Protokoli pametnih telefona

Smojver, Domagoj

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet elektrotehnike, računarstva i internetskih tehnologija Osijek

Preddiplomski stručni studij Računarstva

PROTOKOLI PAMETNIH TELEFONA

Završni rad

Domagoj Smojver

Osijek, 2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1S: Obrazac za ocjenu završnog rada na stručnom prijediplomskom studiju

Ocjena završnog rada na stručnom prijediplomskom studiju

Ime i prezime pristupnika:	Domagoj Smojver
Studij, smjer:	Stručni prijediplomski studij Računarstvo
Mat. br. pristupnika, god.	AR 4818, 27.07.2020.
JMBAG:	0165085260
Mentor:	mr. sc. Anđelko Lišnjić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	prof. dr. sc. Krešimir Grgić
Član Povjerenstva 1:	mr. sc. Anđelko Lišnjić
Član Povjerenstva 2:	dr. sc. Jelena Šuljug
Naslov završnog rada:	Protokoli pametnih telefona
Znanstvena grana završnog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rada:	Komuniciranje putem mobilnih uređaja već je odavno postalo ljudska navika i potreba. Bez mobilnih komunikacija teško je i zamisliti naš život. Interakcije mobilnih uređaja-ljudi su svakodnevne i dugoročne. Jedan od rezultata te interakcije se očituje u implementiranju sve više komunikacijskih protokola u mobilnim uređajima. Zadatak rada je opisati najvažnije komunikacijske protokole pametnih telefona (primjerice: Bluetooth, Wi-Fi, itd.) njihovu funkciju i gdje se koriste te kronologiji nastanka protokola.
Datum ocjene pismenog dijela završnog rada od strane mentora:	19.09.2024.
Ocjena pismenog dijela završnog rada od strane mentora:	Vrlo dobar (4)
Datum obrane završnog rada:	26.09.2024.
Ocjena usmenog dijela završnog rada (obrane):	Izvrstan (5)
Ukupna ocjena završnog rada:	Izvrstan (5)
Datum potvrde mentora o predaji konačne verzije završnog rada čime je pristupnik završio stručni prijediplomski studij:	26.09.2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O IZVORNOSTI RADA

Osijek, 26.09.2024.

Ime i prezime Pristupnika:	Domagoj Smojver
Studij:	Stručni prijediplomski studij Računarstvo
Mat. br. Pristupnika, godina upisa:	AR 4818, 27.07.2020.
Turnitin podudaranje [%]:	8

Ovom izjavom izjavljujem da je rad pod nazivom**: Protokoli pametnih telefona**

izrađen pod vodstvom mentora mr. sc. Anđelko Lišnjić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis pristupnika:

Sadržaj

1. UVOD

Mobilni telefoni transformirali su se iz jednostavnih komunikacijskih uređaja u vrlo sposobna džepna računala. Ova transformacija je velikim dijelom potaknula razvoj novih i evoluciju postojećih protokola potrebnih za komunikaciju između telefona, mreža i perifernih uređaja.

Rani protokoli mobilnih uređaja bili su usredotočeni na omogućavanje glasovnih poziva. Prelaskom s tradicionalnih sustava s komutacijom kanala na paketski komutirane sustave uvjetovalo se i uvođenje novih protokola svojstvenih digitalnom prijenosu podataka. Postignuća poput GPRS-a postavili su temelje za pristup internetu, dok su Wi-Fi i Bluetooth omogućili alternativne puteve za brži prijenos podataka i povezivanje uređaja. Pojavom 3G i 4G mobilnih mreža i njima pridruženih protokola evoluirao je mobilni internet, omogućivši aktivnosti poput *streaminga* i videopoziva, dok je 5G napravio veliku integraciju svih mobilnih mreža nudeći do tada neviđene brzine i otvarajući vrata IoT-u (*Internet of Things*).

Near-Field Communication (NFC), pruža mogućnosti za sigurnu i beskontaktnu komunikaciju na vrlo malim udaljenostima. Integracija NFC-a u pametne telefone omogućila je inovacije u mobilnom plaćanju, kupnji karata i razmjeni informacija.

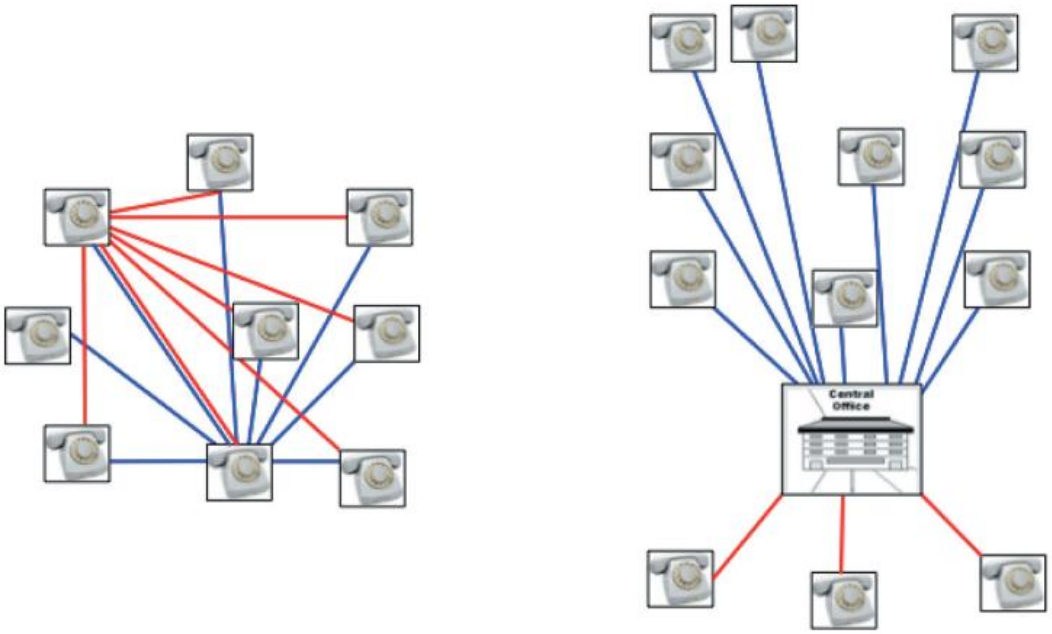
Ovaj rad istražuje tehnološke temelje, napredak i primjene ovih bežičnih komunikacijskih tehnologija, ispitujući povijesni razvoj, tehničke specifikacije i stvarne primjene protokola mobilnih komunikacija, Wi-Fi-ja, Bluetooth-a i NFC-a.

2. PROTOKOLI MOBILNIH KOMUNIKACIJA (1G – 5G)

G označava generaciju; i odnosi se na generacijski tehnološki napredak koji se dogodio u telekomunikacijama zadnjih 50-ak godina. Ta poboljšanja definirana su standardima koje su dogovorile razne nacionalne, međunarodne i industrijske organizacije. Napreci su se odvijali kroz faze, počevši s prvom generacijom (1G) i završavajući s trenutnom, petom (5G).

2.1. Komutacija kanala (eng. *circuit switching*)

U fiksnim linijama da bi dvije stranke komunicirale, potrebna im je namjenska linija, odnosno *circuit* (doslovni prijevod: strujni krug). Kako bi se taj proces izveo, također je potrebna i lokalna telefonska centrala. S njom su povezani svi korisnici, što centrali omogućuje stvaranje namjenskih linija između bilo koja dva korisnika, bez da su iste trajno fizički povezane jedno s drugom.



Slika 1. Lokalna telefonska centrala. LIJEVO: Bez lokalne telefonske centrale, potrebna je odvojena linija koja povezuje svaku stranku sa svakom drugom strankom. DESNO: S lokalnom telefonskom centralom, svaka stranka treba samo jednu vezu: prema centrali.[3]

2.2. Komutacija paketa (eng. *packet switching*)

Iako se komutacija kanala još uvijek koristila u prvoj (1G) i drugoj (2G) generaciji telekomunikacija, u počecima druge govor je digitaliziran. Svaka iduća generacija pretvarala je govor u *pakete*, slične onima korištenima za podatke: SMS, MMS, slike i videa.

Kod komutacije paketa, poruka se paketizira i paketi se zatim različitim putevima samostalno šalju do odredišta. Kako bi se paketi na odredištu mogli pravilnim redoslijedom spojiti, svaki od njih se sastoji od dva glavna dijela, *Data* i *Header*. Rastavljanjem komunikacije u pakete ostvaruje se mogućnost korištenja istog podatkovnog puta za više različitih korisnika mreže.

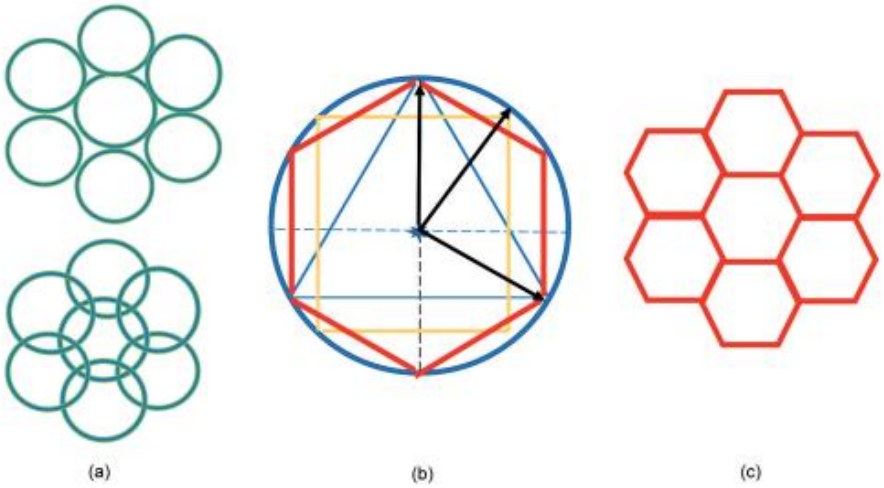
2.3. Mobilna mreža

Koncept mobilne mreže sastoji se od podjele određenog područja pokrivenog odašiljačkom stanicom u manja područja ili *ćelije*. Svaka ćelija bežično komunicira s korisnicima u drugim ćelijama, koristeći ograničeni broj frekvencija. Time se postižu dvije bitne stavke:

1) **Ponovna uporaba frekvencija** – komunikacije u nesusjednim ćelijama mogu koristiti iste frekvencije, koje su dovoljno niske da ne uzrokuju smetnje u susjednim ćelijama koje rade na skupu različitih frekvencija.
2) **Razdjeljivanje ćelija (*cell splitting*)** – smanjivanjem veličine ćelije povećava se broj mogućih istodobnih poziva, bez uporabe novih frekvencijskih opsega.[3]

Ćelije u obliku kružnice najjednostavnije su za implementirati, ali, kako prikazuje Slika 2(a), da se uočiti i nedostatak takve implementacije. Gornji dio slike prikazuje kako se između svake kružne ćelije nalazi i neobuhvaćeni prostor, koji bi uzrokovao nedostatak signala na istima. Ako se kružne ćelije pomaknu na način da se te praznine popune, dolazi do preklapanja ćelija što pak uzrokuje smetnje (donji dio slike 2(a)).

Analizom različitih poligonskih konfiguracija i uzimajući u obzir površinu koju svaki od njih zauzima unutar kružnice (Slika 2(b)), utvrđeno je kako su šesterokutne ćelije najefikasnije jer se njihovim spajanjem u mrežu pokriva najveći dio površine (Slika 2(c)).[1]



Slika 2 Geometrija ćelije: efikasnost kružnica i šesterokuta.[1]

2.4. Prva generacija mobilnih mreža (1G)

1G predstavljen je 1979. godine te se prenosio samo govor u analognom formatu. Korišteni su sustavi bazirani na komutaciji kanala sposobni za prijenos glasa u niskoj kvaliteti.

Prva generacija mobilnih mreža ima i brojne nedostatke, poput loše kvalitete prijenosa i sigurnosti – postojala je mogućnost prisluškivanja.

Standardi prve generacije

Pod prvu generaciju mobilnih mreža spadaju razni standardi, od kojih su najpopularniji i najznačajniji *Advance Mobile Phone Service* (AMPS) i *Nordic Mobile Telephone* (NMT). Svi standardi koriste frekvencijsku modulaciju za glasovne signale. Spektar unutar ćelije podijeljen je u određen broj kanala, te je svakom pozivu dodijeljen jedan par tih kanala.

NMT je razvijen u nordijskim zemljama u dvije verzije: NMT 450 i NMT 900 (brojevi označavaju korišteni frekvencijski pojas u Hz). U početku, podatkovni promet nije bio kriptiran, što je stvaralo mogućnost prisluškivanja tuđih poziva. Primarno se koristio u Europi. Dizajniran s roamingom na umu, omogućavao je korisnicima da se kreću regijom tijekom poziva.

AMPS je razvijen u SAD-u, te je primarni fokus istoga bila Sjeverna Amerika. Funkcionirao je u frekvencijskom pojasu od oko 800 MHz. U početku je imao ograničene roaming sposobnosti, što se u kasnijim verzijama poboljšalo.

1G pristupna tehnologija

Prva generacija mobilnih mreža oslanjala se na višestruki pristup podjele frekvencije (FDMA, *Frequency-Division Multiple Access*) čime omogućuje da više korisnika dijele dostupnu frekvenciju dijeleći je na manje podopsege. Prema FDMA, svaki telefonski poziv dodijeljen je određenom ulaznom frekvencijskom kanalu i drugom silaznom kanalu. Korišteni kanal je zauzet sve dok traje komunikacija.

FDMA tehnike su najmanje učinkoviti sustavi za višestruki pristup budući da ovise o prijenosu analognih signala.[3] Osobito kada se govor pretvara u električni signal i zatim natrag u zvuk: tada se neizbježno stvara određena količina buke koja utječe na kvalitetu poziva. Drugo, kako je usvajanje mobilnih telefona raslo, analogni kanali stvorili su probleme s ograničenim kapacitetom zbog činjenice da se svaki kanal može dodijeliti samo jednom korisniku u bilo kojem trenutku i ne može se *preraspodijeliti*.

2.5. Druga generacija mobilnih mreža (2G)

Druga generacija bežične telefonije nastala je u Finskoj, 1991. godine, pod GSM (*Global System for Mobile Communications*) standardima. Njih je razvio Europski institut za telekomunikacijske standarde (eng. *European Telecommunications Standards Institute,* ETSI). Glas se digitalizira tehnikama kao što su uzorkovanje i filtriranje, što u usporedbi s 1G donosi bolju kvalitetu glasa i pri nižim brzinama prijenosa. Time je omogućeno da se puno više mobilnih korisnika smjesti u radiofrekvencijski spektar u odnosu na 1G.

Druga generacija također je uvela nove usluge kao što su SMS (*Short Message Services*) i MMS (*Multimedia Message Services*). Ove usluge su digitalno šifrirane.

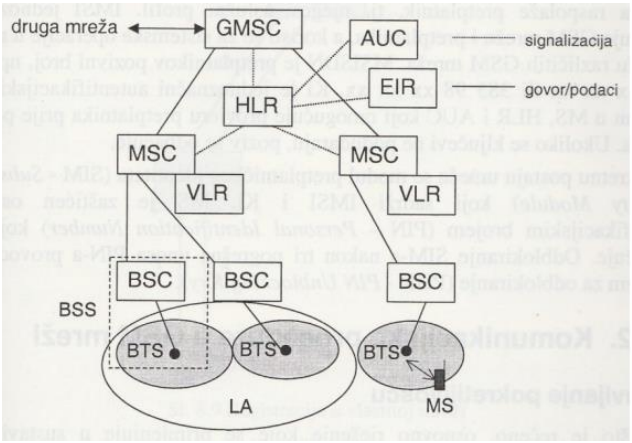
Druga generacija doživjela je mnoga poboljšanja tijekom desetljeća, sa sve boljim performansama u odnosu na izvorne 2G GSM standarde. Izvorni 2G GSM bio je spor sustav s komutacijom kanala koji je bio sposoban rukovati ograničenom količinom podataka. Značajka komutacije paketa uvedena je sa sljedećim poboljšanjem putem GPRS-a (*General Packet Radio Services)* koji se često naziva 2,5G. Daljnja poboljšanja uslijedila su s EDGE-om (*Enhanced Data Rate Evolution)* nazvanim 2,75G.

Standardi druge generacije

Tehnologije druge generacije uglavnom su razvijene na četiri standarda: GSM, D-AMPS, cdmaOne i PDC (*Pulse Data Capture*).[3] Ti su se standardi temeljili na digitalnim komunikacijama. 2G imao je za cilj učiniti globalni roaming realističnijim, budući da je isti u prvoj generaciji bio vrlo ograničen nedostatkom standardizacije i analognom prirodom.

GSM je standard koji ETSI uvodi u Europi kako bi opisao mrežne protokole druge generacije. Godine 1991. bio je prvi komercijalno upravljani digitalni mobilni sustav na svijetu i dizajniran je za pružanje usluga kao što su govorna pošta, tekstualne poruke, međunarodni roaming, prepaid pozivi, SMS i mnoge druge jeftine alternative komunikacije koje su povećale njegovu popularnost.

GSM radi na različitim radio frekvencijama, obično na 900 MHz i/ili 1800 MHz. Radijus ćelije u GSM mreži varira ovisno o visini antene, pojačanjima antene i uvjetima širenja, pa može biti od nekoliko stotina metara do nekoliko kilometara. Slika 3 prikazuje arhitekturu GSM-a.



Slika 3 Arhitektura GSM-a.[22]

GMSC (*Gateway Mobile Switching Centre*) omogućava povezivanje s drugim mrežama i pristup GSM mreži. **MSC** (*Mobile Switching Centre*) je komutacijski centar koji povezuje GMSC i BSS. **BSS** (*Base Station Subsystem*) se sastoji od kontrolnog **BCS**-a (*Base Station Controller*) i primopredajnog BTS-a (*Base Transceiver Station*). BSC upravlja s više BTS-ova koji sadrže antenske sustave. **MS** (*Mobile Station*) predstavlja korisnički terminal, tj. mobilni

uređaj ili telefon. **HLR** (*Home Location Register*) je domaći lokacijski registar koji sadrži sve podatke o pretplatnicima odnosno korisnicima. **VLR** (*Visitor Location Register*) je gostujući lokacijski registar ili registar posjetitelja, koji je sastavni dio svakog MSC-a. **AUC** (*Authentication Centre*) je centar za provjeru autentičnosti, koji sadrži autentifikacijski ključ za provjeru pretplatnika prilikom svakog poziva. **EIR** (*Equipment Identity Register*) je dodatna funkcija koja omogućuje provjeru serijskog broja (IMEI, *International Mobile Equipment Identity*) mobilnog uređaja, kako bi se utvrdilo je li uređaj u vlasništvu pretplatnika.

D-AMPS je digitalna verzija prve generacije AMPS tehnologije popularne u Sjevernoj Americi. Kompatibilan je s AMPS-om prve generacije.

CdmaOne ili **IS-95** je tehnologija popularna u Koreji i SAD-u koja je ponudila konkurenciju GSM tehnologiji. Za razliku od drugih standarda koji se temelje na TDMA ili FDMA tehnikama, CdmaOne se temelji na tehnologiji višestrukog pristupa kodne podjele (CDMA).

PDC je standard koji je postao popularan u Japanu i radio je na frekvencijama između 800 MHz i 1500 MHz.

2G pristupna tehnologija

Jedan od najvećih izazova koje su sustavi druge generacije morali prevladati bilo je povećanje mrežnog kapaciteta, odnosno istovremeno pružanje usluge puno većem broju korisnika. To se u 2G-u postiže korištenjem TDMA i CDMA tehnika.[3]

TDMA ili višestruki pristup s vremenskom raspodjelom je metoda koja je osmišljena s namjerom pružanja usluge velikom broju korisnika istovremeno dijeljenjem signala u različite vremenske odsječke. To se postiže prvo dijeljenjem frekvencije, a zatim dijeljenjem svake od njih po vremenu. Na taj način se jedna frekvencija može dijeliti među različitim korisnicima; korisnici koriste određenu frekvenciju u brzom slijedu, jedan za drugim, svaki koristeći svoj vremenski odsječak.

CDMA ili višestruki pristup s kodnom raspodjelom temelji se na tehnologiji *proširenog* spektra. Signal proširenog spektra je signal s dodatnom modulacijom koja povećava širinu

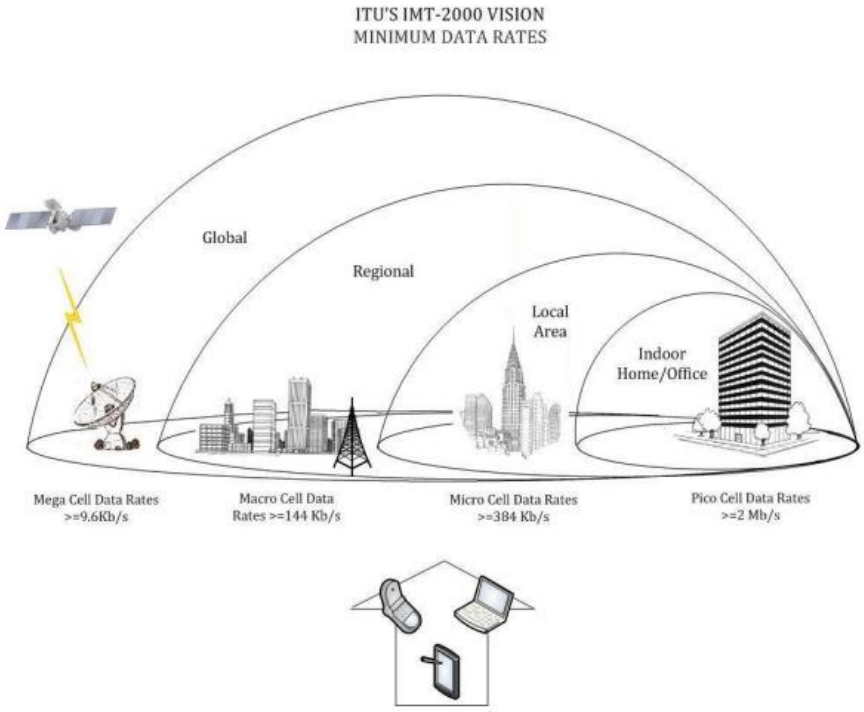
pojasa signala izvan onoga što zahtijeva osnovna modulacija. Smatra se najpraktičnijom i najdominantnijom metodom komunikacije u području raspršenog spektra. CDMA povećava kapacitet spektra omogućavajući svim prijenosima da zauzmu cijelu širinu pojasa u isto vrijeme bez interferencije. Svakom glasovnom ili podatkovnom pozivu dodjeljuje se jedinstveni kod kako bi se razlikovali od ostalih poziva koji se prenose preko istog spektra. U usporedbi s GSM mobilnim sustavom, CDMA zahtijeva manje baznih stanica i omogućuje pet puta veći kapacitet poziva. Također, osigurava više od deset puta veći glasovni promet u usporedbi s analognim sustavom (AMPS).

Za razliku od druge dvije tehnike, FDMA i TDMA, u CDMA nema frekvencijske podjele ni vremenskih odsječaka. Postoje različiti podatkovni kanali koji, kao i prije, prolaze kroz proces kodiranja gdje se protoku podataka dodaje redundantnost. Zatim se odvija proces multipleksiranja i različiti signali iz različitih kanala se množe i kombiniraju. Signal je raširen preko puno šireg pojasa prije nego što se odašilje zrakom. U slučaju da postoji više frekvencijskih nositelja, više CDMA sustava može raditi samostalno i odašiljati kroz antenski sustav. Ova tehnika je poželjnija jer je spektralno učinkovitija i nudi veći kapacitet.[1]

2.6. Treća generacija mobilnih mreža (3G)

Stalno rastuće potrebe korisnika i nekoliko tehnoloških dostignuća koja su postojala u ranim 2000-ima učinili su sustave druge generacije zastarjelima. To je dovelo do razvoja tehnologije treće generacije koja se fokusirala na poboljšanje glasovnih usluga s nekim podatkovnim mogućnostima. Međunarodna telekomunikacijska unija (eng. *International Telecommunication Union*, ITU) definirala je zahtjeve za novu mobilnu mrežu s IMT-2000 standardom, koji mogu podržati raspon podataka velike brzine od 144 kbps do više od 2 Mbps. Organizacija 3GPP (*3rd Generation Partnership Project*) definira sustav koji bi ispunio navedeno. U Europi se razvija standard UMTS (*Universal Mobile Telecommunications System*), dok u Sjevernoj Americi prevladava CDMA2000.

Zahtjevi za treću generaciju



Slika 4 Vizija ITU-a za minimalne brzine prijenosa podataka koje bi 3G trebao podržavati.[1]

Kao što je prikazano na Slici 4, zahtjevi ITU-a za sustave 3. generacije uglavnom su se odnosili na poboljšanja kapaciteta. Zahtjevi IMT-2000 standarda:

- Za velike ćelije ili makro ćelije, koje se najčešće koriste u urbanim i prigradskim područjima, mora se uzeti u obzir udaljenost od bazne stanice. Radijus ćelija se ograničava te s obzirom na to sustavi treće generacije trebaju podržavati najmanje 144Kb/s brzine prijenosa.
- Za manje ćelije ili mikro ćelije, fokus je na povezanosti pješaka. U tom slučaju 3G bi trebao podržavati najmanje 384Kb/s.
- Za najmanje ćelije ili piko ćelije za koje se smatra da su u zatvorenom prostoru, a korisnik je blizu antene, potrebna je podrška za najmanje 2 Mb/s.

Standardi treće generacije

Kako bi se ispunili zahtjevi i mogućnosti, sustavi 3. generacije razvijeni su uglavnom na dvije tehnologije: UMTS i CDMA 2000.

- **UMTS** koristi W-CDMA (širokopojasni CDMA) kao temeljni standard koji nudi veću spektralnu učinkovitost i veću propusnost od GSM-a. Također koristi par kanala od 5 MHz, jedan u rasponu od 1900 MHz za uzlaznu vezu i jedan u rasponu od 2100 MHz za silaznu vezu.
- **CDMA 2000,** poznat i kao *IMT Multi-Carrier* (IMT-MC), je razvijen kao nasljednik cdmaOne (IS-95) standarda i koristi se u Sjevernoj Americi i Južnoj Koreji.

3G pristupna tehnologija

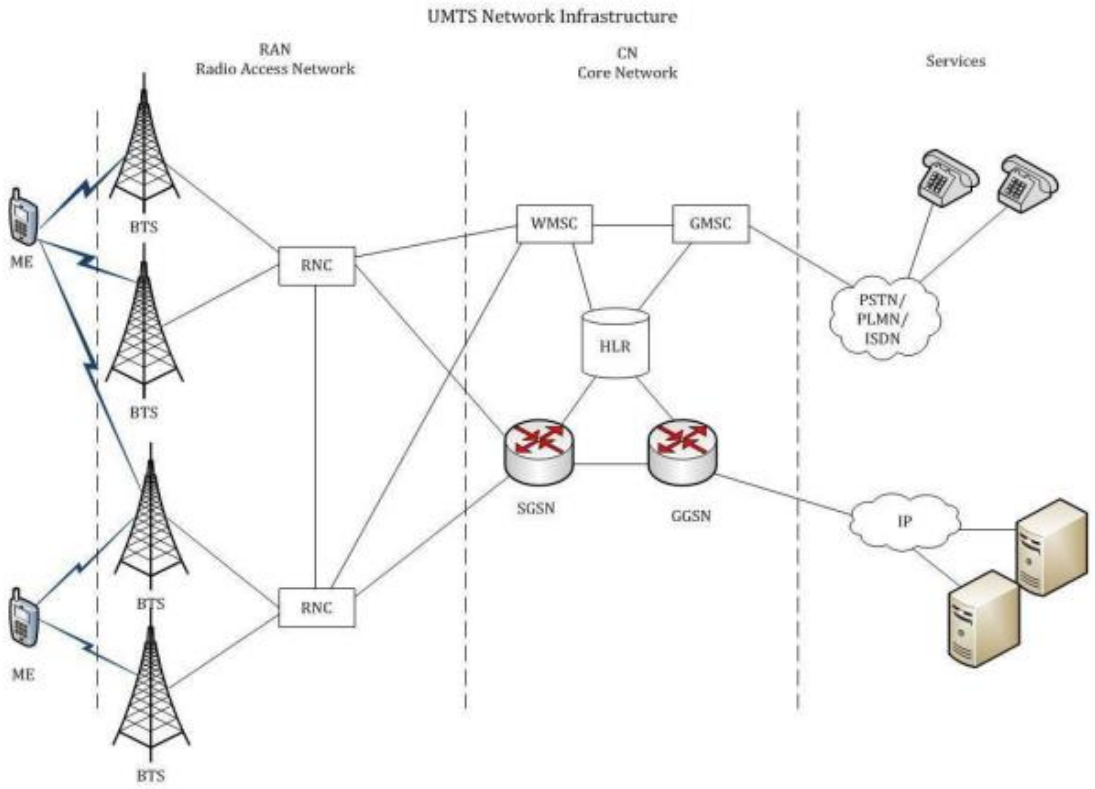
W-CDMA je tehnologija koju je odredio 3GPP za radio-sučelje UMTS-a – UTRA (*Universal Terrestrial Radio Access*). Ovaj standard temeljen na CDMA omogućuje veće brzine prijenosa podataka. Također podržava konvencionalne mobilne glasovne, tekstualne i multimedijske usluge. W-CDMA koristi kanale širine 5 MHz, dok konkurentski sustavi poput CDMA2000 i njegovog prethodnika cdmaOne koriste kanale širine 1,25 MHz. Primjena W-CDMA metode posebno je pogodna za ruralna područja gdje je potrebno uspostaviti širokopojasnu mobilnu mrežu.

Prednosti W-CDMA metode su veći kapacitet, bolja pokrivenost od CDMA i TDMA i varijabilna brzina prijenosa.

Kasnije se pojavljuje nadogradnja HSPA (*High Speed Packet Access*), koja predstavlja kombinaciju dvaju protokola, HSDPA (*High Speed Downlink Packet* Access) i HUSPA (*High Speed Uplink Packet Access*). Ova nadogradnja omogućuje brzine od 14,4 Mbit/s za preuzimanje i 5,75 Mbit/s za *upload*. Daljnjim razvojem 3GPP standarda uveden je HSPA+ (*Evolved High Speed Packet Access*), koji omogućuje brzine od 42,2 Mbit/s za preuzimanje i 22 Mbit/s za *upload*.

Arhitektura UMTS-a

Na slici 5 prikazana je arhitektura UMTS-a.



Slika 5 UMTS arhitektura.[1]

UMTS mreža sastoji se od tri dijela: korisničke/mobilne opreme (na Slici 5 ME, *Mobile Equipment,* može biti i UE (*User Equipment*)), UTRAN-a (*UMTS Terrestrial Radio Access Network*) i osnovne/jezgrene mreže (na slici CN, *Core Network*).

ME sadrži mobilni telefon i SIM (*Subscriber Identity Module*) karticu koja sadrži podatke specifične za korisnika i omogućuje autentificirani pristup pretplatnika u mrežu. Postoje tri načina rada ME: CS (*Circuit Switched*), PS (*Packet Switched)* način i CS/PS način. U CS načinu rada ME je povezan samo s osnovnom mrežom. U PS načinu rada, ME je povezan samo s PS domenom, dok u CS/PS korisnik ima mogućnost korištenja i CS i PS usluga.

Komponente RAN-a (*Radio Access Network*) su:

- Bazne stanice (na slici BTS), također zvanima *Node B*, čije su glavne funkcije modulacija i demodulacija, prijenos i prijem te rukovanje pogreškama.

- Radio mrežni kontroler (na slici RNC) čije su glavne funkcije kontrola i upravljanje radio resursima, dodjela kanala, kontrola pristupa i šifriranje.

Glavna funkcija osnovne mreže (CN) je osigurati komutaciju i usmjeravanje korisničkog prometa. Također sadrži baze podataka i funkcije upravljanja mrežom. Osnovna mreža podijeljena je na CS i PS domene. Komponente su joj sljedeće:

- GMSC (*Gateway Mobile Services Switching Centre*) koji se koristi za usmjeravanje poziva izvan mobilne mreže.
- VLR (*Visitor Location Register*) koji sadrži informacije o gostujućim pretplatnicima iz druge mreže. Primarna uloga VLR-a je minimiziranje broja upita prema registru lokalne, domaće mreže (HLR, *Home Location Register*).
- SGSN (*Serving GPRS Support Node*) koji posreduje u pristupu mrežnim resursima u ime mobilnih pretplatnika.
- GGSN (*Gateway GPRS Support Node*) koji je odgovoran za objavljivanje pretplatničkih adresa, mapiranje adresa, povezivanje i tuneliranje paketa, prikazivanje poruka, te brojanje paketa.

Budući da je treća generacija mobilnih mreža prva uvela podatkovne usluge velike brzine, još uvijek su postojala velika ograničenja povezana s pokrivenošću, sigurnošću i složenošću sustava. Neka od njih su:

- Uz 3G temeljen na WCDMA, kako se brzina podataka povećava, područje pokrivenosti ćelije postaje sve manje i manje.
- Korištenjem WCDMA ćelija, s povećanjem brzine prijenosa podataka, moguća brzina kretanja korisničkog terminala također postaje sve manja.
- Bežični sustavi troše puno energije i stoga imaju ograničen vijek trajanja baterije.

2.7. Četvrta generacija mobilnih mreža (4G)

Prema uvjetima za četvrtu generaciju mobilnih mreža koje je postavio ITU, brzina prijenosa podataka za korisnike u pokretu treba biti 100 Mbit/s za preuzimanje i 50 Mbit/s za slanje, dok za fiksne lokacije treba dosezati 1 Gbit/s. Ove usluge također moraju zadovoljiti zahtjeve za kvalitetom usluge (QoS, *Quality of Service*). Glavna uloga QoS-a je osiguravanje

prioriteta u propusnosti mreže (eng. *Bandwidth*) i kontrola varijacija u latenciji (eng. *Jitter*)[2]. Ovi mehanizmi su ključni za nesmetan rad aplikacija.

Glavni standard 4G-a predstavljen je 2009. godine u Švedskoj i Norveškoj, kao *Long Term Evolution* (LTE) na temelju zahtjeva koje je odredio ITU.

Standardi četvrte generacije

Standardi četvrte generacije uključuju LTE, *Ultra Mobile Broadband* (UMB) i IEEE 802.16 standard također poznat kao WIMAX. WIMAX je uveden u SAD-u od strane IEEE-a (*Institute of Electrical and Electronics Engineers)*. Ni LTE ni WIMAX nisu bili u mogućnosti ispuniti 4 G standarde, te su se smatrali privremenim ili ažuriranim verzijama 3 G standarda.

2011. godine ažuriranu verziju LTE-a, nazvanu LTE-Advanced (LTE-A) odobrio je 3GPP budući da je zadovoljavao 4G standarde koje je uspostavio ITU. Otprilike u isto vrijeme IEEE je objavio ažuriranu verziju WIMAX2 koja je bila konkurentna verziji LTE-A, koji je ipak prevladao. Većina svjetskih mobilnih operatera slijedila je standarde 3GPPA, te je LTE-A predstavljao lakšu i jasniju nadogradnju s prijašnjih standarda. WiMAX je podržavao manji skup dobavljača i operatera, a osim toga je bio više fokusiran na računalne mreže nego na mobilnu telefoniju.

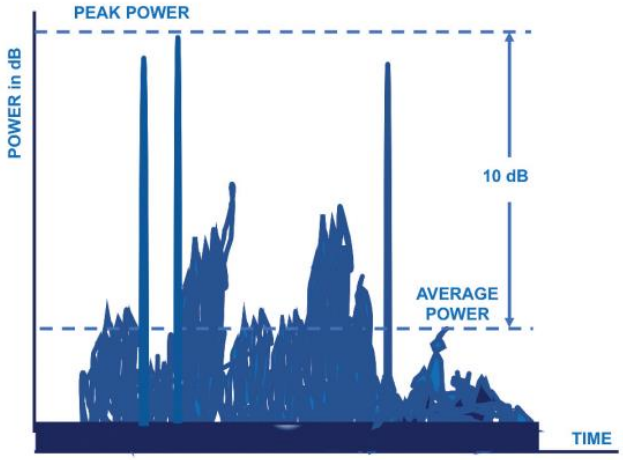
4G pristupna tehnologija

LTE sučelje koristi dvije glavne tehnologije - ortogonalno multipleksiranje frekvencijskim odvajanjem (OFDMA, *Orthogonal Frequency-Division Multiple Access*) za *downlink* odnosno silaznu vezu i višestruki pristup s frekvencijskom raspodjelom na jednom nositelju (SC-FDMA, *Single Carrier (Orthogonal) Frequency-Division Multiple Access)* za *uplink* odnosno uzlaznu vezu. Ortogonalni FDMA sustavi koriste blisko razmaknute susjedne podnositelje koji si ne uzrokuju smetnje. To dovodi do radijskih kanala velikog kapaciteta i omogućuje postizanje visokih brzina prijenosa podataka.

Uz navedeno, važna je i implementacija višestrukih antena na cijeloj opremi, što se postiže korištenjem MIMO (višestruki-ulazi, višestruki-izlazi, *Multiple-Input Multiple-Output*)

tehnologije. Također su značajne tehnike odašiljačke i prijemne raznolikosti (TX/RX) i upravljanje dijagramom zračenja antene (eng. *Beamforming*).

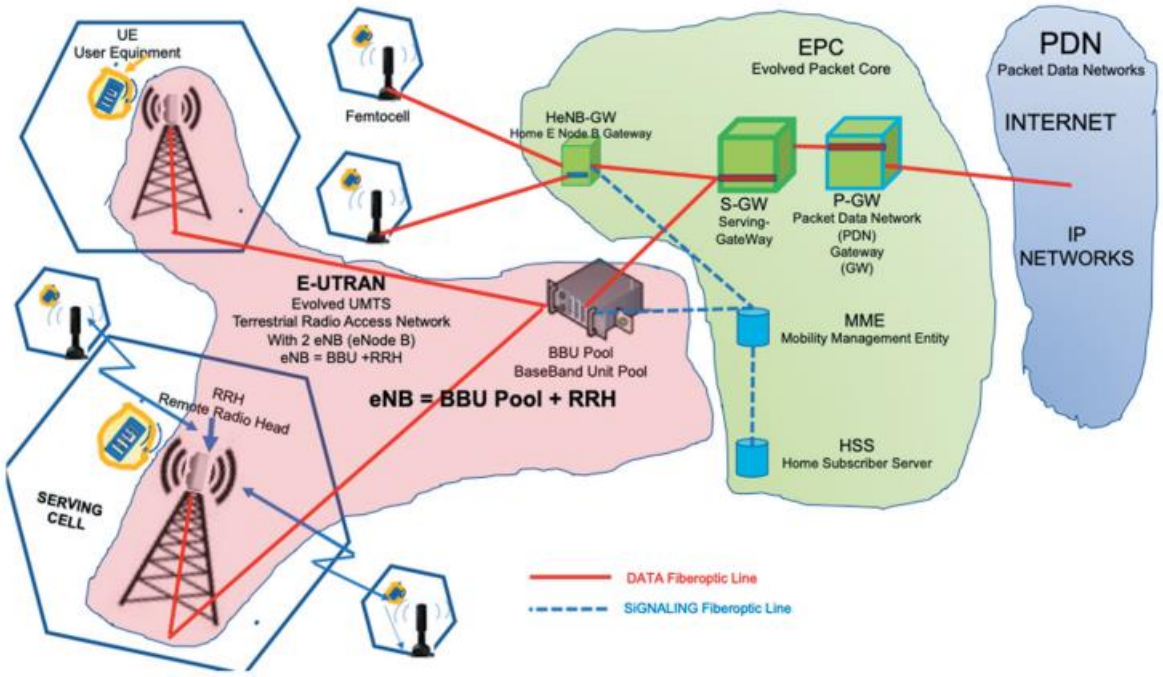
Glavni problem s OFDM-om je njegov visok omjer vršne i prosječne snage (PAPR), što ga čini neprikladnim za uzlaznu vezu s obzirom na malu veličinu mobilne korisničke opreme kao što su pametni telefoni. Na primjer, tipični PAPR od 10 dB značajno bi povećao potrošnju baterije istih na nepraktične razine. To je ilustrirano na slici 6, koja prikazuje omjer vršne i prosječne snage (PAPR). Rješenje ovog problema je korištenje SC-FDMA za uzlaznu vezu.



Slika 6 Odnos PAPR-a u OFDMA prijenosima.[3]

Arhitektura LTE-A

Slika 7 prikazuje arhitekturu LTE Advanced.



Slika 7 LTE Advanced arhitektura.[3]

Mreža se sastoji od tri osnovna elementa:

● Korisnička oprema, UE. To je isti element opisan u arhitekturi 3G UMTS-a (Slika 5) i služi identičnim funkcijama. Ukratko, UE nije ništa drugo nego pametni telefon kojeg netko koristi za mobilnu komunikaciju.

● Drugi element, jezgra sustava, E-UTRAN (*Evolved-UMTS Terrestrial Radio Access Network*) upravlja svim komunikacijama između UE i jezgrene mreže (treći element ove arhitekture), preimenovan u evoluiranu paketnu jezgru (EPC, *Evolved Packet Core*). To je pojednostavljena verzija 3G UTRAN arhitekture sa Slike 5 pri čemu su BTS iliti *Node* B i radio mrežni kontroler, RNC, sada kombinirani u jednu cjelinu, eNB (*Evolved Node B*).

U slučaju LTE-A, ne postoji zasebna domena s komutiranim krugom (CS) kao u slučaju prijašnje generacije. Umjesto toga, 4G je mreža koja se oslanja isključivo na PS domenu za sve vrste komunikacije.

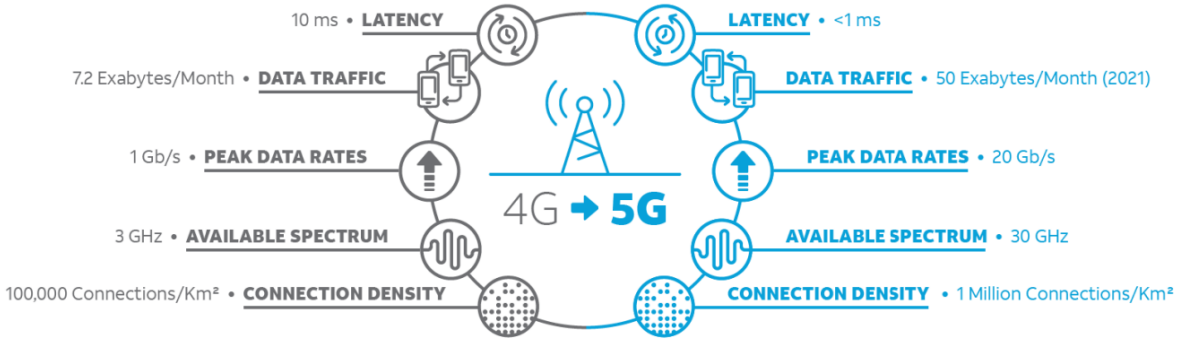
2.8. Peta generacija mobilnih mreža (5G)

Peta generacija mobilnih mreža ima veće brzine prijenosa, s vršnom brzinom od 10 gigabita u sekundi (Gbit/s)[4]. 5G ima veću propusnost za pružanje većih brzina od 4G i može povezati više uređaja, poboljšavajući kvalitetu internetskih usluga u gušćim područjima.[2] Zbog povećane propusnosti, 5G mreže sve se više koristite kao pružatelji općih internetskih usluga (ISP-ovi), a također omogućuje nove aplikacije u području Internet stvari (IoT, eng. *Internet of Things*). Takva masovna povezanost zahtijeva nove standarde prijenosa podataka:

- Brzine do 10 Gb/s u uzlaznoj vezi i 20 Gb/s u silaznoj vezi
- Vrlo niska latencija, od 110 ms do 1 ms
- EE, energetska učinkovitost, povećanje s 1 Mb/J na 1 Gb/J

Kako bi se proširio frekvencijski spektar, koriste se milimetarski valovi (*mmWaves*).

Slika 8 uspoređuje ključne tehnološke metrike između 4G i 5G mreža, ističući napredak koji 5G donosi. Što se tiče latencije, 4G postiže 10 ms, dok 5G to dramatično smanjuje na manje od 1 ms. Podatkovni promet također doživljava značajan porast, sa 7.2 EB mjesečno u 4G-u, na 50 EB mjesečno kod 5G-a. Vršne podatkovne brzine povećavaju se s 1 Gb/s u 4G na 20 Gb/s u 5G. Dostupni spektar se proširuje s 3 GHz u 4G do 30 GHz u 5G, što omogućuje puno veći kapacitet i propusnost. Gustoća povezanosti raste eksponencijalno, sa 100 000 veza po kvadratnom kilometru u 4G na 1 milijun veza po kvadratnom kilometru u 5G.

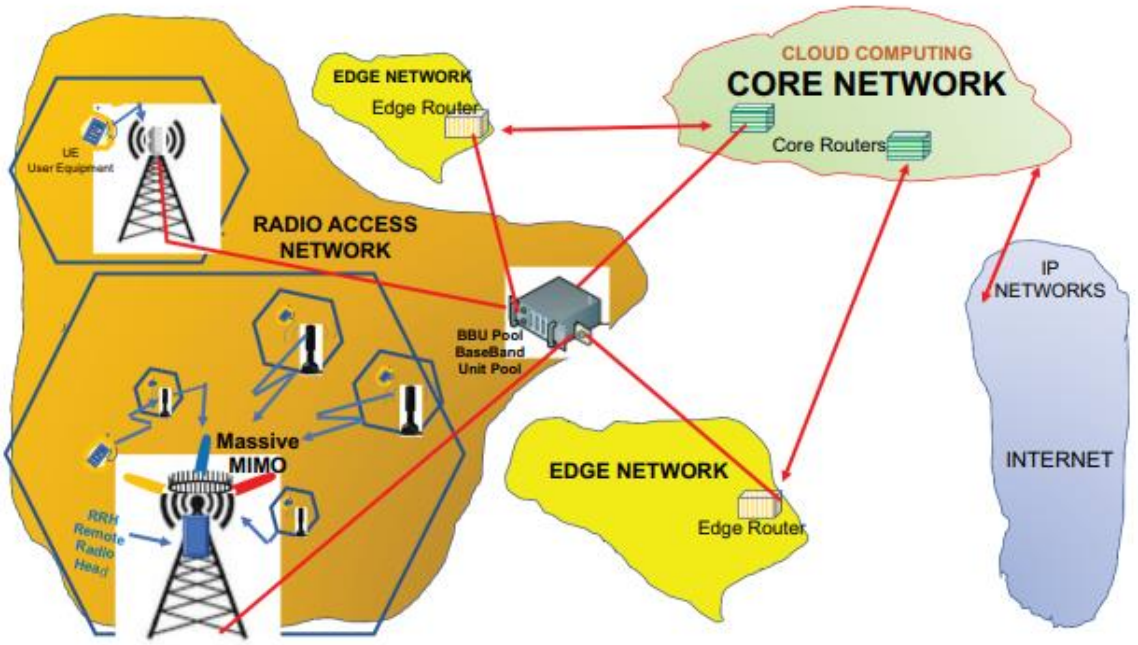


Slika 8 Usporedba četvrte i pete generacije.[17]

Za rad s milimetarskim valovima potrebni su mobilni uređaji s minijaturnim usmjerenim antenama (MIMO).

Cjelokupni frekvencijski spektar kojeg pokriva 5G u principu se proteže od 3 do 300 GHz. Budući da rad 5G mora podržavati stare 4G uređaje, uključuje se i frekvencijski raspon 4G LTE-a ispod 3 GHz pa do 600 MHz.

Arhitektura 5G-a



Slika 9 5G arhitektura.[3]

5G mrežna arhitektura razlikuje se od 4G arhitekture u jednom značajnom pogledu: središnji se poslužitelji nalaze u "oblaku" daleko od mobilne mreže uz dodatak manjih poslužitelja koji se nalaze blizu mreže u takozvanoj rubnoj mreži.

Prednost rubne mreže je njezina blizina mobilnoj mreži, čime se smanjuje kašnjenje, što je važno kod IoT-a gdje se odvija komunikacija između mnoštva uređaja i ljudi.

Sve 5G mreže sastoje se od dva ključna elementa prikazanima na Slici 9: radio pristupna mreža (RAN) i jezgrena mreža (CN) koja se nalazi u oblaku

Kao što se vidi na Slici 9, radio pristupna mreža (RAN) sastoji se od raznih ćelija i baznih stanica, s MIMO (višestruki ulazi-višestruki izlazi). MIMO antene mogu primati više podataka istovremeno.

Mikroćelije i one najmanje zvane femtoćelije jedinstvena su značajka 5G tehnologije. Koriste milimetarske valove koji povećavaju pokrivenost i daju veće brzine prijenosa podataka.

Jezgrena mreža (CN) upravlja svim mobilnim glasovnim, podatkovnim i internetskim vezama. Distribuira se s glavnim poslužiteljima koji se nalaze u oblaku i lokalnim manjim poslužiteljima smještenim u rubnim mrežama koji djeluju kao pružatelji usluga obližnjim korisnicima kojima je potrebna niska latencija.

Sljedeće tehnologije su jedne od najvažnijih u sklopu 5. generacije mobilnih mreža:

- **Milimetarski valovi**
  - Proširena pokrivenost i veće brzine prijenosa podataka.
  - Rad u višem dijelu frekvencijskog spektra (30 GHz do 300GHz).
  - Proširena pokrivenost: postiže se dijeljenjem veličine ćelije na mikro i femtoćelije, dopuštajući višestruku ponovnu upotrebu istog skupa frekvencija korištenih u makroćeliji.

- **Masivne MIMO (višestruki-ulaz, višestruki-izlaz) antene**:
  - Smanjuju smetnje kanala.
  - Male antene stanu u korisnički pametni telefon, osiguravajući rad s milimetarskim valovima.
  - Smještene su na vrhu tornjeva za makro-ćeliju te imaju usmjerene zrake (*beamforing*), kao što se vidi na Slici 9, što omogućuje komunikaciju s više korisnika na istoj frekvenciji.

- **NFV (*Network Function Visualization*)**
  - Odvaja mrežne funkcije, kao što su usmjeravanje i obrada paketa od hardvera i zamjenjuje ih softverom koji radi na takozvanim virtualnim strojevima (VM, *Virtual Machine*)
  - Smanjenje troškova za opremu i energiju, povećana fleksibilnost, te kraće vrijeme i manji rizik prilikom implementacije novih usluga u sustav.[5]

3. PROTOKOLI MOBILNIH TELEFONA

Tri ključna protokola koja imaju središnju ulogu u modernoj mobilnoj komunikaciji su Wi-Fi, Bluetooth i NFC (*Near Field Communication*). Svaki od njih u praksi služi različitim svrhama.

3.1. WI-FI protokol

Standard IEEE 802.11 za bežično lokalno umrežavanje (WLAN, *Wireless Local Area Network*), komercijalno poznat kao *Wi-Fi* i zaštitni znak *WI-Fi Alliance-a* (neprofitna organizacija koja posjeduje zaštitni znak Wi-Fi), postao je neophodan u ljudskom svakodnevnom životu. Preko milijardu Wi-Fi pristupnih točaka povezuje blizu stotinu milijardi IoT uređaja, pametnih telefona, tableta, prijenosnih računala, stolnih računala, pametnih televizora i drugih potrošačkih uređaja s internetom.

Evolucija Wi-Fi tehnologije također je rezultirala prvim komercijalnim lansiranjem tehnologija širokog spektra, optičkih komunikacija velike brzine, OFDM, MIMO i milimetarskih valova, koje su zatim postale šire prihvaćene u industriji mobilnih telefona, o čemu se pisalo ranije u radu.

Postoje dva različita bežična podatkovna sučelja za povezivanje pametnog telefona s internetom: IEEE 802.11 bežične lokalne mreže (Wi-Fi), i mobilne podatkovne mreže (1G-5G). Wi-Fi je primarni izbor za pametne telefone jer može pružiti veću brzinu prijenosa podataka i pouzdanije veze u zatvorenom prostoru po nižoj cijeni - korisnici obično pribjegavaju mobilnim mrežama kao drugom izboru. Vjeruje se da bi se ravnoteža mogla pomaknuti prema mobilnim mrežama, jer su dostupne posvuda, kako se brzine prijenosa podataka povećavaju, a mobilni troškovi smanjuju. Međutim, još je uvijek Wi-Fi najbrži i najisplativiji način bežičnog internetskog povezivanja.

3.1.1. Wi-Fi standardi i generacije

Svaka nova generacija WiFi-a donosila je značajna poboljšanja u brzini, kapacitetu, učinkovitosti i pouzdanosti. U nastavku slijedi nešto više o glavnim Wi-Fi standardima i njihovim karakteristikama.

1.) 802.11 standard

Izvorni standard 802.11, koji je 1997. godine uveo IEE, označio je početak bežičnog lokalnog umrežavanja (WLAN). Ovaj naslijeđeni standard postavio je temelje za kasniji napredak u WiFi tehnologiji.

Standard 802.11 radio je u pojasu od 2,4 GHz u ISM *band*-u (*Industrial, Scientific, and Medical*), koji je nelicenciran i dostupan u cijelom svijetu.[6] Ovaj izbor frekvencijskog pojasa bio je ključan za dostupnost tehnologije i širenje nje.

Izvorni standard 802.11 podržavao je maksimalne brzine prijenosa podataka od 1 Mbps i 2 Mbps. Ove relativno niske brzine prijenosa podataka bile su dovoljne za osnovne mrežne zadatke u to vrijeme, ali su brzo postale neadekvatne kako je rasla potražnja za aplikacijama veće propusnosti. Tehnike modulacije korištene u 802.11 uključivale su:

- Binarno fazno pomicanje (BPSK, *Binary Phase Shift Keying*): Koristi se za podatkovne brzine od 1 Mbps.
- Kvadratni fazni pomak (QPSK, *Quadrature Phase Shift Keying*): koristi se za podatkovne brzine od 2 Mbps.

2.) 802.11a standard

Standard 802.11a, koji je 1999. godine uveo IEE, bio je značajan napredak u tehnologiji bežičnog umrežavanja. Dizajniran za rješavanje ograničenja izvornog standarda 802.11, 802.11a donio je veće brzine prijenosa podataka i smanjene smetnje, što ga čini prikladnim za zahtjevnije aplikacije i okruženja.

802.11a radi u pojasu U-NII (*Unlicensed National Information Infrastructure*) od 5 GHz, koji pruža više dostupnih kanala i manje smetnji u usporedbi s pojasom od 2,4 GHz koji je koristio njegov prethodnik. Ovaj izbor frekvencijskog pojasa bio je ključan za poboljšanje performansi mreže i smanjenje zagušenja od drugih uređaja.

Standard 802.11a podržava brzine prijenosa podataka do 54 Mbps. Ovo poboljšanje postignuto je upotrebom OFDM-a.

Tehnike modulacije uključuju:

- BPSK: Koristi se za brzine prijenosa podataka od 6 Mbps i 9 Mbps.

- QPSK: Koristi se za brzine prijenosa podataka od 12 Mbps i 18 Mbps.
- 16-QAM (kvadraturna amplitudna modulacija): Koristi se za brzine prijenosa podataka od 24 Mbps i 36 Mbps.
- 64-QAM: Koristi se za brzine prijenosa podataka od 48 Mbps i 54 Mbps.

3.) 802.11b standard

802.11b je također uveden 1999. godine. Njegovo uvođenje odigralo je ključnu ulogu u popularizaciji WiFi-a, čineći bežično umrežavanje pristupačnim i praktičnim za kućne i poslovne korisnike.

802.11b radi u ISM pojasu od 2,4 GHz istom frekvencijskom pojasu kao izvorni standard 802.11. To je osiguralo kompatibilnost s prethodnim verzijama. Doduše, njegova neregulirana priroda znači da se može suočiti sa smetnjama od svih drugih uređaja koji koriste raspon od 2,4 GHz.

Standard 802.11b podržava maksimalnu brzinu prijenosa podataka od 11 Mbps, znatno više od 2 Mbps koje nudi izvorni 802.11. Ovo poboljšanje postignuto je korištenjem tehnologije proširenog spektra izravne sekvence (DSSS) i modulacije komplementarnog kodnog ključa (CCK). Ove su tehnike poboljšale protok podataka i otpornost na smetnje.

Iako je podržavao manje brzine nego standard 802.11a, većina proizvođača radije ga je koristila zbog niskih troškova proizvodnje.

Tehnike modulacije uključuju:

- DBPSK (*Differential Binary Phase Shift Keying*) i DQPSK (*Differential Quadrature Phase Shift Keying*): Koriste se za brzine prijenosa podataka od 1 Mbps i 2 Mbps.
- CCK (*Complementary Code Keying*): Koristi se za brzine prijenosa podataka od 12 Mbps.

4.) 802.11g standard

Uveden 2003. godine, standard 802.11g kombinirao je najbolje značajke svojih prethodnika: omogućio je visoke brzine prijenosa podataka usporedive s 802.11a, istovremeno održavajući kompatibilnost s 802.11b uređajima. Ovo se pokazalo privlačnim izborom za potrošače i za tvrtke, što je ubrzalo usvajanje bežičnog umrežavanja.

802.11g također radi u ISM pojasu od 2,4 GHz. Standard podržava maksimalnu brzinu prijenosa podataka od 54 Mbps, što odgovara mogućnostima 802.11a, također korištenjem OFDM-a. Prednosti korištenja OFDM-a uključuju i smanjene efekte višestaznosti u prijemu i povećanu spektralnu učinkovitost.[8]

Tehnike modulacije uključuju:

- 1 Mbps i 2 Mbps: Ove podatkovne brzine koriste DBPSK i DQPSK, kao kod 802.11b.
- 5,5 Mbps i 11 Mbps: ove brzine koriste CCK, kao kod 802.11b.
- 6 Mbps do 54 Mbps: Ove veće brzine prijenosa podataka koriste OFDM, s različitim razinama QAM-a.

5.) 802.11n standard

802.11n standard predstavljen je 2009. godine i koristi više antena za povećanje brzine prijenosa podataka. *Wi-Fi Alliance* također je retroaktivno označio tehnologiju za standard kao Wi-Fi 4[9], dok su prva tri standarda kronološki nazvana Wi-Fi 1, 2 i 3. Standardizirana je podrška za višestruki ulaz-višestruki izlaz, između ostalih značajki, i može se koristiti u frekvencijskim pojasima od 2,4 GHz ili 5 GHz.

Jedna od najznačajnijih značajki 802.11n je korištenje tehnologije višestrukog ulaza višestrukog izlaza (MIMO), koji se u radu spominjao ranije. MIMO koristi više antena i na odašiljaču i na prijamniku za poboljšanje komunikacijskih performansi. Standard 802.11n podržava brzine prijenosa podataka do 600 Mbps, što je značajno povećanje u odnosu na prethodne standarde.

6.) 802.11ac standard

802.11ac standard izdan je 2013. godine i visoke propusnosti na pojasu od 5 GHz. Standard je također poznat kao WI-Fi 5.[9]

802.11ac radi isključivo u pojasu od 5 GHz, koji nudi manje smetnji i veću dostupnu propusnost u usporedbi s pretrpanim pojasom od 2,4 GHz. Ovaj fokus na pojas od 5 GHz omogućuje veće brzine prijenosa podataka i pouzdanije veze.

Standard 802.11ac podržava teoretske maksimalne brzine prijenosa podataka do 6,93 Gbps. Dopušta širine kanala do 160 MHz, u usporedbi s kanalima od 20 MHz ili 40 MHz koji su se koristili u prethodnim standardima. Koristi višekorisnički MIMO (MU-MIMO, *Multi-User MIMO*) koji omogućuje pristupnoj točki da komunicira s više uređaja istovremeno.

Trenutno je to najkorišteniji standard u pametnim telefonima izdanima do 2020. godine.

7.) 802.11ax standard

Wi-Fi 6 ili 802.11ax standard prihvaćen je 2021. godine i radi u pojasima od 2,4 GHz i 5 GHz, s proširenom verzijom Wi-Fi 6E koja dodaje pojas od 6 GHz.[10] Omogućuje bolju izvedbu na mjestima s puno uređaja i interferencija ostalih signala.

Standard 802.11ax podržava teoretske maksimalne brzine prijenosa podataka do 9,6 Gbps. Koristi višestruki pristup s ortogonalnom frekvencijskom podjelom (OFDMA) za povećavanje učinkovitosti i smanjivanje kašnjenja, osobito u okruženjima s mnogo povezanih uređaja. Također koristi TWT (*Target Wake* Time) za smanjenje potrošnje energije mreže, jer stanice koje ga koriste mogu ući u stanje drijemanja dok ne stigne njihov TWT, tek onda pristupaju mediju.

Podržavaju ga *flagship* pametni telefoni izdani nakon 2020. godine.

3.1.2. Sigurnost Wi-Fi mreže

Jedna od najvećih mana današnjih Wi-Fi mreža je sigurnost. Na sigurnosti ovise svi podaci koje korisnik pregledava sa svog uređaja, a loša sigurnost može dovesti do otuđenja tih podataka. Kako je bežično umrežavanje postalo sveprisutno, važnost sigurnosti Wi-Fi mreža

eksponencijalno je porasla. Wi-Fi sigurnost uključuje zaštitu podataka koji se prenose putem bežičnih mreža od neovlaštenog pristupa i osiguravanje da je sama mrežna infrastruktura zaštićena od napada. Razvoj Wi-Fi sigurnosnih protokola evoluirao je tijekom godina kako bi se riješile nove prijetnje i ranjivosti.

Wired Equivalent Privacy **(WEP)** je potvrđen kao sigurnosni protokol 1999. kao dio izvornog standarda IEEE 802.11, označavajući jedan od prvih pokušaja zaštite bežičnih mreža. Primarni cilj WEP-a bio je pružiti razinu sigurnosti usporedivu s onom žičnih mreža, čime se bežični podaci štite od prisluškivanja i neovlaštenog pristupa. Unatoč početnom obećanju, WEP-ovi sigurnosni mehanizmi ubrzo su se pokazali neprikladnima, što je dovelo do njegove eventualne zamjene robusnijim protokolima.

Podržavao je 64-bitne i 128-bitne ključeve, kombinirajući korisničke i tvornički postavljene bitove. WEP je koristio RC4 algoritam za šifriranje podataka, stvarajući jedinstveni ključ za svaki paket kombiniranjem novog inicijalizacijskog vektora sa zajedničkim ključem. Unatoč početnoj upotrebi, WEP-ove značajne ranjivosti dovele su do usvajanja sigurnijih protokola. WEP sigurnosni standard službeno je povučen 2004.

Wi-Fi Protected Access **(WPA)** uveo je Wi-Fi Alliance 2003. godine kao privremeno sigurnosno poboljšanje koje je zamijenilo vrlo ranjivi WEP protokol. WPA je imao za cilj pružiti robusnije sigurnosno rješenje za bežične mreže, dok je IEEE razvio trajniji standard, koji će kasnije postati WPA2. WPA je riješio mnoge slabosti WEP-a ugradnjom jačih metoda šifriranja i poboljšanih mehanizama provjere autentičnosti.

Ključne značajke WPA protokola:

- Protokol integriteta vremenskog ključa (TKIP, *Temporal Key Integrity Protocol*): TKIP koristi funkciju miješanja ključeva po paketu, koja generira jedinstveni ključ šifriranja za svaki paket podataka. Ovo umanjuje rizik ponovne upotrebe ključa.
- Provjera integriteta poruke (MIC, *Message Integrity Check*): služi za otkrivanje i sprječavanje petljanja paketa. Time se osigurava cjelovitost prenesenih podataka.
- Ključevi koje koristi WPA sigurnosni standard su 256-bitni, za razliku od 64-bitnih i 128-bitnih ključeva koje je koristio WEP sustav.

Iako WPA predstavlja značajan napredak u odnosu na WEP, nije bio bez ograničenja. Tijekom vremena otkrivene su određene ranjivosti u TKIP-u, poput mogućnosti izvođenja napada oporavka MIC ključa pod određenim uvjetima. Razlog tomu je taj što je TKIP dizajniran tako da bude unatrag kompatibilan s WEP sustavima, pa je kao takav koristio određene elemente koji se koriste u WEP-u. Ove su ranjivosti dovele do prijelaza na WPA2, koji koristi bolju enkripciju.

Wi-Fi Protected Access 2 **(WPA2)** je 2004. godine zamijenio WPA. Uključuje podršku za CCMP (*Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*), način šifriranja temeljen na AES-u (*Advanced Encription Standard*).[11] Od 2006. do 2020. godine WPA2 certifikacija bila je obavezna za sve nove uređaje koji nose zaštitni znak Wi-Fi.[12] U WLAN-ovima zaštićenim WPA2, sigurna komunikacija uspostavlja se kroz proces u više koraka. U početku se uređaji povezuju s pristupnom točkom (AP) putem zahtjeva za pridruživanjem. Nakon toga slijedi 4-smjerno „rukovanje“, ključni korak koji osigurava da i klijent i AP imaju točan unaprijed dijeljeni ključ (PSK) bez stvarnog prijenosa. Tijekom ovog rukovanja, PTK (*Pairwise Transient Key*) se generira za sigurnu razmjenu podataka.

Četverostruko rukovanje uključuje:

- AP šalje nasumični broj (*ANonce*) klijentu.
- Klijent odgovara svojim nasumičnim brojem (*SNonce*).
- AP izračunava PTK iz tih brojeva i šalje šifriranu poruku klijentu.
- Klijent dešifrira ovu poruku s PTK-om, potvrđujući uspješnu autentifikaciju.

Iako je WPA2 puno sigurniji od svojih prethodnika, nije bez ranjivosti. Takozvani *Krack* napad otkriven je 2016. godine: uzastopnim poništavanjem *nonce*-a poslanog u trećem koraku WPA2 rukovanja, napadač može postupno uskladiti šifrirane pakete koje je prije vidio i saznati cijeli ključ koji se koristi za šifriranje prometa. Slabost se očituje u samom Wi-Fi standardu, a ne zbog pogrešaka u implementaciji, stoga je svaka ispravna implementacija WPA2 ranjiva.

U siječnju 2018. Wi-Fi Alliance najavio je ***Wi-Fi Protected Access 3*** **(WPA3)** kao zamjenu za WPA2.[16] TKIP nije dopušten u WPA3. Standard WPA3 također zamjenjuje PSK sa SAE-om (*Simultaneous Authentication of Equals*), što rezultira sigurnijom početnom

razmjenom ključeva. Kod SAE-a, ključevi nisu izloženi tijekom procesa rukovanja, smanjujući rizik od presretanja.

WPA3 također osigurava da se, čak i ako je ključ sesije ugrožen, ne može koristiti za dešifriranje prošlih komunikacija. To se postiže generiranjem jedinstvenog ključa za šifriranje za svaku sesiju, što sprječava napadače da dešifriraju prošli promet ako ključ dobiju kasnije.

Uvodi se i OWE (*Opportunistic Wireless Encryption*) za otvorene mreže, pružajući enkripciju za pristupne točke koje ne koriste zaporku.

3.2. BLUETOOTH

Bluetooth je bežična komunikacijska tehnologija dizajnirana da omogući razmjenu podataka kratkog dometa između uređaja na malim udaljenostima. Razvijen 1990-ih od strane Ericssona, Bluetooth je od tada postao globalni standard kojim upravlja *Bluetooth Special Interest Group* (SIG).

IEEE je standardizirao Bluetooth kao IEEE 802.15.1, ali više ne održava standard. Bluetooth SIG nadzire razvoj specifikacije i upravlja programom kvalifikacije. Proizvođač mora ispuniti standarde Bluetooth SIG-a da bi prodavao Bluetooth uređaj.[14] Od 2021. godišnje se isporučuje 4,7 milijardi Bluetooth čipova.[6]

Bluetooth tehnologija značajno se razvila od svog početka, sa svakom novom verzijom koja uvodi poboljšanja u brzini, dometu i energetskoj učinkovitosti.

Većina modernih pametnih telefona sadrži Bluetooth v4.0 čipset s integriranim Bluetooth Low Energy (LE) hardverom (više o njemu u naslovu 3.2.4.). Prvi mobilni uređaj s Bluetooth tehnologijom bio je Sony Ericsson R520m[27] (slika 10) koji se pojavio u prodaji početkom 2001. godine.

Slika 10 Sony Ericsson R520m.[26]

Bluetooth omogućuje jednostavno povezivanje pametnog telefona s bežičnim slušalicama, zvučnicima, pametnim satovima i drugim dodacima. Također podržava značajke poput dijeljenja datoteka između uređaja i povezivanja sa sustavima automobila za telefoniranje bez upotrebe ruku.

3.2.1. Princip rada Bluetootha

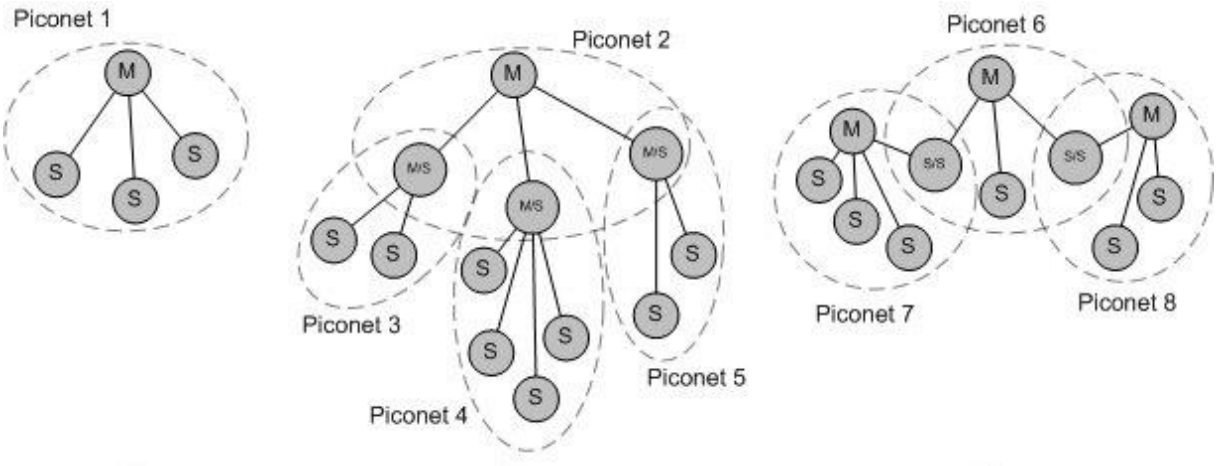
Kao i svaka druga bežična komunikacijska tehnologija, Bluetooth funkcionira slanjem i primanjem podataka uz pomoć Bluetooth adaptera. Funkcija Bluetooth adaptera je slanje i primanje podataka unutar definiranih dometa. Ako su u dometu, mogu komunicirati kroz proces poznat kao uparivanje.

Kada dva uređaja traže jedan drugog za uparivanje, oni traže zajedničku frekvenciju preko koje mogu slati i primati podatke. Koriste radiovalove u ISM opsezima, od 2,402 GHz do 2,48 GHz.[15] Nakon što se otkrije zajednička frekvencija, uređaji mogu slati i primati potrebne podatke. Jedna od prednosti Bluetooth veze je da dva uređaja ne ometaju druge uređaje, čemu pridonosi tehnika skakanja frekvencija (eng. *frequency hopping*), gdje se brzo mijenja frekvencija tijekom prijenosa podataka. Uz to, Bluetooth koristi kraće podatkovne pakete od ostalih standarda, što omogućuje bržu i sigurniju komunikaciju.

Skakanje frekvencija znači da nakon što uređaj pošalje ili primi podatkovni paket, on zajedno s uređajem s kojim komunicira prelazi na drugu frekvenciju za slanje sljedećeg paketa.

Ovaj postupak pomaže u postizanju maksimalne iskorištenosti cijelog ISM pojasa, smanjujući smetnje i osiguravajući osnovnu razinu sigurnosti te se smanjuje mogućnost prisluškivanja.

Jedna od prednosti Bluetooth veze je ta što nije ograničena na samo dva uređaja istovremeno, što znači da više uređaja može slati i primati podatke istovremeno na istom kanalu. Kada se to dogodi, uspostavlja se mala mreža, a takva formirana veza između elektroničkih uređaja naziva se *pikonet* , što je prikazano na Slici 11. U pikonetu mora postojati više od dva uređaja, ali ne više od sedam uređaja. Koristi arhitekturu glavni/podređeni (eng. *master/slave*), u kojoj jedan od uređaja djeluje kao glavni. Glavni uređaj kontrolira komunikaciju između ostalih podređenih uređaja.



Slika 11 Bluetooth mrežne strukture; pikonet.[16]

3.2.2. Bluetooth protokoli

Stog Bluetooth protokola kombinacija je softverske ili hardverske implementacije originalnog protokola. Temeljne protokole karakterizira Bluetooth SIG, a dodatni su usvojeni od treće strane.

Osnovni Bluetooth protokoli su Bluetooth radio, *baseband*, LMP (*Link Management Protocol*), L2CAP (*Logical link Control and Adaptation Protocol*) i SDP (*Service Discovery Protocol*) te predstavljaju temeljne tehnologije koje omogućuju Bluetooth komunikaciju između uređaja. Ovi su protokoli odgovorni za upravljanje otkrivanjem uređaja, postavljanje veze, razmjenu podataka i osiguravanje da Bluetooth uređaji mogu komunicirati učinkovito i pouzdano.

Bluetooth radio protokol je fizičkog sloja kojim se ostvaruje komunikacija između uređaja. Definira frekvenciju brojanja, zračno sučelje, shemu modulacije, frekvencijsko skakanje i kontrolu prijenosa.[24]

Baseband definira format okvira paketa, adresiranje, vrijeme i kontrolu napajanja.[24]

LMP uspostavlja i nadzire vezu između Bluetooth uređaja uključujući sigurnosne mjere kao što su autentifikacija i enkripcija, te kontrolu i raspored veličine paketa osnovnog pojasa.[24]

L2CAP povezuje gornji sloj sa slojem osnovnog pojasa.[24] Ima dva načina rada: ERMT (*Enhanced Retransmission Mode*) koji uključuje retransmisiju na L2CAP kanalu i SM (*Streaming Mode*) koji je jednostavniji način rada bez retransmisije i provjere toka.

SDP omogućuje uređajima otkrivanje usluga koje podržavaju drugi uređaji kao i parametara potrebnih za povezivanje s njima. Svaka usluga označena je s jedinstvenom UUID (*Universally Unique Identifier*) oznakom.[25]

Protokol koji se koristio za nadzor telefonije je **TCS BIN** (*Telephony Control Protocol-Binary*). Ovaj protokol definira signalizaciju kontrole poziva za uspostavu glasovnih i podatkovnih poziva između Bluetooth uređaja. TCS-BIN uglavnom je zastario jer je dizajniran za telefonske usluge s komutacijom kanala preko Bluetootha te ga novi mobilni uređaji ne koriste.

3.2.3. Ranjivosti Bluetooth-a

Unatoč brojnim prednostima Bluetootha, postoji i nekoliko rizika. Kako bi se oni ublažili, Bluetooth sigurnosna arhitektura mora se redovito ažurirati. Kao i drugi bežični komunikacijski sustavi, Bluetooth prijenosi mogu biti presretnuti.

Trenutno i akademska zajednica i industrija aktivno istražuju načine poboljšanja sigurnosti Bluetootha. Uobičajeni sigurnosni rizici uključuju otkrivanje i napade na privatnost, koji mogu otkriti povjerljive podatke, čineći ih posebno štetnima. S druge strane, napadi uskraćivanjem usluge (DoS) općenito ometaju Bluetooth mreže i smatraju se manje opasnima.

Bluesnarfing je neovlašteni pristup informacijama s bežičnog uređaja putem Bluetooth veze. To omogućuje pristup popisima kontakata, e-pošti i tekstualnim porukama, a mogu i kopirati slike i privatne videozapise.

Bluesnarfing iskorištava ranjivosti u protokolu za razmjenu objekata (*OBject Exchange*, OBEX) koji se koristi za komunikaciju Bluetooth uređaja i jedan je od usvojenih Bluetooth protokola. Nakon što se identificira ranjivi uređaj, hakeri uspostavljaju vezu i koriste Bluesnarfing alate za izdvajanje podataka. Ovi alati omogućuju napadačima pristup osjetljivim informacijama s kompromitiranih uređaja.

Svaki uređaj s uključenom Bluetooth vezom i postavljenom na "vidljiv" (mogu ga pronaći drugi Bluetooth uređaji u dometu) može biti osjetljiv na Bluesnarfing. Isključivanjem ove značajke potencijalna žrtva može biti sigurnija; iako uređaj koji je postavljen na "skriven" može biti napadnut pogađanjem MAC adrese uređaja. Kao i kod svih *brute force* napada, glavna prepreka ovom pristupu je sam broj mogućih MAC adresa. Bluetooth koristi 48-bitnu jedinstvenu MAC adresu, od kojih su prva 24 bita zajednička proizvođaču.[28] Preostala 24 bita imaju približno 16,8 milijuna mogućih kombinacija, što zahtijeva prosječno 8,4 milijuna pokušaja.

Kod mobilnih uređaja ova vrsta napada često se koristi za ciljanje IMEI-a. Pristup tome omogućuje napadačima preusmjeravanje dolaznih poziva i poruka na drugi uređaj bez znanja korisnika.

BlueBorne napad ranjivost je koju su otkrili sigurnosni istraživači *u Armis Labs*-u u rujnu 2017. Ovaj napad utječe na širok raspon uređaja s omogućenim Bluetoothom, uključujući pametne telefone, prijenosna računala i IoT uređaje, bez obzira na njihov operativni sustav. BlueBorne iskorištava slabosti u nizu Bluetooth protokola, omogućujući napadačima preuzimanje kontrole nad uređajima, krađu podataka ili širenje zlonamjernog softvera, sve to bez ikakve interakcije korisnika ili potrebe za uparivanjem.

Pronađene su ranjivosti u Bluetooth kodu na platformama Android, iOS, Linux i Windows. Ranjivosti pronađene na Androidu i iOS-u:

- Ranjivost curenja Android informacija - CVE-2017-0785[29]
- Android RCE (*Remote Code Execution*) ranjivost #1 - CVE-2017-0781[30]
- Android RCE ranjivost #2 - CVE-2017-0782[31]
- Bluetooth Pineapple u Androidu - Logički nedostatak CVE-2017-0783[32]

- Apple Low Energy Audio Protocol RCE ranjivost - CVE-2017-14315[33]

Ranjivosti su mješavina ranjivosti curenja informacija, ranjivosti daljinskog izvršavanja koda ili ranjivosti logičkih nedostataka. Ranjivost Apple iOS-a CVE-2017-14315 bila je ranjivost daljinskog izvršavanja koda zbog implementacije LEAP-a (*Low Energy Audio Protocol*). Velika audio naredba mogla se poslati ciljanom uređaju i dovesti do prelijevanja hrpe (*heap*-a) s podacima koje kontrolira napadač. Budući da audio naredbe poslane putem LEAP-a nisu ispravno provjerene, napadač može koristiti ovo prekoračenje kako bi dobio potpunu kontrolu nad uređajem kroz relativno visoke privilegije u iOS-u. Napad zaobilazi kontrolu pristupa Bluetoothu, međutim Bluetooth na mobilnom uređaju mora biti uključen.

3.2.4. Bluetooth verzije

Od svog početka, Bluetooth tehnologija je evoluirala kroz više verzija, a svaka je uvela nove značajke i poboljšanja.

Prva verzija Bluetooth-a započela je Bluetooth-om 1.0 i 1.0b 1999. godine. Ove početne verzije suočavale su se s brojnim problemima koji su ometali sposobnost proizvođača da stvore interoperabilne proizvode. Značajan izazov bio je taj što anonimnost nije bila moguća.

Bluetooth 1.1, objavljen 2001. godine, riješio je nekoliko problema iz ranijih verzija. Glavno poboljšanje bili su poboljšani procesi autentifikacije, koji su osigurali pouzdanije generiranje ključeva i uspostavljanje veze. Ova je verzija također uvela podršku za indikaciju jačine primljenog signala (RSSI, *Received Signal Strength Indicator*), koji je poboljšao uparivanje uređaja i stabilnost veze.

Izdan 2003. godine, Bluetooth 1.2 donio je značajan napredak u odnosu na svoje prethodnike i zadržao kompatibilnost s Bluetoothom 1.1. Značajna poboljšanja uključuju eSCO (*Extended Synchronous Connections*) koji poboljšava kvalitetu zvuka audio veza dopuštajući ponovni prijenos oštećenih paketa, podršku za HCI (Host Controller Interface) koji omogućuje bolju kontrolu i upravljanje Bluetooth uređajima, te veću brzinu prijenosa.[18]

Druga verzija, Bluetooth 2.0, objavljena je 2004. godine. Glavno poboljšanje bilo je uvođenje EDR-a (*Enhanced Data Rate*), koji je povećao brzinu prijenosa na 2,1 Mbit/s i smanjilo potrošnju energije smanjenjem radnog ciklusa.

Otprilike tri godine kasnije, Bluetooth 2.1 je objavljen. Glavna značajka v2.1 je sigurno jednostavno uparivanje (SSP, *Secure Simple Pairing)* koji poboljšava uparivanje Bluetooth uređaja, dok povećava sigurnost.[19] Verzija 2.1 također donosi EIR (*Extended Inquiry Response*) koji pruža više informacija tijekom postupka upita kako bi se omogućilo bolje filtriranje uređaja prije povezivanja i tzv. *sniff subrating*, koji smanjuje potrošnju energije u načinu rada niske potrošnje.

Verzija 3.0 usvojena je 2009. godine. Bluetooth 3.0 pruža teoretske brzine prijenosa podataka do 24 Mbit/s, ali ne preko same Bluetooth veze. Umjesto toga, Bluetooth se koristi za uspostavljanje veze, a promet visoke brzine prijenosa podataka prenosi se preko 802.11 veze (naslov 3.1.). Ova brzina ipak nije usvojena u mobilne uređaje. Glavna nova značajka je AMP (*Alternative MAC/PHY*), dodatak 802.11 koji služi za prijenos pri većim brzinama. UCD (*Unicast Connectionless Data*) još je jedna značajka Bluetootha 3.0. UCD omogućuje slanje kratkih nizova podataka bez potrebe za uspostavljanjem potpune veze. Ova značajka je korisna za senzore gdje su kratki, rijetki prijenosi podataka uobičajeni.

Četvrta verzija Bluetooth-a uključuje tri glavne revizije: verziju 4.0, verziju 4.1 i verziju 4.2. Bluetooth 4.0 uveden je 2010. godine. Najznačajniji dodatak je BLE (*Bluetooth Low* Energy). BLE je dizajniran kako bi omogućio uređajima da prijeđu u stanje mirovanja ili nisku potrošnju energije kada se ne koriste, čime se značajno štedi trajanje baterije. Ova je značajka posebno pridonosila mobilnim uređajima.

Bluetooth 4.1, uveden 2013. godine, donio je dodatna poboljšanja, posebice u upravljanju vezama. Uređaji su se tako mogli automatski ponovno povezati čak i nakon što izađu iz dometa i vrate se, eliminirajući potrebu za ručnim ponovnim povezivanjem od strane korisnika.

Bluetooth 4.2 izašao je 2014. godine i bio je usmjeren na poboljšanje brzine i učinkovitosti. U ovoj verziji kapacitet Bluetooth paketa povećan je gotovo 10 puta u usporedbi s prethodnom verzijom (s 27 bajtova na 251 bajt).[20]

Bluetooth 5 objavljen je 2016. godine. Njegove nove značajke uglavnom su usmjerene na IoT. Počevši s ovom verzijom, izbacuje se nula iza decimalne točke, te se piše samo „Bluetooth 5“ (za razliku od Bluetootha 4.0).[21] Bluetooth 5 pruža opcije koje mogu udvostručiti brzinu prijenosa podataka nauštrb dometa ili pružiti do četiri puta veći domet nauštrb brzine prijenosa podataka.

2019. godine izlaze Bluetooth 5.1 i 5.2 sa značajkama koje se koriste za lociranje uređaja u prostoru (poput AoA-a, *Angle of Arrival*) i dodatnim poboljšanima za *low energy* odnosno način rada u mirovanju. Bluetooth 5.3. izašao je 2021. godine, a zadnja verzija, Bluetooth 5.4, 2023. godine.

Tablica 1 pruža usporedbu različitih verzija Bluetootha (1 do 5) na temelju njihove brzine, energetske učinkovitosti, brzine prijenosa podataka i dometa.

Bluetooth verzija	EDR	*Low energy* (LS)	Brzina	Domet
1	✗	✗	1 Mb/s	10 m
2	✓	✗	2 Mb/s	30 m
3	✓	✗	24 Mb/s	30 m
4	✓	✓	2 Mb/s	60 m
5	✓	✓	2Mb/s	200 m

Tablica 1 Razlike između Bluetooth verzija.[23]

3.3. NEAR-FIELD COMMUNICATION

Near-Field Communication (NFC) tehnologija je bežične komunikacije kratkog dometa koja omogućuje razmjenu podataka između uređaja unutar neposredne blizine, obično nekoliko centimetara. U početku razvijen iz sustava radiofrekvencijske identifikacije (RFID, *Radio-frequency identification),* NFC je svoju najširu primjenu pronašao u pametnim telefonima; najčešće uporabe NFC-a uključuju beskontaktne transakcije.

RFID koristi elektromagnetska polja za automatsku identifikaciju. RFID sustav sastoji se od radio transpondera malih dimenzija koji se naziva tag, antene i kontrolora koji upravlja komunikacijom antene. Kada se pokrene elektromagnetskim ispitnim impulsom, tag odašilje podatke u digitalnom formatu.

NFC standardi pokrivaju komunikacijske protokole i formate razmjene podataka i temelje se na postojećim standardima RFID-a. Standardi uključuju i one koje je definirao *NFC Forum,* neprofitna industrijska udruga koju su 2004. godine osnovali *NXP Semiconductors, Sony* i *Nokia* kako bi unaprijedili korištenje NFC bežične interakcije u potrošačkoj elektronici, mobilnim uređajima i računalima.

3.3.1. Princip rada NFC-a

NFC komunikacija u jednom ili oba smjera koristi frekvenciju od 13,56 MHz u ISM pojasu pri brzinama prijenosa podataka u rasponu od 106 do 848 kbit/s. NFC interakcije uvijek uključuju dva uređaja: jedan od njih (inicijator) generira radiofrekvencijsko (RF) polje koje može napajati drugi uređaj koji može biti i bez unutarnjeg napajanja, poput naljepnica, privjesaka za ključeve i bankovnih kartica.

NFC oznake pohranjuju podatke i obično su samo za čitanje, iako se u određenim slučajevima mogu pisati. Oznake mogu biti unaprijed kodirane od strane proizvođača ili programirane prema specifikacijama *NFC Foruma*.

NFC tehnologija funkcionira koristeći induktivnu spregu između dvije obližnje antene, tvoreći transformator. Budući da je udaljenost između dva uređaja vrlo mala u usporedbi s valnom duljinom radio valova koji se koriste, ova interakcija odvija se unutar bliskog polja (*near field*). Primarni mehanizam spajanja je izmjenično magnetsko polje, s minimalnom energijom koja se zrači kao elektromagnetski valovi. Ovaj dizajn pomaže u smanjenju smetnji

s radiokomunikacijama koje rade na istoj frekvenciji i s drugim NFC uređajima izvan predviđenog dometa.

Dok teoretski maksimalni domet komunikacije sa standardnim antenama i tipičnim razinama snage može biti do 20 cm, u praksi NFC uređaji obično komuniciraju na udaljenostima ne većim od 10 cm. Važno je napomenuti da metalne površine u blizini oznaka mogu prigušiti magnetsko polje, zbog čega je potrebno minimalno odvajanje od takvih površina kako bi se osigurala pravilna funkcionalnost.

Komunikacija između dva uređaja može biti pasivna i aktivna. U pasivnom načinu rada inicijator generira polje nositelja, a pasivni ciljni uređaj komunicira modulirajući ovo polje. U ovom načinu rada ciljni uređaj može crpiti svoju snagu iz magnetskog polja koje stvara inicijator. U aktivnom načinu rada i inicijator i ciljni uređaj naizmjenično generiraju vlastita polja za komunikaciju. U tom slučaju oba uređaja moraju imati vlastita napajanja.

NFC uređaji koriste različite sheme modulacije i kodiranja ovisno o brzini prijenosa podataka:

- 424 kbit/s i 212 kbit/s: i aktivni i pasivni uređaji koriste Manchester kodiranje s 10% modulacijom pomaka amplitude (ASK).
- 106 kbit/s: aktivni uređaji koriste modificirano Millerovo kodiranje sa 100% ASK, dok pasivni uređaji koriste Manchester kodiranje s 10% ASK modulacijom.

Uređaji s NFC-om mogu raditi u tri glavna načina:

- Način rada emuliranjem kartice: Ovaj način rada omogućuje uređajima s omogućenom NFC-om, poput pametnih telefona, da funkcioniraju kao pametne kartice, omogućujući transakcije poput plaćanja. U ovom načinu rada uređaji mogu oponašati ponašanje beskontaktnih kartica.
- Način čitanja/pisanja: U ovom načinu rada NFC uređaji mogu čitati podatke s NFC oznaka ugrađenih u naljepnice ili druge objekte. Uređaji također mogu pisati u NFC oznake, ovisno o konfiguraciji oznake.
- Peer-to-Peer način rada: Ovaj način rada omogućuje izravnu komunikaciju između dva uređaja s omogućenom NFC-om, razmjenjujući podatke kao što su kontakti, datoteke ili mediji. Oba uređaja moraju imati napajanje da bi se mogla odvijati peer-to-peer komunikacija.

NFC omogućuje i bežično punjenje. *NFC Forum* razvio je specifikaciju bežičnog punjenja, poznatu kao NFC bežično punjenje (WLC, eng. NFC *Wireless Charging*), koja omogućuje punjenje uređaja s do 1 W snage na udaljenosti do 2 cm[34]. Ta je mogućnost posebno pogodna za manje uređaje poput slušalica; za mobilne uređaje ta snaga ipak je nedostatna. U usporedbi s poznatijim Qi standardom bežičnog punjenja od strane *Wireless Power Consortium*-a, koji nudi do 15 W snage na udaljenosti do 4 cm, NFC WLC pruža manju izlaznu snagu, ali ima koristi od znatno manje veličine antene.[34]

3.3.2. Sigurnosne ranjivosti NFC-a

Iako je domet NFC-a ograničen na nekoliko centimetara, standardni obični NFC nije zaštićen od prisluškivanja i može biti osjetljiv na izmjene podataka.

RF signal za bežični prijenos podataka može se uhvatiti specijaliziranim antenama podešenim za hvatanje frekvencije od 13,56 MHz na kojoj radi NFC. Udaljenost s koje napadač može prisluškivati RF signal ovisi o više parametara, ali je obično manja od 10 metara.[35] Također, na prisluškivanje jako utječe način komunikacije. Pasivni uređaj koji ne stvara vlastito RF polje puno je teže prisluškivati nego aktivni uređaj. Napadač obično može prisluškivati unutar 10 m od aktivnog uređaja i 1 m za pasivne uređaje.[36]

Osim pasivnog slušanja, napadač može pokušati modificirati podatke koji se prenose putem NFC sučelja. Jednostavan oblik ovoga je korupcija podataka, gdje napadač ima za cilj poremetiti komunikaciju tako da uređaj koji prima ne može razumjeti poslane podatke.

Korupcija podataka može se postići odašiljanjem valjanih frekvencija unutar spektra podataka u točno određeno vrijeme. Napadač može izračunati ovo vrijeme ako dobro razumije shemu modulacije i kodiranje koje koriste NFC uređaji. Iako je ovaj napad relativno jednostavan, on ne dopušta napadaču da promijeni stvarne podatke koji se prenose. Umjesto toga, to je u biti napad uskraćivanja usluge (DoS) usmjeren na sprječavanje uspješne komunikacije.

Relejni napad uključuje napadača koji presreće i prenosi komunikaciju između dva uređaja s omogućenom NFC-om. U sustavu bezgotovinskog plaćanja, recimo, ako napadač izgradi par uređaja koji bežično prenose komunikaciju između terminala za plaćanje i kartice, imao bi mogućnost obavljanja plaćanja karticom koja nije u njihovom fizičkom posjedu. Ova

vrsta napada iskorištava povjerenje u NFC komunikacijsku blizinu, omogućujući lažne transakcije bez znanja korisnika. Relejni napadi posebno su zabrinjavajući jer zaobilaze potrebu da napadač probije enkripciju ili druge sigurnosne protokole.

3.3.3. Usporedba NFC-a, Bluetooth-a i WiFi-a

NFC, WiFi i Bluetooth komunikacijske su tehnologije kratkog dometa koje se koriste u mobilnim telefonima. Iako NFC radi manjim brzinama i ima kraći domet u usporedbi s WiFi-em i Bluetooth-om, troši manje energije i ne zahtijeva uparivanje.

NFC uspostavlja veze brže od standardnog Bluetootha i WiFi-a; potrebno mu je manje od 0,1 sekunde, u usporedbi s vremenom postavljanja Bluetootha od 6 sekundi ili još dužim vremenom postavljanja WiFi-a. Bluetooth zahtijeva od korisnika ručno postavljanje veza između pametnih telefona, kao i WiFi, dok se NFC povezuje automatski. Iako korisnici moraju biti blizu jedan drugome da bi koristili NFC tehnologiju, nju je brže i lakše uspostaviti od preostale dvije.

Dok je maksimalna brzina prijenosa NFC-a 424 kbit/s, Bluetooth nudi značajno veću brzinu (2 Mb/s za u slučaju Bluetooth-a 5), što ga čini praktičnijim izborom za prijenos većih količina podataka. Isto vrijedi i za WiFi s brzinama do 9.6 Gbit/s (WiFi 6)

Ograničeni domet NFC-a od otprilike 4 cm smanjuje šanse za neželjeno prisluškivanje i presretanje prometa.

NFC je kompatibilan s postojećim pasivnim RFID infrastrukturama. Troši puno manje energije od standardnog Bluetootha i WiFi-a; usporediv je s *Bluetooth Low Energy*-em (BLE). Međutim, kada NFC komunicira s nenapajanim uređajima (npr. beskontaktne kartice), njegova se potrošnja energije povećava jer mu je potrebna dodatna energija za napajanje pasivnog taga.[37]

Wi-Fi, Bluetooth i NFC imaju različite uloge u pametnim telefonima. Wi-Fi se pokazao najboljim za brzi pristup internetu i velike prijenose datoteka, nudi povezivost velikog dometa i veliku propusnost, ali troši više energije i zahtijeva postavljanje mreže.

Bluetooth je, s druge strane, dizajniran za veze kraćeg dometa i obično se koristi za periferne uređaje poput slušalica, zvučnika i pametnih satova. Nudi umjerene brzine prijenosa podataka, ali je energetski učinkovitiji od Wi-Fi-ja, uz jednostavan postupak uparivanja.

NFC je najspecijaliziraniji od spomenute tri tehnologije, radi na vrlo malim udaljenostima (nekoliko centimetara), što ga čini pogodnim za beskontaktna plaćanja i brzu razmjenu podataka između uređaja bez potrebe za ručnim uparivanjem. NFC ima malu potrošnju energije, ali vrlo ograničen domet i mogućnosti prijenosa podataka u usporedbi s Bluetoothom i Wi-Fi-em.

Usporedbe te triju tehnologija sumirane su u tablici 2.

Značajka	**Bluetooth**	**NFC**	**WiFi**
Domet	10-200 m	4 cm	10-100 m
Brzina	2 Mbit/s	424 Kbit/s	9.6 Gbit/s
Potrošnja energije	<1 mW	0.1 – 0.5 mW (tijekom komunikacije)	0.5 – 3 W
Vrsta veze	*Point-to-point* ili *multipoin*	*Point-to-point*	*Multipoint*
Uparivanje	Zahtijeva	Ne zahtijeva (automatski)	Zahtijeva
Uobičajene uporabe	Audio *streaming*, dijeljenje datoteka, povezivanje s perifernim uređajima	Mobilna plaćanja	Pristup internetu, *streaming*, dijeljenje datoteka, pristupna točka

Tablica 2 Usporedba Bluetooth, NFC i WiFi tehnologija

4. ZAKLJUČAK

Put od 1G do 5G predstavlja duboku transformaciju u načinu na koji komuniciramo. Svaka generacija uvela je nove mogućnosti i poboljšanja, rješavajući rastuće zahtjeve tržišta za brzinom, učinkovitošću i pouzdanošću. Evolucija WiFi-ja, Bluetootha i NFC-a omogućila je integraciju pametnih telefona u različite sustave. Napredovanje WiFi, Bluetooth i NFC standarda uključuje poboljšanja u bežičnom povezivanju mobilnih uređaja, koji sve češće postaju i višenamjenski.

Razvoj ovih standarda nužno uvjetuje poboljšanja njihovih sigurnosti i ranjivosti, što iziskuje stalni oprez i poboljšanje mjera za zaštitu od potencijalnih prijetnji. Razumijevanje i ublažavanje ovih ranjivosti ključno je za zaštitu osjetljivih informacija.

Tijekom budućeg razvoja protokola pametnih telefona, uključujući i napredovanje prema 6G mreži, ključno je uvažavati dosadašnje tehnologije i kompatibilnost unatrag. Zbog sve bržeg razvoja IoT tehnologije, koja je usko povezana s protokolima pametnih uređaja, vrlo je teško predvidjeti njihove buduće smjerove.

LITERATURA

[1] *The evolution of mobile communications: Moving from 1G to 5G, and from human-to-human to machine-to-machine communications*, Panagiota D. Giotopoulou, 2015.

[2] https://www.cisco.com/c/en/us/products/ios-nx-os-software/quality-of-serviceqos/index.html(15.9.2024)

[3] *From 1G to 5G*, Henri Hodaraa i Edvin Skaljo, 2021.

[4] *What is 5G, and how fast will it be?* Hoffman Chris, 2019.

[5] *Budućnost mobilnih komunikacija i izazovi normizacije*, ms. Sc. Branko Burazer

[6] *Recent US regulatory decisions on civil uses of spread spectrum*, Marcus M.J., 1985.

[7] *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, 1997., https://ieeexplore.ieee.org/document/654749

[8]. *New High Rate Wireless LAN Standards*, Van Nee Richard; Awater Geert; Morikura Masahiro; Takanashi Hitoshi; Webster Mark; Halford Karen, 1999., IEEE Communications Magazine.

[9] *Wi-Fi Alliance introduces Wi-Fi 6, https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-6*

[10] *Wi-Fi 6E expands Wi-Fi® into 6 GHz*, https://www.wi-fi.org/wi-fi-download/36822

[11], "*A Survey on Secure Communication Protocols for IoT Systems*, D. Dragomir, L. Gheorghe, S. Costea and A. Radovici, 2016., International Workshop on Secure Internet of Things (SIoT)

[12] *WPA2 Security Now Mandatory for Wi-Fi CERTIFIED Products*, https://www.wi-fi.org/news-events/newsroom/wpa2-security-now-mandatory-for-wi-fi-certified-products

[13] *Wi-Fi Alliance Launches WPA2 Enhancements and Debuts WPA3*, Dawn Kawamoto, https://www.darkreading.com/endpoint/wi-fi-alliance-launches-wpa2-enhancements-and-debuts-wpa3/d/d-id/1330762

[14] *Brand Enforcement Program, https://www.bluetooth.com/develop-with-bluetooth/marketing-branding/brand-enforcement-program/*

[15] *Networking A to Z*, Muller Nathan J., 2002., https://books.google.hr/books?id=0qv4KbasX7wC&q=bluetooth&pg=PA45&redir_esc=y#v=snippet&q=bluetooth&f=false

[16] *Innovative techniques for extending the range and node limits in Bluetooth based wireless sensor networks*, https://www.researchgate.net/figure/Bluetooth-network-structures-a-single-Piconet-structure-b-master-slave-bridging_fig2_29462775 (28.6.2024)

[17] *5G - the policy forum at at&t*, https://policyforum.att.com/innovation/5g/

[18] *Specifications*, http://bluetooth.50webs.com/bluetooth1_and_1.0b.html

[19] *Simple Pairing* Whitepaper, https://web.archive.org/web/20061018032605/http://www.bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf

[20] *Understanding Bluetooth 4.1, 4.2, and Beyond*, https://community.silabs.com/s/share/a5U1M000000knuTUAQ/understanding-bluetooth-41-42-and-beyond?language=en_US

[21] *Bluetooth 5 Promises Four times the Range, Twice the Speed of Bluetooth 4.0 LE Transmissions*, https://www.cnx-software.com/2016/06/10/bluetooth-5-promises-four-times-the-speed-twice-the-range-of-bluetooth-4-0-le-transmissions/

[22] *Osnove Arhitekture Mreža*, Alen Bažant i dr., 2004.

[23] *Bluetooth versions*, 2017., https://www.rtings.com/headphones/learn/bluetooth-versions-comparison-profiles (12.9.2024)

[24] moumita, 2020., https://www.tutorialspoint.com/thebluetooth-protocol-stack.

[25] https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2009-11- 281.pdf

[26] https://www.mobilephonemuseum.com/phone-detail/r520m

[27] https://en.wikipedia.org/wiki/Ericsson_T39

[28] *Bluetooth Security Review, Part 1*, Bialoglowy Marek, https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=4ac4d5c6-3bf1-4e66-acf0-6f07482cfae1&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[29] *https://nvd.nist.gov/vuln/detail/CVE-2017-0785* (15.9.2024.)

[30] https://nvd.nist.gov/vuln/detail/CVE-2017-0781, (15.9.2024.)

[31] https://nvd.nist.gov/vuln/detail/CVE-2017-0782, (15.9.2024.)

[32] https://nvd.nist.gov/vuln/detail/CVE-2017-0783, (15.9.2024.)

[33] https://nvd.nist.gov/vuln/detail/CVE-2017-14315, (15.9.2024.)

[34] https://nfc-forum.org/learn/use-cases/wireless-charging/

[35] *Eavesdropping Attacks on High-Frequency RFID Tokens*, G.P. Hancke

[36] *Security in Near Field Communication (NFC) Strengths and Weaknesses*, Ernst Haselsteiner, Klemens Breitfuß

[37] http://www.nearfieldcommunication.org/bluetooth.html

SAŽETAK

1G je uveden 1979. godine, prenosio je govor u analognom formatu uz lošu kvalitetu i mogućnost prisluškivanja. 2G je uveden 1991. s GSM standardom, omogućivši digitalizaciju glasa, bolju kvalitetu prijenosa, te nove usluge poput SMS-a i MMS-a. Tehnologija je koristila TDMA i CDMA za učinkovitiji prijenos podataka. 3G je razvijen 2000-ih i omogućavao je brzine prijenosa do 2 Mbps. 4G uveden 2011. godine (LTE-A) omogućavao je brzine do 1 Gbit/s za fiksne lokacije. Wi-Fi (IEEE 802.11 standard) omogućava bežično umrežavanje i povezuje milijarde uređaja s internetom. Wi-Fi je preferiran zbog većih brzina i nižih troškova, osobito u zatvorenim prostorima. Bluetooth tehnologija omogućava razmjenu podataka na kratkim udaljenostima. Razvijen je 1990-ih, a upravlja ga Bluetooth SIG. Najčešće se koristi za povezivanje pametnih telefona s bežičnim slušalicama, pametnim satovima i drugim uređajima. NFC omogućuje bežičnu komunikaciju na vrlo malim udaljenostima, obično nekoliko centimetara. Baziran na RFID-u, NFC se najčešće koristi za beskontaktne transakcije na pametnim telefonima.

Ključne riječi: 1G, 2G, 3G, 4G, 5G, TDMA, FDMA, CDMA, UMTS, LTE, Bluetooth, WiFi, NFC

ABSTRACT

1G was introduced in 1979, it transmitted speech in analog format with poor quality. 2G was introduced in 1991 with the GSM standard, digitalizing the voice, offering better transmission quality, and SMS and MMS. It used TDMA and CDMA for more efficient data transmission. 3G was developed in the 2000s and allowed transmission speeds of up to 2 Mbps. 4G introduced in 2011 enabled speeds of up to 1 Gbit/s for fixed locations. Wi-Fi connects billions of devices to the Internet. Wi-Fi is preferred due to higher speeds and lower costs. Bluetooth technology enables the exchange of data over short distances. It was developed in the 1990s. It is most often used to connect smartphones to wireless headphones and other devices. NFC enables wireless communication over short distances, usually a few centimetres. Based on RFID, NFC is most commonly used for contactless transactions on smartphones.

Keywords: 1G, 2G, 3G, 4G, 5G, TDMA, FDMA, CDMA, UMTS, LTE, Bluetooth, WiFi, NFC

ŽIVOTOPIS

Domagoj Smojver rođen je 23. rujna 2001. godine u Požegi. Pohađao je Osnovnu školu Ivan Goran Kovačić Velika, a nakon toga upisuje Tehničku školu Požega te stječe zvanje Tehničara za računalstvo. Od predškolske dobi pokazuje interes za informatikom. Maturirao je 2020. godine te upisuje stručni studij računarstva na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku.

Domagoj Smojver

_____