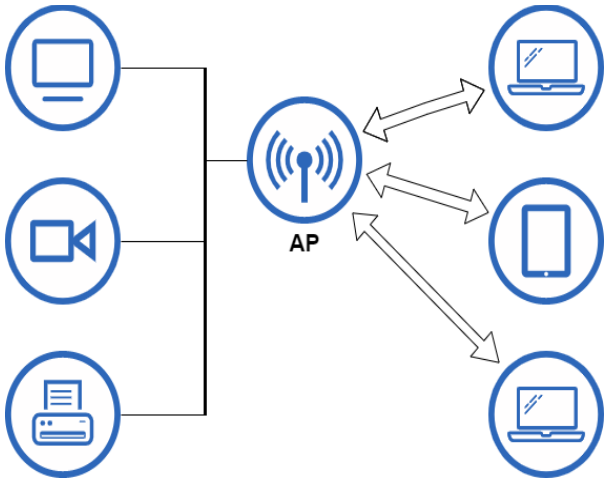
Varijacije mobilnih terminalnih uređaja koji podržavaju pristup Internetu i međusobnu komunikaciju su mnogobrojne. Od monitora za bebe, do pametnih telefona, bežična tehnologija nudi različita rješenja za olakšavanje života ljudi. Bežična tehnologija je usmjerena na potrošače koji je koriste za svakodnevne aktivnosti.

Zbog svoje praktičnosti i univerzalne uporabe, postala je trend u industriji, gdje kompanije kontinuirano razvijaju i prilagođavaju nove tehnologije kako bi zadovoljile potrebe tržišta i ostvarile financijsku dobit. Njezina sveprisutnost u društvu je očita, pokazuje kako se ljudi postepeno adaptiraju na novo digitalno doba.

U ovom poglavlju detaljno ćemo obraditi WiFi mrežu, *Bluetooth* i *Zigbee* mrežu. Svaka od ovih tehnologija ima specifične značajke koje ih čine idealnim za određene namjene.

3.1 WiFi mreža

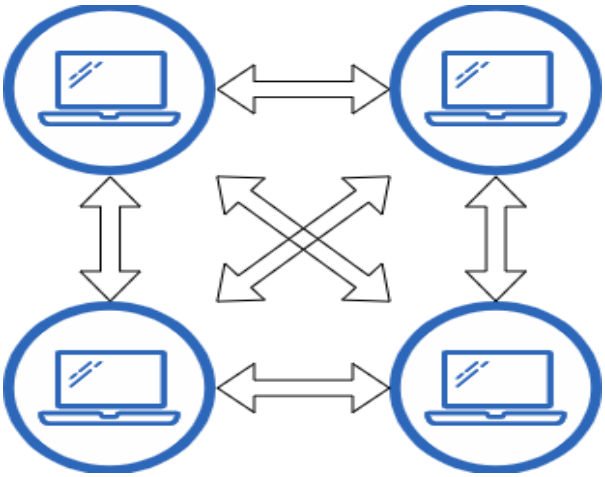
802.11 arhitektura koristi dvije vrste načina rada, infrastrukturni (eng. *Infrastructure*) i *ad hoc*. Infrastrukturni način rada je najpopularniji i koristi se za povezivanje uređaja poput prijenosnih računala i pametnih telefona na mreže kao što je intranet tvrtki ili Internet. U infrastrukturnom načinu rada, svaki je klijent povezan s AP-om koji je pak dalje spojen na drugu mrežu. Klijent šalje i prima pakete podataka putem AP. AP opslužuje sve odašiljače i prijemnike koji su u njegovom izravnom dometu. Svaki klijent u ovoj mreži mora imati konfigurirane sigurnosne postavke koje odgovaraju postavkama AP-a, čime se osigurava visoka razina sigurnosti. Ova vrsta mreže je široko korištena u javnim prostorima kao što su zračne luke, hotelska predvorja i željezničke postaje [10].



Slika 5. Infrastrukturni način rada

Izvor: [10]

S druge strane, kod decentralizirane mreže nema AP-a, računala su povezana tako da mogu izravno slati okvire jedni drugima. *Ad hoc* mreže još uvijek nisu toliko korištene. Komunikacija je ravnopravna između sudionika (eng. *Peer to Peer*) što znači da svaki klijent može komunicirati s bilo kojim drugim klijentom u mreži bez posredovanja AP-a. Zbog nedostatka centralnog AP-a, korisnici moraju konfigurirati sigurnosne postavke koje odgovaraju sigurnosnim zahtjevima svih klijenata u mreži. *Ad hoc* način je posebno koristan u situacijama gdje je potrebna brza i fleksibilna komunikacija među korisnicima, kao što je u vojnim operacijama za dijeljenje informacija među vojnicima ili u LAN mrežama za komunikaciju unutar fiksne grupe ljudi [10].



Slika 6. Ad hoc način rada

Izvor : [10]

Infrastrukturni način omogućuje bolju kontrolu i upravljanje mrežom, što je idealno za velike i stalne mreže, dok *ad hoc* pruža veću fleksibilnost i brzinu postavljanja, što je korisno u privremenim ili specijaliziranim mrežnim okruženjima [10].

Standardiziranjem WiFi-a omogućeno je praćenje njegove evolucije kroz vrijeme. Konstantnim pojavljivanjem novih WiFi standarda poboljšavaju se tehničke specifikacije tehnologije u odnosu na prethodni standard.

Novim generacijama mobilnih sustava, WiFi-u, WiMAX-u i ostalim sofisticiranim bežičnim komunikacijama jedna je značajka ista, korištenje naprednih modulacijskih tehnika višestrukog ulaza i višestrukog izlaza (eng. *Multiple-Input and Multiple-Output* - MIMO) i OFDM-a.

Podnosioci OFDM modulacije su ortogonalni i preklapaju se unutar komunikacijskog kanala. Svaki podnosilaca prenosi malu količinu podataka. OFDM je superioran jer ga obilježava otpornost na interferenciju između simbola, jednostavnost *hardver-a*, robusnost prema frekvencijskom bljeđenju (eng. *Fading*) [11].

OFDM simbol sastoji se od zaštitnog intervala i simbola podataka. Zaštitni interval sadrži ciklički prefiks koji je ključan za zaštitu od interferencije između simbola. Ciklički prefiks je kopija posljednjeg dijela simbola podataka koja se umetne na početak OFDM

simbola. Duljina zaštitnog intervala mora biti veća od maksimalnog kašnjenja u kanalu radi osiguravanja ortogonalnosti između podnosilaca. Simbol podataka je skup podnosilaca koji nose stvarne informacije [11].

MIMO antenski sustavi koriste više od jedne antene na odašiljačkoj i prijemnoj strani bežične komunikacije. Doprinoseći stvaranju više tokova prijenosa podataka. MIMO podupire stabilnost i pouzdanost veze s visokim brzinama prijenosa [11].

Promotrimo 2 x 2 MIMO sustav, dvije antene na odašiljaču i dvije na prijemniku stvaraju četiri neovisna prostorna toka. Tokovi se nazivaju kanali jednostrukog ulaza i jednostrukog izlaza (eng. *Single Input Single Output* - SISO). Svaka od dvije antene na odašiljaču može komunicirati s obje antene na prijemniku (4 kombinacije). Po jedan SISO kanal nalazi se između svake komunikacije. Takav način doprinosi prostornoj raznolikosti i poboljšanju signala. MIMO koristi sve kanale istovremeno, različite podatke može slati kroz različite kanale [11].

Tablica 1. Evolucija IEEE 802.11 standarda i njegove performanse

Standard	Godina	Frekvencijski pojas	Propusnost	Maksimalna brzina prijenosa podataka
802.11	1997	2.4 GHz	20 MHz	2 Mbit/s
802.11b	1999	2.4 GHz	20 MHz	11 Mbit/s
802.11a	1999	5 GHz	20 MHz	54 Mbit/s
802.11g	2003	2.4 GHz	20 MHz	54 Mbit/s
802.11n	2009	2.4 GHz, 5 GHz	20 MHz, 40 MHz	600 Mbit/s
802.11ac	2013	5 GHz	40 MHz, 80 MHz, 160 MHz	6.9 Gbit/s
802.11ax	2019	2.4 GHz, 5 GHz	40 MHz, 80 MHz, 160 MHz	9.6 Gbit/s
802.11be	2024	2.4 GHz, 5 GHz, 6 GHz	20 MHz, 40 MHz, 80 MHz, 160 MHz, 320 MHz	46 Gbit/s

Izvor: [12]

Prema tablici 1. WiFi standard 802.11 godine 1997. postavio je temelj za sve naredne standarde, uvelike je pridonio usvajanju bežičnih mreža u širokoj primjeni. Maksimalna brzina prijenosa podataka od 2 Mbit/s bila je dovoljna za osnovne aplikacije kao što su e-pošta i korištenje Internet pretraživača. Nakon dvije godine IEEE predstavlja 802.11b standard koji koristi isti frekvencijski pojas 2.4 GHz. Riječ je o nelicenciranom pojasu koji je besplatan za korištenje te se time smanjuje trošak implementacije. No, zbog toga mnogi elektronički uređaji ga koriste što povećava vjerojatnost pojave interferencije. 802.11a operira na širem pojasu od 5 GHz kako bi izbjegao takvu pojavu. Više frekvencije podrazumijevaju manji domet signala, jer se frekvencije brže apsorbiraju od strane prepreka i manje su valne duljine. Iskorištavajući prednosti OFDM-a s 52 podnosioca 802.11a postiže maksimalnu brzinu od 54 Mbit/s. 802.11g uspijeva dobiti istu brzinu prijenosa kao 802.11a koristeći 2.4 GHz frekvencijski pojas [12].

Sljedeći WiFi standard koristi oba, do sad navedena pojasa, uvodeći po prvi puta antenski sustav MIMO. Ostvarujući zavidnih 600 Mbit/s uz korištenje 4 x 4 MIMO sustava na propusnosti od 40 MHz. Povećanje performansi povećalo je i cijenu odašiljačko-prijemne opreme. 802.11ac primjenjuje samo 5 GHz-ni pojas, koristeći 8 x 8 MIMO brzine dosežu do 6.9 Gbit/s. Predzadnji standard uvodi novitet višekorisničkog MIMO sustava (eng. *Multi-User* MIMO) koji radi u uzlaznoj i silaznoj vezi za razliku od 802.11ac standarda gdje je taj sustav radio samo u silaznoj vezi. Pružajući AP-ovima mogućnost istodobnog komuniciranja s više uređaja preko istih frekvencija [12]. Najnoviji je 802.11be, on uvod propusnost od 320 MHz koju mu omogućava novi 6 GHz-ni frekvencijski pojas. Niska dostupnost terminalnih uređaja koji podržavaju zadnji WiFi standard u konačnici rezultira njihovom visokom cijenom. Naime, mrežni operatori se susreću s raznim izazovima pri pojavi novih standarda. Za 802.11be moraju dobiti regulatorno odobrenje za korištenje novog frekvencijskog pojasa, implementacija najnovijeg standarda zahtijeva nadogradnju mrežne infrastrukture i niska je dostupnost uređaja koji ga podržavaju [13].

3.2 Bluetooth

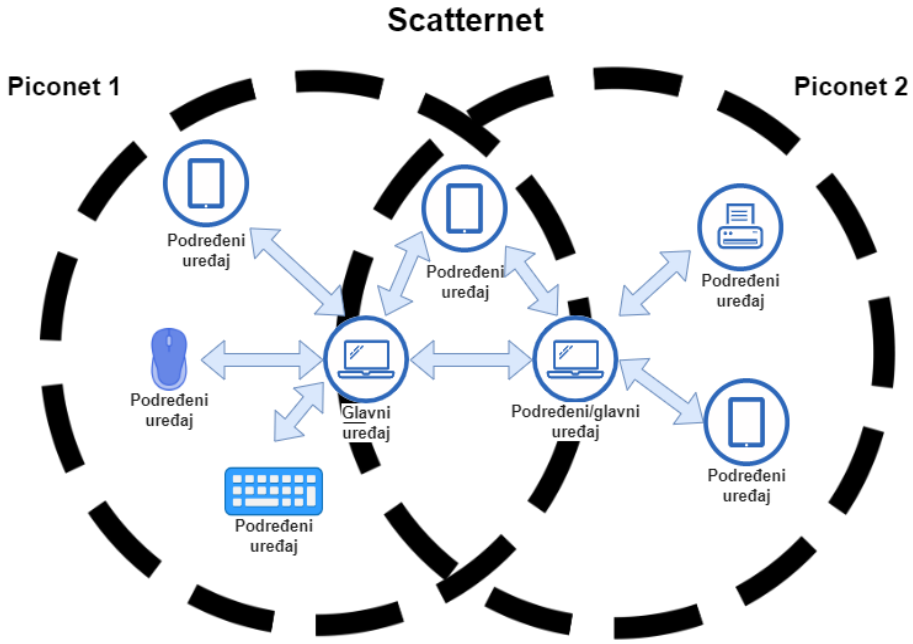
Mnogi prijenosi uređaji za povezivanje s drugim uređajima ne traže velike brzine prijenosa, *hardver-sku* kompleksnost i veliki domet signala. *Bluetooth* (IEEE 802.15.1) se verzijom 4.0 podijelio na klasični *Bluetooth* (eng. *Bluetooth Classic*) i niskoenergetski *Bluetooth* (eng. *Bluetooth Low Energy* – BLE). Klasični *Bluetooth* je temeljena tehnologija *Bluetooth* standarda, koristeći frekvencijski pojas od 2.4 GHz omogućuje uređajima kreiranje PAN mreže, njegova najveća primjena je u uparivanju uređaja za zvučno emitiranje s mobilnim platformama. S druge strane, BLE kako ime nalaže, ima izrazito malu potrošnju energije i optimizirano prelaženje uređaja u stanje spavanja (eng. *Sleep mode*). BLE koristi drugačiju FHSS *shemu* skakanja, sadrži manji broj kanala (40) u usporedbi s klasičnim *Bluetooth-om* (79), te također mijenja frekvencije sporije. Omogućavajući širu primjenu u Internet stvarima (eng. *Internet of Things* - IoT), štedeći bateriju minijaturnih uređaja i podržavajući brzine prijenosa do 1 Mbit/s što je otprilike duplo manje od klasičnog *Bluetooth-a* [14].

Klasični *Bluetooth* dozvoljava sedam uređaja povezanih na jedan glavni (eng. *Master*) uređaj kreirajući *piconet* mrežu. Veza između glavnog uređaja i jednog od tih sedam podređenih (eng. *Slave*) uređaja naziva se uparivanje. Svaki uređaj ima MAC adresu duljine 3 bita. Tijekom uparivanja uređaji razmjenjuju osobne identifikacijske brojeve (eng. *Personal Identification Number* - PIN), zbog sigurnosnih razloga. Ukoliko je isti PIN broj na oba uređaja osigurava se pouzdano uparivanje [15].

Glavni uređaj može komunicirati sa svim podređenim uređajima, ali podređeni uređaji međusobno direktno ne komuniciraju. Glavni uređaj odlučuje kada će poslati podatke podređenim uređajima te isto tako može na zahtjev tražiti podatke od njih. U komunikaciji od točke do više točaka, podređeni uređaji prate FHSS *shemu* skakanja

glavnog uređaja. Što znači da svi uređaji sinkronizirano mijenjaju frekvenciju kako bi poboljšali prijenosa podataka [15].

Komunikaciju od točke do točke prezentira povezanost glavnog uređaja sa samo jednim podređenim. Jednostavna i izravna veza između dva uređaja, često se koristi za slušanje glazbe bežičnim slušalicama ili zvučnikom, prijenos datoteka između pametnih telefona, povezivanje miša i tipkovnice s računalom [15].



Slika 7. Primjer piconet i scatternet mreže

Izvor: [15]

Scatternet mrežu čine povezne dvije ili više *piconet* mreže, kako bi se proširila pokrivenost mreža i omogućila međusobna komunikacija između uređaja iz različitih *piconet* mreža. U takvom slučaju uređaji se moraju ponašati istovremeno kao podređeni i glavni u različitim mrežama. Povezivanjem više mreža proporcionalno se smanjuje propusnost svake pojedinačne mreže zbog povećanog broja uređaja i podataka koji se prenose. Također, dolazi do povećanja vjerojatnosti za pojavom interferencije, zbog većeg broja komunikacija na istom frekvencijskom pojasu. Pružanje takvog vida mobilnosti sinonim je za *ad hoc* mrežu. *Scatternet* mreža podržava više od 8 spojenih uređaja, pružajući veću fleksibilnost i širinu mreže. Povezani uređaji mogu međusobno razmjenjivati podatke, međutim od klasičnog *Bluetooth-a* osnovni protokol neće biti dovoljan. Potreban je dodatni *softver* na uređaju koji želi sudjelovati u razmijeni podataka [15].

3.3 Zigbee mreža

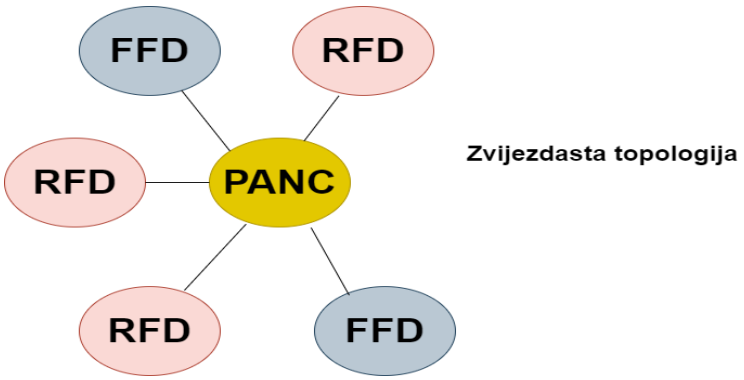
IEEE stoji iza mnogih standarda u bežičnim tehnologijama. *Zigbee* (IEEE 802.15.4) je tehnologija za bežičnu mrežu koja omogućuje niže brzine prijenosa u usporedbi s

Bluetooth-om. Namijenjen je automatizaciji i daljinskom upravljanju uređajima. S najnovijom verzijom, *Zigbee* 3.0, standard je postao interoperabilan između različitih proizvođača, te su dodana sigurnosna poboljšanja i podržavanje frekvencijskog pojasa iznad 2.4 GHz. *Zigbee* 3.0 u Europi radi na 800 MHz dok u Sjevernoj Americi i Australiji na frekvencijama od 900 MHz. Osnažujući snagu signala i podupirući širu upotrebu *Zigbee-a* [16].

Klasifikacija uređaja unutar mreže slična je *Bluetooth-ovoj*, primjenjuje se komunikacija s glavnim uređajem i podređenim uređajima najčešće u zvijezdastoj topologiji. Baterija uređaja koji koriste *Zigbee* tehnologiju može trajati nekoliko godina, jer uređaji povremeno prenose male količine podataka te tijekom razdoblja neaktivnosti prijelaze u stanje mirovanja. *Zigbee* pruža povezanost do 254 čvorova unutar jedne mreže [17].

Zigbee operira u PAN mreži, gdje je potreban bar jedan uređaj pune funkcije (eng. *Full Function Device* - FFD), dok ostali uređaji mogu biti smanjene funkcije (eng. *Reduced Function Device* - RFD). FFD imaju tri načina rada: PAN koordinator (eng. PAN *coordinator* - PANC), koordinator i uređaj. RFD su nužni za jednostavne realizacije, imaju ograničene kapacitete za obradu i pohranu podataka. RFD može komunicirati samo s FFD, mada FFD ovisno o topologiji može komunicirati s RFD ili s još jednim FFD uređajem [17].

Zigbee mreža implementira se u tri topologije: zvijezdasta, *mesh* i klaster-stablo topologija. Zvijezdasta topologija (slika 8) je nezavisna od drugih mreža sastoji se od centralnog uređaja poznatijeg kao PANC, na kojeg se direktno spajaju podređeni uređaji pretežno napajani putem baterije. Kada je FFD prvi puta aktiviran obično s napajanjem iz električne mreže, može stvoriti svoju mrežu u kojoj je on PANC. U svakoj zvijezdastoj topologiji postoji jedan PANC, te on nije istodobno PANC u drugoj mreži [17].

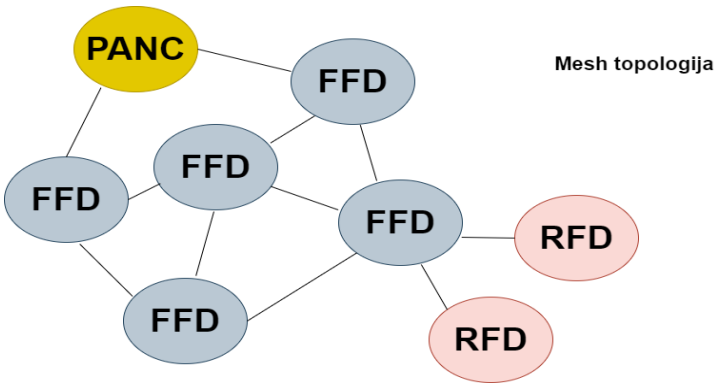


Slika 8. Zvijedasta topologija Zigbee mreže

Izvor: [17]

Mesh topologija (slika 9) u *Zigbee* mreži može funkcionirati kao *ad hoc* mreža te se također sastoji od jednog PANC, gdje svaki čvor uključujući i PANC-a može komunicirati s bilo kojim drugim čvorom koji mu je u dometu. Poruku je moguće usmjeravati s višestrukim skokovima (eng. *Multi hop*) do odredišnog čvora.

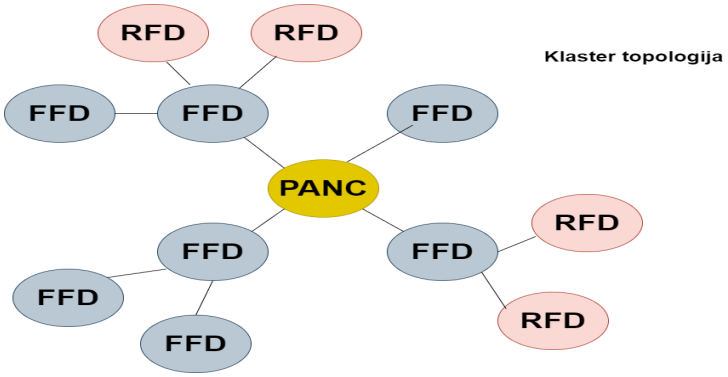
Karakteristično za *mesh* topologiju je moć promjene i zadržavanja strukture zavisno o broju uređaja, snage signala, kvaliteti veze, mrežnoj konfiguraciji i drugim faktorima. Dakle, osim samostalnog organiziranja *mesh* nudi i samostalno obnavljanje koje povećava pouzdanosti i stabilnosti mreže. Samostalnim obnavljanjem mreža se može automatski prilagoditi promjenama, kao što su kvarovi uređaja te preusmjeriti poruku alternativnim putem. *Mesh* topologija se primjenjuje u industrijskoj kontroli i nadzoru, bežičnim senzorskim mrežama, pametnim kućama i tako dalje [17].



Slika 9. Mesh topologija Zigbee mreže

Izvor: [17]

Klaster-stablo topologija (slika 10) sastoji se od većeg broja FFD uređaja, te sadrži više koordinatora od koji je samo jedan PANC. RFD uređaji se povezuju na krajeve grana stabla. PANC se postavlja kao glava klastera s identifikatorom klastera nula. Zatim šalje periodično signalne (eng. *Beacon*) okvire kako bi informirao susjedne uređaje o svojoj prisutnosti. FFD koji primi okvir može zatraži pridruživanje mreži kod PANC-a. Nakon što PANC prihvati zahtjev, taj FFD postaje glava klastera. Drugi uređaji se mogu spojiti na mrežu preko glave klastera. Klaster označava skup uređaja sličnih funkcija ili zadataka pod jedinstvenim identifikatorom klastera. Istodobno svaki uređaj u mreži može biti dio više klastera. U svakom klasteru postoji jedna glava klastera, koja obično ima dodatne funkcionalnosti i odgovornosti u odnosu na druge uređaje u klasteru [17].



Slika 10. Klaster topologija Zigbee mreže

Izvor: [17]

4. ANALIZA WIFI MESH TEHNOLOGIJE U ZATVORENIM PROSTORIMA

Konstantnim porastom broja terminalnih uređaja koji zahtijevaju pristup Internetu, pojavljuju se specifični problemi u mrežama. U zatvorenim prostorima, tradicionalne WiFi mreže često nisu dovoljne. Konkretno, izazove kao što su slaba pokrivenost, prekidi u vezi ili nedostatak kapaciteta može eliminirati bežična *mesh* mreža (eng. *Wireless Mesh Networks* - WMN) [18].

WiFi *mesh* pruža veću pokrivenost kako na otvorenim prostorima poput gradova i stadiona tako i u zatvorenim prostorima kao što su višekatne zgrade i aerodromi. WMN mreža može biti dio MAN-a, premda će i dalje imati jednu lozinku i jedan naziv mreže odnosno *Mesh* ID (eng. Identifier). Čvorovi u *mesh* mreži ne samo da proširuju pokrivenost, već također mogu djelovati kao *ruteri* s prilagodljivim protokolima usmjeravanja i besprijekornim prekapčanjem između čvorova [18].

IEEE 802.11s definira standard koji integrira WMN u 802.11 sustave. Omogućujući *multi – hop* topologiju, s automatskom konfiguracijom i usmjeravanjem na drugom sloju modela međusobnog povezivanja otvorenih sustava (eng. *Open Systems Interconnection* – OSI model) [18].

Jeftini i jednostavni elementi za instalaciju krase WiFi *mesh* tehnologiju. Robusnost WMN-a dolazi od sposobnosti samostalnog organiziranja i obnavljanja mreže. Popriličan broj čvorova spojenih u *mesh* topologiji zapravo pomaže u postizanju veće i brže mreže [18].

Osnovni protokol usmjeravanja u WMN je hibridni bežični *mesh* protokol (eng. *Hybrid Wireless Mesh Protocol* - HWMP). HWMP pronalazi najbolju rutu između čvorova za prijenos podataka. Svaki čvor otkriva svoje susjedne čvorove i bilježi stanje veze pohranjujući informacije u tablicu usmjeravanja. Upotrebljava sekvencijske brojeve odredišta za detektiranje zastarjelih informacija o rutama. Dakle, čvor svakoj ruti dodjeljuje jedinstveni sekvencijski broj. Kada primi novu informaciju o ruti uspoređuje sekvencijski broj od trenutno poznatog sekvencijskog broja te rute. U slučaju da je sekvencijski broj manji, on odbacuje tu informaciju jer ju smatra zastarjelom. HWMP ovakvim postupkom izbjegava pojavljivanje beskonačnih petlji u mreži [19].

CSMA se ne preferira u WMN zbog velikog broja čvorova te kontinuirano mijenjanje strukture mreže dovodi do češće kolizije. 802.11s uvodi novi kontrolirani način pristupa kanalu (eng. *Mesh Coordinated Channel Access*) kojim se smanjuje interferencija između *mesh* čvorova i povećava dostupnost radio kanala. Kontrolirani način opisuje rezerviranje vremenskih intervala u kojima čvorovi prijenose podatke. Također, postoji mehanizam obavještavanja drugih čvorova o rezervacijama i pri dodavanju ili uklanjanu čvorova dinamički se prilagođava potrebama mreže [18].

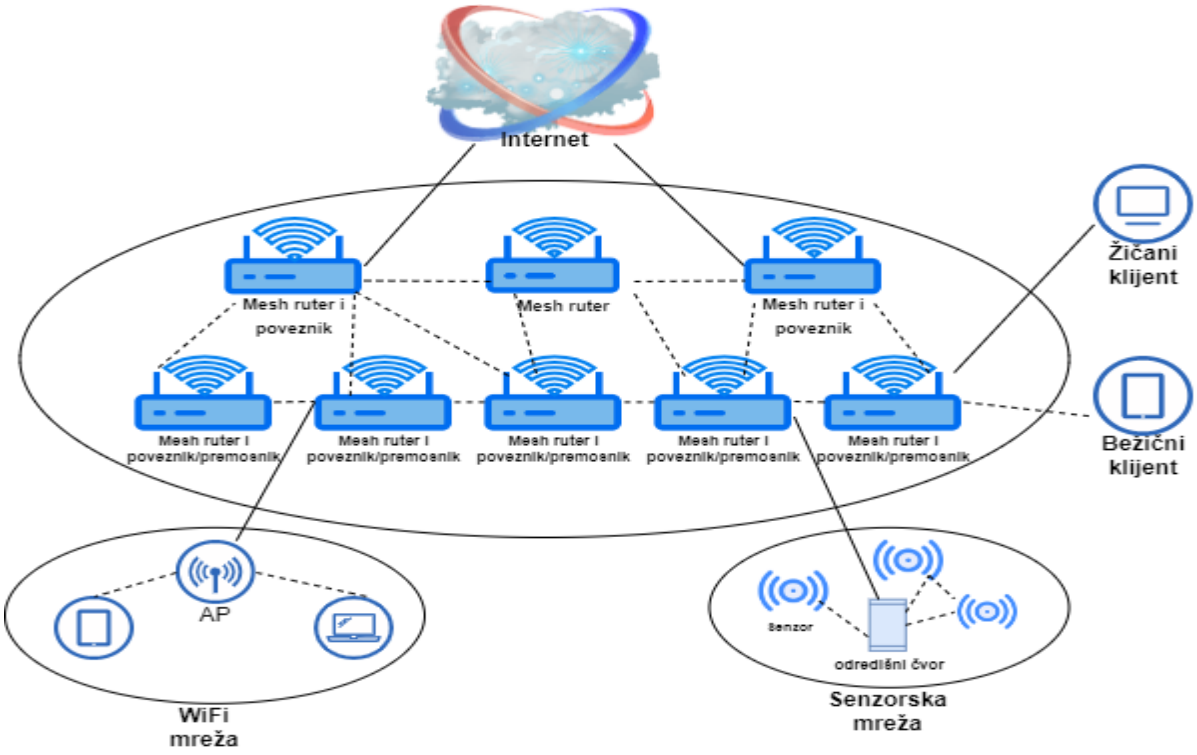
4.1 Arhitektura WiFi mesh tehnologije

WMN ne zavisi od jednog čvora, svaki čvor u mreži sudjeluje u toku podataka. Čvor usmjerava podatke do sljedećeg čvora ovisno o njegovom znanju stanja mreže. WMN je predviđena za povezivanje sa žičnim i bežičnim mrežama korištenjem poveznika. *Mesh ruteri* i *mesh* klijenti *softver-ski* i *hardver-ski* su različiti, te su sastavni dio WMN-a [20].

WiFi *mesh* nudi jednoliku pokrivenost i često ekonomičnije rješenje u prostorima gdje je strukturno kabliranje teško izvedivo ili nepraktično. Primarni *mesh ruter* spaja se s *ruterom* mrežnog operatora, zatim se sekundarni ili više njih postavlja ravnomjerno u prostoru na željenu lokaciju i spajaju se na električnu mrežu. Međusobno povezivanje *mesh rutera* i njihovo konfiguriranje odvit će se automatski. Čine okosnicu WMN-a i najznačajniji element arhitekture. Oni ne započinju niti prekidaju protok podataka već usmjeravaju podatke prema *mesh* klijentu [20].

Krajnji uređaji u WMN-u su stacionarni ili mobilni *mesh* klijenti. To uključuje prijenosna računala, pametne telefone, IoT uređaje i slične uređaje koji se povezuju na WMN bez potrebe za dodatnim modifikacijama. *Mesh* klijenti se mogu ponašati kao *ruteri* u mreži, što znači da ne koriste samo mrežu za pristup internetu ili drugim resursima, već i pomažu u usmjeravanju podataka između drugih uređaja u mreži. Ova sposobnost omogućava kreiranje klijentske WMN-a, gdje svi klijenti mogu aktivno doprinositi funkcionalnosti mreže [20].

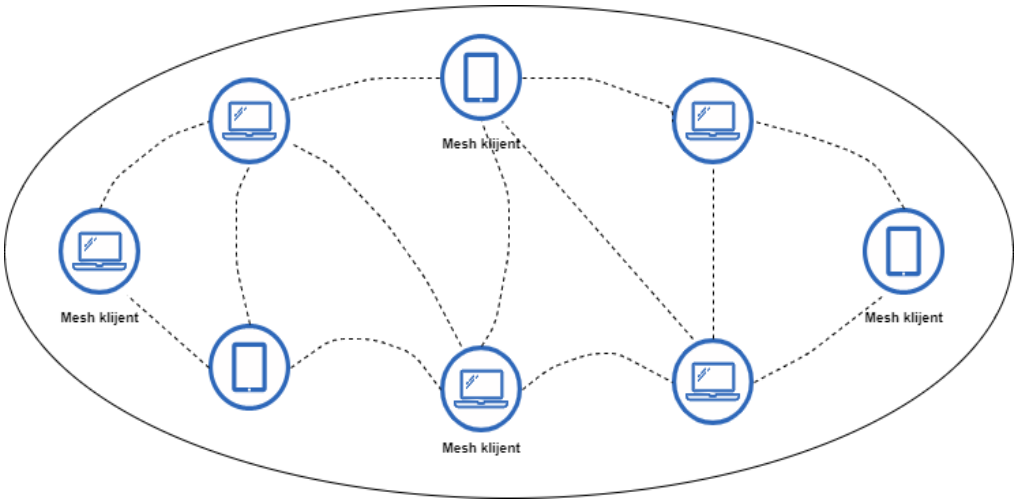
WMN-a može biti podijeljena u tri mrežne arhitekture: klijentska, infrastrukturna i hibridna (eng. *Hybrid*). Arhitektura infrastrukturnog WMN-a funkcionira tako da *mesh ruteri* čine jezgreni dio mreže koji pruža potrebnu infrastrukturu za pružanje usluga *mesh* klijentima. *Mesh ruteri* često služe kao poveznici za povezivanje različitih dijelova mreže. Direkcijske antene visoke usmjerenosti se koriste za povezivanje na velikim udaljenostima između *mesh rutera*. Jednostavna arhitektura olakšava postavljanje mreže, no mreža postane nestabilna zbog problema sa skalabilnošću i visokim zahtjevima za resursima. Komunikacija između *mesh* klijenta i *mesh rutera* uspostavlja se direktno ako koriste iste tehnologije (npr. WiFi). Indirektna komunikacija simbolizira korištenje različitih tehnologija, pri čemu se *mesh* klijent mora povezati s baznom stanicom koja je povezana s *mesh ruterom* putem *Ethernet* kabla [20].



Slika 11. Infrastrukturna arhitektura WMN-a

Izvor: [20]

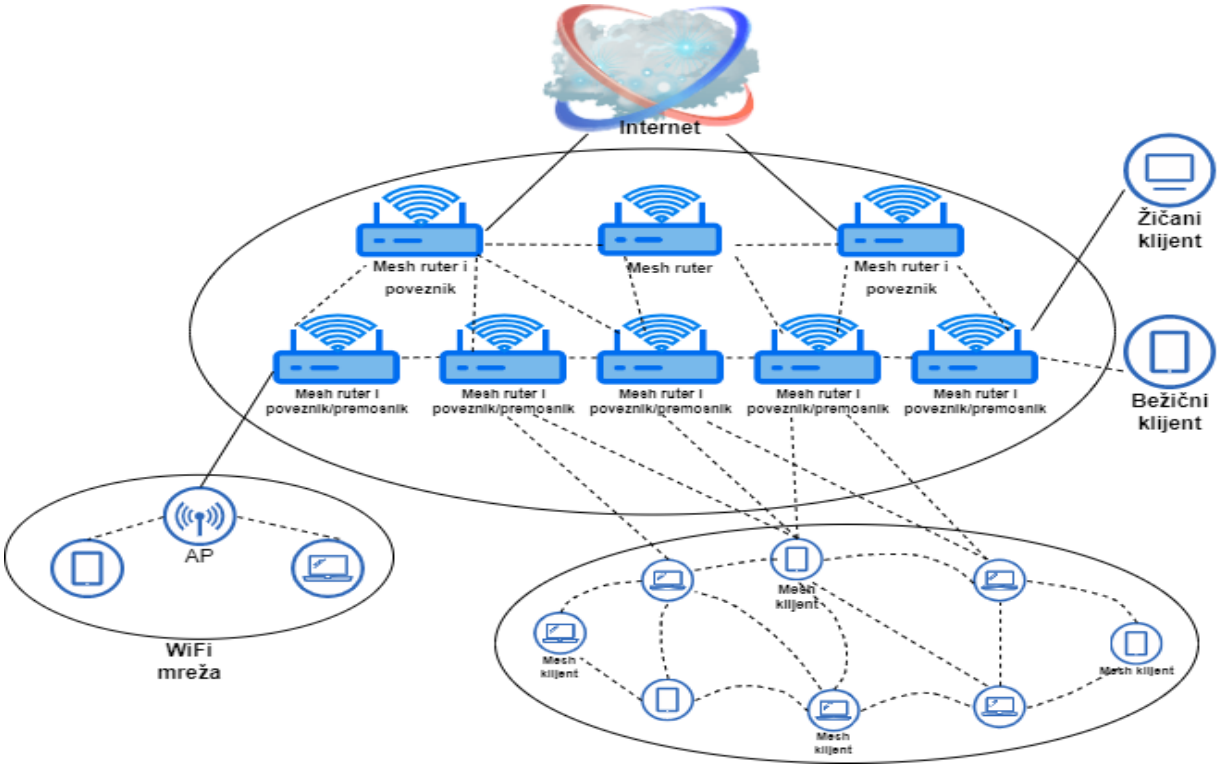
Mesh ruteri nisu potrebni za dizajniranje klijentske WMN-a. Klijentska WMN-a sliči na *ad hoc* mrežu zbog nepostojanja centralnog čvora. Koriste se *mesh* klijenti za kreiranje mreže od kojih svi rade na istoj tehnologiji za održavanje povezanosti, obavljajući funkcije usmjeravanja i samokonfiguriranja. Ravnopravna komunikacija između *mesh* klijenata nema „izlaze“ prema drugim mrežama omogućujući fleksibilnu i decentraliziranu mrežu, a mrežni promet u potpunosti ostaje lokalan. Aspekt lokalnog prometa povećava sigurnost mreže i smanjuje ovisnost o vanjskim infrastrukturama [20].



Slika 12. Klijentska arhitektura WMN-a

Izvor: [20]

Hibridna WMN kombinira elemente infrastrukturnih mreža, gdje postoje centralizirani pristupni čvorovi, i klijentskih mreža, gdje svaki čvor može direktno komunicirati s drugim čvorovima. Smatra se najboljom WMN arhitekturom, zbog toga što *mesh* klijenti mogu pristupiti različitim mrežama poput WiFi-a, WiMAX-a, mobilnih komunikacijskih sustava, bežičnih senzorskih mreža uz istovremenu mogućnost izravnog spajanja među *mesh* klijentima. Hibridna arhitektura omogućava bolje iskorištavanje dostupnih mrežnih resursa i veza, što pridonosi boljim performansama i pouzdanošću mreže. WMN koncept uvelike zavisi o povezivanju s različitim mrežama, što je jedan od razloga zbog čega hibridna arhitektura sve više dobiva na značaju [20].



Slika 13. Hibridna arhitektura WMN-a

Izvor: [20]

4.2 Implementacija WiFi mesh tehnologije u zatvorenim prostorima

Skoro svaka implementacija mreže ima novčani budžet. Buduće prednosti implementacije moraju nadmašiti njezine troškove kako bi bila isplativa. Stoga, prije same implementacije se raznim simulacijskim alatima pokušava predvidjeti način rada mreže. Potrebno je svakako voditi računa o troškovima održavanja, sigurnosti mreže, energetskoj učinkovitosti i svim drugim aspektima koje sa sobom donosi njena implementacija.

U produžetku ovog pod poglavlja obradit ćemo kućni *mesh* (eng. HomeMesh), niskobudžetni sustav bežične mreže koji koristi opće računalne sustave za pružanje povezanosti u stambenim objektima. Ovakav pristup ne obvezuje potrebu za dodatnim specijaliziranim *hardver-om*. *Mesh ruteri* koriste 2.4 i 5 GHz-ne frekvencijske pojaseve, uz jedan algoritam za dodjelu kanala i jednu metriku odabira puta koja se računa s pomoću očekivanog broja prijenosa (eng. *Expected Transmission Count* - ETX) [21].

Također, razmotrit ćemo komparativnu analizu mreže prije i poslije implementacije WiFi *mesh* tehnologije u prostorima Fakulteta računarstva, Tehničkog sveučilišta u Manabi. Važno je napomenuti da se implementacija *mesh* sustava odnosi na *softver-sku* simulaciju, koja pokazuje postoje li zaista prednosti WiFi *mesh-a*. Analiza je izvedena u simulacijskom alatu „Riverbed Modeler Academic Edition 17.5“ omogućujući grafički prikaz mjerenja. Postojeća mreža je zvijezdaste topologije te nije pokrivala fakultetske laboratorije, dvorane, administrativne prostorije i urede od profesora dostatnim WiFi signalom [22].

4.2.1 Stambeni objekti

HomeMesh sastoji se od jednog AP-a, *mesh rutera* i *mesh* klijenata. Jedan radijski modul svakog *mesh rutera* radi na principu glavnog načina rada, a drugi modul u upravljačkom načinu rada. Glavni način radijskog modula prihvaća *mesh* klijente ili druge *mesh rutere*, kod upravljačkog načina rada povezuje se s AP-om ili *drugim mesh ruterom* za pristup Internetu [21].

AP je povezan žičano i djeluje kao poveznik za klijente do Interneta. Jednostavni *mesh* protokol može biti instaliran na krajnjim uređajima kako bi i oni sudjelovali u WMN-a te time smanjili troškove implementacije i proširili pokrivenost signala. Glede perspektive AP-a, *mesh ruteri* su obični *mesh* klijenti jer koriste upravljački način rada. Paralelno tomu, *mesh* klijenti ne vide razliku među *mesh ruterima* [21].

HomeMesh koristi jednostavan i učinkovit algoritam za dodjelu kanala. HomeMesh sustav koristi dva radijska sučelja, pri čemu svako sučelje koristi različite, nepreklapajuće kanale. Na primjeru, 802.11b standarda koji ima 14 kanala (u većini država), jedan radijski modul *mesh rutera* koristio bi kanal 1, a drugi radijski modul će koristiti kanal 6 ili 11. Navedeni kanali su odabrani za nepreklapajuće kanale unutar 2.4 GHz frekvencijskog pojasa prema IEEE-u. Takva strategija dodjeljivanja kanala povećava propusnost i smanjuje interferenciju [21].

Metrika za odabir najbolje rute u WMN-u je bitan faktor. Neki *mesh* sustavi rute odabiru na temelju broja *hop-ova* do odredišta. Budući da gubitak veze i interferencije susjednih veza takvom metrikom nisu uzete u obzir, HomeMesh koristit ETX. Posebno za rute s više od 2 *hop-a* pokazala se veća efikasnost u usporedbi s metrikom minimalnog broja *hop-ova* [21].

Formula (1) računa broj prijenosa uključujući ponovni prijenos *unicast* paketa [21]:

$$\mathrm{ETX} = \frac{1}{df\ x\ dr} \tag{1}$$

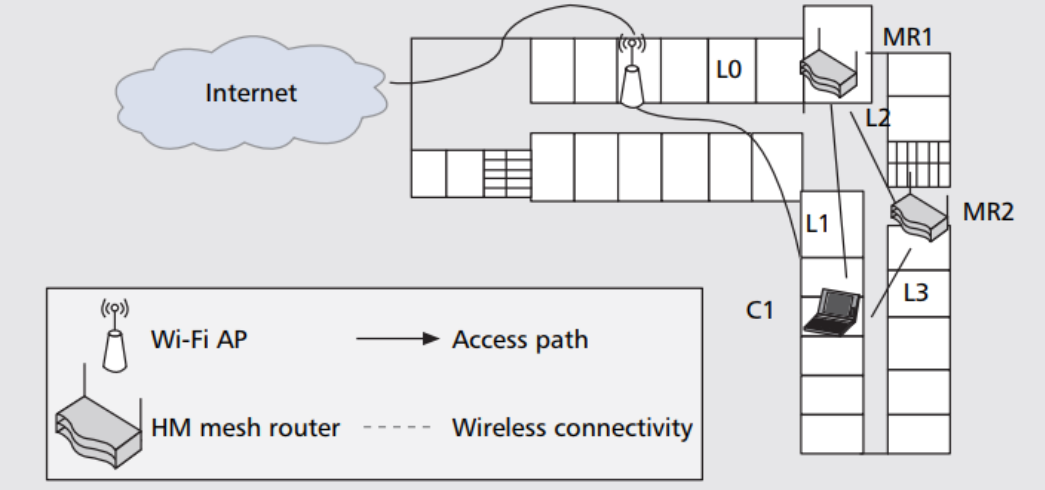
gdje u nazivniku oznake imaju sljedeće značenje:

- df - označava omjer uspješno isporučenih paketa
- dr - označava omjer uspješno potvrđenih paketa (eng. *Acknowledge packet* - ACK)

Drugim riječima, HomeMesh sumiranjem vrijednosti ETX duž cijelog puta kojim se prenose podaci odabire najbolju rutu [21].

Periodičkim slanje *broadcast* poruka *mesh ruteri* održavaju povezanost i ažuriraju svoje tablice usmjeravanja. Sadržaj poruka je sveden na minimum, a sadrži: ID susjednih *mesh rutera*, sumu ETX-a do AP-a i broj *hop-ova* do AP-a. Primajući *broadcast* poruke *mesh ruteri* dodaju u tablici podatak o valjanosti tog unosa. Primarna i zadana metrika koja se uzima u obzir pri odabiru rute je ETX vrijednost, ako je ETX dviju ruta isti odabrat će se ruta s manjim brojem *hop-ova* do AP-a [21].

Softver-ska implementacija može biti izvedena na Windows i Linux operativnim sustavima. Implementacija se vrši pokretanjem skripte HomeMesh-a na terminalnim uređajima koja automatski izvodi niz naredbi i zadataka kako bi „transformirale“ terminalni uređaj u *mesh ruter* [21].

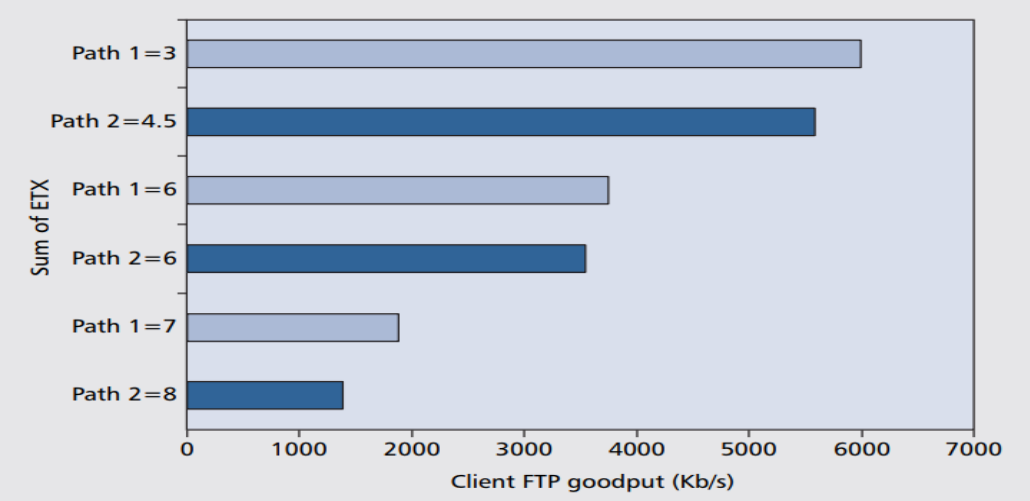


Slika 14. Topologija HomeMesh-a u zgradi fakulteta, [21]

Dokazivanje prednosti HomeMesh sustava potkrijepljeno je eksperimentom (slika 14). Eksperiment je obavljen na drugom katu u dvorani 2 poslijediplomskih studija, Sveučilišta znanosti i tehnologije u Hong Kongu koji dobro simulira zatvoreni stambeni prostor. Korisničkim prijenosnim računalom, AP-om i s *mesh ruterom* 1 (MR1) i *mesh ruterom* 2 (MR2) uspješno se proširila pokrivenost WiFi signala i dokazala teza da manja vrijednost ETX-a itekako povećava korisnu propusnost (eng. *Goodput*) [21].

Tijekom eksperimenta mijenjao se razmak (L1, L2, L3) između terminalnih uređaja s razlogom, jer su se time dobivale drugačije vrijednosti ETX-a. Klijent C1 koristi protokol za premještanje datoteka (eng. *File Transfer Protocol* - FTP) s pomoću kojeg će skinuti

datoteku veličine 10 MB s FTP *server-a*. Do AP-a klijent C1 ima dvije rute. Ruta 1, AP → MR1 → C1, i ruta 2, AP → MR1 → MR2 → C1.



Graf 1. Propusnost klijentskog FTP-a, [21]

Grafom 1. prikazan je odnos sume ETX-a i korisne propusnosti za rutu 1 i 2, s različitim vrijednostima ETX-a. Upotrebljavajući istu brzinu prijenosa ruta 1 s ETX vrijednosti 3 ima veću korisnu propusnost, nego ruta 2 s ETX vrijednosti 4.5. Jer ruta 1 ima manju vrijednost ETX-a i manji broj *hop-ova* do AP-a. Povećani broj izgubljenih paketa često nagovještava smanjenje brzina prijenosa. Na primjer, ako bi na ruti 1 ETX vrijednost bila 6, ruta 2 s ETX vrijednosti 4.5 bila bi bolji izbor iako ima veći broj *hop-ova* [21].

Dakako, ruta 1 i 2 s istim ETX-om ne postižu istu korisnu propusnost. Ruta 1 pokazuje veću korisnu propusnost, zato što ima 2 *hop-a* do AP-a u odnosu na rutu 2 kojoj treba 3 *hop-a* [21].

4.2.2 Sveučilišni prostori

Spomenuta zvijezdasta topologija u sveučilišnom prostoru rabi jednomodni optički kabel čije su brzine prijenosa do 1 Gbit/s. Optički kabel povezuje 11 *server-a* podatkovnog centra fakulteta. Bežična mreža postignuta je postavljanjem 18 AP-ova u zvijezdastoj topologiji. Na prvom katu zgrade fakulteta postavljeno je 8, na drugom katu 6 i na trećem katu zgrade 4 AP-a. Manjkavosti bežične mreže uz poprilično optimalnu raspoređenost AP-ova je ograničenje spojenih korisnika, njih 20 na jedan AP [22].

Simulacijom *mesh* sustava, *mesh ruteri* su razmaknuti na svakom katu i u dvorištu na 100 m (slika 15). U pogledu fizičkog i logičkog dizajna, *mesh* sustav smanjio bi broj elemenata bežične mreže u sveučilišnom prostoru, postavilo bi se 8 *mesh rutera* sljedećim rasporedom [22]:

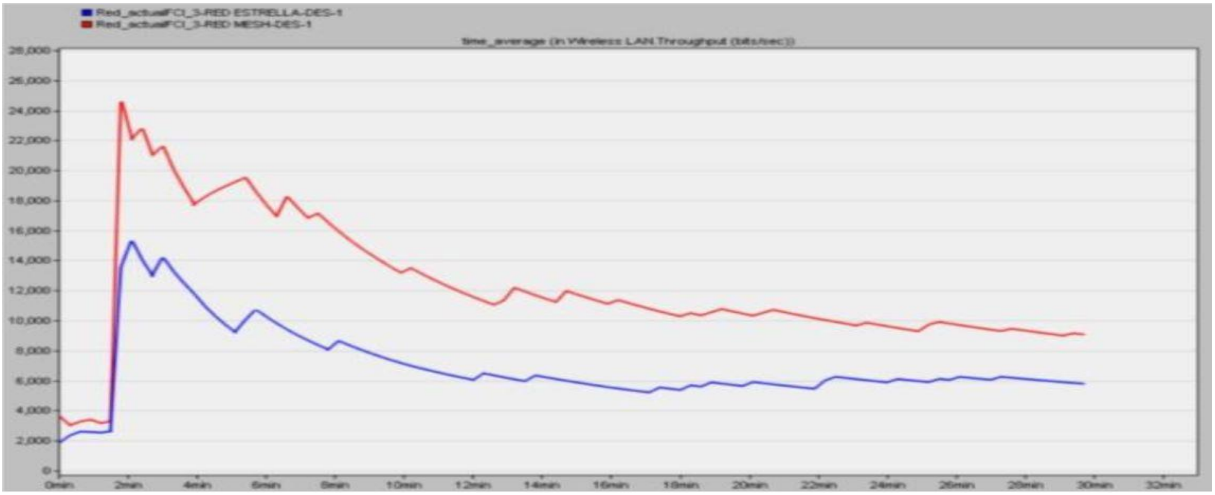
- *Mesh ruteri* A i B na trećem katu
- *Mesh ruteri* C i D na drugom katu

• *Mesh ruteri* E i F na prvom katu
• *Mesh ruteri* G i H u dvorištu

Slika 15. Prikaz budućeg postavljanja mesh sustava, [22]

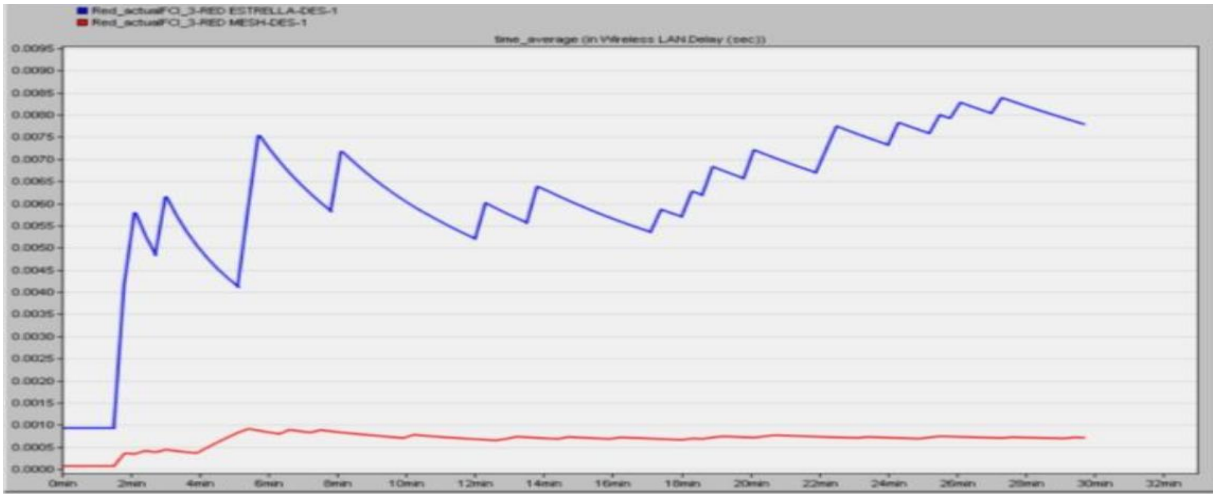
Simulacijskim alatom neophodno je na odgovarajući način konfigurirati niz parametara za *mesh rutere*, poveznika, *server-e*, aplikacijski modul i profile, kako bi se dobili rezultati visoke točnosti. Ujedno će se pretpostaviti da se krajnji korisnici spajaju na WMN osobnim računalom. Parametre koje će simulacijski alat usporediti s trenutnom mrežom su propusnost, kašnjenje, brzina poslanih paketa i brzina primljenih potvrdnih paketa [22].

Crvena linija na grafovima prikazuje ponašanje WMN-a, a plava linija trenutnu mrežu. Graf 2. uspoređuje propusnost dviju mreža u bitovima po sekundi (bit/s) kroz vrijeme (min). Na početku oko 2 minute, obje mreže pokazuju nagli porast propusnosti. WMN-a doseže maksimalnu vrijednost oko 24000 bit/s, dok trenutna mreža doseže oko 15000 bit/s. Sredinom mjerenja obje propusnosti su se stabilizirale i tako ostale do kraja mjerenja, no WMN zadržava veću propusnost [22].



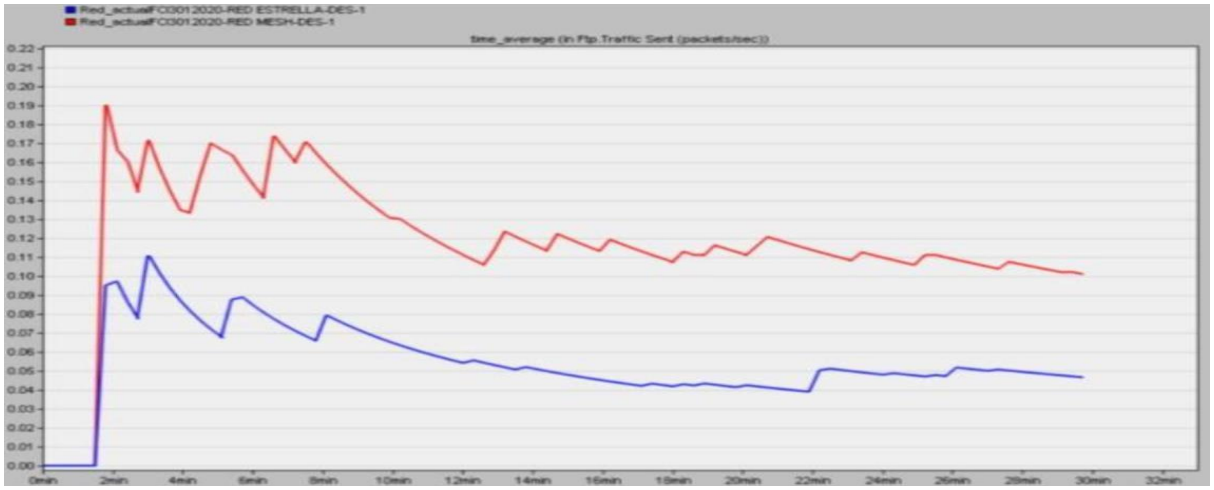
Graf 2. Usporedba propusnosti dviju mreža, [22]

Komparacija kašnjenja je vidljiva grafom 3. Trenutna mreža (plava linija) sveučilišta dominira, ali u negativnom smislu. Ostvarujući kašnjenje od 0.0084 ms, što je skoro 10 puta veće kašnjenje od WMN-a koja ostvaruje kašnjenje od 0.0007 ms. Također, graf ukazuje kako kašnjenje WMN-a je gotovo konstantno tijekom cijelog mjerenja, a kašnjenje trenutne mreže se čak povećava s vremenom [22].



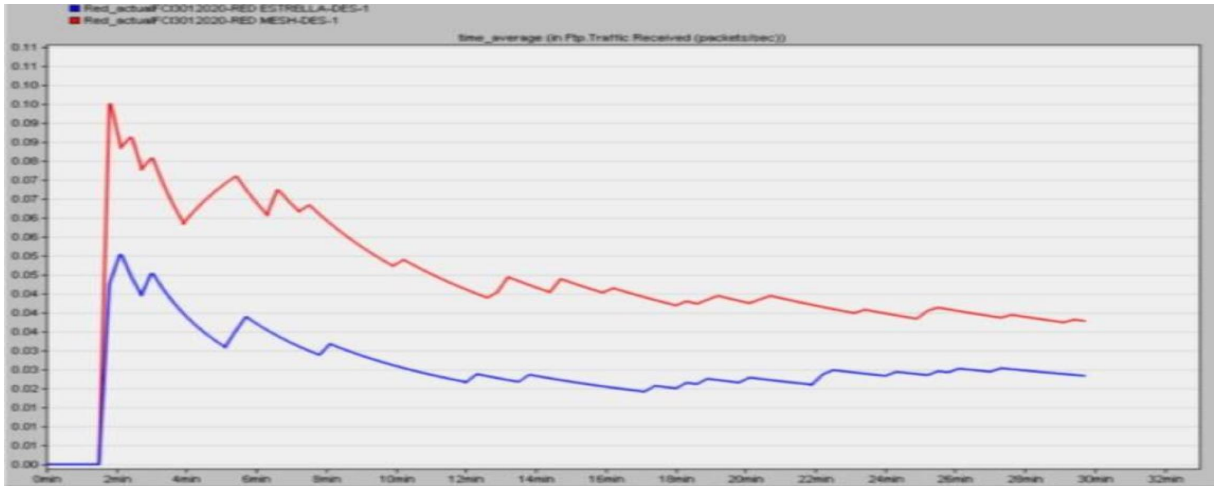
Graf 3. Usporedba kašnjenja dviju mreža, [22]

Maksimalna brzina slanja paketa u WMN-a iznosi oko 0.19 paket/sekunda (graf 4). U usporedbi s trenutnom mrežom čiji maksimum je oko 0.11 paket/sekunda, učinkovitija je u prijenosu paketa. Nedvojbeno, crvena linija ima više fluktuacija, ali zadržava veću brzinu slanja paketa od plave linije tijekom cijelog perioda [22].



Graf 4. Usporedba brzine slanja paketa dviju mreža, [22]

Zadnji parametar usporedbe dviju mreža u simulacijskom *softver-u* je brzina primanja potvrdnih paketa. Dakle, izmjereno je 0.10 paketa/sekundi za WMN što je duplo više od trenutnih mogućnosti mreže koja pokazuje brzinu prijema potvrdnih paketa od 0,05 paketa/sekundi (graf 5). Ubrzo se međusobna razlika dviju mreža počela smanjivati [22].



Graf 5. Usporedba potvrdnih paketa dviju mreža, [22]

Usporedbom parametara mreža, može se zaključiti da WMN-a i trenutna mreža sveučilišta zvijezdaste topologije nisu niti približno istih performansi. Parametar koji se najmanje razlikovao među mrežama je propusnost, a najveća razlika se pokazala s kašnjenjem. Komparativnom analizom dokazale su se prednosti *mesh* sustava i njegove potencijalne implementacije u sveučilišnim prostorima. Svakako, *mesh* sustav smanjuje potrebnu redundantnost uređaja, uz povećanje značajnih parametara mreže [22].

5. SIGURNOSNI ASPEKTI WIFI MESH TEHNOLOGIJE

Inženjeri razvojem novih tehnologija žele nadomjestiti nedostatke postojećih tehnologija ili kreirati potpuni novi pristup određenim problemima. Složene tehnologije dodatno se zakompliciraju integriranjem sigurnosnih zaštita. Digitalizacijom su osjetljive informacije i novčana sredstva postali glavna meta unutarnjih i vanjskih zlonamjernih napada.

Vanjske napade generiraju neovlašteni korisnici koji su izvan mreže organizacije, radi prisluškivanja mrežnog prometa i pristupa mrežnim resursima. Unutarnje napade pokreću korisnici mreže koji imaju valjanu autorizaciju za pristup mrežnim uslugama. Korištenjem raznih metoda, poput socijalnog inženjeringa legitimnim alatima izvode svoje napade čime ih je teže detektirati i adekvatno se zaštiti [24].

Osnova WMN-a je *multi-hop* slanje paketa, velikim brojem intermedijarnih čvorova, mreža se dodatno izlaže sigurnosnim rizicima. Napadač ima više čvorova na raspolaganju za presretanje paketa, što povećava mogućnosti za napade poput prisluškivanja, promjene podataka i distribucije zlonamjernog koda. Uspješno izvedeni napadi uzrokuju degradiranje rada mreže i prekid usluga. Pored toga, moguće je da *mesh ruteri* obave sveobuhvatnu analizu mrežnog prometa za optimizaciju performansi i otkrivanje problema. Ako ove funkcije padnu u ruke napadača ili neovlaštenih osoba, može doći do ugrožavanja privatnost korisnika [24].

5.1 Sigurnosne prijetnje i zaštite u mrežnim slojevima OSI modela

OSI model tumači komunikacijske procese u 7 slojeva [24]:

- Aplikacijski
- Prezentacijski
- Sesijski
- Transportni
- Mrežni
- Podatkovni
- Fizički

Počevši uzlazno po OSI modelu prva tri (donja) sloja nazivaju se mrežni slojevi, dok sljedeća četiri (gornja) sloja nazivaju se aplikacijski slojevi. Svaki sloj ovisi o slojevima ispod sebe i pruža podršku slojevima iznad sebe. Osigurava standardizaciju mrežnih komponenti, odvajanjem u slojeve pojednostavljuje se razumijevanje umrežavanja i odnosa između *hardver-a* i *softver-a*.

WMN je izložena različitim sigurnosnim prijetnjama na svim slojevima OSI modela. Svaki sloj ima svoje specifične ranjivosti koje napadači iskorištavaju za različite vrste napada. Shodno tome, potrebna je čvrsta zaštita mrežnih slojeva koji su temelj za aplikacijske slojeve i funkcioniranje mreže. Jer bilo kakva ranjivost na nižim slojevima može ugroziti aplikacijske slojeve i njihove usluge [24].

5.1.1 Fizički sloj

Žično povezivanje hibridne WMN-a može sadržavati mnogo elemenata uključujući povezivanje različitih mreža. Stručnjaci definiraju potrebnu udaljenost između uređaja, specifikacije prijenosnog medija, konektore i ostale atribute fizičkog sloja. Fizički sloj zadužen je za pretvaranje signala u binarnu vrijednost te njihov prijenos do krajnjeg sustava [24].

WMN-a je bežična mreža, prijenosi mediji je zrak koji je podložan napadima ometanja (eng. *Jamming attack*). Tijekom napada ometanja, zlonamjerni akteri ometaju radiofrekvencije koje čvorovi WMN-a koriste za međusobnu komunikaciju. Potreban pribor za izvođenje napada nije sofisticiran, što implicira njihovu jednostavnost izvođenja [24].

Napadač mora biti u relativnoj blizini mreže te emitirati jak signal koristeći bežični NIC spojen na antenu s visokim pojačanjem. Emitiranjem signala na istim frekvencijama koje koristi WMN-a zauzima se dio propusnosti čime se može srušiti cijela mreža. Povremeno emitiranje jakog signala također se može pokazati štetnim za komunikacije u WMN-u koje su vremenski osjetljive (npr. VoIP). Napadi ometanja još su složeniji za otkrivanje ako napadački NIC ne poštuje CSMA protokol, što ih čini težim za detekciju. Osim toga, napadači mogu koristiti lažne MAC adrese kako bi dodatno otežali identifikaciju izvora napada [24].

Postoji zaštita od napada ometanja u fizičkom sloju korištenjem tehnologija prijenosa u proširenom spektru. Informacija se raspoređuje po većem frekvencijskom području nego što je potrebno za prijenos, povećavajući otpornost na smetnje [24].

Jedna od takvih tehnologija je FHSS, koja konstantno mijenja frekvencijski kanal na kojem se signal prenosi. Zbog toga su male šanse da će dva uređaja biti na istom frekvencijskom kanalu u isto vrijeme. Primjenjujući pseudo-slučajni kod poznat pošiljatelju i primatelju [24].

Druga tehnologija je direktnim proširenjem spektra signala (eng. *Direct sequence spread spectrum* - DSSS) gdje se svi bitovi izvornog signala proširuju dodatnim bitovima prilikom prijenosa signala. Dodatni bitovi se generiraju s pomoću širenja koda (eng. *Spreading code*), koji je specifičan niz bitova. Primatelj signala koristi isti pseudo-slučajni kod za dekodiranje i vraćanje signala u izvorni oblik [24].

Implementacijom ovakvih tehnologija napadaču je skoro nemoguće saznati trenutno korišten frekvencijski pojas, kod za širenje i modulacijske tehnike, kako bi omeo rad

WMN-a. Napadač bi mora ometati širok raspon frekvencija istovremeno kako bi učinkovito prekinuo komunikaciju, što je tehnički zahtjevno i neefikasno [24].

5.1.2 Podatkovni sloj

Napad ponovnog reproduciranja (eng. *Replay attack*) izvedljiv je kao unutarnji i vanjski napad. Zlonamjerni čvor treba se nalaziti između dva čvora koji komuniciraju kako bi neovlašteno pohranio osjetljive informacije. Pohranjene informacije napadaču moraju biti u čitljivom formatu za razumijevanje, a ne u heksadecimalnom ili sličnom formatu, koji predstavlja sigurnosno zaštićene podatke. Informacije koje je napadač presreo šalje jednom od čvorova prethodne komunikacije radi dobivanja pristupa mrežnim resursima. Primanjem istih informacija od napadača, čvor u mreži biva prevaren misleći da je zlonamjerni čvor legitiman čvor s kojim je vodio komunikaciju. Napad se često zove napadom čovjeka u sredini (eng. *Man-in-the-middle attack*), jer napadač presreće komunikaciju između dva entiteta i može steći neovlašteni pristup resursima [24].

Podatkovni sloj dodaje zaglavlja i bavi se fizičkim adresiranjem (MAC adrese), kontrolom protoka, pitanjem mrežnih topologija i osigurava da se podaci sigurno prijenose preko poveznice. Jedinstvena MAC adresa u LAN mrežama dugo se koristi za provjere autentičnosti ili kao jedinstveni identifikator za dodjelu različitih razina pristupa u mreži [24].

Modificiranje MAC adrese terminalnog uređaja naziva se MAC zavaravanje (eng. MAC *spoofing*). Koristi se za izbjegavanje detekcijskih sustava mreže, također za zavaravanje kontrole pristupa mreže koristeći istu MAC adresu legitimnog uređaja. Neovlašteni upad u mrežu napadač može iskoristiti za distribuiranje nepotrebnog prometa u mrežu s ciljem narušavanja mrežnih resursa, što može dovesti do smanjenja performansi i nedostupnosti mreže [24].

Verifikacijskim testom moguće je provjeriti ispravnost MAC adrese terminalnog uređaja. Algoritam provjere integriteta neće dopustiti procesuiranje poruke ako je poruka izmijenjena s lažnom MAC adresom. Dakle, pošiljatelj u poruci integrira i izračun funkcije sažetka (eng. *hash function*). Izračunati sažetak je uvijek predefinirane duljine bez obzira na ulazne vrijednosti kao što su MAC adresa, IP adresa, sadržaj poruke i slično. Primatelj dobivenoj poruci izračunava sažetak koristeći isti algoritam, kako bi provjerio integritet poruke. Ako se sažetak ne podudara, primatelj poruku odbacuje s dodatnom reakcijom slanja upozorenja pošiljatelju, blokiranja pošiljatelja ili druge radnje ovisno o konfiguraciji mreže [24].

Kriptografija je znanstvena disciplina koja se odavno bavi omogućavanjem pouzdane i sigurne komunikacije između dva entiteta uz zadržavanje tajnosti razmijenjenih poruka, čak i u slučajima kada su poruke presretnute. WMN korištenjem autentifikacije i provjere integriteta svakog paketa učinkovito se može zaštiti od napada ponovnog reproduciranja [24].

Zaštite se temelje na kriptografskom ključu koji se računa prije slanja poruke. Svaki paket se šifrira i autentificira s jedinstvenim ključem koji se sinkronizirano generira između pošiljatelja i primatelja. Simetričnim kriptografskim sustavom, napadačev pokušaj ponovnog reproduciranja bit će neuspješan, jer ključ paketa je zastarjeo odnosno već se koristio. Korištenje kriptografskog ključa za svaki paket ne samo da se štiti od napada ponovnog reproduciranja, već i od drugih napada kao što su napadi korištenjem duginih tablica (eng. *Rainbow table*) i djelomičnog podudaranja (eng. *Partial matching*) [24].

5.1.3 Mrežni sloj

Logičko adresiranje, odabir puta između dva računalna sustava, enkapsulacija i dekapsulacija paketa samo su neke od funkcija mrežnog sloja. On se smatra najvažnijim slojem među prva tri sloja OSI modela. Mrežni uređaj *ruter* radi na mrežnom sloju, dok moderniji *ruteri* mogu obavljati i funkcije prospojnika na podatkovnom sloju [24].

Kibernetički napadi u mrežnom sloju spadaju u dvije vrste: napadi kontrolnih paketa i napadi podatkovnih paketa. Oba napada mogu biti obavljena pasivno i aktivno. Napadi kontrolnih paketa ciljaju narušiti glavnu funkciju mrežnog sloja što je usmjeravanje paketa. Osnovni motiv je „natjerati“ mrežu da odabere rutu koja nije najbolja i onu koja sadrži zlonamjerne čvorove ili napraviti sve rute nedostupnim. Napadi podatkovnih paketa spriječavaju prosljeđivanje paketa u mreži. Isto tako napadači šire maliciozni kod u mreži, stvarajući usluge nedostupnima za korisnike mreže [24].

Protokoli usmjeravanja koje karakterizira slanje poruka na zahtjeve susjednim čvorovima u mreži na udaru su ubrzanih napada (eng. *Rushing attacks*). Naime, napadi kontrolnih paketa iskorištavaju mehanizam odabira puta protokola usmjeravanja. Za odabir puta do odredišta čvor šalje poruku zahtjeva rute (eng. *Route Request* - RREQ) svim čvorovima, poruka je identificirana sekvencijskim brojem. Ako čvor koji primi poruku nije odredište on će ju proslijediti susjednim čvorovima do pronalaska odredišnog čvora. Radi izbjegavanja preplavljivanja (eng. *Flooding*) mreže, čvorovi prosljeđuju samo prvu RREQ poruku, odbacujući sve naknadne poruke s istim sekvencijskim brojem. Postavlja se kašnjenje između primanja RREQ poruke i njezinog prosljeđivanja, zbog sprječavanja kolizije. Ignorirajući kašnjenje, maliciozni čvor u mreži odmah prosljeđuje primljenu RREQ poruku, te time postaje prvi čvor kojega ostali čvorovi u mreži vide kao pošiljatelja poruke. Postizanjem navedenoga, maliciozni čvor uključen je u komunikaciju između izvora i odredišta, s mogućnostima ispuštanja paketa, iscrpljivanjem mrežnih resursa i ostalih zlonamjernih radnji [24].

U mrežnom sloju postoje razni mehanizmi, protokoli, tehnike koji se koriste za zaštitu od sigurnosnih prijetnji. WMN primjenjuje mehanizam prevencije od ubrzanih napada (eng. *Rushing Attack Prevention* - RAP). Korištenjem RAP-a čvorovi ne prosljeđuju prvu primljenu RREQ poruku, nego čekaju određeno vrijeme kako bi primili par RREQ

poruka od različitih čvorova. Nakon isteka definiranog vremena, čvor nasumično odabire jednu RREQ koju prosljeđuje susjednim čvorovima u mreži. RAP prevenira ubrzani napad distribuiranim prosljeđivanjem RREQ poruka povećavajući pouzdanost rute i otpornost mreže [24].

6. ZAKLJUČAK

Krajnjim korisnicima primamljive su bežične mreže zbog nepostojanja kabela, mobilnosti, skalabilnosti i jednostavnosti umrežavanja s mobilnim terminalnim uređajima. Razvojem poboljšanih antenskih sustava i modulacijskih tehnika sofisticirani mrežni uređaji bežičnih mreža izvršavaju mnogobrojne kompleksne funkcije, koje su nekada mogli samo elementi žične arhitekture.

Tehničke specifikacije bežičnih tehnologija nastavit će kontinuirano napredovati, uz primjenu u različitim i potencijalno drugačijim scenarijima od onih koje danas poznajemo. Ujedno se tehnologije međusobno integriraju, maksimizirajući performanse i pružajući laku razmjenu informacija i povezanost među različitim uređajima. Tehnološki napredak vidljiv je u svakodnevnom životu, a njegov utjecaj osjetit će se i u industrijama poput medicine, prometa, poljoprivrede i tako dalje.

Sve tri arhitekture bežične mesh mreže imaju svoje prednosti ovisno o upotrebi, ipak izdvaja se hibridna arhitektura. Kombiniranjem klijentske i infrastrukturne arhitekture iskorištavaju se njihove prednosti različitih tehnologija čime se postiže veća fleksibilnost, pouzdanost i pokrivenost mreže. Analizom eksperimenta implementacije kućnog mesh sustava, uočili su se pozitivni učinci za stambene prostore, koji dokazuju bitnost metrika odabira rute i pozicioniranja rutera. Drugom implementacijom u sveučilišnom prostoru simulacijskim softver-om utvrđuju se smanjenje kašnjenja, veća propusnost, veća brzina slanja paketa i primanja potvrdnih paketa.

Glavni nedostatak bežičnih mesh mreža je pitanje sigurnosti. Upravo zbog velikog broja intermedijarnih čvorova zahtjevnije je zaštititi mrežu od kibernetičkih napada. U hibridnoj arhitekturi to posebno dolazi do izražaja, stoga je potrebno uložiti u sigurnost i zaštiti takve mreže. Osiguravajući zaštićenost mrežnih slojeva mreže gradi se temelj za naredne slojeve i njihovu pouzdanost. Budući da su kibernetički napadi u porastu, zaštiti mrežu od sigurnosnih prijetnji bit će najveći izazov budućnosti.

LITERATURA

1. Shukla S, Meghana KM, Manjunath CR, Shantosh N. *Comparison of Wireless Network over Wired Network and Its Type*. International Journal of Research Granthaalayah. 2017.;5:14-20.
2. Periša, M.: Autorizirani nastavni materijali (objavljeno na Merlinu), Arhitektura telekomunikacijske mreže, Fakultet prometnih znanosti, Zagreb, 2023. [Pristupljeno: 5. lipnja 2024.]
3. Geier J. Wireless Networks First-Step. 2004.
4. Electronics Projects Focus. *What is Network Interface Card – Types, Working & Its Components.* Preuzeto s: https://www.elprocus.com/network-interface-card-nic/ [Pristupljeno 20. lipnja 2024.]
5. Solwise. *Managed Wireless Solutions.* Preuzeto s: https://www.solwise.co.uk/controller-managed-solutions.htm [Pristupljeno 20. lipnja 2024.]
6. Sopto. *Optical Fiber and Optical Fiber Classification.* Preuzeto s: https://www.sopto.com.cn/sp_news/show-368.html [Pristupljeno 20. lipnja 2024.]
7. Tanenbaum AS. *Computer Networks.* 2003.
8. Geeks For Geeks. *Difference between Unicast, Broadcast and Multicast in Computer Network.* Preuzeto s: https://www.geeksforgeeks.org/difference-between-unicast-broadcast-and-multicast-in-computer-network/ [Pristupljeno 20. lipnja 2024.]
9. Geeks For Geeks. *Difference between WAN and WWAN.* Preuzeto s: https://www.geeksforgeeks.org/difference-between-wan-and-wwan/ [Pristupljeno 20. lipnja 2024.]
10. Bhattacharya P, Shabbeer Basha KH, Ajmani P, Kannan KR. *Advanced Wireless and Mobile Networks.* 2023.
11. Patil P, Patil MR, Itraj S, Bomble UL. *A review on MIMO OFDM technology basics and more.* 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). IEEE; 2017. str. 119-124.

12. Fan S, Ge Y, Yu X. *Comparison analysis and prediction of modern wi-fi standards.* 2022 International Conference on Big Data, Information and Computer Network (BDICN). IEEE; 2022. str. 581-585.
13. Astound. *What is WiFi 7? (The latest WiFi standard).* Preuzeto s: https://www.astound.com/learn/internet/wifi-7/ [Pristupljeno 20. lipnja 2024.]
14. Moko smart. *A Comprehensive Guide on Different Bluetooth Versions.* Preuzeto s: https://www.mokosmart.com/guide-on-different-bluetooth-versions/ [Pristupljeno 20. srpnja 2024.]
15. Zaidi SAJ. *Basic Study of Bluetooth Networking Topologies.* Onyx Journal of Business and Social Sciences. 2016.;4:2-5.
16. Digi. *What Is Zigbee?* Preuzeto s: https://www.digi.com/solutions/by-technology/zigbee-wireless-standard#advantages-zigbee-3-0 [Pristupljeno 20. srpnja 2024.]
17. Garg V. *Wireless communications and networking.* 2010.
18. Hopjan M. *Mesh Network Application*. International Conference on Military Technologies (ICMT). 2021.;1-4.
19. Yang K, Ma J, Miao Z. *Hybrid Routing Protocol for Wireless Mesh Network*. International Conference on Computational Intelligence and Security. 2009.; 547-551.
20. Shahdad SY, Sabahath A, Parveez R. *Architecture, issues and challenges of wireless mesh network.* 2016 International Conference on Communication and Signal Processing (ICCSP). IEEE; 2016. str. 557-560.
21. He T, Chan HG, Wong F. *HomeMesh: a low-cost indoor wireless mesh for home networking*. IEEE Communications Magazine, 2008.; 46,79-85.
22. Sánchez-Pinargote R, Rodríguez Véliz MJ, Cedeño-Palma E. *MESH Networks to Optimize the Quality of Internet Service via WiFi in University Institutions*. XV Multidisciplinary International Congress on Science and Technology. 2021.;255-267.
23. Sen, J. *Security and privacy issues in wireless mesh networks: A survey.* Wireless networks and security: issues, challenges and research trends. 2013.;189-272.

POPIS KRATICA

ACK	(Acknowledge Packet) primljeni paket
AP	(Access Point) pristupna točka
BLE	(Bluetooth Low Energy) niskoenergetski Bluetooth
CSMA	(Carrier Sense Multiple Access) višestruki pristup s osjetilom nositelja
DSSS	(Direct sequence spread spectrum) direktno proširenje spektra signala
ETX	(Expected Transmission Count) očekivani broja prijenosa
FFD	(Full Function Device) uređaj pune funkcije
FHSS	(Frequency hopping spread spectrum) skokovita promjena nosive frekvencije
FTP	(File Transfer Protocol) protokol za premještanje datoteka
HWMP	(Hybrid Wireless Mesh Protocol) hibridni bežični mesh protokol
ID	(Identifier) identifikator
IEEE	(Institute of Electrical and Electronics Engineers) Institut inženjera elektrotehnike i elektronike
IoT	(Internet of Things) Internet stvari
IP	(Internet Protocol) Internetski protokol
LAN	(Local Area Network) lokalna računalna mreža
LOS	(Line of Sight) linija vidljivost
MAC	(Media Access Control) kontrola pristupa mediju
MAN	(Metropolitan Area Network) metropolitanska računalna mreža
MIMO	(Multiple-Input and Multiple-Output) višestruki ulaz i višestruki izlaz

MR1	mesh ruter 1
MR2	mesh ruter 2
NIC	(Network Interface Card) mrežna kartica
OFDM	(Orthogonal Frequency-Division Multiplexing) frekvencijskom multipleksu ortogonalnih podnosilaca
OSI	(Open Systems Interconnection) međusobno povezivanje otvorenih sustava
PAN	(Personal Area Network) osobna računalna mreža
PANC	(Personal Area Network Coordinator) koordinator osobne mreže
PIN	(Personal Identification Number) osobni identifikacijski broj
RAP	(Rushing Attack Prevention) prevencije od ubrzanih napada
RFID	(Radio Frequency Identification) radiofrekventna identifikacija
RFD	(Reduced Function Device) uređaj smanjene funkcije
RREQ	(Route Request) zahtjev za rutu
SISO	(Single Input Single Output) jednostruki ulaz i jednostruki izlaz
SQL	(Structured Query Language) strukturirani jezik za upite
STP	(Shielded Twisted Pair) zaštićene uparene parice
USB	(Universal Serial Bus) univerzalna serijska sabirnica
UTP	(Unshielded Twisted Pair) nezaštićene uparene parice
VLAN	(Virtual Local Area Network) virtualna lokalna mreža
VoIP	(Voice over Internet Protocol) govor preko internetskog protokola
VPN	(Virtual Private Network) virtualna privatna mreža

WAN	(Wide Area Network) mreža širokog područja
WiMAX	(Worldwide Interoperability for Microwave Access) svjetska interoperabilnost za mikrovalni pristup
WLAN	(Wireless Local Area Network) bežična lokalna mreža
WMAN	(Wireless Metropolitan Area Network) bežična metropolitanska računalna mreža
WMN	(Wireless Mesh Network) bežična mesh mreža
WPAN	(Wireless Personal Area Network) bežična osobna mreža
WWAN	(Wireless Wide Area Network) bežična širokopojasna mreža

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad (*vrsta rada*) isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da 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/diplomskog rada pod naslovom Analiza karakteristika bežičnih mreža i WiFi mesh tehnologije u zatvorenim prostorima, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 6. rujan 2024.

Marko Vrdoljak, Marko Vrdoljak
(ime i prezime, *potpis*)