Bluetooth 5.0

Mišić, Josip

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:288469

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2025-03-21**

Repository / Repozitorij:

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Preddiplomski stručni studij Računarstva

BLUETOOTH 5.0

Završni rad

Josip Mišić

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:	Josip Mišić
Studij, smjer:	Stručni prijediplomski studij Računarstvo
Mat. br. pristupnika, god.	AR 4799, 27.07.2020.
JMBAG:	0165085094
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:	izv. prof. dr. sc. Višnja Križanović
Naslov završnog rada:	Bluetooth 5.0
Znanstvena grana završnog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rada:	Bluetooth je protokol za slanje i primanje podataka za kratke bežične prijenose između dvaju ili više elektroničkih uređaja male snage. Najčešće se koristi za povezivanje bežičnim putem između dva pametna telefona, ali isto tako i tehnoloških gadgeta. Inačica 5.0 donosi poboljšanja u odnosu na prošle verzije protokola. Zadatak je detaljno obraditi Bluetooth 5.0 protokol i potvrditi njegovu kompatibilnost "unatrag" s verzijom 4.0 te to praktično provjeriti putem dva pametna telefona.

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:	08.10.2024.
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:	08.10.2024.

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

IZJAVA O IZVORNOSTI RADA

Osijek, 08.10.2024.

Ime i prezime Pristupnika:	Josip Mišić
Studij:	Stručni prijediplomski studij Računarstvo
Mat. br. Pristupnika, godina upisa:	AR 4799, 27.07.2020.
Turnitin podudaranje [%]:	13

Ovom izjavom izjavljujem da je rad pod nazivom**: Bluetooth 5.0**

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 1
2. TEHNIČKE KARAKTERISTIKE BLUETOOTH TEHNOLOGIJA 2
2.1. Povijesni razvoj 2
2.2. Bluetooth protokoli 7
2.3. Karakteristike po verzijama Bluetooth-a 11
2.4. Uporaba Bluetooth tehnologije 13
2.5. Usporedba s drugim bežičnim tehnologijama 14
2.6. Sigurnost 15
2.7. Upravljanje ključevima 16
2.8. Kriptiranje 17
2.9. Autentikacija 18
2.10. Bluetooth napadi 19
2.11. Mobilni uređaji 23
2.12. Bluetooth u automobilskoj industriji 25
2.13. Prednosti i nedostaci Bluetooth-a 27
3. BLUETOOTH VERZIJA 5 29
4. SNIMANJE SIGNALIZACIJE 36
5. ZAKLJUČAK 40
LITERATURA 41
SAŽETAK 42
SUMMARY 43
ŽIVOTOPIS 44

1. UVOD

Bluetooth je bežična tehnologija iznimno kratkog dometa dizajnirana za omogućavanje komunikacije između uređaja. Namijenjena je povezivanju prijenosnih i/ili fiksnih elektroničkih uređaja i razvijena je 1994. godine. Uporabom hardvera i softvera, Bluetooth je postao pametna tehnologija za učinkovite i fleksibilne bežične komunikacijske sustave. Danas je Bluetooth tehnologija definirana standardom IEEE 802.15. IEEE 802.15 je skup standarda za bežične osobne mreže.

Namjena Bluetooth-a obuhvaća širok spektar uređaja, od različitih pametnih uređaja u kući (svjetla, sigurnosne kamere) preko različitih audio uređaja i periferije (bežične slušalice, tipkovnice, zvučnici) pa sve do zdravstva (telemedicina, rehabilitacijski uređaji).

Tehničke karakteristike Bluetooth tehnologije odnose se većinom na frekvencijske opsege, doseg, brzinu prijenosa podataka i sigurnost. U drugome dijelu ovoga rada detaljno su opisane karakteristike Bluetooth-a.

Svi Bluetooth uređaji su kompatibilni unazad. Svaka nova verzija Bluetooth-a donosi poboljšanja u brzini prijenosa, energetskoj učinkovitosti, sigurnosti i dodatnoj funkcionalnosti kako bi zadovoljila sve veće zahtjeve korisnika i razvijajućih tehnologija. Detaljan opis i usporedba pojedinih verzija opisana je u drugome dijelu ovoga rada.

U trećemu dijelu rada detaljno su opisane karakteristike Bluetooth verzije 5, a u četvrtom, praktičnom dijelu rada snimljena je signalizacija između dva Bluetooth uređaja.

2. TEHNIČKE KARAKTERISTIKE BLUETOOTH TEHNOLOGIJA

Bluetooth tehnologija koristi frekvencijske opsege od 2,402 GHz do 2,480 GHz za komunikaciju.

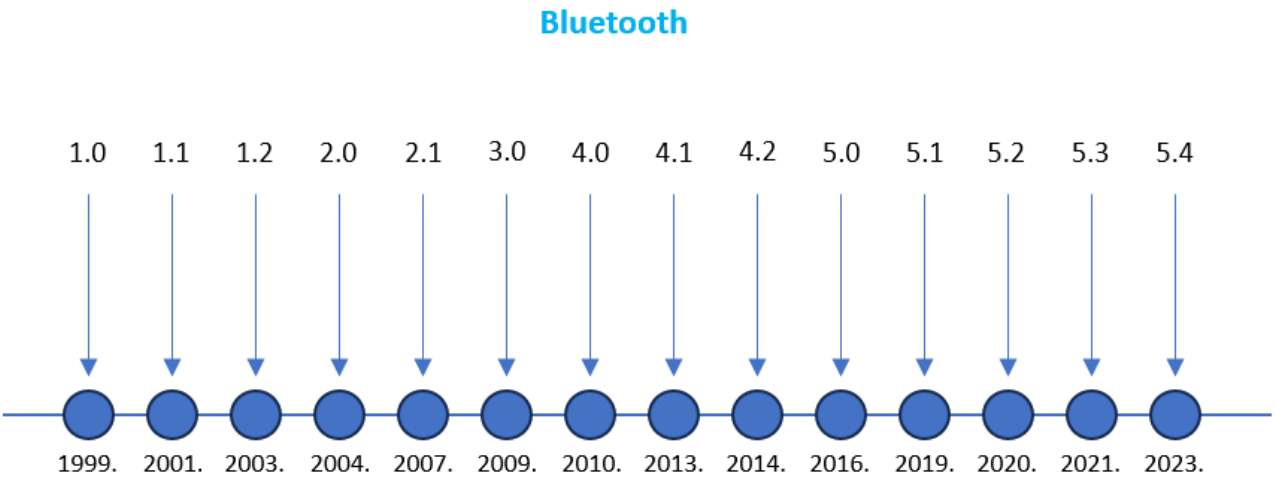
Razvitkom radijske tehnologije, dr. Jaap Haartsen dobio je zadatak od Ericssona da iskoristi ovu tehnologiju za povećanje upotrebljivosti mobilnih uređaja. [1]

Ubrzo nakon osnivanja SIG-a (*Special Interest Group*), neprofitne udruge koja se bavi proučavanjem i razvojem tehnoloških standarda, Jim Kardach nazvao je ovo rješenje 'Bluetooth' po danskom kralju koji je spojio Dansku i Norvešku. [1]

Komercijalna uporaba Bluetooth uređaja počela je 1999. godine razvojem bežičnih slušalica. Danas gotovo svaki pametni uređaj koristi Bluetooth tehnologiju. [1]

2.1. Povijesni razvoj

Bluetooth tehnologija prošla je nekoliko razvojnih faza u kojima je stalno bila poboljšavana. Razvojne faze Bluetooth-a prikazane su na slici 2.1. U svakoj verziji Bluetooth-a frekvencijski opseg je 2,4 GHz, a maksimalan broj uređaja je sedam. Detaljne tehničke karakteristike pojedinih verzija napisane su u tablici 2.1.



Slika 2.1. Prikaz povijesnog razvoja verzija Bluetooth-a po godinama.

Bluetooth 1.0:

Prva verzija Bluetootha objavljena je 1999. godine, a prvenstveno je bila usmjerena na bežičnu podatkovnu komunikaciju. Imala je mnogo problema s kompatibilnošću i povezivanjem uređaja. Implementacija tehnologije bila je zahtjevna, a povezivanje između uređaja nije uvijek bilo pouzdano. Maksimalna brzina prijenosa podataka je 721 kbps. Usluge uključuju osnovnu bežičnu komunikaciju za prijenos datoteka.

Bluetooth 1.1:

Godine 2001. predstavljen je Bluetooth 1.1, koji je dodao podršku za osnovne audio mogućnosti koje se nazivaju Bluetooth *Headset Profile* (HSP) i *Hands-Free Profile* (HFP). To su Bluetooth profili koji omogućuju specifične funkcionalnosti za bežičnu komunikaciju između uređaja, najčešće za prijenos zvuka, osobito u *hands-free* okruženjima kao što su automobili ili bežične slušalice. Riješeni su ključni problemi iz verzije 1.0. Dodana je podrška za kvalitetu usluge što je poboljšalo stabilnost veze. Verzija je postala službeni IEEE standard (802.15.1). Maksimalna brzina je 721 kbps. Ima širu upotrebu u mobilnim telefonima, laptopima, bežičnim perifernim uređajima.

Bluetooth 1.2:

Objavljen 2003. godine, Bluetooth 1.2 uveo je *Advanced Audio Distribution Profile* (A2DP). To je Bluetooth profil koji omogućuje bežični prijenos visoko kvalitetnog audio sadržaja između dva uređaja putem Bluetooth veze. Primarno je dizajniran za slanje stereo audio signala iz izvora (primjerice pametnog telefona ili računala) prema uređaju za reprodukciju zvuka (primjerice bežičnim slušalicama). Uveden je *Adaptive Frequency Hopping* (AFH). AFH je tehnologija koja se koristi u Bluetooth tehnologiji kako bi se smanjila interferencija s drugim bežičnim tehnologijama poput Wi-Fi mreža tako što se signal konstantno mijenja između frekvencija unutar 2,4 GHz opsega. Poboljšana je brzina uparivanja uređaja i stabilnost veze. Maksimalna brzina prijenosa je 1 Mbps.

Bluetooth 2.0:

Godine 2004. predstavljen je Bluetooth 2.0, s poboljšanim brzinama prijenosa podataka (do 3 Mbps). Razvijena je i podrška za *Audio/Video Remote Control Profile* (AVRCP). AVRCP je Bluetooth profil za daljinsko upravljanje audio ili video uređajima putem Bluetooth veze. To znači da se može koristiti jedan uređaj, poput pametnog telefona, za daljinsko upravljanje

funkcijama reprodukcije na drugom uređaju, poput Bluetooth zvučnika ili bežičnih slušalica. Ova verzija donosi značajno povećanje brzine prijenosa podataka zahvaljujući *Enhanced Data Rate* (EDR) tehnologiji. Glavna svrha ove tehnologije je poboljšanje performansi bežičnih komunikacija kroz povećanje brzine prijenosa podataka i smanjenje potrošnje energije.

Bluetooth 2.1:

Izdan 2007., Bluetooth 2.1 uključivao je sigurnosno poboljšanje. Implementiran je mehanizam sigurnog jednostavnog uparivanja SSP (*Secure Simple Pairing*). SSP tehnologija omogućuje lakše, brže i sigurnije povezivanje Bluetooth uređaja bez potrebe za unosom dugih kodova ili PIN-ova. Ovo je omogućilo lakše povezivanje bez ugrožavanja sigurnosti. Brzina prijenosa podataka nije se mijenjala.

Bluetooth 3.0:

Godine 2009. predstavljen je Bluetooth 3.0, koji uključuje novu značajku pod nazivom Bluetooth velike brzine (HS – *High Speed*). Ova je značajka omogućila Bluetooth uređajima da iskoriste Wi-Fi za brži prijenos podataka (do 24 Mbps), primarno ciljajući na prijenos datoteka, dok je Bluetooth služio za upravljanje vezom. Frekvencijski opseg za Bluetooth je 2.4 GHz, a 5 GHz za Wi-Fi kod velikih brzina.

Bluetooth 4.0:

Godine 2010. izdan je Bluetooth 4.0, uvodeći Bluetooth *Low Energy* (LE) tehnologiju. Bluetooth LE je verzija Bluetooth tehnologije koja je dizajnirana za uređaje koji zahtijevaju povremenu komunikaciju, nisku potrošnju energije i dugotrajan rad na baterijama, ali ne trebaju velike brzine prijenosa podataka (oko 1 Mbps). Bluetooth LE učinio je ovu verziju idealnom za povezivanje uređaja poput pametnih satova, fitness narukvica, senzora i bežične periferije koji mogu raditi mjesecima ili godinama na jednoj bateriji. Maksimalna brzina za klasični Bluetooth bez LE tehnologije koji zahtijeva kontinuiranu vezu za prijenos velikih datoteka je 3 Mbps.

Bluetooth 4.1:

Izlaskom Bluetooth-a 4.1 2013. godine, poboljšana je međusobna suradnja s LTE (*Long Term Evolution*) mrežama kako bi se smanjila interferencija. Dodana je podrška za uređaje da istovremeno funkcioniraju kao Bluetooth čvor i poslužitelj. Primjerice, pametni telefon može

primati podatke s fitness senzora (kao čvor) i istovremeno biti poslužitelj za pametni sat koji pristupa tim podacima. Brzine prijenosa podataka su iste kao u prethodnoj verziji.

Bluetooth 4.2:

2014. godine, izlaskom 4.2 verzije Bluetooth tehnologije, poboljšane su sigurnosne značajke pomoću SSP-a, šifriranja i autentikacije. Povećana je privatnost koja se odnosi na zaštitu korisničkih podataka i sprječavanje praćenja ili neovlaštenog pristupa uređajima. Uvedena je podrška za IPv6, najnoviju verziju IP (*Internet Protocol*) adrese čime je Bluetooth mogao biti integriran s Internetom stvari (IoT). IoT se odnosi na mrežu fizičkih uređaja, vozila i kućanskih aparata koji su opremljeni senzorima, softverom i mrežnom povezanošću kako bi međusobno komunicirali i dijelili podatke putem interneta. Brzine prijenosa su iste, 1 Mbps za Bluetooth LE i 3 Mbps za klasični Bluetooth.

Bluetooth 5.0

Izdan 2016., Bluetooth 5.0 uveo je nekoliko poboljšanja, uključujući povećani domet do 240 m u otvorenom prostoru uz korištenje Bluetooth LE tehnologije i veće brzine prijenosa podataka (do 2 Mbps) uz BLE tehnologiju. Postavio je temelje za buduća poboljšanja Bluetooth audio tehnologije tako što je uz pomoć veće brzine prijenosa podataka omogućena i veća propusnost za audio prijenos. Ova verzija je značajno unaprijedila IoT primjene i omogućila širu primjenu u pametnim domovima.

Bluetooth 5.1:

Izlaskom Bluetooth-a 5.1 2019. godine, dodana je značajka pozicioniranja u prostoru (*Direction Finding*) koja omogućava preciznije praćenje lokacije uređaja s visokom točnošću, što je korisno za navigaciju unutar zgrada ili praćenje objekata. Tehničke karakteristike iste su kao u prethodnoj verziji.

Bluetooth 5.2:

Uvedena je nova značajka *Isochronous Channels* koja omogućuje istovremeni prijenos podataka s jednog izvora na više prijemnika, osiguravajući da svi uređaji primaju podatke u isto vrijeme, što je ključno za uređaje poput stereo slušalica. Bluetooth 5.2 uveo je i LE Audio (*Low Energy Audio*), novu tehnologiju za prijenos zvuka koja je dizajnirana kako bi omogućila bolju kvalitetu zvuka uz manju potrošnju energije. LE audio koristi novi LC3 audio kodek (*Low*

Complexity Communication Codec) koji je učinkovitiji od starijih kodeka jer uređaji mogu prenositi zvuk visoke kvalitete pri manjoj propusnosti, što omogućuje dulje trajanje baterije i stabilniji prijenos bez smetnji ili prekida. Tehničke specifikacije nisu se mijenjale.

Bluetooth 5.3:

Bluetooth 5.3, objavljen sredinom 2021. godine, donosi poboljšanja u radu uređaja putem poboljšanog mehanizma rotacije kanala (*Channel Classification Enhancement*). Ova tehnologija omogućuje pametnije upravljanje frekvencijama koje uređaji koriste, što smanjuje smetnje i povećava stabilnost veze. Uvodi se preciznija kontrola potrošnje energije kroz značajku *Subrate*. Ova funkcija omogućuje optimizaciju potrošnje energije prilagođavanjem intervala prijenosa podataka za uređaje koji komuniciraju povremeno, umjesto kontinuirano. Tehničke karakteristike ostale su iste.

Bluetooth 5.4

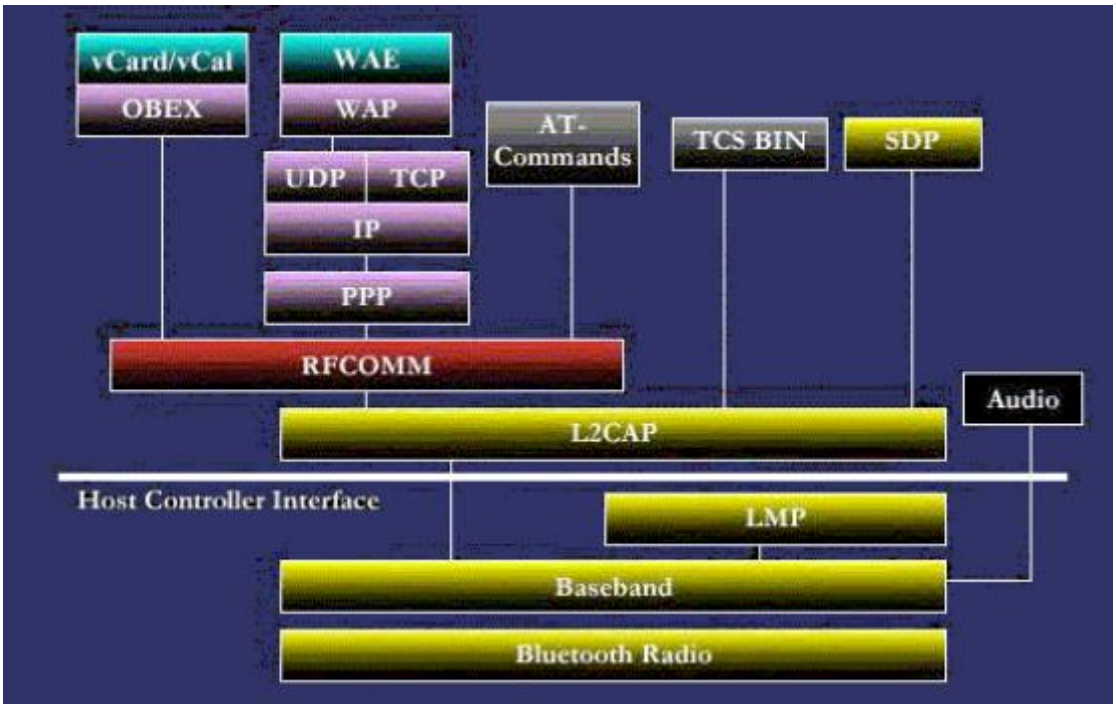
Bluetooth 5.4, objavljen 2023. godine, donosi ključne inovacije za IoT (*Internet of Things*) uređaje. Fokusira se na povezivanje većeg broja uređaja, pritom ne misleći na klasično povezivanje u smislu stalne veze sa 7 uređaja. Ovo povezivanje organizirano je povremenim slanjem ili primanjem podataka između uređaja bez stalne veze, čime se smanjuje opterećenje na mreži i omogućuje povezivanje s velikim brojem čvorova. To se radi korištenjem PAwR-a (*Periodic Advertising with Response*). PAwR je nova značajka koja omogućuje efikasniju komunikaciju između centralnog uređaja i velikog broja čvorova (senzora, pametnih uređaja) uz manju potrošnju energije. Brzina prijenosa podataka ostaje ista, ali je prijenos poboljšan koristeći EATT (*Enhanced Attribute Protocol*). EATT protokol poboljšava sigurnost i efikasnost veza omogućavanjem paralelnog prijenosa više podataka u istom vremenskom okviru i boljom enkripcijom podataka.

2.2. Bluetooth protokoli

Stog Bluetooth protokola kombinacija je softverske ili hardverske implementacije izvornog protokola navedenog u standardu. Bluetooth koristi različite protokole. Osnovne protokole definirao je Bluetooth SIG, dok su dodatni protokoli usvojeni od drugih tijela. Bluetooth protokolni stog prikazan je na slici 2.2.

Protokoli se dijele u četiri kategorije kako je prikazano na slici 2.2:

1. temeljni Bluetooth protokoli,
2. protokoli za zamjenu kabela,
3. protokoli za nadzor telefonije,
4. preuzeti protokoli. [2]



Slika 2.2. Bluetooth protokolni stog. [3]

2.2.1. Temeljni Bluetooth protokoli

Bluetooth temeljni protokoli su skupovi standarda i specifikacija koje omogućavaju uspostavljanje i održavanje komunikacije između Bluetooth uređaja. Ovi protokoli definiraju kako uređaji komuniciraju, kako se podaci prenose i kako se uspostavljaju veze.

Temeljni protokoli su sljedeći: Bluetooth Radio, Baseband, LMP (*Link Management Protocol*), HCI (*Host/Controller Interface*), L2CAP (Protokol logičkog linka i adaptacije) i SDP (*Service Discovery Protocol*).

Bluetooth Radio je protokol fizičkog sloja kojim se ostvaruje komunikacija između uređaja. Uređaji komuniciraju u nelicenciranom 2.4 GHz (2400 - 2483.5 MHz) ISM pojasu uz primjenu frekvencijskog skakanja (AFH). Definirana su dva načina rada:

- obavezan način rada koji se naziva „*Basic Rate*“ i
- opcionalni način rada - „*Enhanced Data Rate*“. [2]

Definira frekvenciju brojanja, zračno sučelje, shemu modulacije, frekvencijsko skakanje i kontrolu prijenosa. [3]

Baseband protokol rješava radijsku vezu dva uređaja. Predviđene su dvije mogućnosti:

- sinkrona, spojno orijentirana veza prikladna za prijenos govora i
- asinkrona, nespojna veza prikladna za prijenos podataka. [2]

Ovaj protokol definira format okvira paketa, adresiranje, vrijeme i kontrolu napajanja.[4]

LMP (*Link Management Protocol*) koristi se za nadzor i uspostavu svih aspekata radio veze između dva uređaja. Ovo uključuje uspostavu i nadzor logičke veze, kao i provjeru fizičke veze. Sadrži podatkovne protokolne jedinice (PDU) koje nose informacije o:

- nadzoru veze,
- sigurnosti,
- zahtjevima,
- načinu rada,
- logičkom prijenosu i
- ispitivanju. [2]

Uspostavlja postavku veze između Bluetooth uređaja i upravlja tekućim vezama, uključujući sigurnosne aspekte poput provjere autentičnosti i enkripcije, kao i kontrolu i konfiguraciju veličine paketa osnovnog pojasa. [4]

HCI (*Host/Controller Interface*) omogućava standardiziranu komunikaciju između upravljačkih i poslužiteljskih slojeva. Postoji nekoliko različitih HCI transportnih slojeva, a svaki od njih koristi drugo sučelje za prijenos istih naredbi, događaja i podataka. Obično se koriste tehnologije USB (*Universal Serial Bus*) kod osobnih računala te UART (*Universal Asynchronous Receiver/Transmitter*) kod mobilnih uređaja. [2]

L2CAP (Protokol logičkog linka i adaptacije) je protokol za nadzor veze i prilagodbu višim protokolima pružajući dijeljenje paketa, multipleksiranje i kvalitetu usluge. Postoje dva načina rada:

- ERMT (*Enhanced Retransmission Mode*) – uključuje retransmisiju na L2CAP kanalu.
- SM (*Streaming Mode*) – jednostavniji način rada bez retransmisije i provjere toka.

Temelji se na konceptu kanala, a svaka krajnja točka referencirana je s CID (*Channel Identifier*) vrijednosti koja definira krajnju točku logičkog kanala na uređajima.[2]

Prilagođava gornje slojeve sloju osnovnog pojasa, pružajući usluge usmjerene na povezivanje i usluge bez povezivanja. [3]

SDP (*Service Discovery Protocol*) 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. [2]

Obrađuje usluge, informacije o uređaju i upite za karakteristike usluge između dva ili više Bluetooth uređaja. [4]

2.2.2. Protokoli za nadzor telefonije

Protokoli koji se koriste za nadzor telefonije su: TCS BIN i AT komande.

TCS BIN (*Telephony Control Specification - Binary*) – protokol koji definira signalizaciju poziva za uspostave prijenosa govora i podataka između Bluetooth uređaja. Dodatno definira procedure upravljanja pokretljivošću uređajima.

AT komande – su skupina komandi za komunikaciju s vanjskim aplikacijskim slojem. [2]

2.2.3. Protokoli za emulaciju serijskih priključaka

Protokol za emulaciju serijskih priključaka **RFCOMM** (*Radio Frequency Communication*) pruža emulaciju serijskih priključaka preko L2CAP protokola. Radi se o jednostavnom transportnom protokolu koji podržava do 60 simultanih veza između dva uređaja. Pruža stvarni prijenos niza podataka, a koriste ga mnogi Bluetooth programi zbog široke podrške (uporaba u pisačima, modemima i računalima). Omogućuje prijenos podataka „AT komandi“, a može služiti i kao transportni sloj za OBEX (*Object Exchange Protocol*). [2]

RFCOMM funkcionira kao virtualni serijski port i prenosi binarne digitalne podatke. U biti emulira RS232 specifikacije preko Bluetooth fizičkog sloja. [5]

2.2.4. Preuzeti protokoli

Ove protokole već su definirala druga standardna tijela i ugrađeni su bez ikakvih promjena u arhitekturu stoga Bluetooth protokola. [5]

U skupinu preuzetih protokola uključeni su: PPP (*Point-to-Point Protocol*), UDP (*User Datagram Protocol*), TCP (*Transmission Control Protocol*), IP (*Internet Protocol*), WAP (*Wireless Application Protocol*), vCARD (*Virtual Card*), vCAL (*Virtual Calendar File*) i OBEX (*Object Exchange Protocol*).

PPP (*Point-to-Point Protocol*) – standardni internetski protokol za prijenos IP datagrama preko „point-to-point“ veze. Spomenuta veza obično se koristi za povezivanje dvaju sustava preko WAN (*Wide Area Network*) mreža, a jedna od uobičajenih uporaba je razmjena podataka između lokalnog i udaljenog sustava.

UDP (*User Datagram Protocol*) – protokol koji omogućuje prijenos IP datagrama kroz Internetsku mrežu bez potrebe za uspostavom kanala.

TCP (*Transmission Control Protocol*) – protokol koji omogućuje prijenos niza podataka uz provjeru toka podataka, veličine segmenata i brzine prijenosa.

IP (*Internet Protocol*) – osnovni protokol koji omogućuje prijenos datagrama preko mreže pomoću adresa odredišnih čvorova.

WAP (*Wireless Application Protocol*) – otvoreni standard koji korisnicima mobilnih telefona omogućuje uporabu telefonskih i informacijskih usluga.

vCARD (*Virtual Card*) – jedan od formata sadržaja – digitalni format elektronske posjetnice koji omogućava razmjenu kontakt informacija između uređaja.

vCAL (*Virtual Calendar File*) – jedan od formata sadržaja – elektronički osobni kalendar s rasporedom aktivnosti.

OBEX (*Object Exchange Protocol*) – sjednički protokol koji je razvila udruga IrDA (*Infrared Data Association*) za jednostavnu i spontanu izmjenu objekata u modelu klijent – poslužitelj. U općem obliku radi se o pojednostavljenoj inačici HTTP (*Hypertext Transfer Protocol*) protokola. [2]

2.3. Karakteristike po verzijama Bluetooth-a

U tablici 2.1 prikazane su osnovne karakteristike Bluetooth protokola po verzijama.

Verzija	Frekvencijski opseg	Broj uređaja	Brzina	Domet	Način kodiranja
1.0	2.4 GHz	7	721 kbps	Do 10 metara	GFSK
1.1	2.4 GHz	7	721 kbps	Do 10 metara	GFSK
1.2	2.4 GHz	7	1 Mbps	Do 10 metara	GFSK
2.0 + EDR	2.4 GHz	7	3 Mbps (EDR)	Do 10 metara	GFSK, π/4-DQPSK, 8-DPSK
2.1 + EDR	2.4 GHz	7	3 Mbps (EDR)	Do 10 metara	GFSK, π/4-DQPSK, 8-DPSK

3.0 + HS	2.4 GHz	7	24 Mbps (HS – preko Wi-Fi)	Do 10 metara	GFSK, π/4-DQPSK, 8-DPSK
4.0	2.4 GHz	7	1 Mbps (LE), 3 Mbps (BR/EDR)	Do 60 metara (LE), do 10 metara (BR/EDR)	GFSK
4.1	2.4 GHz	7	1 Mbps (LE), 3 Mbps (BR/EDR)	Do 60 metara (LE), do 10 metara (BR/EDR)	GFSK
4.2	2.4 GHz	7	1 Mbps (LE), 3 Mbps (BR/EDR)	Do 60 metara (LE), do 10 metara (BR/EDR)	GFSK
5.0	2.4 GHz	7	2 Mbps (LE), 3 Mbps (BR/EDR)	Do 240 metara (LE), do 10 metara (BR/EDR)	GFSK
5.1	2.4 GHz	7	2 Mbps (LE), 3 Mbps (BR/EDR)	Do 240 metara (LE), do 10 metara (BR/EDR)	GFSK
5.2	2.4 GHz	7	2 Mbps (LE), 3 Mbps (BR/EDR), izokroni kanali	Do 240 metara (LE), do 10 metara (BR/EDR)	GFSK
5.3	2.4 GHz	7	2 Mbps (LE), 3 Mbps (BR/EDR)	Do 240 metara (LE), do 10 metara (BR/EDR)	GFSK
5.4	2.4 GHz	7	2 Mbps (LE), 3 Mbps (BR/EDR)	Do 240 metara (LE), do 10 metara (BR/EDR)	GFSK

Tablica 2.1. Prikaz karakteristika pojedinih verzija Bluetooth-a.

Tablica 2.1 prikazuje karakteristike različitih verzija Bluetooth tehnologije. U tablici je prikazano da sve verzije koriste frekvencijski opseg od 2.4 GHz i omogućuju povezivanje maksimalno 7 uređaja, što je ograničeno Bluetooth protokolom, jer bi veći broj povezanih uređaja mogao negativno utjecati na kvalitetu veze. Verzije 1.0 i 1.1 imaju brzinu prijenosa od 721 kbps, a verzija 1.2 povećava brzinu na 1 Mbps. Verzija 2.0 uvodi dodatni dio Bluetooth specifikacije koji omogućuje veću brzinu podataka pod nazivom EDR (*Enhanced Data Rate*) pa je zbog toga

brzina povećana na 3 Mbps. Verzija 3.0 koristi HS (*High Speed*) tehnologiju za postizanje brzine od 24 Mbps putem Wi-Fi-a. Od verzije 4.0 uveden je LE (*Low Energy*) način rada s brzinama do 1 Mbps (za verzije 4.0, 4.1 i 4.2) i 2 Mbps za verzije 5.0 i novije. Osnovna brzina prijenosa podataka BR (*Basic Rate*) za klasični Bluetooth sa EDR-om ostaje 3 Mbps i u novijim verzijama. Domet je isti u svim verzijama za klasični Bluetooth (do 10 metara), a za uređaje i aplikacije koje koriste Bluetooth LE domet je od 60 do 240 metara. Sve verzije koriste GFSK (*Gaussian Frequency Shift Keying*) koji je osnovni oblik kodiranja promjenom frekvencije nositelja za prijenos podataka. Neke verzije (2.0, 2.1 i 3.0) uvele su π/4-DQPSK (*Differential Quadrature Phase Shift Keying*) i 8-DPSK (8 *Differential Phase Shift Keying*), koji omogućuju prijenos više informacija po simbolu, čime se povećava brzina prijenosa podataka. Načini kodiranja π/4-DQPSK i 8-DPSK više se ne koriste u novijim verzijama Bluetooth-a, zbog promjena prioriteta u dizajnu tehnologije. Novije verzije Bluetooth-a sve više naglašavaju energetsku efikasnost, stabilnost veze i duži domet, a ne samo brzinu prijenosa podataka.

2.4. Uporaba Bluetooth tehnologije

Uporaba Bluetooth tehnologije sve se više povećavala s razvojem novih verzija, a danas se koristi u raznim svakodnevnim situacijama. Najčešće primjene uključuju bežičnu komunikaciju između mobilnih uređaja i slušalica, kao i uspostavljanje bežičnih mreža između osobnih računala u uvjetima ograničene širine pojasa. Bluetooth omogućava bežičnu povezanost s ulaznim i izlaznim uređajima računala, poput miša, tipkovnice ili printera.

Bluetooth tehnologija koristi se za prijenos datoteka i podataka između uređaja putem OBEX protokola, a može poslužiti i kao zamjena za tradicionalne žične komunikacije u različitim uređajima, kao što su ispitna oprema, GPS uređaji, medicinska oprema i BarCode skeneri. Primjenjuje se i u sustavima koji koriste infracrvenu tehnologiju (*Infrared Radiation*).

Bluetooth je često korišten kao bežični most između industrijskih Ethernet mreža te za nadzor igraćih konzola. Omogućava i pristup internetu na osobnim računalima putem mobilnih uređaja koji služe kao modemi. [2]

Danas se Bluetooth tehnologija sve više primjenjuje u pametnim uređajima (IoT) kao što su pametne brave na vratima i sigurnosne kamere. Koristi se u automobilima i u "*beacon*" uređajima koji pružaju informacije o lokaciji, šaljući informacije korisnicima dok prolaze pored određenih točaka.

2.5. Usporedba s drugim bežičnim tehnologijama

Usporedba Bluetootha sa osnovnim bežičnim tehnologijama dana je u tablici 2.2. Usporedba je napravljena sa Bluetooth verzijom 5.0.

	Bluetooth 5.0	**UWB**	**Wi-Fi (802.11b)**	**Wi-Fi (802.11g)**	**Wi-Fi (802.11a)**	**Wi-Fi (802.11n)**	**ZigBee**
Brzina (Mbps)	2-3	200	11	54	54	Do 600	0,03
Najveći raspon (m)	240	30	100	100	50	250	75
Energija (mW)	100	400	750	1000	1500	2000	30
BW (MHz)	2	500	22	20	20	40	0,6
Spektralna učinkovitost (b/Hz)	2,5	0,4	0,5	2,7	2,7	5	0,05

Tablica 2.2. Usporedba bežičnih tehnologija.

***Ultra-Wideband* (UWB)** je bežična komunikacijska tehnologija koja koristi široki spektar frekvencija za prijenos podataka na kratke udaljenosti. UWB može prenositi podatke pri visokim brzinama, ali ima relativno kratak raspon, obično do 30 metara. Prepoznata je kao međunarodni standard (ECMA-368, ISO/IEC 26970). Glavne karakteristike uključuju široki pojas od najmanje 500 MHz, probojnost signala kroz prepreke, nisku snagu, preciznu lokaciju i visoku brzinu prijenosa podataka.

Wi-Fi (*Wireless Fidelity*) je bežična mreža (WLAN) s različitim standardima koji omogućuju brzine prijenosa od 11 Mbps (802.11b) do 600 Mbps (802.11n). Temelji se na standardu IEEE 802.11, koji definira kako se podaci prenose bežičnim putem. Uključuje više verzija koje poboljšavaju kvalitetu usluge, sigurnost i brzinu.

ZigBee (IEEE 802.15.4) tehnologija dizajnirana je za prijenos podataka na kratke udaljenosti od 10 do 75 metara, uz vrlo nisku potrošnju energije (oko 30 mW) i male brzine prijenosa (oko 250 Kbps). Namijenjena je prvenstveno za primjenu u uređajima koji zahtijevaju malu potrošnju i dug vijek trajanja baterije. [2]

Iz tablice 2.2 vidljivo je da Bluetooth 5.0, u usporedbi s tehnologijama kao što su Wi-Fi, UWB, i ZigBee, ima specifične prednosti i ograničenja ovisno o namjeni. Bluetooth 5.0 nudi brzinu prijenosa podataka do 2 Mbps (u načinu rada Low Energy) ili 3 Mbps (BR/EDR), što je

znatno niže u odnosu na Wi-Fi standarde poput 802.11n, koji može doseći brzine do 600 Mbps. Prednost Bluetooth-a je u rasponu, može dosegnuti 240 metara, što ga čini pogodnim za bežičnu komunikaciju na velikim udaljenostima. Za razliku od njega, UWB ima vrlo kratki raspon od samo 30 metara, ali kompenzira to visokom brzinom prijenosa od 200 Mbps.

Bluetooth se izdvaja svojom učinkovitom potrošnjom energije od oko 100 mW, što ga čini pogodnim za uređaje s malim izvorima energije. Nasuprot tome, Wi-Fi standardi, posebno 802.11n, troše značajno više energije (do 2000 mW), ali omogućuju veće brzine prijenosa podataka (do 600 Mbps). ZigBee tehnologija koristi minimalno energije (oko 30 mW) i nudi nisku brzinu prijenosa podataka (0,03 Mbps), što je dovoljno za aplikacije poput senzorskih mreža, ali nije prikladno za prijenos velikih količina podataka.

Spektralna učinkovitost (b/Hz) je važan pojam koji pokazuje koliko podataka se može prenijeti kroz određeni frekvencijski pojas. Bluetooth 5.0 ima dobru spektralnu učinkovitost od 2,5 b/Hz, dok Wi-Fi standardi poput 802.11n dostižu 5 b/Hz, što znači da mogu prenijeti više podataka kroz isti frekvencijski spektar. Širina pojasa (BW) označava koliko frekvencijskog spektra koristi tehnologija za prijenos podataka. Bluetooth koristi samo 2 MHz, dok UWB ima ogromnu širinu pojasa od 500 MHz, što mu omogućuje veće brzine na kraćim udaljenostima.

Bluetooth 5.0 ističe se po dometu i pruža kompromis između Wi-Fi-evih visokih brzina i ZigBee-ove energetske učinkovitosti, ali kad je u pitanju brzina, ostaje ispod UWB-a i Wi-Fi-a.

2.6. Sigurnost

Tijekom razvoja Bluetooth standarda uvedeni su brojni postupci i tehnologije za zaštitu komunikacije i prijenos podataka između Bluetooth uređaja.

Postoje četiri entiteta koji upravljaju sigurnošću na razini veze:

1. BD_ADDR (*Bluetooth Device Address*) - adresa duga 48 bita koja jedinstveno određuje svaki uređaj, a definira ju organizacija IEEE (*Institute of Electrical and Electronics Engineers*),
2. Privatni autentikacijski ključ (*Private authentication key*) - slučajni broj duljine 128 bita koji se koristi za provođenje postupaka autentikacije.
3. Privatni ključ za kriptiranje (*Private encryption key*) - broj dug 8-128 bita koji se koristi za šifriranje podataka.
4. RAND (*random number*) - slučajni ili pseudo-slučajni broj duljine 128 bita koji se periodički mijenja, a stvara ga sam Bluetooth uređaj.

Bluetooth sigurnost dijeli se na tri razine:

- Razina 1 – nesigurna,
- Razina 2 – sigurnost na razini usluga,
- Razina 3 – sigurnost na razini veze.

Razlika između razine 2 i 3 je što kod razine 3 uređaji iniciraju procedure sigurnosti prije uspostave kanala, dok se kod razine 2 to obavlja na razini usluge.

Definirana su dva stupnja sigurnosti kod uređaja:

1. povjerljivi uređaj – neograničen pristup svim uslugama,

2. nepovjerljivi uređaj – ne postoji pristup uslugama.

Kod usluga postoje tri razine sigurnosti:

1. usluge koje zahtijevaju autorizaciju i autentikaciju,

2. usluge koje zahtijevaju autentikaciju,

3. usluge koje nemaju sigurnosnih zahtjeva. [2]

2.7. Upravljanje ključevima

Svaki prijenos podataka između uređaja odvija se pomoću ključa veze. Generira se 128-bitni slučajni broj koji se koristi u procesu autentikacije kao parametar za stvaranje ključa za kriptiranje.

Postoji nekoliko vrsta ovog ključa: kombinacijski, pojedinačni, glavni i inicijalizacijski ključ.

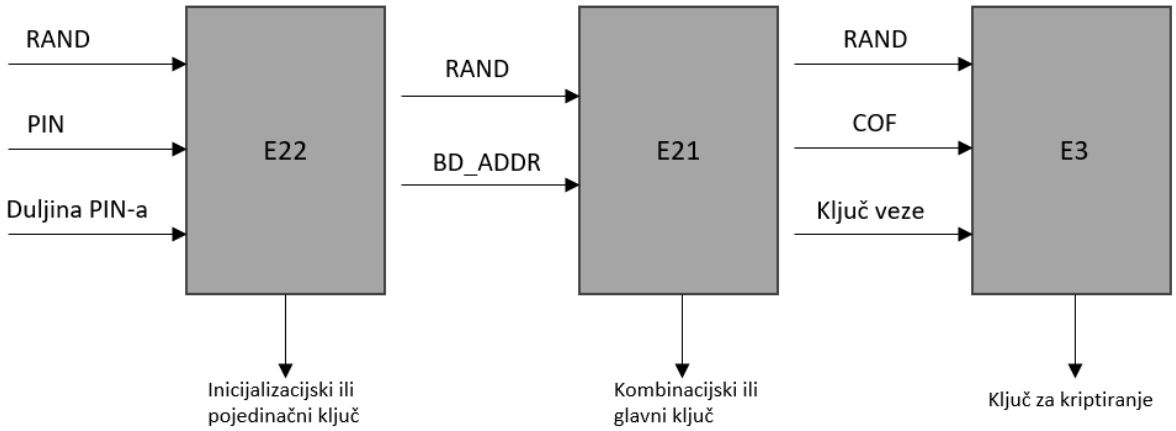
Kombinacijski ključ (*combination key*) – stvoren pomoću informacija iz oba uređaja u isto vrijeme preko algoritma E21 uz uporabu slučajnog broja i adrese uređaja. Algoritam E21 je kriptografski algoritam korišten u mobilnim komunikacijama. Njegova uloga vezana je za sigurnost i autentifikaciju.

Pojedinačni ključ (*unit key*) – stvoren u jednom uređaju, a izračunava se preko algoritma E21 prilikom prve uporabe uređaja, nakon čega se pohranjuje u memoriju.

Glavni ključ (*master key*) – privremeni ključ koji mijenja trenutni ključ veze, a stvara ga glavni uređaj (*master*) uporabom dva slučajna broja duljine 128 bita. Dobiveni broj šalje se drugom uređaju da bi se odredio trenutni ključ veze.

Inicijalizacijski ključ (*initialization key*) – koristi se kao ključ veze tijekom inicijalizacije, prije nego se stvaraju kombinacijski i pojedinačni ključevi. Stvara se preko E22 algoritma koji koristi PIN broj, adresu uređaja i slučajni broj dug 128 bita. Algoritam E22 osigurava da je komunikacija između korisnika i mreže zaštićena od prisluškivanja ili neovlaštenog pristupa. Duljina PIN vrijednosti može varirati između 1 i 16 okteta, a tijekom procesa inicijalizacije unosi se u oba uređaja.

Ključ veze određuje se iz trenutnog ključa veze, COF (*Ciphering Offset Number*) vrijednosti i slučajnog 128-bitnog broja preko algoritma E3. COF je broj koji pomaže u određivanju trenutnog ključa veze ili pomaku unutar serije šifriranih podataka kako bi se povećala sigurnost komunikacije. E3 algoritam koristi se za enkripciju podataka koji se prenose između korisnika, primjerice mobilnog telefona i mreže. Ključ za kriptiranje stvara se svaki put kada uređaj uđe u način rada za kriptiranje. Slika 2.3 prikazuje algoritme preko kojih se provodi stvaranje ključeva. [2]



Slika 2.3. Algoritmi za stvaranje ključeva.

2.8. Kriptiranje

Bluetooth sustav koristi E0 algoritam za šifriranje paketa, pri čemu se za svaki novi podatak generira novi niz. E0 algoritam koristi se za osiguravanje privatnosti i zaštitu podataka tijekom bežičnog prijenosa između uređaja. Šifrira podatke koji se šalju putem bežične veze, čime se

osigurava da neovlašteni korisnici ne mogu lako presresti ili dekodirati komunikaciju. Ovaj proces uključuje tri glavna dijela: generator ključa za inicijalizaciju, generator niza ključa i komponentu za šifriranje i dešifriranje.

Generator ključa za inicijalizaciju kombinira ulazne bitove i prosljeđuje ih LSFR (*Linear Feedback Shift Registers*) registrima unutar generatora niza ključa. Ako se koriste pojedinačni ili kombinirani ključevi, promet koji se prenosi prema višestrukim odredištima ostaje nešifriran, dok pojedinačni promet može, ali ne mora, biti šifriran. Kod korištenja glavnog ključa, razlikujemo tri razine šifriranja:

1. bez šifriranja,
2. višestruki promet je nešifriran, a pojedinačni je šifriran glavnim ključem,
3. sav promet je šifriran glavnim ključem.

Prije početka šifriranja, uređaji dogovaraju duljinu ključa, prema maksimalnim dopuštenim veličinama koje uređaji podržavaju. Svaki uređaj ima definiranu minimalnu duljinu ključa i može odbiti povezivanje ako se ne može koristiti adekvatno šifriranje. Ovo je važno za sprječavanje napada gdje bi napadači mogli namjerno pokušati sniziti razinu sigurnosti korištenjem slabijeg ključa.

2.9. Autentikacija

Bluetooth autentikacijska metoda koristi pristup "upit-odgovor" kako bi provjerila posjeduje li druga strana ispravan tajni ključ. Ovaj proces temelji se na simetričnim ključevima, pri čemu oba sudionika moraju dijeliti isti ključ kako bi autentikacija bila uspješna. Uređaji izračunavaju i pohranjuju ACO (*Authenticated Ciphering Offset*) vrijednost, koja se kasnije koristi za generiranje ključa.

U prvom koraku autentikacije, jedan uređaj generira slučajni broj i šalje ga drugom uređaju, koji na temelju tog broja kreira SRES (*Signed Response*) vrijednost. Ova vrijednost nastaje primjenom E1 funkcije koja kao ulaz uzima slučajni broj, BD_ADDR adresu drugog uređaja i ključ veze. Oba uređaja izračunavaju SRES koristeći iste parametre, a zatim uspoređuju rezultate. Ako autentikacija ne uspije, treba proći unaprijed određeni vremenski period prije nego što se postupak može ponoviti.

Softver određuje koji uređaj inicira autentikaciju i hoće li se proces provoditi u jednom smjeru ili dvosmjerno. [2]

2.10. Bluetooth napadi

2.10.1. Bluejacking

Bluejacking je tehnika kojom se putem Bluetooth tehnologije šalju neželjene poruke uređajima poput mobitela i prijenosnih računala. Poruke obično sadrže nepotreban sadržaj, često s ciljem oglašavanja ili ometanja korisnika. Napad se provodi slanjem vCard datoteka koje u polju „name“ sadrže poruku, a prijenos se vrši putem OBEX protokola. Najčešće se koriste uređaji klase 1, koji omogućuju brzinu prijenosa do 1 Mbit/s na udaljenostima do 10 metara.
Prvi dokumentirani slučaj Bluejacking-a izveo je IT stručnjak koji je svoj mobitel koristio za promidžbu Sony Ericssona. Naziv "bluejacking" potječe od riječi "jacking", što znači preuzimanje ili otmica. [6]

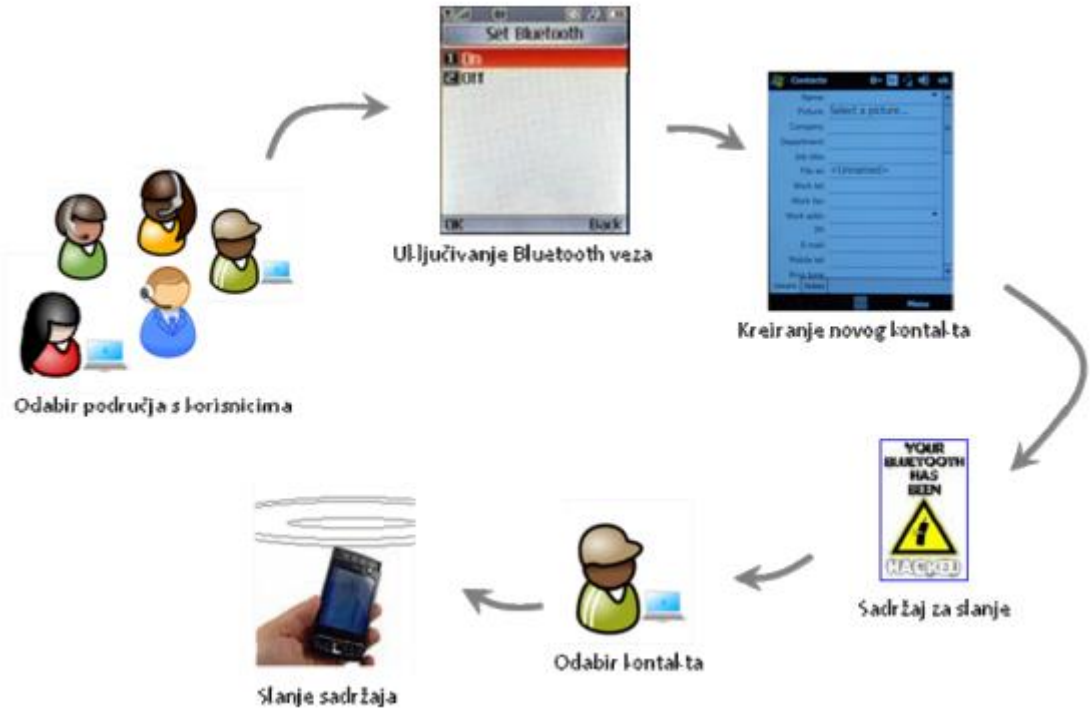
Na slici 2.4 prikazan je primjer Bluejacking napada na uređaj Sony Ericsson. U ovome primjeru napadač je poslao tekstualnu poruku sa informacijom da je izvršen Bluejacking napad.

Slika 2.4. Primjer uspješnog Bluejacking napada. [6]

Izvođenje napada uključuje sljedeće korake:

1. Odabir područja s mnogo korisnika Bluetooth uređaja,
2. Omogućavanje Bluetooth veza na vlastitom uređaju,
3. Kreiranje novog kontakta i pripremanje sadržaja za slanje,
4. Aktiviranje funkcije slanja preko Bluetooth veze na adresu novog kontakta što pokreće skeniranje uređaja s omogućenim Bluetooth vezama,
5. Odabir jednog korisnika u popisu vidljivih uređaja te slanje pripremljenog sadržaja,
6. Primanje potvrde o uspješno poslanom sadržaju,
7. Ponavljanje postupka slanja poruka na isti/drugi uređaj. [2]

Grafički prikaz odvijanja napada prikazan je na slici 2.5.



Slika 2.5. Koraci Bluejacking napada. [2]

Ova vrsta napada uglavnom je bezopasna, ali može biti zbunjujuća jer napadnuti korisnici često vjeruju da im je uređaj neispravan. Napadači obično šalju tekstualne poruke, ali s modernim uređajima moguće je slati i slike te audio zapise. Povremeno se koristi kao metoda za promociju i oglašavanje proizvoda. [6]

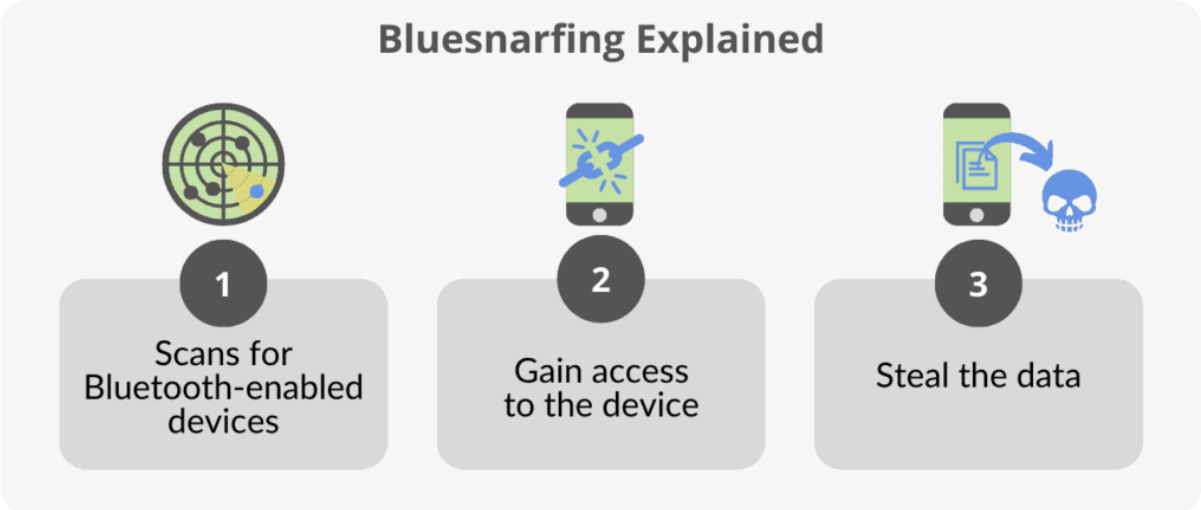
2.10.2. Bluesnarfing

Bluesnarfing je vrsta napada koja omogućuje neovlašten pristup podacima na uređaju (poput mobitela i prijenosnog računala) putem Bluetooth veze. Ovaj napad omogućuje dohvaćanje podataka poput kalendara, kontakata, e-mailova i SMS poruka, a na nekim uređajima i multimedijalnih sadržaja poput slika i zvučnih zapisa. [7]

Postoje softverski alati koji omogućuju povezivanje s ciljnim uređajem radi kopiranja sadržaja, ali napadač mora imati odgovarajući program koji omogućuje pristup uređaju. Jedna verzija Bluesnarfing alata razvijena je kako bi pokazala ranjivost Bluetooth veze kod određenih modela mobilnih uređaja. Ta sigurnosna rupa kasnije je zakrpana u novijim verzijama Bluetooth standarda. [7]

Bluesnarfing je opasniji napad u usporedbi s Bluejacking-om, iako oba iskorištavaju Bluetooth vezu bez korisnikova znanja. Svaki uređaj koji je vidljiv drugim uređajima može biti meta oba napada. Onemogućavanjem vidljivosti uređaja može se smanjiti rizik od napada, ali čak i skriveni uređaji mogu biti napadnuti metodama poput *brute force* pogađanja MAC adrese. Bluetooth koristi 48-bitnu MAC adresu, gdje prvih 24 bita identificira proizvođača, a preostalih 24 bita nudi 16,8 milijuna mogućih kombinacija, što znači da je potrebno oko 8,4 milijuna pokušaja za uspješno pogađanje adrese. [7]

Koraci Bluesnarfing napada prikazani su na slici 2.6.



Slika 2.6. Koraci Bluesnarfing napada. [8]

Slika 2.6 opisuje tri osnovna koraka u napadu: skeniranje Bluetooth uređaja, pristup uređaju i krađu podataka. Napadač prvo skenira okolinu tražeći uređaje koji imaju uključen Bluetooth i koji su ranjivi. Nakon identificiranja ranjivog uređaja, napadač pokušava dobiti neovlašteni pristup uređaju koristeći ranjivosti u Bluetooth protokolu. Nakon dobivanja pristupa, napadač može ukrasti osjetljive podatke sa uređaja, poput kontakata, SMS poruka, e-pošte, slika i drugih privatnih informacija. Ovaj napad obično se događa kada uređaj nije adekvatno zaštićen, primjerice kada je Bluetooth stalno uključen i vidljiv za druge uređaje.

Naprednija verzija Bluesnarfing-a je Bluebugging, gdje napadač ne samo da može pristupiti podacima, već može preuzeti kontrolu nad uređajem. Omogućuje pozivanje, slanje poruka, prisluškivanje razgovora i pristup internetu s ciljanog uređaja.

2.10.3. BlueBorne

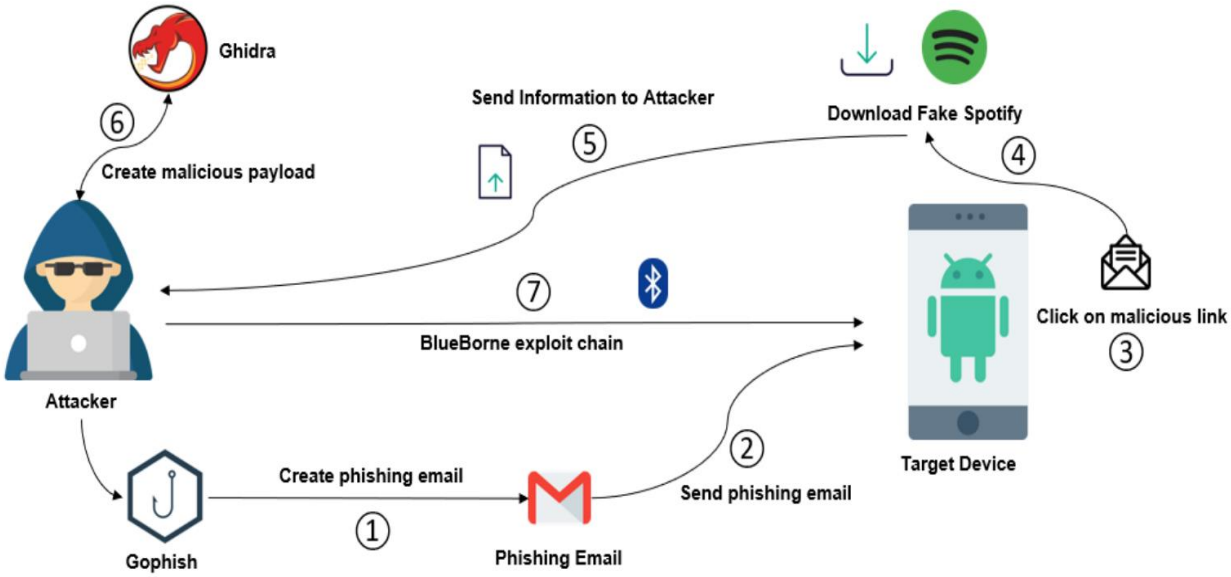
Značajan napad koji omogućuje napadaču potpunu kontrolu nad uređajem kroz ranjivosti u Bluetooth protokolu, bez potrebe za uparivanjem ili vidljivošću uređaja. Može zaraziti uređaje zlonamjernim softverom i širiti se na druge uređaje.

BlueBorne je vrsta ranjivosti s implementacijom Bluetooth-a u sustavima koja je prisutna na svim operativnim sustavima Android, iOS, Linux i Windows. Utječe na mnoge elektroničke uređaje poput prijenosnih računala, pametnih automobila, pametnih telefona i nosivih naprava. [9]

Godine 2017. procijenjeno je da bi BlueBorne potencijalno mogao utjecati na 8,2 milijarde Bluetooth uređaja diljem svijeta, iako pojašnjavaju da je 5,3 milijarde Bluetooth uređaja u opasnosti. Godine 2018., procijenjeno je da je više od 2 milijarde uređaja još uvijek ranjivo. [9]

Slika 2.7 prikazuje primjer BlueBorne napada na Android uređaju. Napadač započinje napad kreiranjem lažnog phishing emaila koristeći alat Gophish. Cilj ovog emaila je navesti žrtvu da klikne na zlonamjernu poveznicu. Nakon kreiranja phishing emaila, napadač ga šalje na ciljani Android uređaj žrtve, koristeći tehnike socijalnog inženjeringa kako bi uvjerio korisnika da otvori email i klikne na priloženi link. Kada žrtva primi phishing email i klikne na zlonamjernu poveznicu, ona automatski preuzima lažnu verziju popularne aplikacije (u ovom slučaju lažnu verziju Spotifyja) na svoj uređaj. Ova aplikacija, međutim, sadrži zlonamjerni softver koji omogućuje napadaču da potajno prima informacije s uređaja, kao što su osjetljivi podaci i drugi osobni sadržaji. Napadač dalje koristi alat pod nazivom Ghidra za kreiranje zlonamjernog

programa, poznatog kao payload. Ovaj program omogućuje napadaču iskorištavanje Bluetooth ranjivosti na uređaju koristeći BlueBorne exploit chain. Exploit chain odnosi se na niz ranjivosti ili sigurnosnih propusta koje napadač iskorištava kako bi postigao konačni cilj, a to je preuzimanje kontrole nad sistemom. Napadač zatim ima mogućnost daljinskog preuzimanja kontrole nad uređajem, a da žrtva nije ni svjesna da se napad događa.



Slika 2.7. Primjer BlueBorne napada na Android uređaju. [10]

2.11. Mobilni uređaji

Većina pametnih telefona i prijenosnih računala dizajniranih u posljednje dvije godine uključuje Bluetooth v4.0 čipset koji integrira Bluetooth LE hardver. Kao i kod mnogih inovacija, potrebno je vrijeme da operativni sustav platforme uključi potrebne upravljačke programe i API-je. iOS operativni sustav bio je prvi mobilni OS koji je to učinio, i kao rezultat toga, mnogi proizvodi temeljeni na Bluetooth LE-u funkcioniraju samo u kombinaciji s iPhone aplikacijom.

Prvi Bluetooth mobilni uređaj bio je Sony Ericsson T36 i prikazan je na slici 2.8.

Slika 2.8. Prvi mobilni telefon Sony Ericsson T36 s Bluetooth konfiguracijom. [11]

Kako Bluetooth uređaji rade na 2,4 GHz u ISM (*Industrial, Scientific, and Medical band*) radijskom pojasu, problem se javlja jer taj pojas dijele s drugim protokolima koji rade na istom frekvencijskom pojasu. Da bi se riješio navedeni problem Bluetooth koristi brzo skakanje frekvencije ili AFH te koristi kraće pakete od ostalih standarda. Time je komunikacija između uređaja brža i sigurnija. Nakon što Bluetooth uređaj pošalje ili primi paket, upareni uređaji prebacuju se na drugi frekvencijski opseg prije slanja sljedećeg paketa.

Ovakvim rješenjem prelaska s frekvencije na frekvenciju postiže se: iskorištenost cjelokupnog ISM pojasa, komunikacija uz minimalne smetnje i veća razina sigurnosti.

Upareni uređaji prema dogovoru mijenjaju frekvenciju koju će koristiti sljedeću. Bluetooth uređaj koji radi u glavnom načinu rada može komunicirati s do sedam uređaja konfiguriranih u podređenom načinu rada. Za svaki od podređenih uređaja glavnog uređaja Bluetooth uređaj emitira vlastitu jedinstvenu adresu. Poslane informacije zatim se koriste za izračunavanje serije skakanja frekvencije.

Povezani uređaji uvijek će komunicirati zajedno na sljedećoj frekvenciji koju su dogovorili zbog činjenice da glavni uređaj i svaki od podređenih uređaja koriste potpuno isti algoritam s istim početnim unosom.

Bluetooth uređaji obično se napajaju baterijama, kao što su bežični miševi i mobilni telefoni na baterije. Radi uštede energije većina uređaja radi na niskoj snazi. To omogućuje

Bluetooth uređajima da dosegnu određeni domet. Taj je domet dovoljno daleko za bežičnu komunikaciju, ali dovoljno blizu da se izbjegne previše energije iz izvora napajanja uređaja.

iPhone podržava različite verzije Bluetooth standarda. Stariji iPhone modeli koriste Bluetooth verzije 4.0 i 4.2, dok su noviji modeli prešli na Bluetooth 5.0 i novije. Apple koristi Bluetooth *Low Energy* (LE) tehnologiju. Ovo je posebno korisno za povezivanje uređaja poput pametnih satova, primjerice Apple Watch-a ili bežičnih slušalica (AirPods).

iPhone koristi Bluetooth kao ključnu tehnologiju za Appleove funkcionalnosti kao što su:

- *Handoff* i *Continuity*, koje omogućuju korisnicima prijenos aktivnosti s jednog Apple uređaja na drugi, primjerice s iPhone-a na MacBook ili iPad,
- *AirDrop,* Appleovu tehnologiju za dijeljenje datoteka,
- *AirPlay*, za bežično slanje zvuka ili videa na kompatibilne uređaje poput Apple TV-a.

Bluetooth profili koji se koriste kod iPhone-a:

- A2DP (*Advanced Audio Distribution Profile*) za stereo prijenos zvuka.
- HFP (*Hands-Free Profile*) za hands-free pozive.
- AVRCP (*Audio/Video Remote Control Profile*) za upravljanje multimedijskim uređajima.
- BLE (Bluetooth *Low Energy*) za povezivanje s uređajima poput senzora ili fitness trackera.

iPhone 15 modeli podržavaju Bluetooth 5.3 i Bluetooth LE Audio tehnologiju.

2.12. Bluetooth u automobilskoj industriji

Bluetooth tehnologija u automobilskoj industriji koristi se u različitim verzijama, ovisno o namjeni i funkcionalnostima koje se implementiraju u automobilu. Bluetooth 4.0 i 4.2 (BLE) koristi se za sustave koji zahtijevaju nisku potrošnju energije, poput senzora pritiska u gumama, daljinskog upravljanja funkcijama automobila i povezivanja s pametnim telefonima.

Verzija 5.0 i novije, koriste se za napredne multimedijske sustave, komunikaciju između različitih sustava u vozilu, poput naprednih senzora i sigurnosnih sustava te navigaciju i *hands-free* pozive u automobilima.

Bluetooth u automobilima koristi se zbog sljedećih razloga: povezivanja uređaja, sigurnosti i praktičnosti, bežičnog prijenosa podataka i povezivanja senzora.

Povezivanje uređaja – Bluetooth omogućuje bežičnu vezu između pametnih telefona, tableta i automobilskih sustava, kao što su multimedija, navigacija i *hands-free* pozivi.

Sigurnost i praktičnost - *hands-free* pozivi omogućuju vozaču razgovaranje bez korištenja ruku, što poboljšava sigurnost tijekom vožnje.

Bežični prijenos podataka - Bluetooth omogućuje automatsko ažuriranje softvera, dijagnostiku i povezivanje s vanjskim uređajima bez potrebe za kabelima.

Povezivanje senzora - Bluetooth povezuje senzore unutar automobila, omogućujući sustavima poput sustava za nadzor tlaka u gumama da prenose podatke o stanju vozila.

Sustav za nadzor tlaka u gumama TPMS (*Tire Pressure Monitoring System*) koristi senzore za praćenje tlaka u gumama u stvarnom vremenu. Senzori u svakoj gumi mjere tlak i temperaturu te šalju podatke putem Bluetooth-a u središnji sustav automobila ili izravno u aplikaciju na pametnom telefonu. Moderni TPMS sustavi koriste Bluetooth *Low Energy* (BLE) za prijenos podataka, jer BLE troši vrlo malo energije za prijenos podataka poput tlaka u gumama.

Bluetooth veza u automobilima, kao i svaka Bluetooth veza, može biti ranjiva. Najpoznatiji napad na Bluetooth vezu u automobilu zove se *Car Whisperer*. Ovaj napad iskorištava sigurnosne slabosti u sustavima *hands-free* komunikacije putem Bluetootha, posebice u sustavima instaliranim u automobilima. Ime "*Car Whisperer*" dolazi od sposobnosti alata da "sluša" i "šapuće" (snima i emitira) glasovne podatke putem Bluetooth veze unutar automobila.

Napadač koristi uređaj s Bluetooth vezom, primjerice prijenosno računalo ili mobitel kako bi se povezao s *hands-free* sustavom automobila. Budući da je PIN često lako pogađanje ili čak zanemaren, napadač se može povezati s automobilom bez znanja vlasnika. Nakon povezivanja, napadač može:

- Slušati razgovore koje vodi vozač (ili putnici) putem *hands-free* sustava automobila.
- Emitirati zvukove ili glasovne poruke kroz sustav zvučnika automobila, zbunjujući ili ometajući vozača i putnike.

2.13. Prednosti i nedostaci Bluetooth-a

U tablici 2.3 prikazani su prednosti i nedostaci pojedinih verzija Bluetooth-a.

Verzija	Prednosti	Nedostaci
1.0	• Omogućuje bežičnu komunikaciju	• Niska brzina prijenosa podataka (721 kbps) • Kratki domet (do 10 metara) • Problemi s kompatibilnošću i stabilnošću veze
1.1	• Popravljena kompatibilnost • Poboljšana stabilnost veze	• I dalje niska brzina prijenosa • Kratki domet
1.2	• Bolje suzbijanje smetnji • Poboljšana brzina prijenosa (1 Mbps)	• Još uvijek relativno niska brzina u usporedbi s novijim verzijama • Ograničen domet
2.0 + EDR	• Povećana brzina prijenosa podataka (3 Mbps) • Bolja energetska učinkovitost	• Ograničen domet • Veća potrošnja energije u EDR modu • Sigurnosni problemi
2.1 + EDR	• Poboljšana sigurnost (*Secure Simple Pairing*) • Bolja energetska učinkovitost	• Brzina prijenosa podataka ostaje ista (3 Mbps) • Ograničen domet
3.0 + HS	• Vrlo visoka brzina prijenosa podataka (24 Mbps) • Korištenje Wi-Fi-a za velike brzine	• Veća potrošnja energije • Ograničena kompatibilnost s ranijim verzijama
4.0	• Bluetooth *Low Energy* (LE) za uređaje s niskom potrošnjom energije • Dugotrajni rad na baterijama • Bolji domet	• Brzina prijenosa podataka do 1 Mbps (LE) • Ograničen domet za BR/EDR veze • Nedostatak podrške za brzi prijenos velikih datoteka
4.1	• Poboljšana komunikacija i rad između različitih uređaja • Mogućnost korištenja uređaja kao *hub* (istovremeno povezivanje više Bluetooth uređaja)	• Slične brzine i domet kao 4.0 verzija
4.2	• Poboljšana sigurnost • Povećana brzina prijenosa za IPv6 podršku	• Nema značajnog povećanja brzine prijenosa podataka za ostale aplikacije

5.0	• Veći domet (do 240 metara) • Veće brzine prijenosa (2 Mbps za LE) • Poboljšana audio kvaliteta • Podrška za IoT uređaje	• Potrebna kompatibilnost s novijim uređajima • Potencijalno veća potrošnja energije pri većim brzinama i dometu
5.1	• Preciznije praćenje lokacije • Poboljšana učinkovitost kod povezivanja uređaja	• Potrebna kompatibilnost s novijim uređajima • Nema značajnog povećanja brzine ili dometa
5.2	• Uveden LE Audio s poboljšanom kvalitetom zvuka i nižom potrošnjom energije • Poboljšana dvosmjerna komunikacija	• Potreban novi hardver za iskorištavanje svih funkcija • Kompatibilnost ovisi o podršci uređaja
5.3	• Smanjena potrošnja energije • Poboljšana stabilnost veze • Manje interferencije • Poboljšana sigurnost	• Zadržana brzina prijenosa (2 Mbps za LE) • Specifične funkcije ovise o implementaciji proizvođača
5.4	• Optimiziran za IoT uređaje (ušteda energije)	• Ograničen na uređaje koji podržavaju Bluetooth LE • Specifične funkcionalnosti zahtijevaju nove uređaje

Tablica 2.3. Prikaz prednosti i nedostataka pojedinih verzija Bluetooth-a.

Iz tablice 2.3 vidimo kako su se prednosti Bluetooth tehnologije postupno razvijale kroz verzije, dok su se nedostaci smanjivali. Prve verzije (1.0 do 1.2) omogućile su osnovnu bežičnu komunikaciju, ali su imale niz problema, poput niske brzine prijenosa i kratkog dometa. S verzijama 2.0 i 2.1, brzina se povećala (do 3 Mbps), ali domet je ostao ograničen, a potrošnja energije i dalje relativno visoka. Poboljšanja postaju vidljivija s verzijom 3.0 + HS, koja koristi Wi-Fi za velike brzine (24 Mbps), ali raste i potrošnja energije. Bluetooth 4.0 donosi značajnu novinu uvođenjem Bluetooth *Low Energy* (LE) tehnologije, što smanjuje potrošnju energije i poboljšava domet, ali brzina prijenosa ostaje niska. Verzije 5.0 i novije donose veće brzine, veći domet i bolju podršku za IoT uređaje, ali zahtijevaju kompatibilnost s novijim uređajima. Razvoj Bluetooth-a karakterizira balansiranje između brzine, dometa i energetske učinkovitosti, s posebnim fokusom na smanjenje potrošnje energije u novijim verzijama.

3. BLUETOOTH VERZIJA 5

Šest godina nakon usvajanja standarda 4.0, SIG je službeno objavio glavne značajke Bluetootha 5.0. Ovo je jedan od značajnih razvoja u tehnologiji bežične komunikacije kratkog dometa. Prema navodima SIG-a, novi standard će zauvijek promijeniti način na koji ljudi pristupaju Internetu stvari (IoT), pretvarajući ga u nešto što se odvija oko njih na gotovo prirodan i transparentan način. [12]

Za razliku od ranijih verzija Bluetooth standarda, poput 4.0 i njegovih ažuriranja (4.1 i 4.2), nova verzija nosi naziv Bluetooth 5, bez dodatnih oznaka. Osnovna verzija Bluetootha 5 ostaje slična prethodnim, dok su ključne promjene uvedene u BLE varijanti. Prema specifikacijama koje je predstavila SIG organizacija hardverske ploče mogu podržavati tri vrste Bluetooth veza: BLE 4.x, Bluetooth 5 sa brzinom prijenosa od 2 Mbps i Bluetooth 5 *Coded*. Bluetooth 5 *Coded* posebna je značajka koja omogućuje prijenos podataka na većim udaljenostima uz smanjenu brzinu prijenosa. Ova funkcija koristi dva moda kodiranja. Prvi mod smanjuje brzinu prijenosa podataka na polovicu (1 Mbps), ali povećava domet. Drugi mod smanjuje brzinu prijenosa na 125 kbps, što omogućuje još veći domet. BLE 4.x odnosi se na verzije 4.0, 4.1 i 4.2, s maksimalnom brzinom od 1 Mbps na osnovnom sloju. Bluetooth 5 sa 2 Mbps predstavlja novu, bržu vezu, gdje brzina na fizičkom sloju iznosi 2 Mbps. Jasno je da je novi standard osmišljen kako bi omogućio stvaranje komunikacijske mreže koja, na malim udaljenostima, omogućuje razmjenu podataka između uređaja i pametnih IoT uređaja. To omogućuje razvoj mreža za automatizaciju, što ubrzava implementaciju pametnih, međusobno povezanih uređaja. Organizacija Bluetooth SIG naglašava ključne inovacije koje donosi ovaj novi standard u usporedbi s prethodnim verzijama. [12]

Prvo veliko poboljšanje odnosi se na značajno povećanje dometa. Bluetooth 4.x omogućuje raspon između 50 i 100 metara na otvorenom, bez prepreka, dok se u zatvorenim prostorima smanjuje na 10 do 20 metara. Bluetooth 5 povećava domet BLE uređaja do četiri puta. U najnepovoljnijim uvjetima, to znači domet od 240 metara na otvorenom i oko 40 metara u zatvorenom prostoru. Ove promjene donijele su značajne uštede u elektroničkoj industriji. Bluetooth 5 uvodi posebnu vrstu veze namijenjenu dugom dometu, ali nije prikladna za uređaje poput Bluetooth zvučnika ili sinkronizaciju pametnih telefona. Namijenjena je IoT uređajima, gdje je potrebno postaviti jeftine module diljem zgrade ili na otvorenom za prikupljanje podataka o svjetlu, vlazi, temperaturi, prometu i sl. Ovi uređaji zahtijevaju napajanje, koje ne predstavlja problem ako su priključeni na mrežu.

Jedan način za povećanje dometa bez povećanja potrošnje energije je smanjenje brzine prijenosa podataka. Bluetooth 5 uvodi LE kodirani način rada koji poboljšava osjetljivost signala. U standardnim BLE načinima rada (1 Mbps i 2 Mbps), 1 bit jednak je jednom simbolu. U LE kodiranom načinu rada, brzina prijenosa može biti 500 kbps ili 125 kbps, gdje je za svaki bit dodijeljeno više simbola, čime se poboljšava tolerancija na smetnje u signalu i omogućuje oporavak podataka. Ovaj proces uključuje kodiranje podataka u više faza i koristi FEC (*Forward Error Correction*) za oporavak podataka u slučaju grešaka.

Povećanje dometa smanjuje potrebu za većim brojem pristupnih točaka, što je ključno za održavanje povezivosti u IoT mrežama. Veći domet omogućuje lakše stvaranje komunikacijskih kanala s beacon-ima na različitim lokacijama, poput zračnih luka, kolodvora i trgovačkih centara, te olakšava pružanje usluga temeljenih na lokaciji. Prema dosadašnjim karakteristikama, Bluetooth 5 mogao bi zamijeniti Wi-Fi u mnogim IoT aplikacijama. Izbor između brzine prijenosa podataka od 125 kbps ili 500 kbps ovisi o specifičnim potrebama. S 500 kbps može se postići dvostruko veći domet u odnosu na standardni BLE pri 1 Mbps, dok 125 kbps omogućuje još veći domet, ali uz sporiju komunikaciju. Kod jednostavnijih senzorskih zadataka, razlika između 500 kbps i 125 kbps nije toliko značajna u smislu uštede energije ili izbjegavanja smetnji.

Za jednostavne senzorske operacije optimalno je koristiti brzine od 125 kbps kako bi se postigao veći domet, dok je za veće količine podataka, poput prijenosa od nekoliko desetaka bajtova ili više, prikladnije odabrati brzinu od 500 kbps zbog prednosti koje nudi. [12]

Povećanje brzine prijenosa podataka jedna je od ključnih prednosti novog Bluetooth 5 standarda. Dok Bluetooth 4.x omogućuje maksimalnu brzinu od 1 Mbps, Bluetooth 5 može podržati brzinu do 2 Mbps, što znači da će budući nosivi uređaji moći sinkronizirati podatke dvostruko brže. Iako je trenutna brzina Bluetootha dovoljna za većinu aplikacija, posebice u IoT sustavima gdje prijenos podataka nije kritičan, kao što su nosivi uređaji poput fitness narukvica, veća brzina ipak donosi koristi. Zahvaljujući povećanoj propusnosti podataka u odnosu na Bluetooth 4.x, novi standard podržava prijenos većih količina podataka između različitih pametnih uređaja, ne ograničavajući se samo na pametne telefone i tablete. To znači da uređaji u automobilskoj industriji, kućanstvima, poslovnim prostorima i industriji mogu međusobno komunicirati. Bluetooth 5 unapređuje mogućnosti proširenja paketa predstavljene u verziji 4.2, što znači da se više podataka može prenijeti u jednom prijenosu. Iako podaci prolaze brže, vremenski razmak između paketa ostaje isti. Osim bržeg prijenosa, brzina od 2 Mbps donosi i uštedu energije. [12]

Jedno od ključnih poboljšanja koje donosi Bluetooth 5 je prošireni kapacitet emitiranja što se odnosi na sposobnost uređaja da šalju više informacija putem broadcast poruka. Broadcast poruke su jednostrane poruke koje Bluetooth uređaj šalje svim drugim uređajima u svom dometu, bez potrebe za uspostavljanjem direktne veze s njima. Ovo unapređenje ima značajan utjecaj na svijet beacon tehnologije. Beacon sustavi i uređaji koriste se za automatsko slanje lokaliziranih informacija, poput jelovnika, promocija ili prometnih podataka, svim uređajima u blizini. To je ključna značajka za razvoj IoT mreža.

Jedna od prednosti Bluetooth 5 standarda u odnosu na prethodne verzije je efikasnije upravljanje beacon porukama. Beacon-i omogućuju prijenos informacija korisnicima u blizini, poput vlasnika pametnih telefona, tableta ili nosivih uređaja, bez potrebe za uparivanjem kao kod slušalica ili zvučnika. Beacon može emitirati sadržaj čim se uređaj s omogućenim Bluetoothom nađe u njegovom dometu, omogućujući primjenu poput marketinga temeljenog na lokaciji ili ažuriranja sadržaja.

S prethodnim verzijama Bluetootha (4.x), beacon-i su mogli slati poruke od samo 31 bajta, što je ograničavajuće za veće informacije, poput URL-ova koji nisu mogli stati u 31 bajt. Bluetooth 5 to rješava povećanjem veličine poruke na 255 bajtova, omogućujući slanje znatno većih količina podataka.

Bluetooth 5 podržava umrežavanje, iako ta mogućnost nije bila uključena u prve specifikacije Bluetooth protokola. Nešto kasnije je uveden i Bluetooth Mesh. Bluetooth Mesh je mrežna tehnologija koja omogućuje stvaranje velikih mreža između više Bluetooth uređaja, gdje svaki uređaj može komunicirati s drugim uređajima preko posrednika. Umjesto tradicionalne Bluetooth veze "jedan na jedan" ili "jedan na više", Bluetooth Mesh omogućuje "mnogi na mnoge" komunikaciju u velikom broju uređaja unutar mreže. [12]

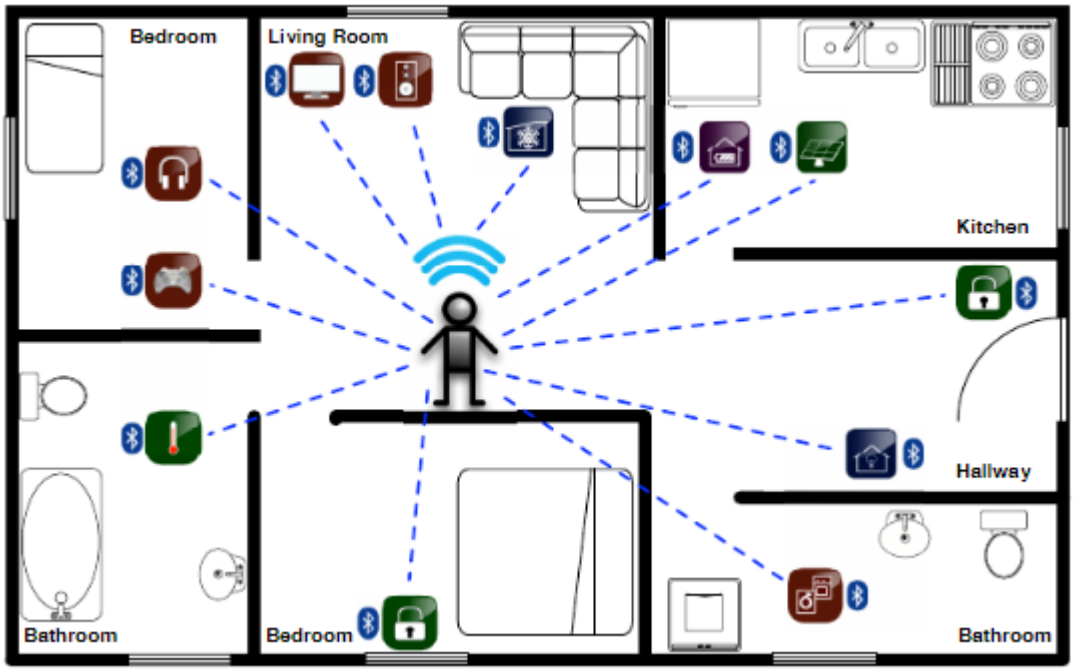
Prošireni domet i povećana brzina impliciraju veću potrošnju energije, ali zahvaljujući pametnom dizajnu, poput modulacije signala i napretka u korištenju frekvencijskog spektra, Bluetooth 5 zapravo troši manje energije. U optimalnim uvjetima, može koristiti otprilike dvostruko manje energije u usporedbi s prethodnim verzijama. Kod žičanih uređaja povećanje brzine obično rezultira i većom potrošnjom energije, ali Bluetooth, koji koristi frekvenciju od 2,4 GHz, prilagođava potrošnju energije na temelju frekvencije, a ne brzine prijenosa podataka. S Bluetoothom 5, omogućena je dvostruka količina prenesenih podataka uz istu potrošnju energije, što znači da uređaj koristi upola manje energije za isti volumen podataka.

Bluetooth 5 je dizajniran da bude jednako učinkovit, ako ne i bolji, od konkurentnih tehnologija poput IEEE 802.15.4, primjerice ZigBee, kako bi postao ozbiljan izazivač na tržištu. U tu svrhu uvedene su nove BLE klase izlazne snage:

- LE klasa 1: Maksimalno +20 dBm; Minimalno >+10 dBm
- LE klasa 1.5: Maksimalno +10 dBm; Minimalno -20 dBm
- LE klasa 2: Maksimalno +4 dBm; Minimalno -20 dBm
- LE klasa 3: Maksimalno 0 dBm; Minimalno -20 dBm.

Kod odabira bežičnog standarda za IoT uređaje napajane baterijama, mogućnost prijenosa iste količine podataka uz dvostruko manju potrošnju energije velika je prednost. Uz to, smanjuju se troškovi infrastrukture jer nisu potrebne pristupne točke ili ruteri. Zbog toga, Bluetooth omogućuje dulji vijek trajanja baterije u usporedbi s Wi-Fi tehnologijom, što olakšava razvoj malih, izdržljivih IoT uređaja za industrijsku i potrošačku upotrebu. [12]

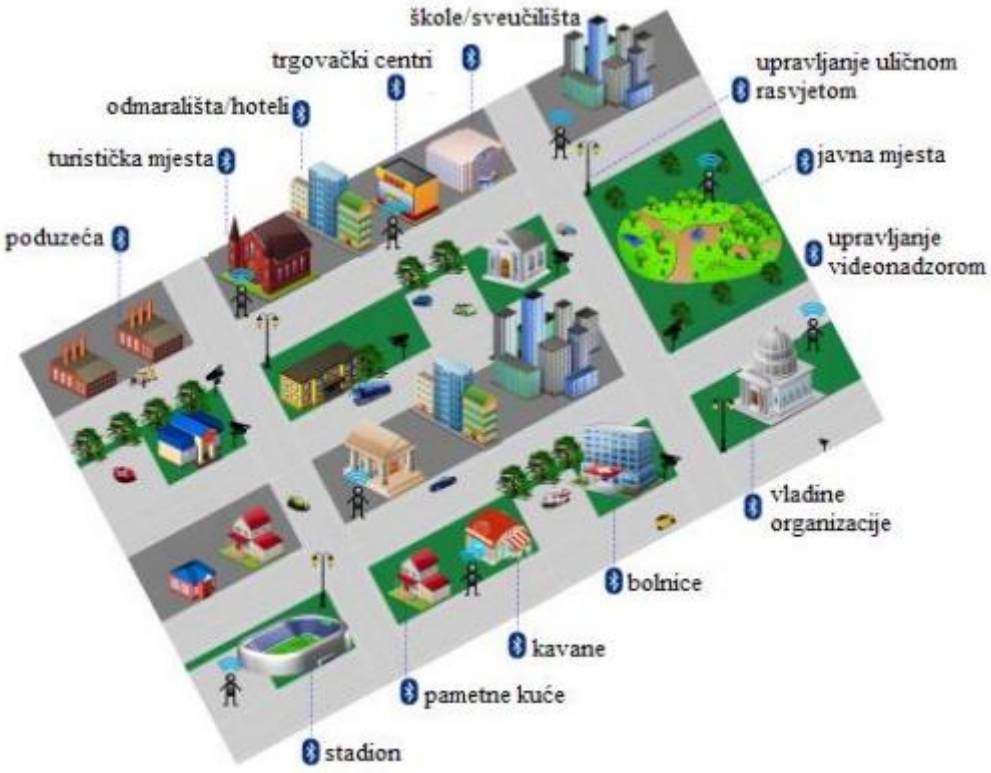
Poboljšanja poput većeg pokrivenog raspona, bržeg prijenosa podataka i povećanja veličine paketa osmišljena su kako bi potaknula širenje i prihvaćanje novog Bluetooth 5 standarda, posebno u svijetu IoT-a.



Slika 3.1. Sustav kućne automatizacije temeljen na Bluetooth-u. [8]

U kontekstu pametnog doma, koji je prikazan na slici 3.1, proširena pokrivenost omogućuje, primjerice korištenje Bluetooth zvučnika bez potrebe za stalnim premještanjem pametnog telefona iz sobe u sobu, dok se istovremeno poboljšava brzina komunikacije između pametnih telefona i nosivih uređaja poput pametnih satova. Vlasnici kuća mogu putem pametnog telefona, tableta ili prijenosnog računala upravljati svjetlima, temperaturom, uređajima, bravama i sigurnosnim sustavima čak i kada su izvan doma, zahvaljujući Bluetooth senzorima raspoređenim po cijelom domu. Ovi senzori, namijenjeni nadzoru temperature, svjetala, vrata, prozora i pokreta, omogućuju jednostavno upravljanje putem aplikacija koje su prilagođene korisnicima. Budući da većina ljudi već posjeduje barem jedan uređaj kompatibilan s Bluetooth-om, poput pametnog telefona, sata ili tableta, lako mogu iskoristiti prednosti tih sustava bez potrebe za učenjem novih tehnologija.

Bluetooth 5 omogućava IoT uređajima, poput pametnih satova, da postanu neovisniji od trenutnog modela uparivanja s aplikacijama. To znači da uparivanje za povezivanje i autorizaciju više nije nužno, čime se povećava autonomija tih uređaja. Na taj način, pametni satovi ili nosivi uređaji, koji su ograničeni veličinom zaslona i kapacitetom baterije, mogu funkcionirati samostalno bez potrebe za stalnim povezivanjem s pametnim telefonom. [12]



Slika 3.2. Bluetooth 5: Omogućavanje povezanog pametnog grada. [8].

U pametnim gradovima koji koriste IoT tehnologije (Slika 3.2), ključno je razviti infrastrukturu koja podržava lokacijske i automatske usluge. U tom kontekstu, upotreba beacon-a postaje izuzetno korisna. Mreža beacon-a može se postaviti na javnim ili privatnim mrežama kako bi prikupljala i slala podatke prema centraliziranom čvorištu. Jedna od glavnih prednosti beacon-a je njihova isplativost u usporedbi s drugim tehnologijama za pametne gradove. Korištenjem Bluetootha 5 kao mehanizma kontrole, gradovi mogu daljinski upravljati različitim vrstama opreme, čime se dodatno povećava učinkovitost. Bluetooth rješenja za pametne gradove mogu poslužiti kao temelj za inovativne usluge nove generacije, osnažujući vlade ili tvrtke te omogućujući stvaranje pametnijih gradova. Ova transformacija postiže se kroz ekosustav koji povezuje različite pružatelje usluga.

Primjerice, voditelji supermarketa, trgovačkih centara ili muzeja mogu iskoristiti ovu tehnologiju. U supermarketima, beacon-i mogu usmjeravati kupce unutar trgovine, slati kupone za popuste i obavijesti o aktualnim ponudama na temelju njihovih profila i navika kupovanja – sve automatski, bez dodatnih radnji korisnika. U muzejima Bluetooth može zamijeniti tradicionalne audio vodiče, pružajući posjetiteljima informacije o izloženim umjetninama putem njihovih pametnih telefona. Sve to uz minimalnu potrošnju energije.

Bluetooth 5 može se koristiti i za upravljanje uličnom rasvjetom, omogućujući precizno daljinsko upravljanje svjetlima u gradu. Ova tehnologija može pružiti povratne informacije u stvarnom vremenu o promjenama u mreži, smanjujući gubitak energije i omogućujući bolju optimizaciju održavanja.

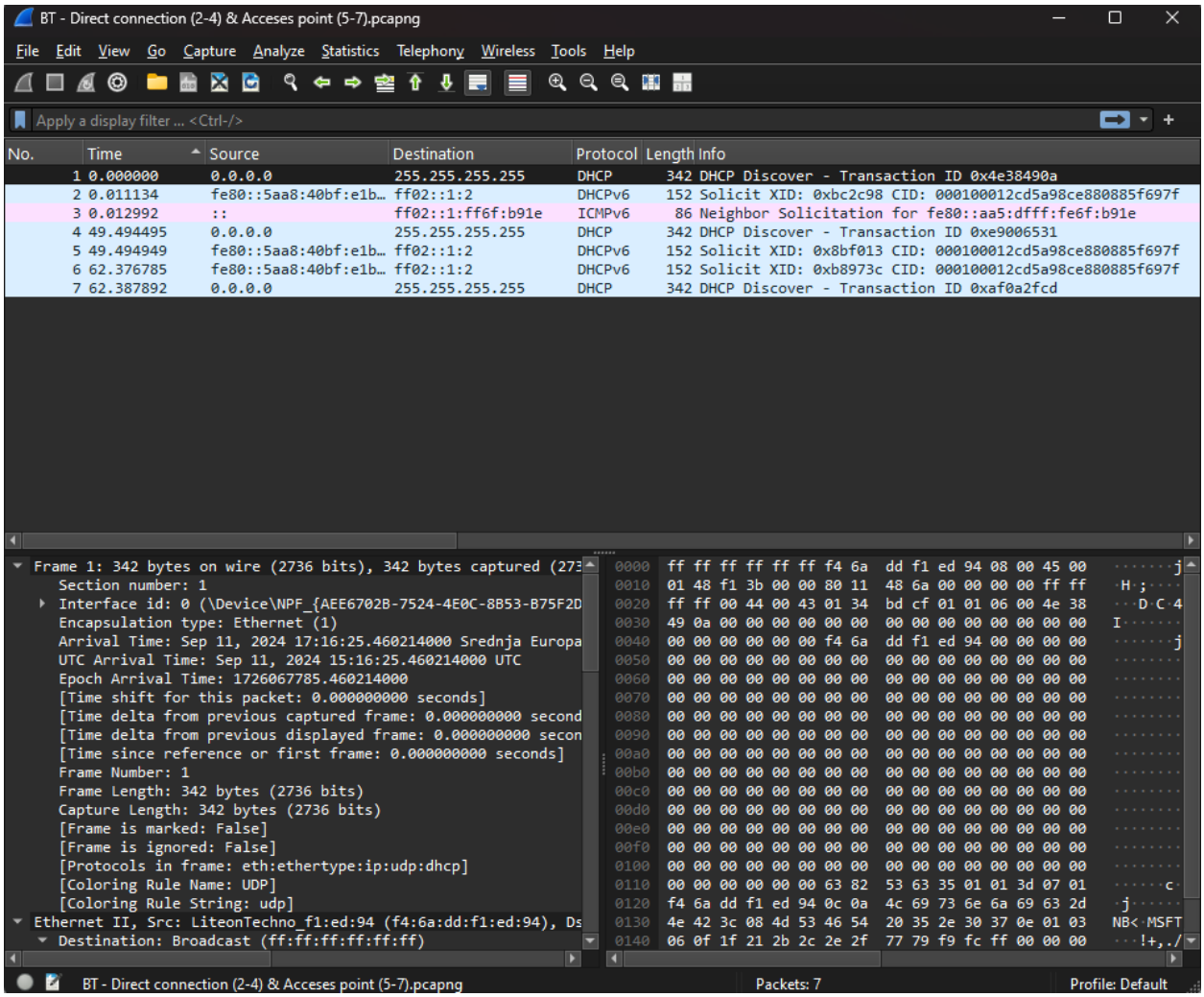
Bluetooth 5 donosi mogućnost emitiranja bogatijih podataka, uključujući informacije o lokaciji, URL-ove i multimedijske datoteke. Primjerice, senzori unutar trgovine mogli bi omogućiti navigaciju do specifičnog artikla, olakšavajući kupcima pronalaženje proizvoda bez potrebe za pitanjem osoblja. Bluetooth 5 mogao bi biti koristan za automobile sa autopilotom, omogućujući im komunikaciju s različitim vanjskim senzorima poput semafora.

Širenje upotrebe beacon-a i dolazak Bluetootha 5 donijet će velike koristi za IoT industriju, iako se trenutačno većina tvrtki fokusira na uređaje temeljene na Bluetooth 4.x tehnologiji. Ako Bluetooth 5 ispuni očekivanja, vjerojatno će još više dobavljača ući na IoT tržište, ponajprije zahvaljujući nižim troškovima čipova.

Bluetooth 5 nije kompatibilan s ažuriranjem starih Bluetooth uređaja. Nova verzija zahtijeva nove čipove koji se moraju instalirati na novije uređaje. Starije verzije Bluetootha mogu raditi s Bluetooth-om 5, ali neće imati napredne značajke poput veće brzine ili dometa. [12]

4. SNIMANJE SIGNALIZACIJE

U praktičnome dijelu snimljena je signalizacija između prijenosnog računala i pametnog telefona. Za snimanje signalizacije korišteno je računalo marke Lenovo, pametni telefon Samsung Galaxy S24 sa ugrađenom Bluetooth verzijom 5.3 i program *Wireshark*, verzija 4.4.0. Na slici 4.1 prikazan je prozor programa nakon snimljene signalizacije između uređaja.



Slika 4.1. Prozor programa Wireshark nakon snimljene signalizacije.

Gornji dio (*Packet List Panel*) prikazuje snimljene pakete s informacijama kao što su vrijeme, izvorna adresa, odredišna adresa, protokol, veličina paketa i dodatne informacije. Snimljeno je sedam paketa. Paketi koriste DHCP (*Dynamic Host Configuration Protocol*) protokol, koji omogućava automatsko dodjeljivanje IP adresa uređajima na mreži. Njegova glavna uloga je olakšavanje procesa postavljanja mrežnih uređaja. Donji lijevi dio (*Packet Details Panel*)

detaljno prikazuje slojeve protokola za odabrani paket. Donji desni dio (*Packet Bytes Panel*) prikazuje podatke paketa u heksadecimalnom i ASCII formatu. To su stvarni bajtovi prenijeti preko mreže i predstavljeni u lako čitljivom formatu.

Prvi paket je inicijalni DHCP Discover paket, gdje klijent pokušava otkriti dostupne DHCP poslužitelje. Kada se uređaj poveže na mrežu, šalje discover poruku kako bi našao DHCP server. Ovaj paket šalje se putem broadcast-a na adresu 255.255.255.255 jer klijent u ovoj fazi nema IP adresu. Broadcast u mrežnim terminima predstavlja način slanja podataka svim uređajima na mreži. Prikazani su razni podaci, primjerice vrijeme: 0.0 s, protokol: DHCP, tip: DHCP Discover, izvor: 0.0.0.0, odredište: 255.255.255.255, duljina: 342 bajta. U Ethernet sloju vidljive su MAC adrese, izvorna: 44:6a:dd:f1:dd:94 i odredišna: ff:ff:ff:ff:ff. U IP sloju vidljiva je verzija IP protokola: IPv4 i protokol: UDP. U UDP sloju, od bitnijih informacija izdvajaju se izvorni port: 68 (klijent) i odredišni port: 67 (DHCP poslužitelj). Iz DHCP sloja vidljivi su podaci poput ID-a transakcije i zahtjevi za informacijama koji se šalju: subnet maska, router, domena.

U paketu broj 2 radi se o IPv6 protokolu i DHCPv6 protokolu. Šalje se DHCPv6 Solicit poruka, koja se koristi u IPv6 mrežama kada klijent traži DHCPv6 servere. Klijent šalje multicast poruku sa adrese fe80::a6ae:bad8:e808:8569 na adresu ff02::1:2 (adresa svih DHCPv6 servera), tražeći konfiguracijske informacije uključujući IPv6 adresu. Multicast poruka oblik je mrežne komunikacije u kojoj se podaci šalju grupi specifičnih uređaja unutar mreže, umjesto svim uređajima kao kod broadcast-a ili samo jednom uređaju kao kod unicast poruka. Odredišne adrese i portovi sada su promijenjeni za DHCPv6 servere i klijente, primjerice izvorni port za DHCPv6 klijente je 546, a odredišni za servere 547.

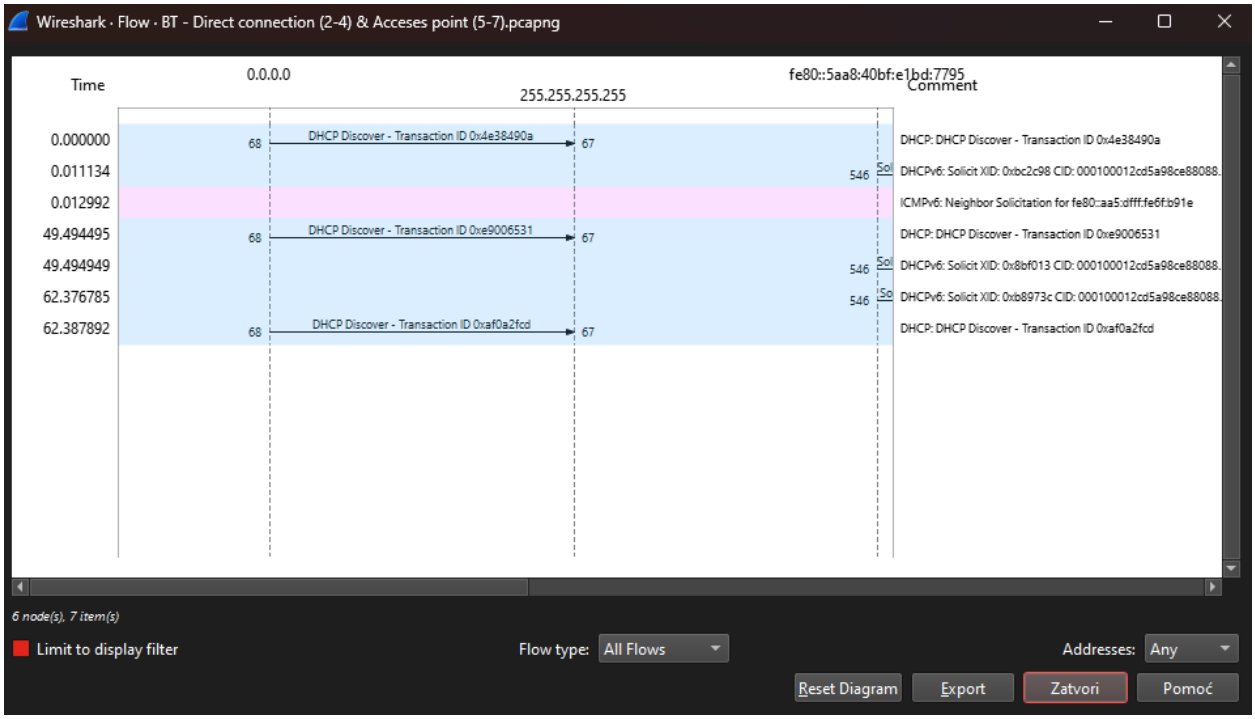
Treći paket je ICMPv6 *Neighbor Solicitation* poruka, koja se koristi u IPv6 mrežama za otkrivanje drugih uređaja. Klijent šalje ovu poruku putem multicast-a u pokušaju da otkrije MAC adresu uređaja koji koristi određenu IPv6 adresu. To je ekvivalent ARP *request* poruci u IPv4 mrežama. Paket se koristi u Neighbor Discovery Protocol-u za IPv6 mreže, što omogućava pravilno funkcioniranje lokalne mreže.

Paket broj 4 je praktično isti kao prvi paket, jer su oba DHCP Discover poruke. Razlog zašto se DHCP Discover poruka u snimljenim paketima ponavlja je zbog toga što je klijent više puta pokušao pronaći DHCP server, ako nije odmah dobio odgovor ili je ponovno tražio IP adresu nakon određenog vremenskog perioda.

Paketi 5 i 6 slični su kao i paket broj 2. Svi ovi paketi šalju Solicit poruku putem DHCPv6 protokola, tražeći DHCPv6 server koji može dodijeliti IPv6 adresu klijentu. Svi koriste multicast adresu ff02::1:2 kao odredište, što je standardna multicast adresa za DHCPv6 servere. Klijent se identificira putem DUID-a (*DHCP Unique Identifier*), što je unikatni identifikator baziran na MAC adresi. Ethernet, IPv6, UDP i DHCPv6 slojevi identični su po strukturi u svim paketima. Razlika je jedino što svaki paket ima drugačiji *Transaction ID*, što služi za identifikaciju i praćenje komunikacije između klijenta i servera. U nekim slučajevima, DUID može varirati ako se radi o različitim klijentima, ali ako je uređaj isti, onda će DUID ostati isti.

Zadnji, sedmi paket po strukturi i funkciji identičan je prvom i četvrtom paketu, osim što se razlikuje u ID-u transakcije (0xa0a72fcd). Klijent ponovo šalje broadcast poruku i traži određene mrežne parametre, kao što su Subnet Mask, Router, DNS server.

Ova snimljena komunikacija pokazuje proces mrežne konfiguracije klijentskog uređaja, koji pokušava dobiti IP adresu i druge mrežne parametre putem DHCP-a za oba protokola (IPv4 i IPv6), što možemo vidjeti i na slici 4.2.



Slika 4.2. Prozor Flow grafa u programu Wireshark.

Na slici 4.2 prikazan je *Flow Graph* iz Wireshark-a koji prikazuje različite mrežne tokove između klijenta i mreže. Iz slike se vidi kako klijent komunicira sa mrežom u pokušaju da dobije

mrežnu konfiguraciju (IPv4 i IPv6 adresu) putem DHCP-a i kako koristi ICMPv6 *Neighbor Solicitation* za otkrivanje susjednih uređaja u IPv6 mreži. Ova slika pokazuje samo inicijalne pokušaje komunikacije od strane klijenta, ali ne pokazuje uspješnu konfiguraciju mreže, jer nema odgovora od servera.

5. ZAKLJUČAK

Bluetooth 5.0 predstavlja značajan korak naprijed u razvoju bežičnih komunikacija, posebno u kontekstu Interneta stvari (IoT). Ova verzija donosi poboljšanja u dometu, brzini prijenosa podataka te energetskoj učinkovitosti u usporedbi s prethodnim verzijama. Povećani kapacitet prijenosa podataka i niža potrošnja energije čine ovu tehnologiju pogodnom za širok raspon uređaja i aplikacija, od pametnih domova do industrijske automatizacije i automobilske industrije.

Upravo su ove prednosti, zajedno s unaprijeđenom sigurnosnom arhitekturom, ključne za sve veću integraciju Bluetooth tehnologije u svakodnevne uređaje i aplikacije.

Bluetooth 5.0 neusporediv je sa starijim verzijama, a njegova fleksibilnost i mogućnosti prilagodbe novim tehnološkim izazovima čine ga tehnologijom budućnosti. S obzirom na sve veće potrebe korisnika za bržom i sigurnijom povezanošću, Bluetooth 5.0 ima potencijal postati temeljna tehnologija u razvoju novih IoT rješenja.

LITERATURA

[1] The History of Bluetooth. *The Auris*. https://theauris.com/blogs/blog/the-history-of-bluetooth

[2] (2009.) Ranjivosti Bluetooth tehnologije. *CERT*. https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2009-11-281.pdf

[3] Browning, D., Kessler G.C. Bluetooth Hacking: A Case Study. *GaryKessler*. https://www.garykessler.net/library/bluetooth_hacking_browning_kessler.pdf

[4] (2023.) The Bluetooth Protocol Stack. *Tutorialspoint*. https://www.tutorialspoint.com/the-bluetooth-protocol-stack

[5] Understanding the Bluetooth Protocol Stack in Mobile Computing: A Layered Architecture with Diagram. *RF Wireless World*. https://www.rfwireless-world.com/Tutorials/Bluetooth-protocol-stack.html#:~:text=between bluetooth devices.-,Cable replacement protocol,specifications over bluetooth physical layer

[6] Bluejacking. *Wikipedia.* https://en.wikipedia.org/wiki/Bluejacking

[7] Bluesnarfing. *Wikipedia*. https://en.wikipedia.org/wiki/Bluesnarfing#Bluesniping

[8] Viescinski, A. (2024.). Bluejacking vs. Bluesnarfing. *Baeldung*. https://www.baeldung.com/cs/bluejacking-vs-bluesnarfing

[9] BlueBorne (security vulnerability). *Wikipedia*. https://en.wikipedia.org/wiki/BlueBorne_(security_vulnerability)

[10] BlueBorne kill-chain on Dockerized Android. *SecSI*. https://secsi.io/blog/blueborne-kill-chain-on-dockerized-android/

[11] Ericsson Unveils the First Bluetooth Phone. *Mobic.* http://www.mobic.com/oldnews/2000/06/ericsson_unveils_the_first_bluet.htm

[12] Collotta, M., Pau, G., Talty T., Tonguz (2018.). Bluetooth 5: A Concrete Step Forward toward the IoT, *ResearchGate*. https://www.researchgate.net/publication/320781837_Bluetooth_5_A_Concrete_Step_Forward_toward_the_IoT

SAŽETAK

Bluetooth tehnologija je od svog osnutka 1994. godine jedan od ključnih pokretača bežične komunikacije između uređaja. Svojim kontinuiranim razvojem, svaka nova verzija Bluetooth-a donosi poboljšanja u brzini prijenosa podataka, energetskoj učinkovitosti, sigurnosti i cjelokupnoj funkcionalnosti. Ovaj rad usmjeren je na Bluetooth verziju 5.0 koja je uvela značajna poboljšanja, uključujući povećani domet, veću brzinu prijenosa podataka i unaprijeđenu podršku za IoT (*Internet of Things*) uređaje. Rad pruža detaljnu analizu tehničkih karakteristika, sigurnosnih protokola i praktičnih primjena Bluetooth 5.0. Uspoređuje se Bluetooth tehnologija s drugim bežičnim tehnologijama, naglašava se njegova uloga u različitim industrijama te raspravlja o potencijalnim sigurnosnim rizicima. Na kraju, prikazana je praktična demonstracija signalizacije između Bluetooth uređaja, pokazujući njegovu primjenu i performanse u stvarnom svijetu.

KLJUČNE RIJEČI: Bluetooth 5.0, bežična komunikacija, IoT, prijenos podataka, sigurnost, enkripcija, mobilni uređaji, prijenos signala.

SUMMARY

Bluetooth technology has been one of the key drivers of wireless communication between devices since its inception in 1994. With its continuous development, each new version of Bluetooth brings improvements in data transfer speed, energy efficiency, security and overall functionality. This paper focuses on Bluetooth version 5.0, which introduced significant advancements, including increased range, higher data transfer speeds, and enhanced support for IoT (*Internet of Things*) devices. The paper provides a detailed analysis of the technical characteristics, security protocols, and practical applications of Bluetooth 5.0. It compares Bluetooth technology with other wireless technologies, highlights its role in various industries, and discusses potential security risks. Finally, a practical demonstration of signaling between Bluetooth devices is presented, showcasing its real-world application and performance.

KEYWORDS: Bluetooth 5.0, wireless communication, IoT, data transfer, security, encryption, mobile devices, signal transmission.

ŽIVOTOPIS

Josip Mišić rođen je 3. siječnja 2001. godine u Požegi. Pohađao je Područnu školu fra Kaje Adžića u Kuzmici, a zatim Osnovnu školu Antuna Kanižlića u Požegi. Srednju Tehničku školu u Požegi upisuje 2016. godine. Maturirao je 2020. godine s odličnim uspjehom i stekao zvanje Tehničara za računalstvo. Na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, 2020. godine upisuje stručni studij računarstva. Interes za računalstvom pokazuje još u osnovnoškolskim danima, što dokazuje i odabir obrazovanja.

Josip Mišić