# Bluetooth Low Energy (BLE) i njegove primjene

**Flisar, Stjepan**



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

**SVEUČILIŠNI STUDIJ**

# BLUETOOTH LOW ENERGY (BLE) I NJEGOVE PRIMJENE

**Diplomski rad**

**Stjepan Flisar**

**Osijek, 2021.**

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

**Obrazac D1: Obrazac za imenovanje Povjerenstva za diplomski ispit**

**Osijek, 06.12.2021.**

**Odboru za završne i diplomske ispite**

# Imenovanje Povjerenstva za diplomski ispit

| | |
|---|---|
| **Ime i prezime studenta:** | Stjepan Flisar |
| **Studij, smjer:** | Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika' |
| **Mat. br. studenta, godina upisa:** | D-1213, 06.10.2019. |
| **OIB studenta:** | 10509221278 |
| **Mentor:** | Izv. prof. dr. sc. Krešimir Grgić |
| **Sumentor:** | |
| **Sumentor iz tvrtke:** | |
| **Predsjednik Povjerenstva:** | Prof.dr.sc. Drago Žagar |
| **Član Povjerenstva 1:** | Izv. prof. dr. sc. Krešimir Grgić |
| **Član Povjerenstva 2:** | Mr.sc. Anđelko Lišnjić |
| **Naslov diplomskog rada:** | Bluetooth Low Energy (BLE) i njegove primjene |
| **Znanstvena grana rada:** | **Telekomunikacije i informatika (zn. polje elektrotehnika)** |
| **Zadatak diplomskog rada:** | Bluetooth Low Energy (BLE) komunikacijski je standard niske energetske potrošnje, prikladan za komunikaciju na manjim udaljenostima. Potrebno je analizirati i objasniti najvažnije karakteristike ovog standarda, te prikazati i usporediti različite primjere njegove praktične primjene, uključujući i rezultate laboratorijskog testiranja. (Student: Stjepan Flisar) |
| **Prijedlog ocjene pismenog dijela ispita (diplomskog rada):** | Vrlo dobar (4) |
| **Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:** | Primjena znanja stečenih na fakultetu: 2 bod/boda<br>Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda<br>Jasnoća pismenog izražavanja: 2 bod/boda<br>Razina samostalnosti: 2 razina |
| **Datum prijedloga ocjene mentora:** | 06.12.2021. |

| | |
|---|---|
| Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija: | Potpis: |
| | Datum: |

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

# IZJAVA O ORIGINALNOSTI RADA

**Osijek, 15.12.2021.**

| | |
|---|---|
| **Ime i prezime studenta:** | Stjepan Flisar |
| **Studij**: | Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika' |
| **Mat. br. studenta, godina upisa:** | D-1213, 06.10.2019. |
| **Turnitin podudaranje [%]:** | 7% |

Ovom izjavom izjavljujem da je rad pod nazivom**: Bluetooth Low Energy (BLE) i njegove primjene**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Krešimir Grgić

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 studenta:

# SADRŽAJ

# 1. UVOD

*Bluetooth Low Energy* (BLE), predstavljen je kao dio specifikacija Bluetooth 4.0 inačice. BLE kao nova bežična tehnologija djeluje jako zanimljiva i uzbudljiva programerima mobilnih aplikacija jer im omogućava besprijekoran pristup, jednostavnost i pouzdanost vanjskim povezanim uređajima. Osobina koju BLE ističe među mnogim sličnim tehnologijama je niska potrošnja energije povezanih perifernih uređaja, gdje jedan povezani senzor može raditi i na dugmastoj litij-ion bateriji mjesecima. Znatno se razlikuje od BR/EDR (engl. *Bluetooth Basic Rate/Enhanced Data Rate*) uređaja starijih inačica Bluetooth-a koji imaju kraći domet, te kontinuiranu bežičnu vezu što ga čini idealnim za uporabe kao što je slušanje glazbe sa pametnog telefona preko slušalica. BLE omogućuje kratke nizove radijskih veza velikog dometa, što ga čini idealnim za IoT (engl. *Internet of Things*) aplikacije koje ovise o trajanju baterije. U komunikaciji mogu sudjelovati 4 vrste uređaja koji svojim karakteristikama izvršavaju određene radnje. Prije same uspostave komunikacije svaki uređaj izvršava određene radnje kako bi se međusobno „vidjeli“ i vršili prijenos podataka. BLE uvodi nove koncepte kao što su *Generic Attributes* (GATT) profile koji opisuju upotrebu, ulogu, i općenito ponašanje na temelju GATT funkcionalnosti. Spomenuti profili dopuštaju programerima brzo i jednostavno razvijanje aplikacija za povezivanje uređaja izravno s aplikacijama na pametnim telefonima, osobnim računalima ili tabletima. Također podržan na iOS, Android, macOS, Windows 10 i Linux. Povećana uporaba pametnih uređaja u svim procesima rada povećava razvoj novih jeftinih BLE uređaja na tržištu koji svojim mogućnostima mogu pridonijeti boljem praćenju, analiziranju i boljitku radnih procesa. Kao i kod ostalih bežičnih tehnologija potrebno je pronaći i implementirati različita rješenja kako bi se dobila veća sigurnost u komunikaciji protiv neželjenih napada.

Zadatak ovog rada je objasniti arhitekturu i glavne koncepte BLE-a koje ga čine boljim u odnosu na druge mobilne mreže kratkog dometa. Bit će objašnjeni koji uređaji sudjeluju u komunikaciji, njihov princip uspostave međusobne veze i sigurnosne značajke i faze prilikom uspostavljanja veze. Također će biti objašnjen *Bluetooth mesh* koji svojim poboljšanjima pronalazi veliku primjenu unutar IoT okruženja. Primjena BLE-a biti će predstavljena u primjerima iz IoT okruženja i u testnom okruženju sa BLE modulima i kompatibilnim BLE pametnim uređajima.

# 2. BLUETOOTH TEHNOLOGIJA

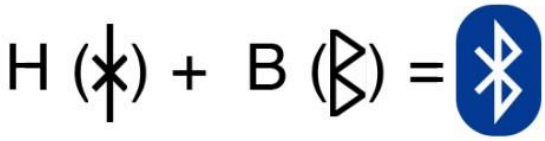
*Bluetooth* je telekomunikacijski standard bežične tehnologije kratkog dometa koji se koristi za povezivanje više različitih uređaja, čime se omogućava slanje podataka između istih. Inicijalna ideja razvoja i pojave *Bluetooth*-a se pojavila radi potrebe povezivanja mobilnih uređaja, mobilnih uređaja i slušalica, ali mu se s vremenom povećalo korištenje u drugim primjenama. Danas je *Bluetooth* neizostavna tehnologija koja se nalazi gotovo u svim uređajima svakodnevne upotrebe kao što su pametni telefoni, bežične slušalice, pisači, automobili, računala itd.


*Slika 2.1. Logo Bluetooth-a* [1]

## 2.1. Razvoj Bluetooth-a i Bluetooth SIG-a

Razvoj *Bluetooth* tehnologije započeo je 1994. godine. Tvrtka Ericsson predstavila je koncept bežične mreže koja povezuje uređaje poput mobitela i slušalica, ali iza prvotne ideje, koja još nije dobila svoj službeni naziv, krila se puno veća mogućnost a to je spajanje različitih uređaja. Kako bi se ideja mogla razvijati, bila je potreba postojanja industrijskog standarda, stoga su se u veljači 1998. g. 5 velikih tvrtki udružilo i formiralo interesnu skupinu pod nazivom *Bluetooth* SIG (engl. *Bluetooth Special Interest Group*). Skupinu su tad činile tvrtke Ericsson, Nokia, IBM, Toshiba i Intel. Danas ta brojka prelazi 36 000 tvrtki [1].

Sami naziv *Bluetooth* je dobio po danskom kralju Harald Blåtand (engl. *Harald Bluetooth*). Bio je poznat po svojim komunikacijskim vještinama i kao mirotvorac zaraćenih naroda na području Skandinavije. Stoga je naziv „Bluetooth“ odabran jer omogućuje komunikaciju između različitih uređaja. Logo *Bluetooth*-a prikazan je na slici 2.2., te je kombinacija dvaju nordijskih znakova a koja predstavljaju inicijale, H i B, danskog kralja.



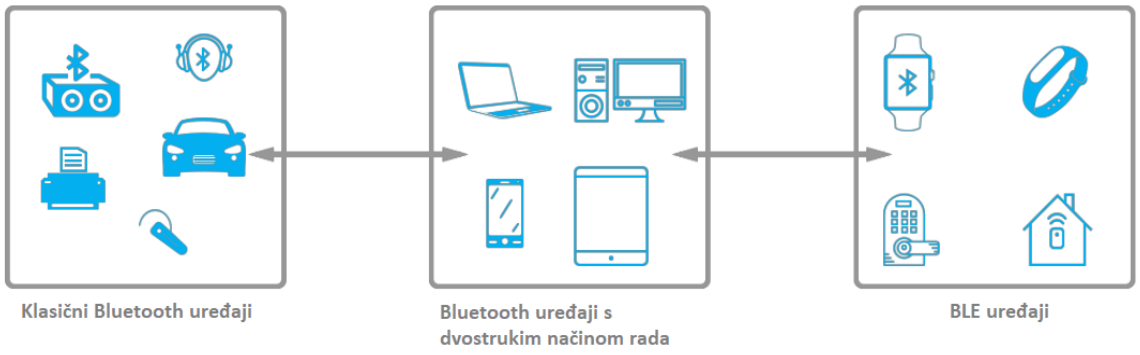

*Slika 2.2. Logo Bluetooth-a sa kombinacijom nordijskih znakova* [1]

# 3. BLUETOOTH LOW ENERGY TEHNOLOGIJA

Postoje dvije vrste *Bluetooth* uređaja: jedni se nazivaju klasični *Bluetooth* uređajima (BR/EDR), a drugi su *Bluetooth Low Energy* (BLE) uređaji. *Bluetooth* inačica 4.0 predstavlja *Bluetooth Low Energy* (BLE), također poznat pod nazivom *Bluetooth Smart*, odnosno *Bluetooth* sa smanjenom potrošnjom energije. Sami naziv ističe njegovu najveću prednost, a to je niska potrošnje energije u sustavima gdje je ona presudna, poput uređaja na baterije i gdje se male količine podataka prenose rijetko, npr. u aplikacijama gdje očitavamo vrijednost sa senzora. Iako dijele slične specifikacije i nazive ove dvije vrste uređaja su nekompatibilne [3].


*Slika 3.1. Logo Bluetooth Smart-a*

Klasični Bluetooth uređaj ne može komunicirati sa BLE uređajima. To je razlog zašto neki uređaji , poput pametnih telefona, odlučili implementirati oba tipa te im dopustiti komunikaciju s obim vrstama uređaja. Takvi uređaji nazivaju se *Bluetooth* uređaji s dvostrukim načinom rada, engl. *Dual Mode Bluetooth Devices*.




*Slika 3.1. Tipovi Bluetooth uređaja* [3]

Budući da mnogi sustavi IoT-a (engl. *Internet of Things*) uključuju male uređaje i senzore, BLE postaje šire upotrjebljena tehnologija u odnosu na klasični *Bluetooth* u IoT-u.

## 3.1. Razlika u odnosu na klasični Bluetooth

Važno je napomenuti da postoji velika razlika u tehničkim specifikacijama, implementaciji i vrsti primjene između klasičnog *Bluetooth*-a i BLE-a. Dodatak je činjenici da su međusobno nekompatibilni. Neke od značajnih razlika prikazane su u tablici 3.1.:

*Tablica 3.1. Razlika između klasičnog Bluetooth-a i Bluetooth Low Energy-a*

| Klasični Bluetooth | Bluetooth Low Energy |
|---|---|
| Koristi se u *streaming* aplikacijama za prijenos podataka, slušalice i prijenos multimedije uživo | Koristi se za podatke senzora, kontrolu uređaja, i aplikacije niske propusnosti |
| Nije optimiziran za rad s malom snagom, ali ima veću brzinu prijenosa podataka (maksimalno 3Mbps u usporedbi s 2Mbps za BLE) | Namijenjen za rad na niskim snagama i niskim opterećenjima podatkovnih ciklusa |
| Radi na preko 79 radio frekvencijskih kanala | Radi na više od 40 RF kanala |
| Otkrivanje se događa na 32 kanala. | Do pronalaženja uređaja dolazi na 3 kanala, brže i otkrivanje i povezivanje u odnosu na klasični Bluetooth |

BLE je prošao kroz velike promjene u kratkom vremenu od službenog objavljivanja 2010. godine, a posljednje veliko ažuriranje je *Bluetooth* 5 objavljen u prosincu 2016. *Bluetooth* 5 uveo je mnoge nadogradnje u *Bluetooth* specifikaciju a usmjerene na BLE. Neka od najvažnijih poboljšanja uključuju dvostruko veća brzina, četiri puta veća od raspona i osam puta veća od oglasnih podataka.

## 3.2. Tehničke specifikacije

Neke od najvažnijih tehničkih specifikacija BLE-a:

- Frekvencijski spektar kreće se od 2,400 do 2,4835 GHz
- Frekvencijski spektar je segmentiran na 40 kanala od 2MHz
- Maksimalna brzina prijenosa podataka koju podržava je 2Mbps

- Raspon ovisi o okruženju komuniciranja BLE uređaja, kao i načinu rada. Tipična udaljenost iznosi 10 do 30 metara
- Potrošnja baterije varira, a ovisi o radu aplikacije, BLE parametrima i korištenom setu čipa. Najveća potrošnja struje BLE set čipova tijekom radijskog prijenosa ispod 15mA
- Sigurnost ovisi o uređaju i aplikaciji
- Za sve operacije kriptiranja, BLE koristi AES CCM sa 128-bitnim ključem.
- BLE je dizajniran za aplikacije niske propusnosti prilikom prijenosa. Implementacija BLE-a za aplikacije velike propusnosti ugrožavaju nisku potrošnju baterije.
- *Bluetooth* inačice (odnoseći na BLE) međusobno su kompatibilne. Međutim, komunikacija može biti ograničena na između komunikacije dva uređaja starije inačice *Bluetooth*-a. Na primjer, *Bluetooth* 5 BLE uređaj može komunicirati s *Bluetooth* 4.1. uređajem, ali specifične značajke za inačicu 5 neće biti podržane [4].

## 3.3. Prednosti i ograničenja

Svaka tehnologija ima svoja ograničenja i prednosti, pa tako i BLE. BLE tehnologija najprikladnija je za aplikacije s relativno kratkim dometom komunikacije i neučestalim prijenosom podataka niske propusnosti.

### 3.3.1. Ograničenja

Protok podataka BLE-a ograničen je fizičkom brzinom prijenosa radijskih podataka, što je brzina pri kojoj radio frekvencije prenose podatke. Ova brzina ovisi o korištenoj inačici *Bluetooth*-a. Na aplikacijskom sloju za krajnjeg korisnika brzina prijenosa podataka znatno je niža od standardne brzine *Bluetooth*-a pojedine inačice zbog slijedećih čimbenika:

- Praznina između paketa: *Bluetooth* specifikacija definira praznine od 150 milisekundi između paketa koji se prenose kao uvjet pridržavanja pojedinih inačica. Ta praznina je izgubljeno vrijeme bez razmjene podataka između dva uređaja.
- Opterećenja paketa: svi paketi sadrže informacije zaglavlja i podatke kojima se rukuje na nižim slojevima od aplikacijskoga, koje se računaju u podatke i prenose ali nisu dio podatka koje ta aplikacija koristi.
- Zahtjeva za pakete podataka perifernog uređaja: zahtjev za slanje paketa od perifernog uređaja, čak i kada nije potrebno da se oni šalju te se šalju prazni paketi.
- Ponovni prijenos paketa: u slučaju gubitka paketa ili smetnji uređaja u okolini, gubitku korumpiranog paketa budu poslani ponovo od pošiljatelja [4].

BLE je dizajniran za primjenu na kratkome dometu i zbog toga je njegov opseg rada ograničen. Postoji nekoliko čimbenika koji ograničavaju raspon BLE-a, uključujući:

- Radi u području 2.4 MHz ISM (engl. *Industrial, Scientific and Medical band*) spektru na koji uveliko utječu prepreke oko nas, poput metalnih predmeta, zidova i vode (osobito ljudskih tijela)
- Performanse i dizajn antene BLE uređaja
- Fizičko kućište uređaja koje utječe na performanse antene, osobito ako se radi o unutarnjoj anteni
- Orijentaciji uređaja, koja se učinkovito odnosi na pozicioniranje antene (npr. pametni telefoni)

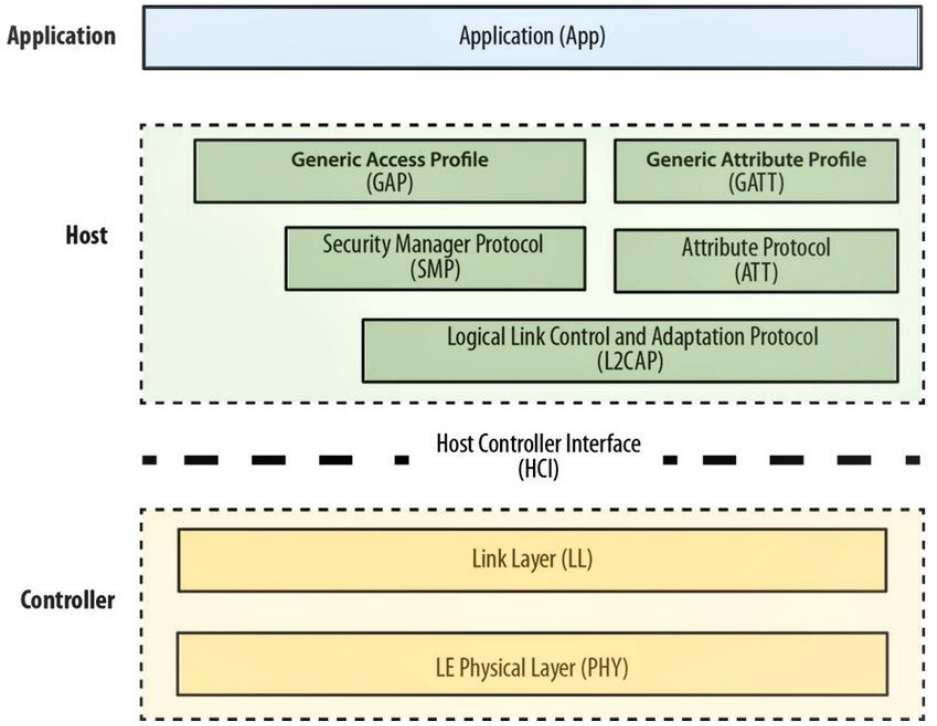
### 3.3.2. Prednosti

Čak i s prethodno spomenutim ograničenjima, BLE ima neke značajne prednosti u odnosu na neke druge tehnologije koje se koriste u IoT okolini. Neke od prednosti uključuju:

- Manja potrošnja energije: čak i u usporedbi s drugim tehnologijama niske potrošnje energije, BLE postiže još manju potrošnju energije od konkurenata. Troši manje energije čestim isključivanjem veze, uz slanje malih količina podataka na niskim razinama brzine prijenosa
- Besplatan pristup službenim dokumentima specifikacija: kod većine drugih bežičnih protokola i drugih tehnologija potrebno je postati član službene grupe kako bi se pristupilo službenim specifikacijama, koje se naplaćuju. Kod BLE-a (verzije 4.0., 4.1., 4.2., i 5) dokumenti sa specifikacijama dostupni su besplatno i mogu se preuzeti sa službene *Bluetooth* stranice
- Niži troškovi modula i čipova: u usporedbi s drugim sličnim tehnologijama
- Njegovo postojanje u većini pametnih telefona na tržištu: jedna od najvećih prednosti koju BLE ima u odnosu na konkurente [3]

# 4. ARHITEKTURA BLE-a

Korisnici, uređaji, će komunicirati izravno samo sa gornjim slojevima protokolnog stoga BLE arhitekture, a kako bi razumjeli kako i zašto stvari funkcioniraju i na koji način bit će objašnjeno od donjih početnih slojeva. Slika 4.1. prikazuje arhitekturu protokolnog stoga BLE-a koji je podijeljen u tri sloja: sloj kontroler-a, sloj host-a i aplikacijski slij.




*Slika 4.1. Arhitektura protokolnog stoga BLE-a [8]*

Svaki od navedenih slojeva stoga sastoji se od zasebnih slojeva koji pružaju funkcionalan rad BLE-a.

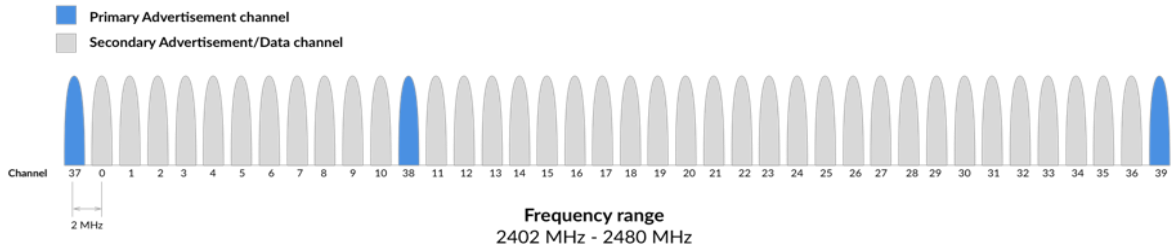
## 4.1. Kontroler

Kontroler se sastoji od slijedećih slojeva:

- Fizički sloj
- Sloj linka
- *Host Controller Interface* (HCI) – na strani kontrolera

Fizički sloj odnosi se na radijski hardver koji se koristi za komunikaciju i modulaciju/demodulaciju podataka. BLE radi u pojasu širine 2.4 GHz (ISM) koji je

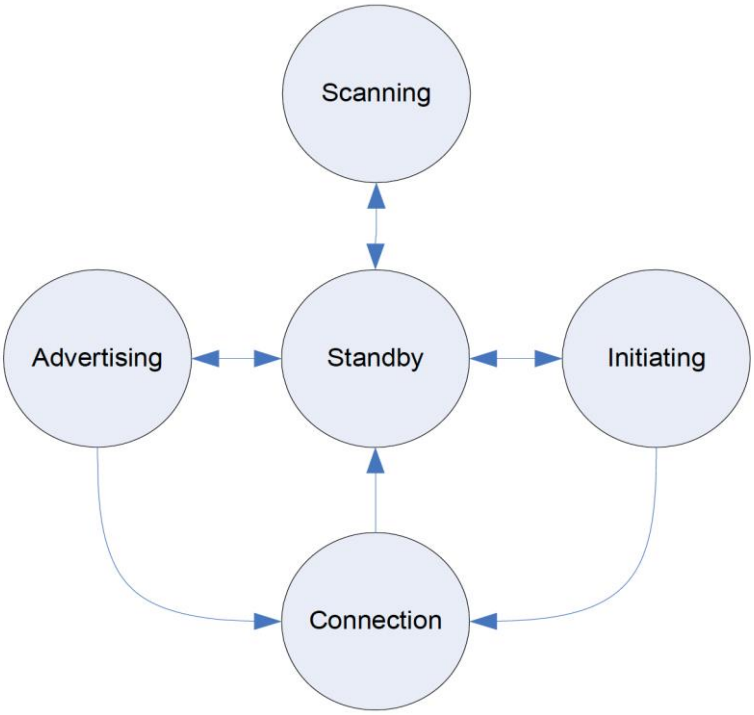
segmentiran u 40 radio frekvencijskih kanala, svaki širine po 2 MHz (od središta jednog kanala do drugog). Slika 4.2. prikazuje BLE frekvencijski spektar [8].




*Slika 4.2. Frekvencijski spektar BLE-a [3]*

BLE od ukupnih 40 kanala posljednja tri kanala koristi za oglašavanje, sa indeksima 37, 38, i 39, dok se preostalih 37 od indeksa 0 do 36 se koriste za prijenos podataka tijekom veze. Kanali za oglašavanje nazivaju se također i primarnim kanalima dok kanali za prijenos podataka sekundarnim kanalima. Oglašavanje uvijek započinje slanjem oglašivačkih paketa primarnim kanalima za oglašavanje, ili podskupom tih kanala. Fizički sloj koristi *Frequency Hopping Spread Spectrum* (FHSS) koji omogućuje u komunikaciji između dva uređaja odabir slučajnog odabranog sekundarnog kanala za razmjenu podataka. Time se postiže pouzdanost i izbjegava korištenje već zauzetog kanala koji mogu onda biti zagušeni.

Sloj linka je sloj koji povezuje i komunicira, fizički sloj sa slojevima više razine. Odgovoran je za upravljanje stanjima u fizičkom sloju kao i vremenskim zahtjevima potrebnim za zadovoljavanje BLE specifikacija. Odgovoran je također za upravljanje operacijama kao što su: CRC, generiranje slučajnih brojeva i šifriranje. Tri stanja u kojima BLE uređaji rade su stanje oglašavanja, stanje skeniranja i povezano stanje. Kada se uređaj oglašava, dopušta drugim uređajima koji skeniraju da ih pronađu i omoguće povezivanje s njima. Ako uređaj koji se oglašava dopusti vezu i uređaj koji skenira pronađe i odluči se spojiti, oba uređaja ulaze u stanje povezivanja. Sloj veze upravlja različitim stanjima, prikazana su na slici 4.3. [3].




*Slika 4.3. Stanja na sloju linka [4]*

Stanje čekanja (engl. *Standby*) je zadano stanje u kojem se ne odašilju niti primaju podaci. Stanje oglašavanje (engl. *Advertising*) je stanje gdje uređaj šalje pakete za oglašavanje drugim uređajima kako bi se mogli prepoznati i pročitati. Stanje skeniranja (engl. *Scanning*) je stanje gdje uređaj skenira uređaje koji su u stanju oglašavanja. Stanje iniciranja (engl. *Initiating*) je stanje gdje uređaj koji skenira odluči uspostaviti komunikaciju sa uređajem koji se oglašava. Stanje ostvarene veze (engl. *Connection*) je stanje u kojem uređaj ima uspostavljenu vezu s drugim uređajem te razmjenjuju međusobno podatke. U stanju ostvarene veze uređaj koji inicira komunikaciju naziva se centralni uređaj, dok uređaj koji se oglašavao naziva periferni uređaj. BLE uređaji se identificiraju s 48-bitnom adresom, slično kao i MAC adresa. Postoje dvije glavne vrste adresa, javne i nasumične. Javne adrese (engl. *Public Address*) su tvorničke postavljene adrese koje su registrirane sa IEEE. Nasumična adresa (engl. *Random Address*) ne mora biti registrirana u IEEE-u te može biti ugrađena u uređaju ili generirana.

HCI sloj na strani kontrolera je standardni protokol koji omogućuje komunikaciju između kontrolera i hosta. Kontroler i host mogu postojati u jednom skupu čipova ili biti razdvojeni. Zadaća HCI-a je prenijeti naredbe od hosta do kontrolera i slanje odgovora s kontrolera prema hostu [4].

## 4.2. Host

Host dio protokolnog stoga sastoji se od:

- *Logical Link Control and Adaptation Protocol* (L2CAP)
- *Attribute Protocol* (ATT)
- *Generic Access Profile* (GAP)
- *Generic Attribute Profile* (GATT)
- *Security Manager* (SM)
- *Host Controller Interface* (HCI) — na strani host-a

L2CAP djeluje kao protokol-multipleks. Također je sastavio dio starijih inačica *Bluetooth*-a te kao zadatak u BLE-u ima sljedeće:

- Uzima više protokola iz gornjih slojeva i smješta ih u standardne BLE pakete koji se prenose u donje slojeve
- Rukuje fragmentacijom i rekombinacijom. Uzima veće pakete od gornjih slojeva i dijeli ih na dijelove koji odgovaraju najvećem podržanom BLE prometu. Na strani primatelja uzima više paketa i spaja ih u jedan paket koji može biti podržan u gornjem sloju [4].

Za BLE L2CAP rukuje sa ATT-om i SMP-om. ATT čini osnovu razmjene podataka u BLE aplikacijama, dok SMP pruža okvir za generiranje i distribuciju sigurnosnih ključeva među povezanim uređajima.

*Attribute Protocol* (ATT), *Generic Access Profile* (GAP), *Generic Attribute Profile* (GATT), i *Security Manager* (SM) obrađeni su detaljnije u sljedećim poglavljima.

# 5. BLE CENTRALNI I PERIFERNI UREĐAJ

Periferni uređaj je uređaj koji najavljuje svoju prisutnost slanjem oglašivačkih paketa i prihvaća vezu s drugim BLE uređajima. Srodni pojam koji se koristi je BLE emiter. Oba uređaja šalju oglašivačke pakete ali razlika se očituje u BLE emiteru, koji ne uspostavlja vezu sa drugim BLE uređajem.

Centralni uređaj je uređaj koji otkriva i osluškuje druge BLE uređaje koji se oglašavaju. Posjeduje mogućnost uspostavljanja veze perifernim uređajima. Promatrač (engl. *Observer*) je sličan tip BLE centralnog uređaja ali nema mogućnost pokretanje veze s drugim perifernim uređajima. Tablica 5.1. prikazuje razlike između perifernih uređaja, emitera, centralnog uređaja i promatrača [3].

*Tablica 5.1. Razlika između emitera, perifernog uređaja, promatrača i centralnog uređaja [3]*

| Emiter | Periferni uređaj | Promatrač | Centralni uređaj |
|---|---|---|---|
| Nije potreban prijemnik | Potrebni prijemnik i predajnik | Nije potreban predajnik | Potrebni prijemnik i predajnik |
| Ne podržava dvosmjeran prijenos podataka | Podržava dvosmjeran prijenos podataka | Ne podržava dvosmjeran prijenos podataka | Podržava dvosmjeran prijenos podataka |
| Smanjeni hardver, smanjeni BLE protokolni stog | Zahtjeva cjeloviti BLE protokolni stog | Smanjeni hardver, smanjeni BLE protokolni stog | Zahtjeva cjeloviti BLE protokolni stog |

BLE je po dizajnu asimetričan jer se veći dio poslova u vezi upravljanja vezama, vremenom i procesnim odgovornostima za obradu podataka nalazi na centralnoj strani komunikacije. Upravo zbog toga potrošnja energije i zahtjevi za procesnom snagom perifernih uređaja je smanjena čime se daje mogućnost integriranje BLE-a u manje uređaje napajane baterijama. Centralni uređaj se također može napajati baterijama, ali će ona biti veća. U najčešćim slučajevima centralni uređaj je pametnih telefon, tablet, ili računalo. Centralni uređaj ima mogućnost povezivanja s više perifernih uređaja istovremeno. Tipični primjer su pametni telefoni koji održavaju vezu sa pametnim satom, *fitness tracker*-om, termostatom pametne kuće, sve istovremeno [3].

U nekim slučajevima, BLE uređaj može istovremeno djelovati u više uloga. Na primjer, uređaj može nadzirati više senzora (periferni uređaj), a u isto vrijeme moći oglašavati svoju prisutnost pametnom telefonu kako bi omogućio pristup podacima senzora sa sučelja mobilne aplikacije [3].

# 6. OGLAŠAVANJE I SKENIRANJE

## 6.1. GAP

GAP definira interakciju između uređaja. To uključuje sljedeće:

- Načini i uloge BLE uređaja
- Oglašavanje
- Uspostavu veze
- Sigurnost

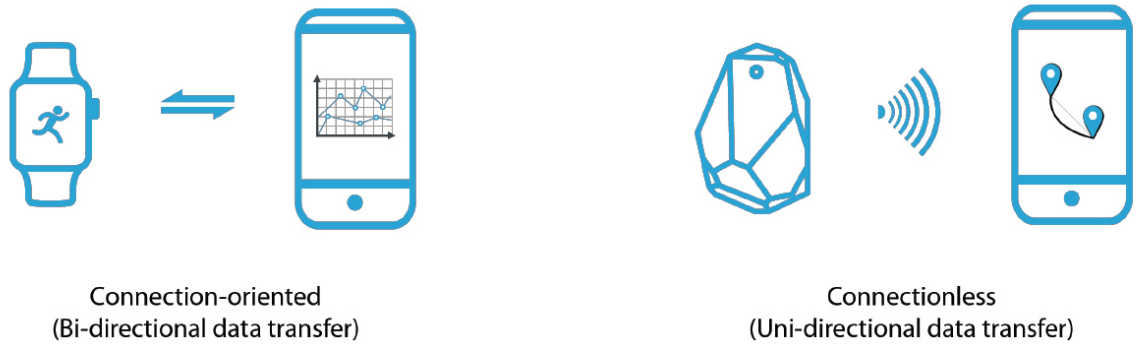
Implementacija GAP-a obavezna je prema službenoj specifikaciji BLE-a, i daje mogućnost da dva ili više BLE uređaja međusobno surađuju, komuniciraju i mogu razmjenjivati podatke jedan s drugim.

BLE uređaj uvijek se pokreće u stanju oglašavanja. Čak i kad većinu vremena želi raditi u povezanom stanju. Kako bi dva BLE uređaja otkrili jedan drugoga, jedan se mora oglašavati, dok drugi skenira tri primarna kanala oglašavanja tražeći oglašivačke pakete koje šalje uređaj. Ako uređaj koji se oglašava podržava vezu i centralni uređaj ju otkrije, može odabrati hoće li uspostaviti vezu [11].

## 6.2. Stanje oglašavanja

U stanju oglašavanja, uređaj šalje pakete koji sadrže korisne podatke drugima koji ih primaju i obrađuju. Paketi se šalju u fiksnom intervalu definiranom kao interval oglašavanja. Oglašavanje započinje s oglašivačkim paketima koji se šalju primarnim kanalima oglašavanja (ili podskupa tih kanala). To omogućuje centralnom uređaju da pronađe uređaj koji se oglašava (periferni) i raščlani njegove oglasne pakete. Centralni uređaj tada pokreće vezu ako to oglašivač dopušta. Centralni uređaj također može zatražiti ono što se naziva zahtjevom za skeniranje, a ako ga oglašivač podržava, odgovorit će mu skeniranjem. Zahtjevi za skeniranje i odgovori omogućuju oglašivaču slanje dodatnih podataka o oglašavanju koji se ne bi uklopili u početni paket. Primarni podaci oglašavanja ograničeni su na 31 bajt, a sekundarni podržavaju 254 bajta podataka. Neki uređaji (emiteri) ostaju u stanju oglašavanja i ne prihvaćaju veze (bez veze), dok druge (periferne jedinice) dopuštaju prijelaz na povezano stanje ako centralni uređaj započinje vezu (orijentirano na povezivanje). Na primjer, većina BLE transmitera ostaje u stanju oglašavanja tijekom vijeka trajanja uređaja. Glavna prednost zadržavanja u stanju oglašavanja je to što više centralnih uređaja može otkriti oglasne podatke bez potrebe za

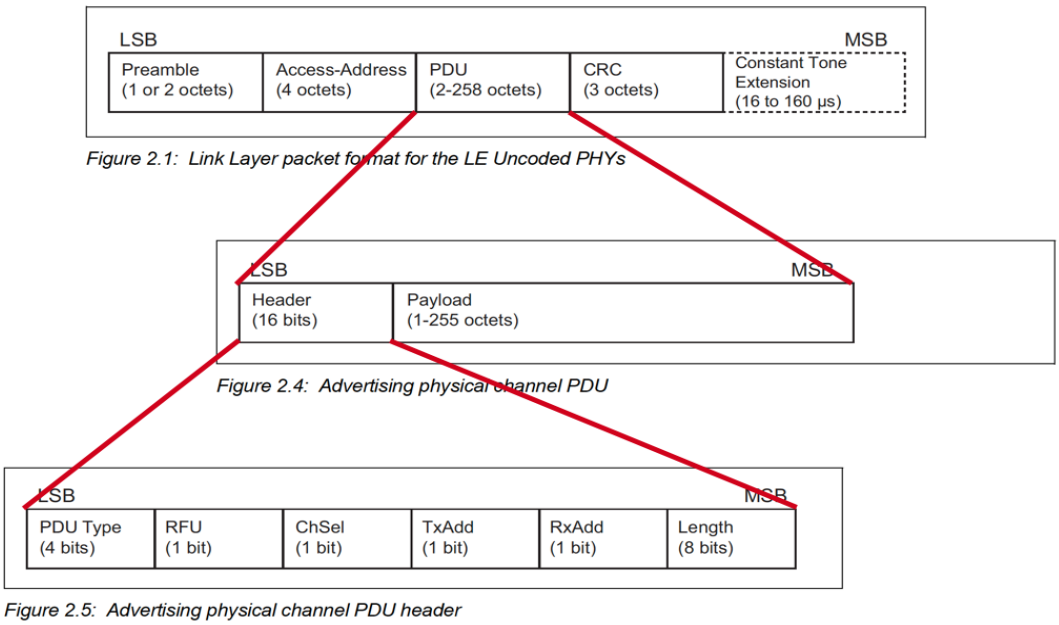
povezivanjem. Međutim, postoje i nedostaci, a to su slaba sigurnost i nemogućnost oglašivača da prima podatke od centralnog uređaja (prijenos podataka je jednosmjeran) [11].




*Slika 6.1. Dvosmjerno i jednosmjerno komuniciranje [11]*

Prilikom stanja oglašavanja sudjeluju parametri kao što su:

- Interval oglašavanja: predstavlja najznačajniji parametar. Vrijednost mu se kreće u rasponu od 20 milisekundi do 10.24 sekunde u malim koracima od 625 mikro sekundi. Interval oglašavanja utječe na trajnost baterije uređaja i treba ga pažljivo definirati. Preporuča se odabir najdužeg intervala koji će osigurati ravnotežu između brzog povezivanja i smanjenje potrošnje energije
- Podaci odgovora na oglašavanje/skeniranje: slika 6.2. prikazuje format jednog paketa prilikom oglašavanja. Odgovor na skeniranje dijeli isti format paketa.




*Slika 6.2. Format jednog paketa oglašavanja [11]*

Podaci oglašavanja ulaze u PDU dio BLE paketa i sadrži slijedeće:

- Duljinu: prikazana duljinom samog podatka
- Vrstu podatka (AD *Type*)
- Podacima oglašavanja

Postoje 4 različita tipa paketa oglašavanja koji su prikazani u tablici 6.1..

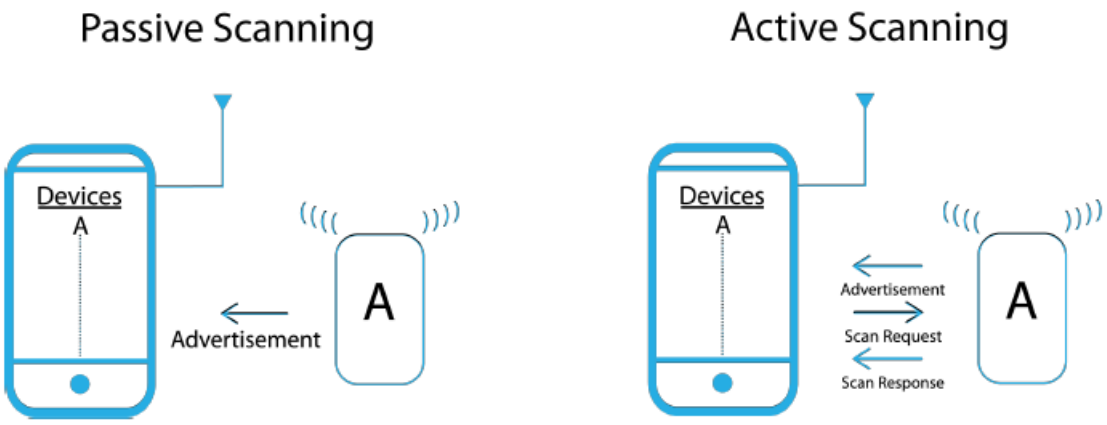
*Tablica 6.1. 4 različita tipa paketa oglašavanja* [11]

| Oglašivački PDU | Opis | Max. duljina podataka oglašavanja podatka | Maksimalna duljina resursa skeniranja | Dopušteno povezivanje |
|---|---|---|---|---|
| ADV_IND | Koristi se za slanje povezivih neusmjerenih oglasa | 31 bajt | 31 bajt | Da |
| ADV_DIRECT_IND | Koristi se za slanje povezivih usmjerenih oglasa | N/A | N/A | Da |
| ADV_SCAN_IND | Koristi se za slanje neusmjerenih oglasa koji mogu biti skenirani | 31 bajt | 31 bajt | Ne |
| ADV_NONCONN_IND | Koristi se za slanje ne povezivih neusmjerenih oglasa | 31 bajt | N/A | Ne |

## 6.3. Stanje skeniranja

Centralni uređaji podešavaju se na tri primarna kanala za oglašavanje jedan po jedan. Kako bi centralni uređaj otkrio periferni uređaj, on se mora podesiti na isti kanal na kojemu se periferni uređaj oglašava. Kako bi se povećala mogućnost da se to dogodi i kako bi se to brže dogodilo, pruža se mogućnost prilagođavanja nekoliko parametara za oglašavanje i skeniranje. Uređaj koji osluškuje oglašivače, a zatim šalje zahtjeve za skeniranje od oglašivača, definira aktivan

način skeniranja, dok je uređaj koji pasivno osluškuje oglašivačke pakete i ne šalje zahtjeve za skeniranje definiran pasivnom načinu skeniranja.

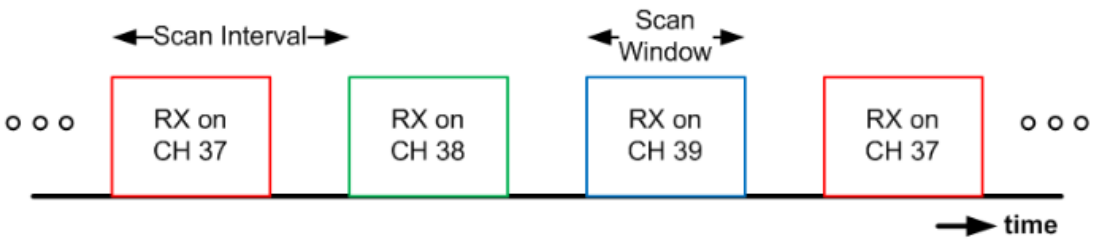



*Slika 6.3. Pasivno i aktivno skeniranje* [6]

Skeniranje se sastoji od tri glavna parametra:

- Vrste skeniranja (engl. *Scan Type*): pasivno ili aktivno skeniranje
- Prozora skeniranja (engl. *Scan Window*): pokazuje koliko vremenski dugo skenira oglašivače
- Intervala skeniranja (engl. *Scan Interval*): označava koliko često treba skenirati za oglašivačima

Uređaj koji skenira osluškivati će cjeloviti prozor u trajanju svakog intervala skeniranja, i u svakom prozoru skeniranja osluškivati će na različitim primarnim kanalima oglašavanja. Prozor skeniranja i interval su konfiguracijski aspekti ponašanja uređaja koji skenira. Slika 6.4. prikazuje graf sa intervalom i prozorom skeniranja [6].




*Slika 6.4. Graf intervala i prozora skeniranja* [8]

# 7. SERVISI I KARAKTERISTIKE

Kao uvod u servise i karakteristike, trebamo detaljnije objasniti vrlo važna dva koncepta: *Generic Attribute Profile* (GATT) i *Attribute Protokol* (ATT). Temeljni okvir za GATT je ATT protokol. GATT se pojavljuje samo nakon uspostavljene veze između dva BLE uređaja.

## 7.1. ATT

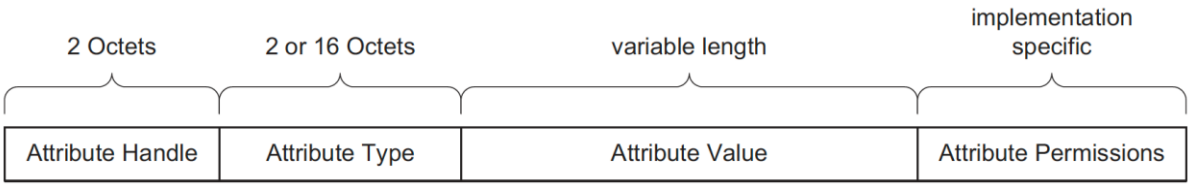
ATT definira komunikaciju između dva uređaja te način na koji će jedan od uređaja, poslužitelj, predočiti svoje podatke klijentu, drugom uređaju. Podaci koji se izlažu međusobno strukturirani su kao atributi. Uloge u ATT-u:

- Poslužitelj: uređaj koji pohranjuje podatke kao jedan ili više atributa
- Klijent: uređaj koji prikuplja informacije za jednog ili više poslužitelja

Atribut je generički pojam za bilo koju vrstu podataka koje poslužitelj izlaže i definira strukturu tih podataka. Sastoji se od:

- *Attribute Handle*: 16-bitna vrijednost koju poslužitelj dodjeljuje svakom od svojih atributa – može je promatrati i kao njihovu adresu. Klijent koristi ovu vrijednost za referenciranje određenog atributa i poslužitelj garantira jedinstvenu identifikaciju atributa tijekom veze između dva uređaja. Raspon je između 0x0001 do 0xFFF, gdje je vrijednost 0x000 rezervirana.
- *Attribute type - (Universally Unique Identifier or UUID)*: 16-bitni vrijednost ( u slučaju Bluetooth SIG prihvaćenih atributa) ili 128-bitna vrijednost (u slučaju prilagođenih vrsta atributa koje definira sam programer, UUID specifični za pojedinog dobavljača opreme). Prednost korištenja usvojenih SIG UUID je manja veličina paketa jer će biti prenesena kao 16-bitna vrijednost.
- *Attribute value*: vrijednost koja može biti fiksne ili varijabilne duljine
- *Attribute Permissions*: određuje može li se atributi pročitati ili biti zapisan, obavješten ili naznačen te koje su razine sigurnosti potrebne za svaku od tih operacija [7].

Slika 7.1. prikazuje jedan ATT blok sa navedenim dijelovima.




*Slika 7.1. ATT blok [7]*

## 7.2. GATT

Osim koncepta ATT, postoje još neki važni koncepti u BLE, kao što su:

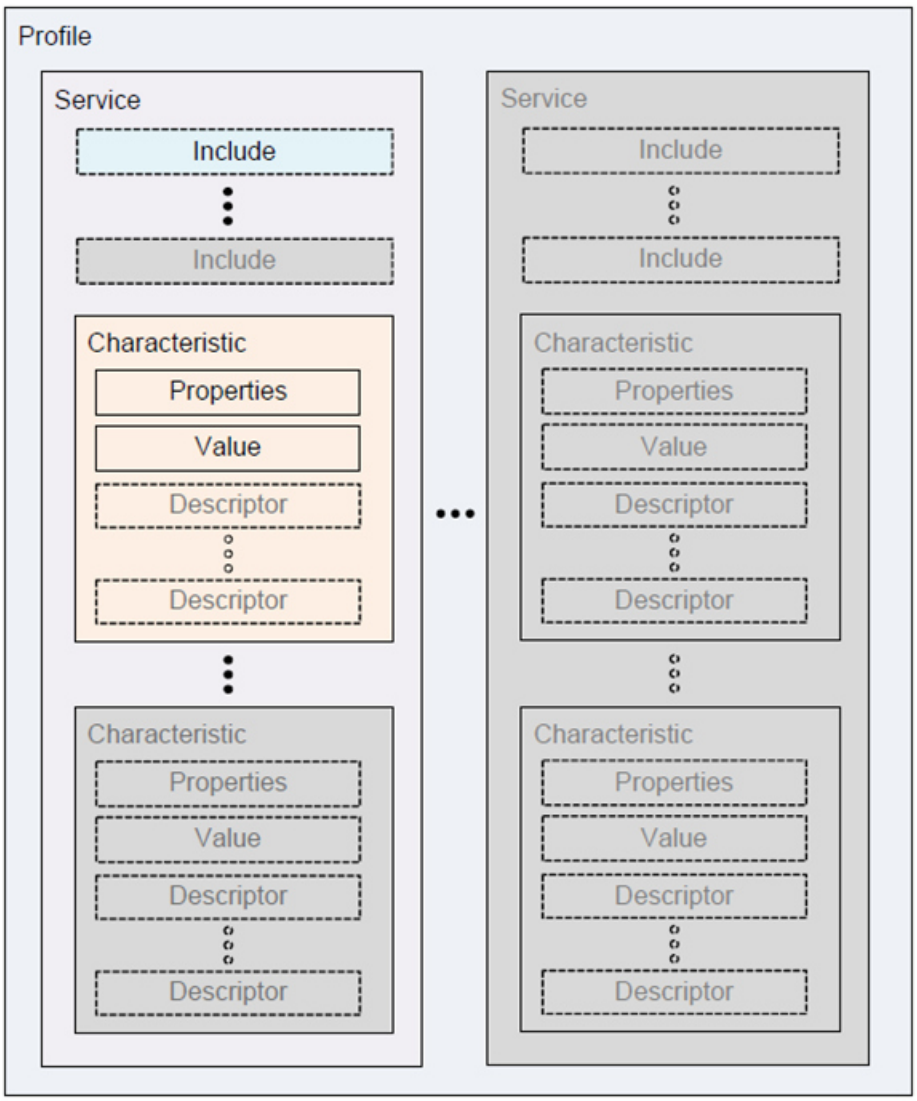
- Servisi
- Karakteristike
- Profili

Ti se koncepti koriste posebno kako bi se omogućila hijerarhija u strukturiranju podataka koje poslužitelj izlaže. Servisi i karakteristike vrsta su atributa koje imaju određenu svrhu. Karakteristike su atributi najniže razine u bazi podataka atributa [5].

GATT definira format servisa i njihovih karakteristika te postupke koje se koriste za povezivanje s tim atributima. GATT preuzima uloge kao i ATT protokol. Uloge nisu određene prema uređaju nego se određuju prema transakciji (poput zahtjev – odgovor, indikacija – potvrda, obavijest). U tom smislu uređaj može djelovati kao poslužitelj, poslužujući podatke za klijente, a u isto vrijeme djelujući kao klijent koji čita podatke koje poslužuje drugi poslužitelj, i to svi tokom iste veze.

## 7.3. Servisi i karakteristike

Servis je grupa jednog ili više atributa, od kojih su neki karakteristike. Uloga mu je grupirati zajedničke atribute koji označavaju specificiranu funkciju na serveru. Servis također sadrži druge atribute koji pomažu pri strukturiranju podataka u njemu ( kao npr. deklaracija servisa, deklaracija karakteristike, itd.). Slika 7.2. prikazuje jedan okvir servisa.




*Slika 7.2. Okvir jednog servisa [7]*

Sa slike možemo vidjeti različite atribute od kojih se servis sastoji:

- Jedne ili više uključenih servisa
- jedne ili više karakteristika, koje sadrže svoja svojstva, vrijednosti te nijedne ili više opisa

Uključeni servisi omogućuju servisu referenciranje prema drugim servisima za potrebe kao što su proširenje postojećeg servisa. Postoje dva tipa servisa:

- Primarni servis: predstavlja primarnu funkciju uređaja
- Sekundarni servis: pruža dodatne funkcije uređaja i uključenih od najmanje jednog drugog primarnog servisa na uređaju

Karakteristike možemo shvatiti kao spremnike za korisničke podatke. Uključuju najmanje dva podatka:

- deklaraciju karakteristike: pruža meta podatke o stvarnim korisničkim podacima
- vrijednost karakteristike: puna vrijednost atributa koji sadrži podatke korisnika u polju vrijednosti

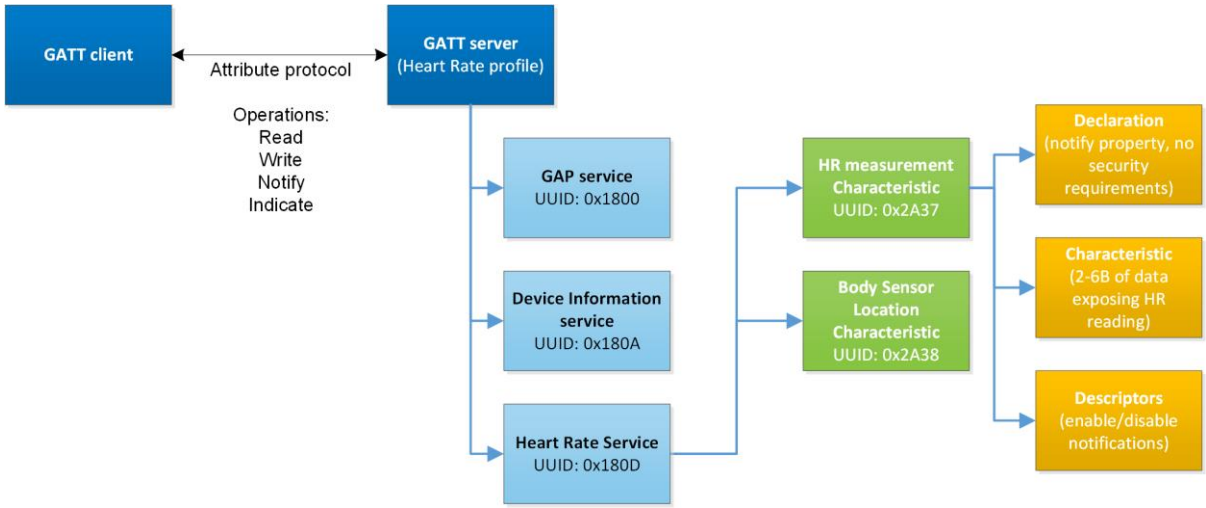
Dodatno, vrijednost karakteristike mogu pratiti deskriptori, koji dodatno proširuju meta podatke sadržane u deklaraciji karakteristike. Deklaracija, vrijednost i deskriptori zajedno tvore karakteristiku. Sve GATT karakteristike su dio jednog servisa, stoga ih se uvijek može pronaći u jednome servisu [3].

## 7.4. Profili

Profili imaju opširnije definicije za razliku od servisa. Profili su zaduženi za definiranje ponašanja klijenta i poslužitelja kada su u pitanju servisi, karakteristike, veze i sigurnosni zahtjevi. Dok s druge strane, servisi i njezine karakteristike djeluju samo na strani poslužitelja. Kao i u slučaju kod servisa, adaptirane su od strane SIG-a. U specifikaciji profila, možemo pronaći:

- Definiciju uloga i vezu između GATT poslužitelja i klijenta
- Potrebne servise
- Zahtjeve servisa
- Kako se koriste potrebni servisi i karakteristike
- Pojedinosti o zahtjevima za uspostavu veze, uključujući parametre za oglašavanje i povezivanje
- Sigurnosna razmatranja

Slika 7.3. prikazuje odnos između GATT klijenta, poslužitelja, servisa, karakteristika i deklaracija karakteristika, podataka i deskriptora.




*7.3. GATT koncept [4]*

# 8. SIGURNOST

Sigurnost je postala jedna od najizraženijih briga u IoT (engl. *Internet of things*) sustavima. Uz sve vijesti u kojima se spominju razni računalni napadi i ranjivosti otkriveni u mnogim IoT proizvodima, sigurnost je postala jedna od glavnih briga proizvođača i programera IoT uređaja. Kako bi se osigurala sigurna i zaštićena komunikacija, BLE tehnologija pruža nekoliko značajki za osiguravanje povjerenja, integriteta, privatnosti i kriptiranja podataka.

## 8.1. Sigurnosne prijetnje

Neki od najčešćih sigurnosnih problema u bilo kojem sustavu uključuju:

- Autentifikacija: autentifikacija predstavlja dokaz da je druga strana ona za koju se predstavlja. Dakle, ako se povezujete s BLE uređajem, želite biti sigurni da to povezivanje zaista jeste povezivanje s uređajem koji vas zanima – a ne s nekim drugim zlonamjernim uređajem koji se pretvara biti željeni uređaj.
- Integritet: integritet nam osigurava da primljeni podaci na sadrže koruptivne i neovlaštene podatke
- Povjerljivost: povjerljivost se odnosi na osiguravanje da podaci nisu čitljivi od strane neovlaštenih korisnika ili uređaja
- Privatnost: privatnost upućuje na to koliko je komunikacija privatna i da li je treća strana u mogućnosti pratiti naš uređaj – posebno putem *Bluetooth* adrese.

Navedene prijetnje su neke od općih briga vezane za sigurnost u bilo kojem sustavu. Važnost svake od navedenih prijetnji ovisi o primjeni i slučaju upotrebe pojedine aplikacije ili sustava.

### 8.1.1. Tipovi napada

Na temelju navedeni prijetnji, postoje različite vrste koje zlonamjerni uređaji ili osoba mogu implementirati. Neki od njih uključuju:

- Pasivno prisluškivanje: opisuje kada zlonamjerni uređaj prisluškuje komunikaciju između dva uređaja, te je u stanju razumjeti podatke – obično putem dobivanja pristupnog ključa u slučaju da su podaci kriptirani.
- Aktivno prisluškivanje: također poznato pod nazivom napad čovjeka u sredini, (engl. *Man-In-The-Middle attack)*. U ovom napadu zlonamjerni uređaj lažno se predstavlja kao oba uređaja (periferni i središnji). Tada bi mogao presresti komunikaciju među njima,

usmjeriti ga tako da ne shvaćaju da se napad događa, a možda čak i dodavati podatke u pakete koji se prenose međusobno.

- Praćenje privatnosti i identiteta: u ovom napadu uređaje i korisnike prati uređaj pomoću Bluetooth adrese – omogućuje otkrivanje njihove lokacije i njeno povezivanje s njihovim ponašanjem u komunikaciji [9].

## 8.2. Sigurnost u BLE

Sigurnost u BLE tehnologiji upravlja sloj upravitelj sigurnosti, engl. *Security Manager* (SM) u BLE arhitekturi. SM definira protokole i algoritme za generiranje i razmjenu ključeva između dva uređaja. Uključuje pet sigurnosnih značajki:

- Uparivanje: postupak stvaranja izmjenjivih zajedničkih tajnih ključeva između dva uređaja
- Vezivanje: proces stvaranja i pohranjivanja zajedničkih tajnih ključeva sa svake strane (periferni i središnji) za uporabu u naknadnim vezama između uređaja
- Autentifikacija: postupak provjere da li dva uređaja dijele isti tajne ključeve
- Šifriranje: postupak šifriranja podataka razmijenjenih između uređaja. Šifriranje u BLE-u koristi 128-bitni AES (engl. *Advanced Encryption Standard*) standard šifriranja, simetrični algoritam što znači da se isti ključ koristi za šifriranje i dešifriranje podataka na obje strane
- Integritet poruke: proces potpisivanja podataka i provjere potpisa na drugome kraju. To nadilazi jednostavnu provjeru integriteta izračunatog cikličke provjere zalihosti, (engl. *Cyclic redundancy check* , CRC)

Bluetooth specifikacija se vremenom razvijala kako bi pružila snažnije sigurnosne mjere. To se posebno odnosilo na BLE, koji je uveo koncept *LE Secure Connections* (LESC) u inačici 4.2. LESC koristi *Elliptic-curve Diffie-Hellman* (ECDH) protokol tijekom procesa uparivanja, što komunikaciju čini mnogo sigurnijom u odnosu na metode korištene u ranijim inačicama *Bluetootha*. Inačica 4.2. također je uvela termin naslijeđene uparivanje (engl. *Legacy pairing*), koji kolektivno odnosi sa metodama uparivanja definirane ranijim specifikacijama inačica. Važno je napomenuti, da su naslijeđene veze još uvijek podržane u Bluetooth-u 4.2 i novijim inačicama [11].

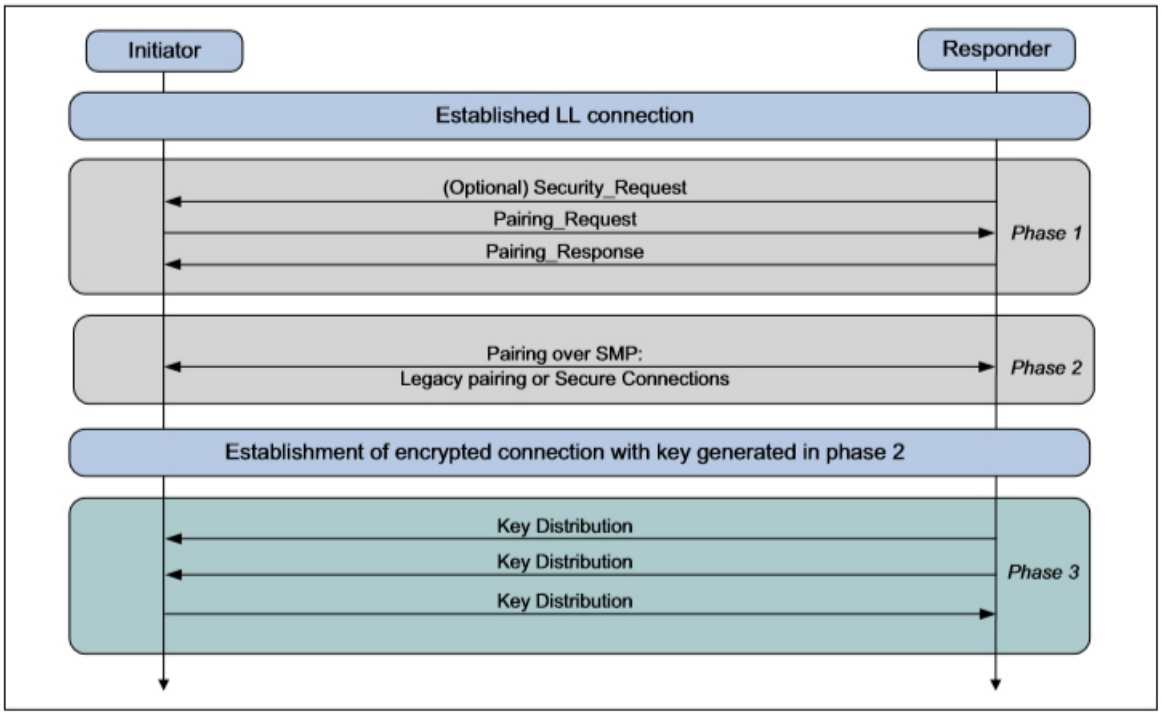
Upravitelj sigurnosti rješava različite sigurnosne probleme na slijedeći način:

- Povjerljivost putem enkripcije

- Autentifikacija pomoću uparivanja i povezivanja
- Integritet putem digitalnih potpisa
- Privatnost putem rješivih privatnih adresa

U BLE, glavni uređaj je pokretač sigurnosnih provjera. Uređaj koji šalje odgovore može zatražiti početak sigurnosnog postupka slanjem sigurnosnog zahtjeva glavnom uređaju, ali je sve na glavnom uređaju da da po primitku zahtjeva zatim pošalje paket koji službeno pokreće sigurnosni postupak [10].

Radi boljeg razumijevanja kako funkcionira sigurnosni sustav u BLE, moramo razumjeti dva bitna koncepta: uparivanja i povezivanja. Zbog daljnjeg objašnjavanja bitnih koncepta na slici 8.1. prikazan je jedan sigurnosni proces :




*Slika 8.1. Faze uparivanja* [11]

Proces uparivanja je kombinacija faze 1 i faze 2. Povezivanje je predstavljeno fazom 3. Važno je napomenuti da je druga faza jedina faza koja razlikuje *LE Legacy Pairing* i *LE Secure Connections*.

### 8.2.1. Faze uparivanja i povezivanja

Faza uparivanja je kratkoročna sigurnosna mjera koja ne postoji u svim povezivanjima. Inicira se i završi kada se dva uređaja ponovo povežu i kada kriptiraju konekciju između sebe. Pokrene

se i završi svaki puta kada se dva uređaja ponovo povežu i kriptiraju svoju komunikaciju. Kako bi se produljila enkripcija sljedećih sekvencijalnih konekcija, mora doći do povezivanja između uređaja.

#### 8.2.1.1. Prva faza

U prvoj fazi podređeni uređaj mora zatražiti početak procesa uparivanja. Nadređeni uređaj inicira proces uparivanja šaljući zahtjev za uparivanje podređenom uređaju, koji zatim reagira s porukom odgovora za uparivanje. Zahtjev za uparivanje i odgovor za uparivanje predstavljaju razmjenu značajki koje podržava svaki uređaj, kao i sigurnosne zahtjeve za svaki uređaj. Svaka poruka uključuje sljedeće :

- Ulazno/izlazne (engl. *Input/Output*) mogućnosti : podrška zaslona, podrška tipkovnice, podršku da/ne unosa
- Podršku za metode izvan opsega (engl. *Out-Of-Band (OOB) method support*)
- Zahtjevi za provjeru autentičnosti (engl. *Authentication requirements*): uključuje zahtjev za zaštitu MITM napada (engl. *man-in-the-middle ,MITM, attacks*), zahtjev za spajanje, podršku sigurnosnim vezama
- Maksimalna veličina ključa za šifriranje koju uređaj podržava
- Različite sigurnosne ključeve koje uređaj zahtjeva za korištenje

Informacije razmijenjene između dva uređaja u ovoj fazi određuju koja metoda uparivanja će se koristiti. Tablica 8.1. prikazuje različite kombinacije razmijenjenih I/O mogućnosti (na dva uređaja za uparivanje) i rezultate odabrane metode uparivanja [10].

*Tablica 8.1. Metoda uparivanja i I/O mogućnosti [11]*

| | **Inicijator** | | | | |
|---|---|---|---|---|---|
| **Odgovorilac** | SamoZaslon | ZaslonDa/Ne | SamoTipkovnica | Bez I/O | TipkovnicaZaslon |
| Samo Zaslon | Just Works metoda<br><br>Bez autentifikacije | Just Works metoda<br><br>Bez autentifikacije | Passkey metoda (odgovorilac prikazuje, inicijator unosi)<br><br>Autentifikacija | Just Works metoda<br><br>Bez autentifikacije | Passkey metoda (odgovorilac prikazuje, inicijator unosi)<br><br>Autentifikacija |
| Zaslon Da/Ne | Just Works metoda: inicijator prikazuje, odgovorilac unosi<br><br>Bez autentifikacije | Just Works metoda (Za LE naslijeđeno uparivanje)<br><br>Bez autentifikacije<br><br>Numeric Comparison metoda (Za LE sigurne veze)<br><br>Autentifikacija | Passkey metoda: odgovorilac prikazuje, inicijator unosi<br><br>Autentifikacija | Just Works metoda<br><br>Bez autentifikacije | Passkey metoda (Za naslijeđeno uparivanje): odgovorilac prikazuje, inicijator unosi<br><br>Autentifikacija<br><br>Numeric Comparison metoda (Za LE sigurne veze)<br><br>Autentifikacija |
| SamoTipkovnica | Passkey metoda (inicijator prikazuje, odgovorilac unosi)<br><br>Autentifikacija | Passkey metoda (inicijator prikazuje, odgovorilac unosi)<br><br>Autentifikacija | Passkey metoda (inicijator prikazuje, odgovorilac unosi)<br><br>Autentifikacija | Just Works metoda<br><br>Bez autentifikacije | Passkey metoda (inicijator prikazuje, odgovorilac unosi)<br><br>Autentifikacija |
| Bez I/O | Just Works metoda<br><br>Bez autentifikacije | Just Works metoda<br><br>Bez autentifikacije | Just Works metoda<br><br>Bez autentifikacije | Just Works metoda<br><br>Bez autentifikacije | Just Works metoda<br><br>Bez autentifikacije |
| Tipkovnica Zaslon | Passkey metoda (inicijator prikazuje, odgovorilac unosi)<br><br>Autentifikacija | Passkey metoda [Za naslijeđeno uparivanje]: inicijator prikazuje, odgovorilac unosi<br><br>Autentifikacija<br><br>Numeric Comparison metoda (Za LE sigurne veze)<br><br>Autentifikacija | Passkey metoda (inicijator prikazuje, odgovorilac unosi)<br><br>Autentifikacija | Just Works metoda<br><br>Bez autentifikacije | Passkey metoda (Za naslijeđeno uparivanje): inicijator prikazuje, odgovorilac unosi<br><br>Autentifikacija<br><br>Numeric Comparison metoda (Za LE sigurne veze)<br><br>Autentifikacija |

#### 8.2.1.2. Druga faza

Druga faza, kao što je već spomenuto, razlikuje se ovisno o metodi koja se koristi: LE naslijeđeno uparivanje (engl. *Low Energy Legacy Pairing*) ili LE sigurnu vezu (engl. *Low Energy Secure Connection*)

Razlike između te dvije metode:

- LE naslijeđeno uparivanje: koriste se dva ključa, Privremeni ključ (engl. T) i kratkoročni ključ (engl. ). Privremeni ključ se koristi zajedno s drugim vrijednostima koje se razmjenjuju između dva uređaja za generiranje kratkoročnog ključa.
- LE sigurna veza: u sigurnim povezivanjima, metoda uparivanja ne uključuje zamjenu ključa bežično između dva uređaja nego uređaji koriste ECDH (engl. *Elliptic Curve Diffie–Hellman Key Exchange*) protokol za svako generiranje para javnog/privatnog

ključa. Uređaji tada izmjenjuju samo javne ključeve i iz njega generiraju zajednički tajni ključ koji se naziva trajni ključ (engl. *Temporary Key*)

Prednost korištenja ECDH protokola je što sprječava prisluškivače da otkriju zajednički tajni ključ čak i ako im prisluškujući otkriju oba javna ključa. ECDH protokol je protokol za razmjenu tajnog ključa zasnovan na eliptičnim krivuljama u asimetričnim kriptografskim sustavima.

#### 8.2.1.3. Treća faza

Treća faza obuhvaća fazu povezivanja. Ova faza je također opcionalna, kako bi se izbjeglo ponovo povezivanje prilikom svake veze te se omogućio siguran komunikacijski kanal. Rezultat povezivanja je da svaki uređaj pohranjuje skup ključeva koji se mogu koristiti u svakom naknadnom povezivanju i omogućuje uređajima preskakanje faze uparivanja. Ovi ključevi se razmjenjuju između dva uređaja putem veze koja je kriptirana putem dobivenih ključeva iz druge faze.

### 8.2.2. Metode uparivanja

Naslijeđeno uparivanje i sigurna veza imaju različite metode uparivanja. Neke metode dijele isto ime, ali imaju različite procese i podatke koje razmjenjuju. Metoda uparivanja određuje se na temelju razmijenjenih značajki između dva uređaja u prvoj fazi.

#### 8.2.2.1. Naslijeđeno uparivanje

Metoda naslijeđenog uparivanja, koristi prilagođeni protokol razmjene ključeva jedinstven za BLE standard. Uređaji razmjenjuju privremeni ključ (TK) i koriste ga za stvaranje kratkoročnog ključa (STK) koji se koristi za kriptiranje veze. Razina sigurnosti navedenog procesa ovisi o metodi uparivanja koja se koristi za razmjenu privremenog ključa (TK) [18].

Metode:

- *Just Works* metoda: privremeni ključ (TK) postavljen je na vrijednost 0. Također razmjena između uređaja nije obvezna. Nudi najmanju sigurnost jer je napadaču lako grubo prisiliti kratkoročni ključ (STK) i prisluškivati vezu. Također ova metoda ne nudi načine provjere uređaja koji sudjeluju u povezivanju, pa stoga ne nudi MITM zaštitu.
- *Out Of Band* (OOB) metoda: u ovoj metodi privremeni ključ (TK) između dva uređaja se razmjenjuje drugom bežičnom tehnologijom, kao što je NFC (engl. *Near-field communication*). Glavna prednost ove metode korištenje velikog privremenog ključa

(TK), do 128 bita, što uvelike povećava sigurnost veze. Ako je OOB kanal zaštićen od MITM napada, tada se može pretpostaviti da je BLE veza zaštićena i od MITM napada. Slično, sve dok je OOB kanal imun na prisluškivanje tijekom procesa uparivanja, tada će i BLE veza biti imuna na pasivno prisluškivanje. OOB je daleko najsigurnija metoda pod uvjetom da OOB kanal koristi dovoljne sigurnosne metode.

- *Passkey* metoda: u ovoj metoda privremeni ključ (TK) je 6-znamenkasti broj koji korisnik prenosi između uređaja. Način prijenosa ovog broja može varirati. Jedan primjer bi bio da jedan od uređaja generira 6-znamenkasti broj i prikaže ga na LCD zaslonu. Korisnik bi zatim pročitao broj i unio ga u drugi uređaj pomoću tipkovnice. Ako napadač ne prisluškuje prilikom procesa uparivanja, tada metoda pruža prilično dobru zaštitu od pasivnog prisluškivanja.

OOB se čini sigurnijom metodom u razliku od *Just Works* i *Passkey* metode jer koristi drugačije bežično sučelje za razmjenu privremenog ključa.

#### 8.2.2.2. Sigurna veza

Za razliku od metode naslijeđenog uparivanja, metoda sigurne veze umjesto korištenja privremenog ključa (TK) i kratkoročnog ključa (STK) koristi jedan dugoročni ključ (LTK) za kriptiranje veze. Ovaj se LTK razmjenjuje/generira pomoću kriptografije javnog ključa, ECDH protokolom, koja nudi znatno jaču sigurnost u usporedbi s izvornim BLE protokolom za razmjenu ključeva.

Metode:

- *Just Works* metoda: javni ključevi svakog uređaja zajedno s drugim generiranim vrijednostima razmjenjuju preko BLE između dva uređaja.
- *Out Of Band* (OOB) metoda: prilikom uparivanja javni ključevi, početne vrijednosti i vrijednosti potvrde razmjenjuju se putem različite bežične tehnologije, poput NFC-a. Kao i kod naslijeđenog uparivanja, OOB uparivanje kod sigurnih veza pruža zaštitu samo od pasivnog prisluškivanja i MITM napada ako je OOB kanal siguran.
- *Passkey* metoda: u ovoj metodi koristi se identičan šesteroznamenkasti broj koji može biti unesen u uređaj od strane korisnika u svaki uređaj ili će ga jedan od uređaja generirati a drugi korisnik ručno unijeti u svoj uređaj.
- *Numeric Comparison* metoda: metoda funkcionira prilično isto kao i spomenuta *Just Works* metoda, ali ima jedan korak više na kraju. Nakon što uređaji potvrde da se vrijednosti potvrde podudaraju, oba će uređaja neovisno generirati konačnu vrijednost

od 6 znamenki potvrde koristeći oba svoja nasumična broja od početka uparivanja. Korisnik tada ručno provjerava odgovaraju li obje vrijednosti i time potvrđuje da je veza sigurna. Ovaj dodatni korak omogućuje ovoj metodi uparivanja zaštitu od MITM napada i najsigurnija je metoda uparivanja od svih navedenih.

## 8.3. Korišteni sigurnosni ključevi

Tijekom različitih sigurnosnih postupaka koristi se niz ključeva i varijabli:

- Privremeni ključ (engl. *Temporary Key*): generiranje privremenog ključa ovisi o odabranoj metodi uparivanja. TK se generira prilikom svakog procesa uparivanja.
- Kratkoročni ključ (engl. *Short Term Key*): ovaj ključ generira se iz privremenog ključa (TK) koji se razmjenjuje između uređaja. Kratkoročni se ključ generira svaki put kada dođe do procesa uparivanja i koristi se za šifriranje podataka tijekom cijele trenutne veze.
- Dugoročni ključ (engl. *Long Term Key*): Dugoročni ključ generira se i pohranjuje tijekom treće faze sigurnosnog procesa u naslijeđenim vezama i tijekom druge faze u LE sigurnim vezama. Pohranjuje se na svakom od dva uređaja koji su spojeni i koji se koriste u naknadnim vezama između ta dva uređaja.
- *Encrypted Diversifier* (EDIV) i slučajni broj (RAND): ove dvije vrijednosti koriste se za stvaranje i identifikaciju LTK-a. Također se pohranjuju tijekom procesa spajanja.
- *Connection Signature Resolving Key* (CSRK): koristi se za potpisivanje podataka i provjeru potpisa koji je priložen podacima na drugom kraju. Ovaj ključ je pohranjen na svakom od dva spojena uređaja
- *Identity Resolving Key* (IRK): koristi se za rješavanje nasumičnih privatnih adresa. Jedinstven je po uređaju. IRK glavnog uređaja pohranjuje se na strani drugog uređaja, a IRK drugovo uređaja pohranjuje se na glavnom uređaju

## 8.4. Sigurnosni modeli i razine

Postoje dva različita sigurnosna modela u BLE: Sigurnosni model 1 i sigurnosni model 2. Razlika se očituje u tome što kod modela 1 fokus na šifriranje, dok u modelu 2 na potpisivanje podataka.

Razine Sigurnosnog modela 1 su:

- Razina 1: bez sigurnosti (bez autentifikacije i šifriranja)

- Razina 2: uparivanje bez autentifikacije i sa šifriranjem
- Razina 3: uparivanje s autentifikacijom i sa šifriranjem
- Razina 4: uparivanje s LE *secure connection* autentifikacijom sa šifriranjem

Razine Sigurnosnog modela 2 su:

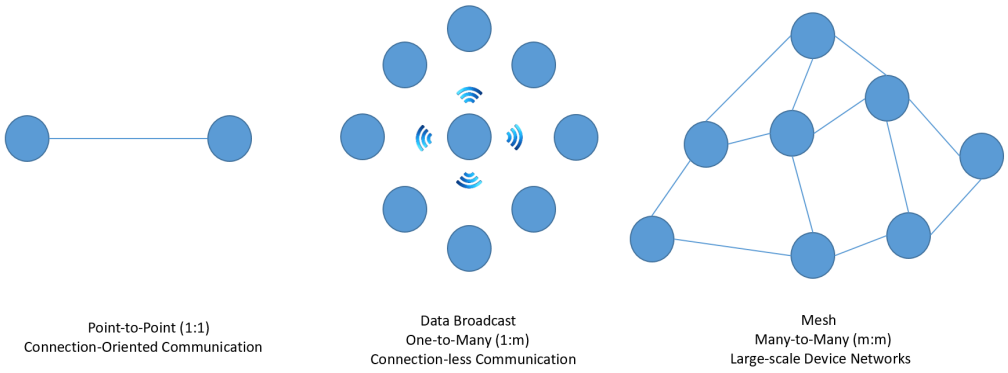
- Razina 1: uparivanje bez autentifikacije s potpisivanjem podataka
- Razina : uparivanje sa autentifikacijom s potpisivanjem podataka

Veza se smatra autoriziranom ili neautoriziranom na temelju korištene metode uparivanja. Gledajući na tablicu navedenoj u poglavlju o prvoj fazi uparivanja, možemo primijetiti da svako povezivanje se provjerava da li se metoda smatra provjerenom ili neovlaštenom. Veza između dva uređaja radi samo u jednom sigurnosnom modelu, ali može funkcionirati na različitim razinama unutar istog modela.

# 9. BLUETOOTH MESH

Nakon predstavljanja BLE tehnologije, 2010. godine, radi brzorastuće upotrebe u IoT-u, u različitim senzorima, medicinskim uređajima itd. 2017. godine Bluetooth SIG predstavio je Bluetooth mrežni standard (eng. *Bluetooth mesh*). Nedostatak prvog koncepta BLE-a je bila podrška topologije *many-to-many* (mrežasta mreža) BLE uređaja gdje više uređaja mogu međusobno slati poruke.

Cilj *Bluetooth mesh*-a je povećanje raspona BLE mreže i podrška za industrijske aplikacije koje koriste BLE tehnologiju. Prvi koncepti topologije koje je BLE podržavao su bili One-to-one gdje su povezana samo dva BLE uređaja, i One-to-many gdje BLE uređaji ostaju u stanju oglašavanja. Bluetooth mesh-om uvedena je nova topologija many-to-many što omogućuje komunikaciju između više uređaja i optimiziran je za stvaranje velikih mreža uređaja. Slika 9.1. prikazuje navedene topologije [14].



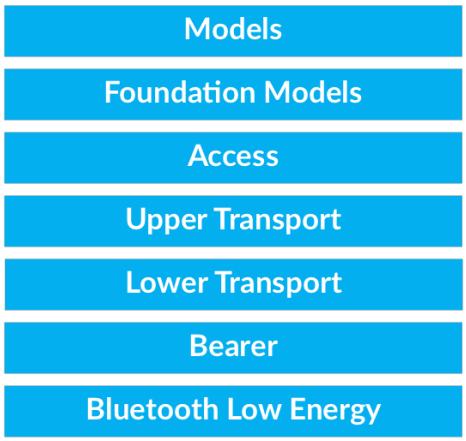

*Slika 9.1. Bluetooth topologije Point-to-Point, One-to-Many i Many-to-Many [19]*

Dva su glavna benefita *mesh* mreže:

- Prošireni raspon: kako čvorovi mogu prenositi poruke do udaljenih čvorova putem čvorova između njih, ovo omogućuje mreži da proširi svoj raspon i doseg uređaja
- Sposobnost samoliječenja (engl. *Self-healing capabilities*): odnosi se na činjenicu da ne postoji jedinstvena točka pogreške. Ako jedan o čvorova *mesh* mreže padne, drugi čvorovi mogu i dalje sudjelovati i slati poruke između sebe. Međutim, to vrijedi djelomično budući da razlikujemo vrste čvorova unutar mreže, od kojih neki mogu ovisiti o drugim čvorovima.

## 9.1. Arhitektura Bluetooth Mesh-a

Bluetooth mesh je zapravo nadogradnja smještena iznad BLE-a. Posebno je vezan za stanje oglašavanja BLE uređaja. Uređaji unutar Bluetooth mesh-a se ne povezuju isto kao i kod normalnih BLE uređaja. Koriste stanje oglašavanja i skeniranja za prijenos poruka jedni drugima. Slika 9.2. prikazuje slojeviti prikaz arhitekture Bluetooth mesh-a.




*Slika 9.2. Slojevita arhitektura Bluetooth Mesh-a [19]*

Arhitektura se sastoji od:

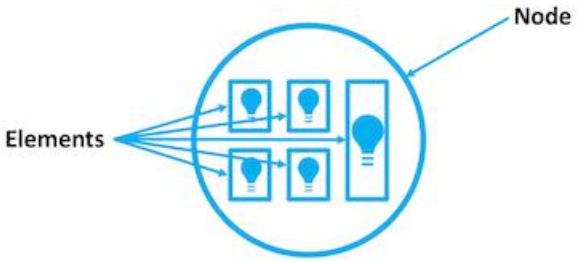
- BLE-a: Bluetooth mesh se nadograđuje na BLE, što zahtjeva potpuni BLE protokolni stog koji će biti pokrenut na uređaju. Koristi stanja oglašavanja i skeniranja za slanje i primanje poruka između uređaja unutar mrežaste mreže. Također podržava povezano stanje i GATT za posebne uređaje koji se nazivaju *proxy* čvorovi.
- Nosilački sloj (engl. *Bearer*): definira kako se rukuju određeni mesh paketi PDU (engl. *Protocol Data Units*).
- Donji transportni sloj (engl. *Lower Transport*): ovaj sloj rješava dva zadatka – segmentaciju paketa od gornjeg sloja i ponovno sastavljanje paketa u donjem sloju
- Gornji transportni sloj (engl. *Upper Transport*): odgovoran je za šifriranje, dešifriranje, autentifikaciju i prijenos kontrolnih poruka
- Pristupni sloj (engl. *Access*): definira način na koji aplikacija koristi gornji transportni sloj. Zadaća mu je definiranje oblika podataka aplikacije, šifriranje i dešifriranje te provjeru podataka
- Temeljni sloj modela (engl. *Foundation Models*): brine se za mrežnu konfiguraciju i modele mrežnog modela

- Sloj modela (engl. Model): zadaća mu je implementacija modela uključujući ponašanje, poruke, stanja. i stanja povezivanja

## 9.2. Koncept i terminologija Bluetooth Mesh-a

Uređaji koji je pridružen Bluetooth mesh-a nazivaju se čvorovima. Uređaji koji nisu unutar mesh-a nazivaju se nepridruženi uređaji, a postaju pridruženi tek kada im se omogući pridruživanje.

Čvor može sadržavati više dijelova koji se mogu neovisno upravljati. Na primjer, rasvjetno tijelo može sadržavati više žarulja koje se mogu uključiti/isključiti neovisno jedni o drugima. Ti različiti dijelovima jednog čvora nazivaju se elementima. Slika 9.3. grafički prikazuje odnose čvora i elementa.




*Slika 9.3. Odnos čvor-element* [19]

Elementi mogu biti u različitim uvjetima, predstavljeni vrijednošću stanja. Vezano za prošli primjer, uključeno i isključena žarulja je njezino stanje unutar rasvjetnog tijela. Promjena iz jednog stanja u drugo naziva se tranzicija stanja. Stanje može biti trenutačno, ili se može dogoditi s vremenom, nakon nekog vremena koje nazivamo prijelaznim vremenom. Kada dođe do promjene stanja to će uzrokovati promjenu u ponašanju elementa. Neka stanja mogu biti međusobno povezana, što znači da promjena u jednom stanju pokreće promjenu u drugom, te takvi mogu postojati dva ili više međusobno ovisnih.

Svojstva dodaju kontekst vrijednosti stanja. Na primjer, definiranje vrijednosti temperature zraka koja može biti unutarnja ili vanjska. Postoje dvije vrste svojstava:

- Svojstvo proizvođača: omogućuje pristup samo za čitanje
- Svojstvo administratora: omogućuje pristup za čitanje i pisanje

U Bluetooth mesh-u sva komunikacija unutar mreže orijentirana je na porukama, a čvorovi šalju poruke za međusobnu kontrolu ili prijenos informacija. Poruke su mehanizam kojim se

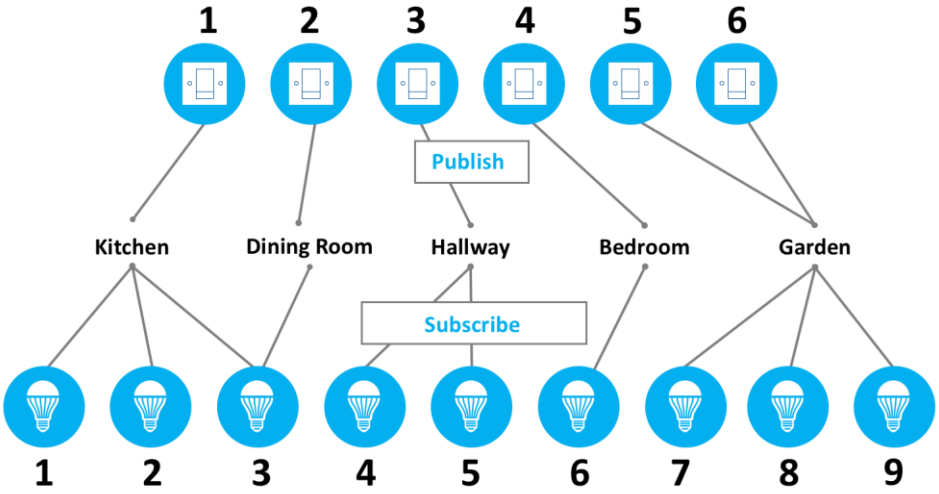
pozivaju operacije na čvorovima. Vrste poruke koja se šalje predstavlja operaciju nad stanjem ili više vrijednosti stanja. Postoje tri vrste poruka:

- GET poruka: poruka koja traži stanje od jednog ili više čvorova
- SET poruka: poruka za promjenu vrijednosti određenog stanja
- STATUS poruka: koristi se u različitim scenarijima, kao odgovor na GET poruku sadržavajući vrijednost stanja, kao odgovor na potvrđenu SET poruku, itd.

Poruke u mreži moraju se slati sa i na adrese. Postoje tri vrste adresa:

- *Unicast* adresa: adresa koja jedinstveno identificira jedan čvor tijekom procesa pridruživanja
- Grupna adresa: adresa koja se koristi za identifikaciju grupe čvorova. Obično odražava fizičko grupiranje čvorova kao što su čvorovi unutar određene prostorije. Može biti definirana od SIG-a ili dinamička koju korisnik definira
- Virtualna adresa: adresa koja se može dodijeliti jednom ili većem broju elemenata, koja obuhvaća jedan ili više čvorova.

Objavljivanje (engl. *Publishing*) je pojam slanja poruka. Pretplata (eng. *Subscribing*) je konfiguracija koja se koristi za dopuštanje slanja odabranih poruka na određene adrese radi obrade. Poruke se obično adresiraju na grupne ili virtualne adrese. Na slici 9.4. prikazana je mrežasta mreža kuće koja se sastoji od 6 prekidača za svjetlo i 9 žarulja. Mreža koristi metode objavljivanja i pretplate kako bi omogućila čvorovima međusobno slanje poruka. Čvorovi se mogu pretplatiti na više adresa, kao što se može vidjeti na primjeru sa slike 9.4. gdje žarulja pod brojem 3 pretplaćena u grupne adrese kuhinje i blagovaonice. Također više čvorova mogu objavljivati na istu adresu, kao što vidimo prekidače pod brojevima 5 i 6 gdje kontroliraju istu grupu adresa žarulja lociranih u vrtu. Benefit korištenja grupa adresa ili virtualnih adresa je ta da dodavanjem ili uklanjanjem čvorova ne zahtjeva ponovnu konfiguraciju čvorova [14].




*Slika 9.4. Primjer preplate i objavljivanja* [19]

Bluetooth mesh koristi tehniku kompromisa, odnosno *managed flooding,* za usmjeravanje poruka u mreži. Tehnika se oslanja na emitiranje poruka svim čvorovima u dometu čvora pošiljatelja. Koristi dodatne optimizacije kao što je TTL (engl. *Time to live*) vrijeme ograničavajući poruci broj skokova na čvorovima mreže.

Još jedan važan koncept Bluetooth mesh-a je model koji definira neke ili sve funkcionalnosti datom elementu. Postoje tri kategorije:

- Server model: kolekcija stanja, tranzicije stanja, dodjeljivanja stanja, poruka koje element sadrži
- Klijent model: definira samo poruke kao što su GET, SET i STATUS koje se šalju serveru
- Kontrolni model: sadrži server i klijent model dopuštajući komunikaciju sa drugim serverima i klijentima

Koncept scena u Bluetooth mesh-u je pohranjena zbirka stanja i identificirana je 16-bitnim brojem koji je jedinstven unutar mreže. Scene omogućuju pokretanje jedne radnje za postavljanje više stanja različitim čvorovima. One mogu biti pokrenute na zahtjev ili u određeno vrijeme. Primjer scene može se prikazati na postavljanju određene temperature u prostoriji, postavljanje određene jačine svjetlosti u prostorijama gdje se rolete na prozorima zatvaraju itd.

## 9.3. Vrste čvorova

Sve vrste čvorova mogu slati i primati mesh poruke ali se razlikuju po izbornim značajkama koje im daju posebne mogućnosti. Razlikujemo ove vrste čvorova:

- Relejni čvorovi (engl. *Relay nodes*): takav čvor koji može ponovo poslati poruke koje emitiraju drugi čvorovi. Ta značajka omogućuje proširenje dosega poruka i omogućuje im da prođu cijelu mrežu izvan dosega izvornog odašiljačkog čvora
- Proxy čvorovi (engl. *Proxy nodes*): daje mogućnost komuniciranja uređaja koji ne podržava mesh mrežu. Djeluje kao posrednik i koristi GATT operacije za dopuštanje ostalih čvorova van mreže povezivanje i interakciju s mrežom. Koristi proxy protokol koji omogućuje uređaju čitanje i pisanje PDU-ova iz GATT karakteristike. Omogućava uređaji koji nema implementirani Bluetooth mesh protokol interakciju sa mesh mrežom putem proxy uređaja GATT operacijama
- Prijateljski čvor (engl. *Friend Node*) i čvor niske snage (engl. *Low Power Node*): dva usko povezana čvora jer kako bi LPN čvor sudjelovao u mreži, zahtjeva se prijateljski odnos s drugim čvorom, zvanim prijateljskim čvorom. LPN značajno smanjuje radne cikluse prijemnika smanjivanjem vremena uključivanja prijemnika te dovodi do manje potrošnje energije. Prijateljski čvor pomaže LPN-u u radu spremanjem poruka njemu namijenjenih i prosljeđivanjem samo kad LPN izričito zatraži poruke od prijateljskog čvora [14].

## 9.4. Provisioning

*Provisioning* je proces kojim se uređaj pridružuje mesh mreži i postaje čvorom. Sam proces uključuje nekoliko faza, što rezultira generiranjem različitih sigurnosnih ključeva te čini sigurnim procesom. *Provisioning* se ostvaruje pomoću aplikacije na uređaju te se taj uređaj u procesu pridruživanja naziva *Provisioner*. Proces se sastoji od 5 koraka:

- 1. korak uključuje proces pod nazivom *Beaconing*. Nepridruženi uređaj najavljuje svoju dostupnost da bude pridružen, slanjem Beacon mesh oglašivače u paketima oglašavanja
- 2. korak uključuje proces pod nazivom *Invitation* gdje pridruženi uređaj šalje pozivnicu uređaju koji se oglašava, u obliku oglašivačke pozivnice PDU-a. Nepridruženi uređaj odgovara sa informacijama o sebi

- 3. korak uključuje razmjenu javnih ključeva gdje pridruženi i nepridruženi uređaji razmjenjuju javne ključeve. Proces se izvršava izravno preko BLE-a ili putem OOB kanala
- 4. korak uključuje autentifikaciju tijekom koje nepridruženi uređaj daje nasumični jednoznamenkasti ili višeznamenkasti broj korisniku, koristeći radnju u skladu s mogućnostima. Korisnik unosi broj dobiven od novog pridruženog uređaja te se šifrira veza između njih, uključujući slučajnom broju, dovršavanje procesa autentifikacije oba uređaja
- 5. korak uključuje distribuciju podataka pridruženom uređaju. Nakon autentifikacije svaki uređaj dobiva ključ sesije koristeći svoj privatni i javni ključ poslanih od drugog uređaja. Ključ sesije se koristi za osiguravanje veze za razmjenu dodatnih podataka, kao što je mrežni ključ (engl. *NetKey*), ključ uređaja, sigurnosni parametar poznat kao IV indeks i adresu za slanje koja je pridružena novom uređaju u mreži. Nakon ovog koraka nepridruženi uređaj postaje pridružen *mesh* mreži [14].

# 10. PRIMJENA BLE-a

Brzi razvoj bežične komunikacije i tehnologija koje se koristi u IoT smještaju BLE visoko na ljestvici u primjeni. BLE sa svojom jednostavnošću, najvećim adutom što je mala potrošnja energije i isplativošću pridonosi raznim tehnološkim aspektima u poboljšanju djelovanja u medicini, pametnim gradovima, poljoprivredi, turizmu, industriji, čovjekovom zdravlju itd.

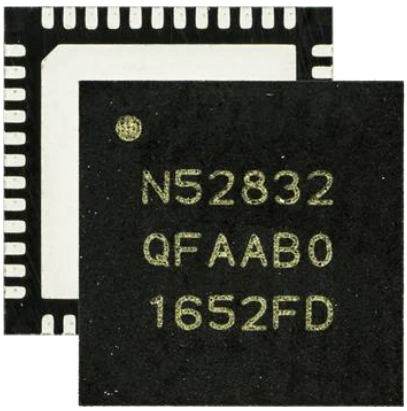
## 10.1. BLE bežično punjenje baterije

Sve je veća potreba za bežičnim sustavima napajanja u bliskom polju. Stoga se pažnja posvećuje bežičnom prijenosu energije na srednje i male udaljenosti unutar, recimo, jedne prostorije. Bežični prijenos energije je proces gdje se u sustavu energija prenosi od izvora do nekog trošila, bez spajanja tih trošila u električni krug. Zbog toga instalacije se su samo na mjestu gdje se odašilje energija i na mjesta trošila koja primaju energiju.

Tvrtka *Powercast*, tvrtka iz Pittsburgh-a, koja razvija rješenja za bežična napajanja 2019. godine predstavila je *Powercast Wireless Charging Grip,* prikazan na slici 10.1., uređaj za bežično punjenje *Joy-Con* kontrolera *Nitendo Switch*-a.

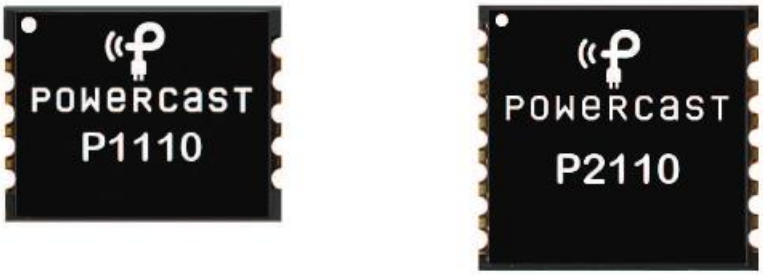
*Slika 10.1. Powercast Wireless Charging Grip* [25]

Glavni elementi koji osiguravaju tom uređaju bežično punjenje i povezivanje je nRF5283 BLE procesor i bežični prijemnici *Powerharvester.* nRF5283 procesor, prikazan na slici 10.2., odgovara najviše zahtjevima širokog spektra aplikacija koje trebaju napredne BLE značajke. Sadrži svojstvo multi protokola, podržava BLE, uključujući velike brzine od 2 Mbps [26].




*Slika 10.2. nRF5283 BLE procesor [26]*

Bežični prijemnici *Powerharvester* snage, prikazani na slici 10.3., imaju mogućnost upravljanja energijom skupljajući direktno ili preko RF energije pretvoriti u DC energiju uređaja sa ili bez baterije. Prijemnik P1110 pruža mogućnost napajanja baterija sa izlaznim naponima do 4,2 V. Dok Prijemnik P2110 napaja uređaje bez baterija i podržava napone izlazne snage do 5,25 V [28].

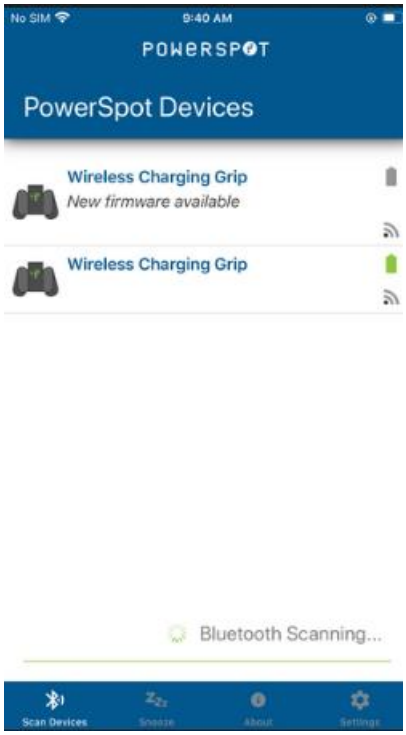



*Slika 10.3. Bežični prijemnici P1110 i P2110 [25]*

*Powercast Wireless Charging Grip* je dizajniran za punjenje unutarnjih baterija bežično dok je u dometu *PowerSpot,* prikazan na slici 10.3., RF bežičnog odašiljača energije, dizajniran od iste tvrtke. BLE omogućuje inteligentno bežično punjenje gdje se energija šalje samo prema potrebi. Grip traži napajanje od odašiljača kad su mu baterije prazne i govori mu da se zaustavi kad se napuni. Pohranjenu energiju u baterijama koristi za punjenje kompatibilnog *Nitendo Switch* kontrolera [25].

*Slika 10.3. PowerSpot [27]*

Za praćenje statusa razine baterije kontrolera i drugih uređaja, *PowerSpot* dolazi sa popratnom mobilnom aplikacijom *PowerSpot* za Android i iOS mobilne uređaje, dostupna besplatno na Google Play-u i App Store-u. *PowerSpot* aplikacija daje prikaz svih uređaja koji se bežično pune u dometu, nadogradnju sustava, prekid odašiljanja itd. Slika 10.4. prikazuje sučelje aplikacije *PowerSpot*.




*Slika 10.4. Sučelje PowerSpot aplikacije [25]*

## 10.2. BLE u zdravstvu i medicinskoj skrbi

Medicinska skrb često se oslanja se na skupu opremu, i stručno osoblje. Ako bi učinkovitije koristili ljudske resurse, postoji veliki potencijal za uštedom, osobito smanjene izdatke za rutinske poslove. BLE se čini vrlo korisnom tehnologijom u zdravstvu. Neke od potencijalnih primjena koja su se razvila, a neke i razvijene su:

- *Connected home health* – Pruža se mogućnost praćenja zdravlja pacijenata gdje god se nalazili. Uređaji za praćenje, poput medicinskih vaga, mjerača otkucaja srca i mjerača krvnog tlaka, mogu pratiti zdravlje i upozoravati pacijente, obitelji i njegovatelje na promjene vitalnih znakova ili propuštene lijekove. BLE omogućuje povezivanje više uređaja koje koristi komunikacijske tehnologije veće udaljenosti za sigurno slanje podataka putem interneta na analizu od strane njegovatelja. uređaji mogu godinama raditi na jednoj sićušnoj bateriji. Radi jednostavnije uporabe, neki BLE hardver, poput u-blox NINA -B1, podržava opcionalnu metodu uparivanja koja štedi OOB u kojoj dva uređaja moraju biti u blizini kako bi postigli automatsko sigurno uparivanje.
- Umreženi lijekovi - Bolnički pacijenti često su povezani s više zdravstvenih uređaja. Uklanjanjem žica dovodi do prednosti, štedi vrijeme osoblja, smanjuje rizik od pogreške i čini pacijente ugodnijim. Elektrokardiografski (EKG) monitori i senzori krvnog tlaka mogu bežično prenijeti podatke vitalnih znakova u centralne bolničke sustave za nadzor. U tipičnoj bolničkoj primjeni, medicinska sestra koristi lagani ručni skener za skeniranje pacijentovog barkoda na zapešću, a skener kontaktira pacijentovu infuzijsku pumpu putem *Bluetootha* radi identifikacije pacijenta. Uz nadzor iz bolničkog centralnog nadzornog sustava, unos s nosivih monitora na pacijenta i druge mjere zaštite, infuzijska pumpa tada može pacijentu osigurati ispravnu tekućinu i lijekove s određenim vremenom [21].


*Slika 10.5. Primjena BLE-a u zdravstvu* [21]

Također od primjena su praćenje stanja pacijenta, praćenje stanja medicinskih potrepština, lijekova [21].

### 10.2.1. Pametni nadzor astme

Američka tvrtka ADAMM pruža pametna rješenja upravljanja i nadzora astmom. Razvili su pametni nosivi monitor prikazan na slici 10.6. koji se nosi ispod odjeće i koji otkriva simptome napada astme i njegovog početka te prati obrasce disanja, kašalj, brzinu otkucaja srca, temperaturu kože i razinu aktivnosti.

*Slika 10.6. ADAMM nosivi monitor [29]*

Osim navedenih podataka nadzora može se pratiti unos lijekova, bilježiti svoje bilješke, postavljati obavijesti i podsjetnike i dijeliti podatke s skrbnicima i pružateljima zdravstvenih usluga pomoću uparene mobilne aplikacije putem Bluetootha, ili preko interneta na web sučelju. Slika 10.7. prikazuje mobilno sučelje aplikacije koja se uparuje sa uređajem.


*Slika 10.7. Mobilno sučelje mobilne aplikacije [29]*

Nosivi monitor vibrira kako bi obavijestio osobu koja ga nosi o predstojećem napadu astme, a može istovremeno poslati i tekstualnu poruku skrbniku. ADAMM monitor koristi algoritam koji s vremenom „uči“ što je jedinstveno za pojedinu osobu, odnosno što je „normalno“. Svi prikupljeni podaci o osobi se prikupljaju, obrađuju na uređaju i razvijaju razumijevanje da li je osoba u svojoj normi ili se odaljava od nje. Rezultat se šalje pomoću Bluetooth-a uparenom pametnom uređaju i mogućnost slanja rezultata u stvarnom vremenu njihovim skrbnicima. Kako se radi o nosivom uređaju, ne ovisi o procesorskoj snazi uparenog pametnog telefona, čime se pruža istinska autonomija – ne moramo biti u blizini pametnog telefona. Ukoliko se ne želi nositi preko noći postavlja se u adapter koji služi za punjenje ali pri tome prati i dalje kašalj, najčešći noćni simptom astme. [29]

## 10.3. BLE u automobilskoj industriji

Automobilska industrija u posljednjim godinama doživjela je ogromnu transformaciju te su moderni auti predstavljeni kao moderna središta i primjene bežičnih tehnologija kao što su GPS, Bluetooth, Wi-Fi, NFC, mobilne 4G/5G, i danas već i BLE. Svi oni omogućuju poboljšane funkcionalnosti povezivanja, sigurnost samog korisnika i udobnost. BLE kao zadnja tehnologija u automobilskoj industriji omogućuje korištenje pametnih mobilnih uređaja kako bi upravljali aplikacijama i sustavom u vozilu, pratili dijagnostiku i stanje, profile pristupa, dijeljenje i pilot parkiranje. Uređaji putem BLE-a mogu obnašati ulogu ključa, te pomoću njega također iznajmljivati vozilo što se postiže provjerom autentičnosti u aplikaciji na mobilnom uređaju te može biti i vremenski ograničeno. Jedno od najzanimljivijih primjena BLE-a je bežično praćenje dijagnostike vozila poput tlaka u gumama, dijagnostičke informacije, temperaturu i stanje baterija itd. Najvažnija karakteristika se očituje u pravovremenom dijagnosticiranju kvarova, što vozače čini sigurnijim u vožnji [23].


*Slika 10.8. Primjena BLE-a u automobilskoj industriji* [23]

Jedan od popularnijih te lako dostupnih nadzornih sustava u automobilima zasnovan na BLE tehnologiji je sustav nadzora tlaka unutar pneumatskih guma (*eng. Tire Pressure Monitoring Systems*, TPMS) na različitim tipovima vozila. Sustav javlja vozaču vozila u stvarnom vremenu informacije o tlaku i temperaturi guma preko RF signala na uređaj za prikaz rezultata. Vozač može znati trenutno stanje guma, što dodatno smanjuje vjerojatnost nesreće. Osim sigurnosti sustav može poboljšati uštedu goriva u prosjeku za oko 2% i smanjiti emisiju ugljičnog dioksida. Kada sustav otkrije ne običajan status guma, alarmirati će se vozača i prikazati podatke i lokaciju gume. Sustav uključuje 4 senzora za svaku gumu automobila i odgovarajuće aplikacije dostupne za Android i iOS. TMPS sustavi najzastupljeniji su na kineskom tržištu gdje e mogu naručiti preko Amazona i eBay-a. Postoje dvije vrste senzora interni, slika 10.9. i eksterni, 10.10.[30].

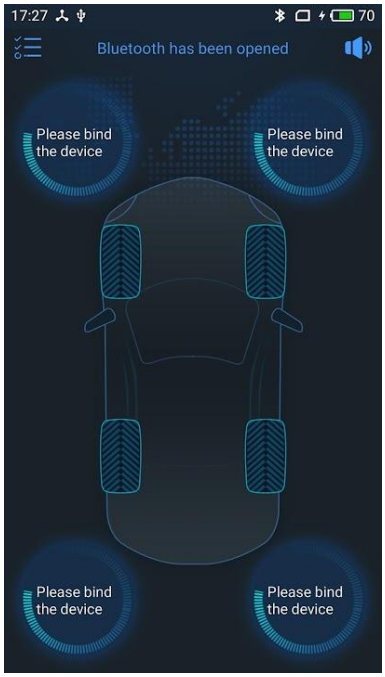
*Slika 10.9. Interni senzor[31]*


*Slika 10.10. Eksterni senzor[31]*

Eksterni senzori ugrađuju se na vanjski dio gume točnije na ventil, što ih čini lakšim za ugradnju u odnosu na interne senzore koji se ugrađuju u samu gumu umjesto originalnog ventila što zahtjeva skidanje gume sa felgi. Oba tipa senzora napajana su dugmastom litij-ion baterijom koja im omogućava rad i to par godina. Slika 10.11. prikazuje jedan paket TMPS Bluetooth sustava koji se sastoji od 4 eksterna senzora, alata za ugradnju, korisničkih uputa i QR koda mobilne aplikacije.

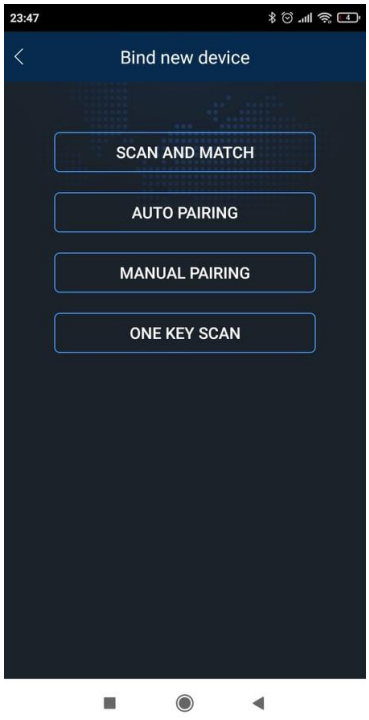

*Slika 10.11. TMPS paket [31]*

Nakon ugradnje senzora pametnim se telefonom skenirana dobiveni QR kod kako bi se instalirala aplikacija TMPSII. Slika 10.12. prikazuje sučelje aplikacije prije uparivanja sa senzorima.




*Slika 10.12. Početno sučelje TMPSII aplikacije [30]*

Aplikacija ima više načina kako se povezati sa senzorima kao što su skeniranje i podudaranje, automatsko uparivanje, ručno uparivanje i skeniranje ključa, prikazano na slici 10.13.



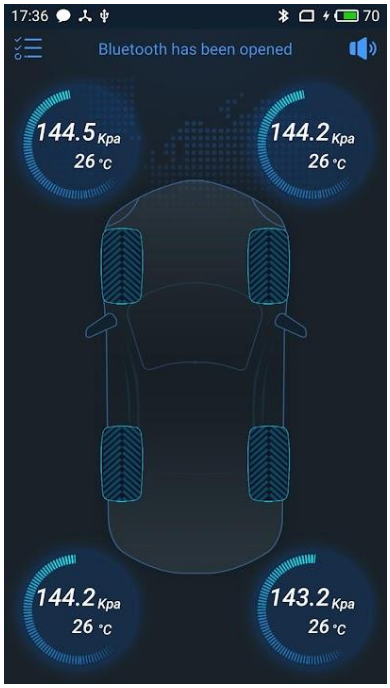

*Slika 10.13. Načini povezivanja sa senzorima*

Jedan od najčešćih načina povezivanja je skeniranje dobivenih barkodova za pojedini senzor što je prvi na listi odabira načina povezivanja, skeniranje i podudaranje. Skeniranje dobivenog

barkoda senzora sa aplikacijom je prikazano na slici 10.14. gdje aplikacija koristi kameru pametnog telefona.

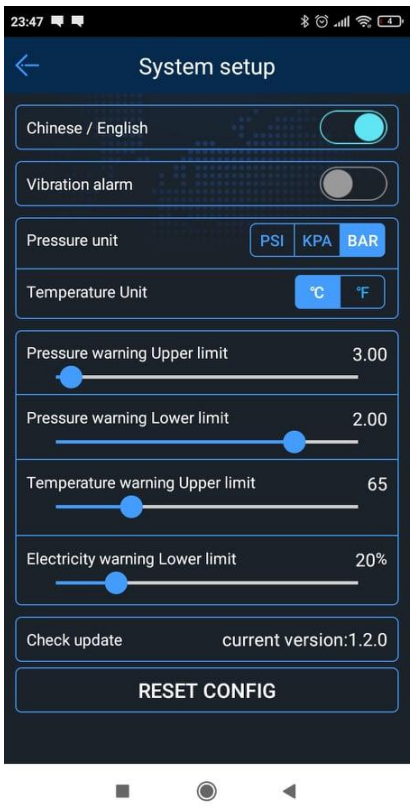

*Slika 10.14. Skeniranje barkoda senzora[30]*

Nakon što se skeniraju barkodovi, senzori budu povezani sa aplikacijom te se prikazuju vrijednosti tlaka i temperature guma, slika 10.15.




*Slika 10.15. Očitane vrijednosti tlaka i temperature guma[30]*

U postavkama aplikacije moguće je odabrati željenu mjernu jedinicu prikaza vrijednosti, željene maksimalne i minimalne vrijednosti alarmiranja očitanih vrijednosti, željenu minimalnu vrijednost slanja obavijesti o statusu baterije i povratak svih postavi na tvorničke postavke. Slika 10.16. prikazuje postavke aplikacije. [31]

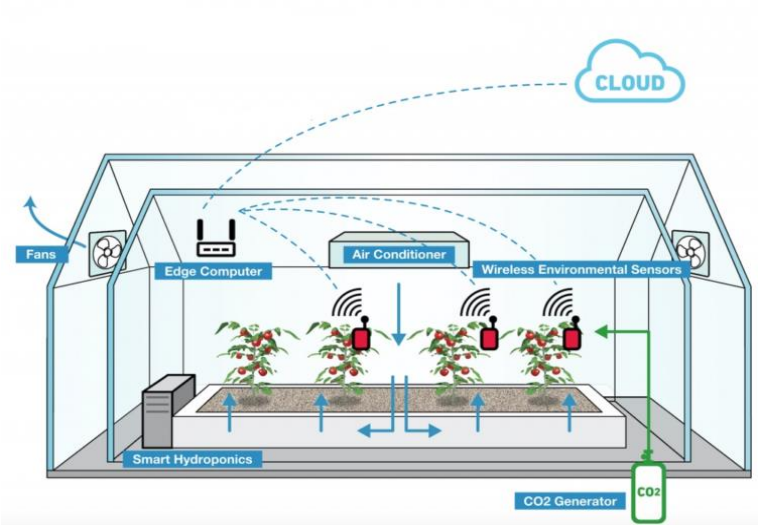



*Slika 10.16. Postavke aplikacije*

## 10.4. BLE u poljoprivredi

Poljoprivreda i poljoprivredna industrija godinama su napredovale. Mnoge njegove inovacije uvelike se oslanjaju na tehnološki napredak kako bi pomogle povećati prinos usjeva i poboljšale poslovanje farmi. Razne tvrtke koje proizvode poljoprivredne strojeve pružaju rješenja za određivanje osjetljivosti za različita poljoprivredna okruženja kako bi poljoprivrednicima pružila točne podatke za preciznu poljoprivredu. Kako tehnologija napreduje, operacije na farmi postale su sve automatizirane s bežičnim senzorima i uređajima za poboljšanje učinkovitosti i točnosti načina na koji poljoprivrednici sade, proizvode i brinu o svojoj stoci. Danas je IoT glavna snaga povećane poljoprivredne proizvodnje po smanjenim troškovima. Neke od primjena su:

- Monitoring tla i biljaka: koristeći razne senzore današnji poljoprivrednici mogu donijeti bolje usjeve i smanjiti troškove. Na primjer, IoT senzori prikupljaju podatke koji se odnose na temperaturu, sadržaj vode, oborine i druge potrebne parametre u stvarnom vremenu. Poljoprivrednici mogu koristiti te podatke za identifikaciju trendova i predviđanje potreba za navodnjavanjem. Bežični nadzor omogućuje im daljinsku provjeru razine vode usjeva, čime se štedi vrijeme, novac i trud. Mogućnost pristupa tim podacima na bilo kojem ručnom uređaju ili računalu omogućuje veću fleksibilnost i preciznu poljoprivredu.
- Monitoring stoke: Mnogi vlasnici farmi koriste IoT aplikacije za prikupljanje kritičnih podataka o lokaciji, dobrobiti i zdravlju svoje stoke. Ove informacije im pomažu da identificiraju bolesne životinje kako bi se mogle odvojiti od stada, sprječavajući širenje bolesti. Osim toga, poljoprivrednici također koriste bežične senzore za prikupljanje važnih informacija o trudnim životinjama. *SmartShepherd*, tvrtka usmjerena na pomaganje poljoprivrednicima u uzgoju bolje stoke, razvila je bežičnu pametnu ogrlicu koja koristi BLE tehnologiju za praćenje stoke.
- Pametni staklenici: današnji poljoprivrednici koriste IoT i povezane uređaje za stvaranje samo regulirajuće mikroklime korisne za proizvodnju usjeva. Ova kontrolirana okruženja opremljena bežičnim senzorima eliminiraju borbu s ekstremnim vremenskim uvjetima, a poljoprivrednicima donose uvide u stvarnom vremenu radi poboljšane učinkovitosti. Ovi uvidi iz podataka i analitike pomažu poljoprivrednicima da reguliraju navodnjavanje, osvjetljenje, temperaturu i drugo kako bi optimizirali prinos i smanjili ručne intervencije [22].

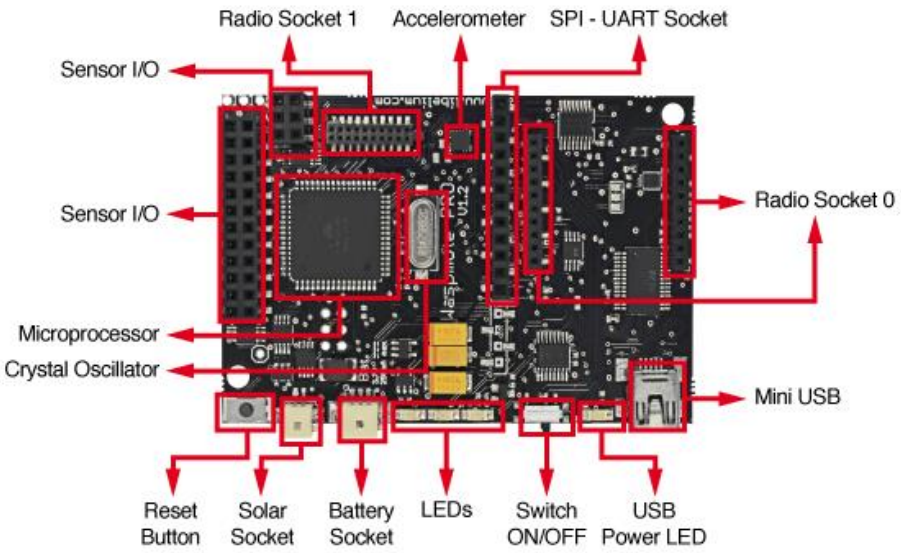



*Slika 10.17. Pametni staklenik* [22]

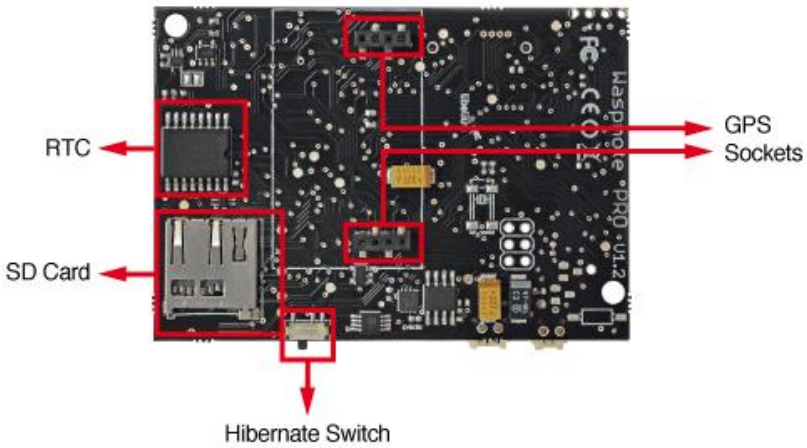
# 11. WASPMOTE I BLE MODUL

Za praktični primjer BLE tehnologije korišteni su *Waspmote* i BLE modul, laptop i pametni telefon. *Waspmote* je *open-source* platforma senzora posebno usmjerena na implementaciju načina rada s malom potrošnjo energije koja omogućuje čvorovima senzora ("*nodes*") da budu potpuno autonomni i napajani baterijom, nudeći promjenjiv životni vijek između 1 i 5 godina ovisno o radnom ciklusu korištenja [20].

Slike 11.1. i 11.2. prikazuju komponente Waspmote-a gornje i donje strane pločice.




*Slika 11.1. Waspmote komponente – gornja strana*




*Slika 11.2. Waspmote komponente – donja strana*

BLE modul ima dva glavna dijela, prethodno dizajnirani modul i vanjsku antenu. Postoji 7 različitih razina snage koje idu od -27 dBm do 3 dBm kako bi se postavile različite zone upita od 10 do 50 m. Ove se zone također mogu povećati ili smanjiti korištenjem druge antene za modul. Korišteni BLE modul prikazan je na slici 11.3.

*Slika 11.3. BLE modul* [15]

Osnovne karakteristika modula su :

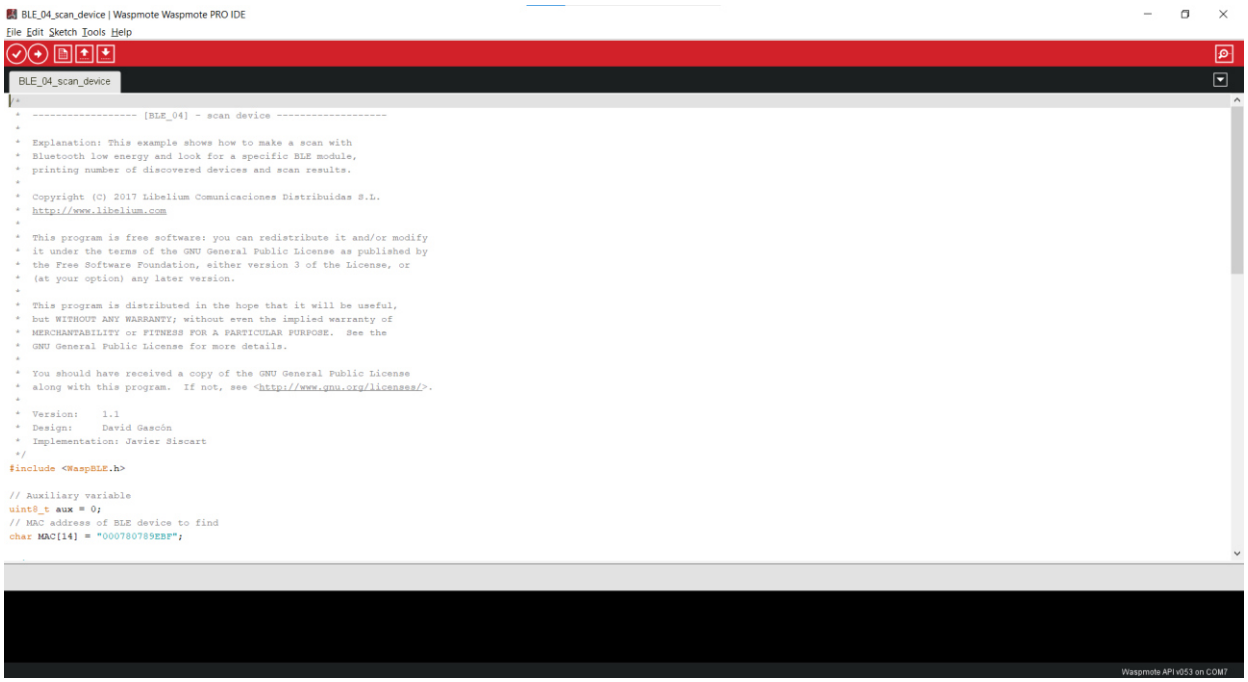
- Protokol: Bluetooth v4.0 / Bluetooth Smart
- Set čipova: BLE112
- RX osjetljivost: -103 dBm
- TX snaga: [-23 dBm, +3 dBm]
- Antena: 2 dBi/5 dBi
- Sigurnost: AES 128
- Domet: 100 metara pri maksimalnoj snazi TX-a
- Potrošnja: mirovanje (0.4 uA) / RX (8 mA) / TX (36 mA)

Radnje koje podržava su:

- Slanje emitiranih oglašivačkih paketa (*iBeacon*)
- Povezivanje s ostalim uređajima kao centralni uređaj/periferni uređaj
- Povezivanje s pametnim telefonima i tabletima
- Postavljanje automatskih ciklusa mirovanja/prijenosa
- Izračunavanje udaljenosti korištenjem RSSI vrijednosti
- Savršeno za unutarnje lokalne mreže (RTLS) [15]

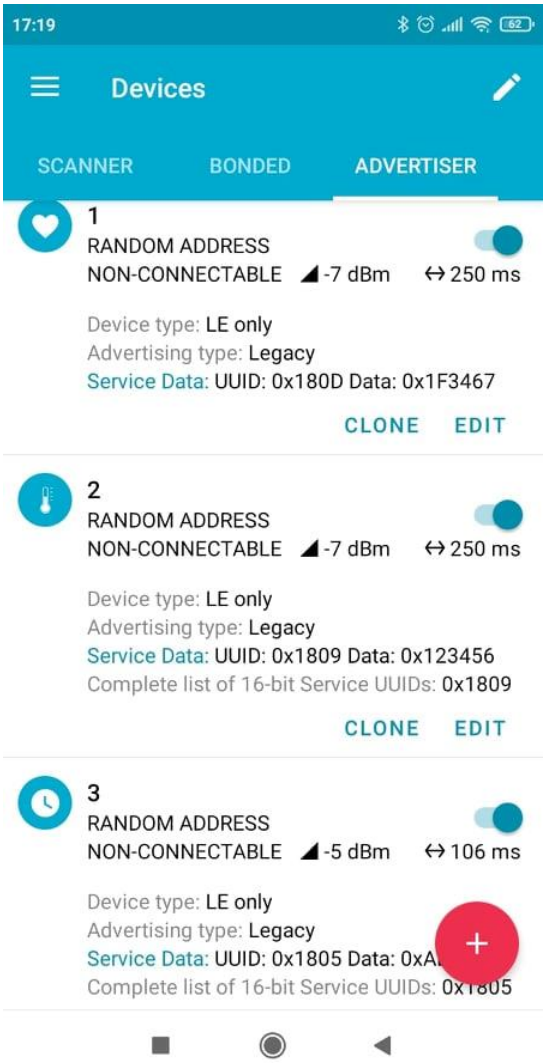
Na laptopu je korišten *Waspmote* IDE a na pametnom telefonu *nRF Connect* Android aplikacija, također dostupna i za iOS. U *Waspmote* IDE-u koji je prikazan na slici 11.4. učitali

smo napisani primjer programskog koda koji kada se prenese na modul omogućuje skeniranje BLE uređaja koji se oglašavaju.



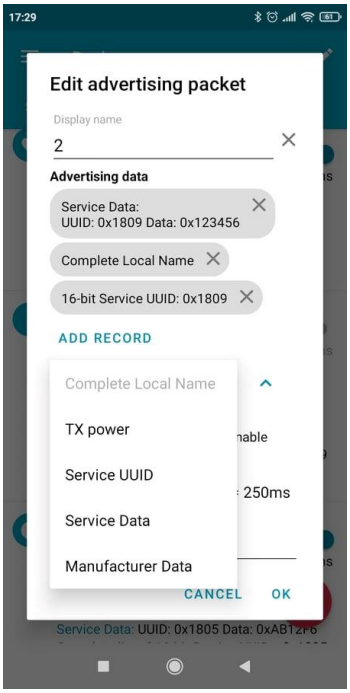

*Slika 11.4. Waspmote IDE*

Mobilna aplikacija *nRF Connect* ima mogućnost dodavanja virtualnih oglašivačkih uređaja sa određenim servisom i karakteristikama. Prvi uređaj postavljen je kao uređaj za mjerenje brzine otkucaja srca sa servisnim podacima UUID 0x180D i vrijednosti 0x1F3467, grudi uređaj postavljen je kao uređaj za mjerenje tjelesne temperature kojemu je UUID 0x1809 sa vrijednošću podatka 0x123456 i treći uređaj za prikazivanje trenutnog vremena kojemu je UUID 0x1805 sa vrijednošću podatka 0Xab12f6 . Slika 11.5. prikazuje dodane virtualne BLE oglašivače sa njihovim podacima.

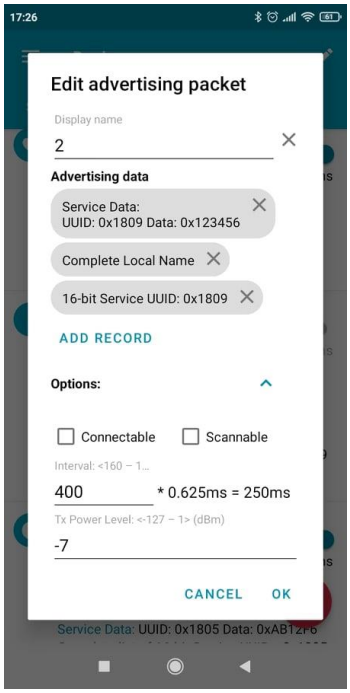



*Slika 11.5. Virtualni oglašivači*

Aplikacija ima mogućnost raznih podešenja za pojedini virtualni oglašivač, kao što su odabir koji će se podaci prikazivati na drugom uređaju, interval ponovnog oglašavanja, odabir servisa i unos njihovih vrijednosti te da li će uređaj biti moguće samo skenirati ili imati i mogućnost povezivanja. Slika 11.6. i 11.7. prikazuju spomenute dodatne mogućnosti za pojedinog virtualnog oglašivača.

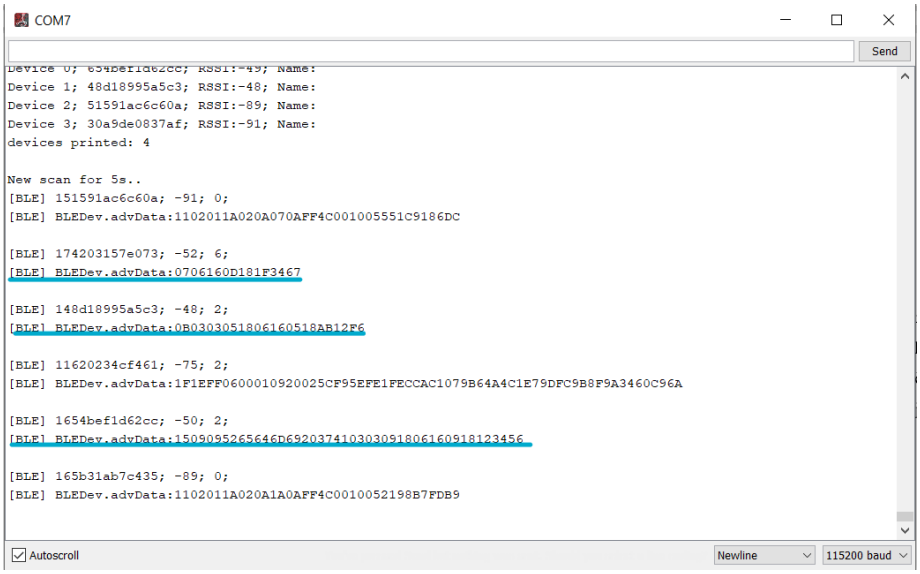



*Slika 11.6. Dodatni podaci za prikaz i unos*



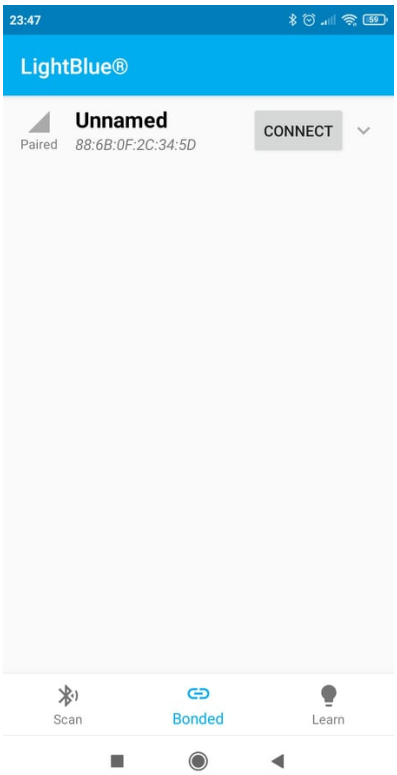

*Slika 11.7. Postavljanje Tx snage i intervala oglašavanja i mogućnost skeniranja i povezivanja*

Nakon što se pokrene kod na *Waspmote* IDE-u, *Serial Monitor* prikazuje broj oglašivačkih uređaja. Prilikom skeniranja pojavilo se još oglašivačkih uređaja koji su bili u blizini BLE modula iz susjednih prostorija, ali se naši definirani uređaji mogu jasno uočiti po zadnjih znamenkama paketa oglašavanja. Na slici 11.8. plavom bojom podcrtani su skenirani virtualni uređaji.



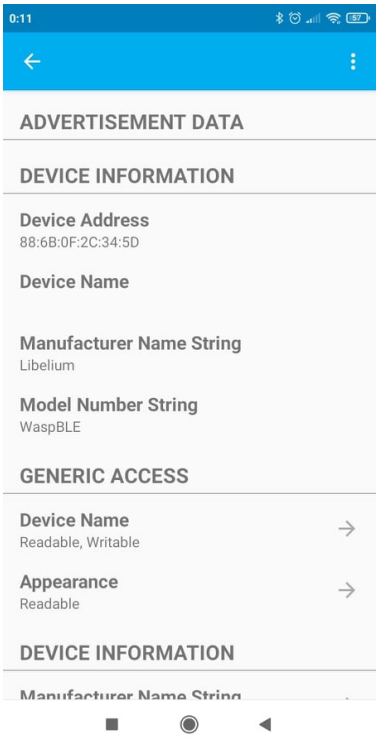

*Slika 11.8. Skenirani uređaji BLE modulom*

Postoje razne aplikacije kao što je *nRF Connect*. Jedna jako slična i jednostavna aplikacija za povezivanje BLE modula sa pametnim telefon je *LightBlue* aplikacija, koja je dostupna za Android i za iOS. Za povezivanje *LightBlue* aplikacije sa pametnim telefonom koristimo iste korake kao i u prethodnom primjeru sa nRF Connect aplikacijom. Prvo učitamo gotovi kod primjera sa Waspmote-a na BLE  i nakon toga LightBLlue skenira BLE modul se uspostavlja konekcija sa aplikacijom. Slika 11.9 prikazuje skeniran BLE uređaj sa MAC adresom.



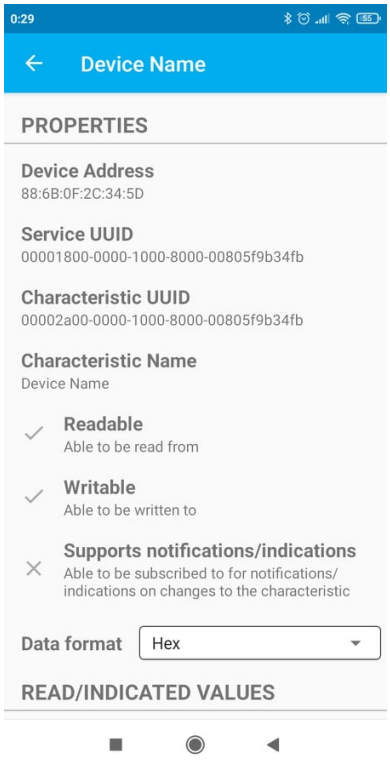

*Slika 11.9. Skenirani BLE modul LightBlue aplikacijom*

Nakon povezivanja prikazuju se informacije profila BLE modula, prikazano na slici 11.10.



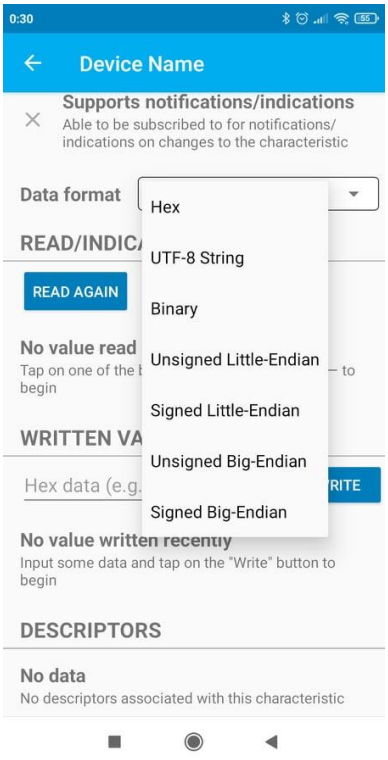

*Slika 11.10. Informacije BLE modula*

U ovom primjeru sa aplikacijom *LightBlue* prikazana će biti svojstva koje pojedine karakteristike modula mogu imati. Moguća svojstva su čitanje, unos, pretplata i indikacija. Kao što je vidljivo na slici 11.10. pojedine karakteristike su samo za čitanje dok neke imaju svojstvo čitanja i unosa vrijednosti kao što je naziv uređaja (*engl. Device Name*). Pritiskom na karakteristiku naziv uređaja prikazuje nam se MAC adresa, servis UUID, UUID karakteristike, naziv karakteristike i svojstvo karakteristike, prikazano na slici 11.11., koja može biti pročitana te joj se može mijenjati vrijednost unosom.



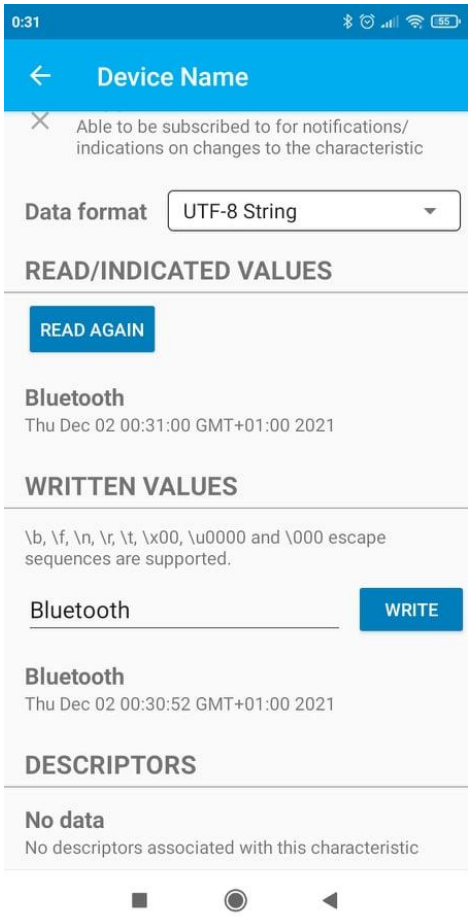

*Slika 11.11. Informacije karakteristike naziva uređaja*

Prilikom unosa imena uređaja imamo mogućnost odabira formata unosa što je prikazano na slici 11.12..




*Slika 11.12. Formati podataka prilikom unosa*

Odabrani format podatka je UTF-8 String te se upisuje željeni naziv uređaja, u ovom slučaju „Bluetooth“, u pripadajuće polje i pritiskom na dugme *Write* pohranjujemo uneseni naziv. Odmah nakon pohrane prikazuje se naziv sa vremenom i datumom čitanja što je prikazanom slikom 11.13. Pritiskom na dugme Read again ispisuje se zadnji uneseni naziv sa vremenom i datumom čitanja.




*Slika 11.13. Ispis unesenog naziva uređaja*

# 12. ZAKLJUČAK

Bluetooth tehnologija je dobro poznata tehnologija koja od svog nastajanja do danas pronašla široku primjenu. Svojim razvojem kroz godine je uključivao sve više različitih uređaja te ih umrežavao, što je postignuto novijim verzijama gdje je u verziji 4 predstavljen Bluetooth Low Energy (BLE). BLE je je tehnologija niske potrošnje energije spojenih uređaja, gdje uređaji mogu biti napajani baterijski. Kako je mala količina podataka koja se prenosi potrošnja energije je niska. Brzina veze BLE-a može osigurati da uređaj brzo uspostavi vezu i dovrši prijenos podataka, a zatim brzo ući u stanje mirovanja. Glavni dijelovi BLE arhitekture su kontroler i host a između njih djeluje *Host Controller Interface* koji omogućuje njihovu međusobnu komunikaciju. BLE u svojoj arhitekturi je predstavio nove uvedene koncepte koji poboljšavaju rad i što ga čine idealnim za IoT. U komunikaciji sudjeluju periferni i centralni uređaji koji svojim stanjima oglašavanja i skeniranja stvaraju vezu, gdje se prenose podaci. Vrsta implementirane opreme u uređajima određuje postoji li mogućnost komunikacije klasičnim Bluetooth-om ili BLE-om, što određuje sami proizvođač uređaja. Kako bi se osigurala komunikacija između svih Bluetooth uređaja proizvođači uređaja implementiraju obje tehnologije, što najviše uočavamo u pametnim mobilnim uređajima. Frekvencijski spektar BLE-a je od 2,400 do 2,4835 GHz podijeljen na 40 kanala od koja su 3 za oglašavanje a preostalih 37 za skeniranje. BLE pruža veliku sigurnost svojim mehanizmima protiv pasivnog prisluškivanja i *man-in-the-middle* napada. Teško je predvidjeti domet razvoja BLE tehnologije i njegove primjene jer je već sad prisutna u medicini, poslovnim i stambenim prostorima, proizvodnjama, industrijama itd. Korištenjem bežičnih tehnologija izbačeni su brojni bespotrebni kablovi čime se štedi energija, i čini ljudima život ugodnijima a i ekološki prihvatljivo.

# LITERATURA


[1] Bluetooth, dostupno na: https://hr2.wiki/wiki/Bluetooth, zadnja posjeta: 20.08.2021

[2] Bluetooth low Energy Beacon, dostupno na: https://en.wikipedia.org/wiki/Bluetooth_low_energy_beacon, zadnja posjeta 22.08.2021

[3] M. Afaneh, Intro to Bluetooth Low Energy, Novel Bits, 2018.

[4] Introduction - BLE Networking Guide, dostupno na: https://development.libelium.com/ble-networking-guide/introduction, zadnja posjeta: 3.9.2021

[5] K. Townsend, C. Cufi, A. i R. Davidson, Getting started with Bluetooth Low Energy, O'Reilly, April 2014.

[6] D. Bikić, Ispitivanje Near Field Communication i Bluetooth Low Energy tehnologija na Android uređajima, Sveučilište u Rijeci, Tehnički fakultet, Svibanj 2016.

[7] How GAP and GATT Work, dostupno na: https://punchthrough.com/how-gap-and-gatt-work/, zadnja posjeta: 3.9.2021.

[8] The Basics of Bluetooth Low Energy, dostupno na: https://www.novelbits.io/basics-bluetooth-low-energy/, zadnja posjeta: 7.9.2021

[9] Core Specification 4.2, dostupno na: https://www.bluetooth.com/specifications/specs/core-specification-4-2/, zadnja posjeta: 10.9.2021

[10] Bluetooth Smart Security BTLE, dostupno na: https://davidhoglund.typepad.com/integra_systems_inc_david/2015/04/bluetooth-smart-security-btle.html, zadnja posjeta: 10.9.2021

[11] BLE Advertising and Scanning, dostupno na: https://github-wiki-see.page/m/qdfreqchip/FR801x-SDK/wiki/BLE-Advertising-and-Scanning, zadnja posjeta: 7.9.2021

[12] GATT (Services and Characteristics), dostupno na: https://www.oreilly.com/library/view/getting-started-with/9781491900550/ch04.html, zadnja posjeta 6.9.2021

[13] J. Lindh, Bluetooth low energy Beacons, Texas Instruments, October 2016.

https://dev.ti.com/tirex/explore/node?node=AD4sGbaamTCyn0DvZgBAsg__krol.2c__LATEST, zadnja posjeta: 15.9.2021

[14] Bluetooth Mesh, dostupno na: https://www.novelbits.io/bluetooth-mesh-tutorial-part-3/, zadnja posjeta: 9.9.2021

[15] Waspmote documentation, dostupno na: https://www.cooking-hacks.com/documentation/tutorials/waspmote.html#applications, zadnja posjeta 16.9.2021

[16] Bluetooth Low Energy: A Detailed Guide for Beginners. Part 2, dostupno na: https://tech-en.netlify.app/articles/en533580/index.html, zadnja posjeta 4.9.2021

[17] Bluetooth LE Fundamentals, dostupno na: https://www.silabs.com/support/training/getting-started-with-bluetooth/bluetooth-le-fundamentals, zadnja posjeta 12.9.2021.

[18] BLE Advertising and Scaninng, dostupno na: https://github-wiki-see.page/m/qdfreqchip/FR801x-SDK/wiki/BLE-Advertising-and-Scanning, zadnja posjeta: 10.9.2021

[19] Bluetooth Mesh, dostupno na: https://www.novelbits.io/bluetooth-mesh-tutorial-part-1/, zadnja posjeta: 14.9.2021

[20] BLE pairing process combing, dostupno na: https://programmersought.com/article/15215490100/, zadnja posjeta: 18.9.2021

[21] Bluetooth low energy possibilities in healthcare, dostupno na: https://www.electronicspecifier.com/news/blog/bluetooth-low-energy-possibilities-in-healthcare, zadnja posjeta: 13.9.2021.

[22] IoT smart Farming, dostupno na: https://www.cassianetworks.com/blog/iotforsmartfarming/, zadnja posjeta: 17.9.2021

[23] Khanh Tuan Le, Bluetooth low energy and the automotive transformation, Texas Instruments, September 2017

[24] Waspmote, dostupno na: https://www.cooking-hacks.com/documentation/tutorials/waspmote.html, zadnja posjeta: 17.9.2021

[25] Wireless Charging Grip (WCG91501), dostupno na: https://www.powercastco.com/grips/#images, zadnja posjeta: 24.09.2021

[26] Versatile Bluetooth 5.2 SoC supporting Bluetooth Low Energy, Bluetooth mesh and NFC, dostupno na: https://www.nordicsemi.com/products/nrf52832, zadnja posjeta: 24.09.2021

[27] PowerCast, dostupno na: https://www.powercastco.com/products/powerspot/, zadnja posjeta: 24.09.2021

[28] RF prijemnici žetve, upravljanje snagom, dostupno na: https://hr.answersexpress.com/rf-receivers-harvest-18912 , zadnja posjeta: 24.09.2021

[29] ADAMM monitor, dostupno na: https://healthcareoriginals.com/personal/#web, zadnja posjeta 5.10.2021.

[30] TMPSII sdsaplikacija, dostupna na: https://play.google.com/store/apps/details?id=com.chaoyue.tyed&hl=hr&gl=US, zadnja posjeta 28.10.2021.

[31] Smart 4 Vanjski senzori Auto TPMS Bluetooth 4.0 sustav nadzora tlaka u gumama, dostupno na: https://hr.woopshop.com/products/smart-4-external-sensors-car-tpms-bluetooth-4-0-tire-pressure-monitoring-system, zadnja posjeta 28.10.2021.

# SAŽETAK

*Bluetooth Low Energy* (BLE) predstavljen je u inačici Bluetooth 4.0., sa svojstvom smanjene potrošnje energije uređaja koji međusobno komuniciraju. BLE radi u pojasu širine 2.4 GHz (ISM) koji je segmentiran u 40 radio frekvencijskih kanala, svaki širine po 2 MHz gdje se tri posljednja kanala koriste za oglašavanje a preostalih 37 za prijenos podataka. Arhitektura protokolnog stoga BLE-a čine slojevi kontroler, host i aplikacijski sloj sa pripadajućima slojevima. U komunikaciji mogu sudjelovati uređaji kao što su periferni uređaja, emiter, centralni uređaj i promatrač. Prije uspostave komunikacije uređaji se oglašavaju i skeniraju kako bi mogli prenositi međusobno podatke. U stanju oglašavanja, uređaj šalje pakete koji sadrže korisne podatke drugima koji ih primaju i obrađuju. Nakon uspostavljene veze definira se način na koji će jedan od uređaja, poslužitelj, predočiti svoje podatke klijentu što predstavlja ATT i format servisa i njihove karakteristike što predstavlja GATT. Sigurnost u BLE tehnologiji upravlja S*ecurity Manager* (SM) koji definira protokole i algoritme za generiranje i razmjenu ključeva između dva uređaja. 2017. godine Bluetooth SIG predstavio je Bluetooth mrežni standard (eng. *Bluetooth mesh*) gdje više uređaja mogu međusobno slati poruke.

**Ključne riječi:** Bluetooth Low Energy (BLE), centralni uređaj, oglašavanje, periferni uređaj, skeniranje

# BLUETOOTH LOW ENERGY (BLE) AND ITS APPLICATIONS

## ABSTRACT

Bluetooth Low Energy (BLE) is introduced in Bluetooth version 4.0, with the property of reduced power consumption of devices that communicate with each other. The BLE operates in the 2.4 GHz band (ISM) which is segmented into 40 radio frequency channels, each 2 MHz wide where the last three channels are used for advertising and the remaining 37 for data transmission. The BLE protocol stack architecture consists of a controller, host, and an application layer with associated layers. Devices such as a peripheral device, emitter, central device, and an observer can participate in communication. Before establishing communication, the devices are advertised and scanned so that they can transmit data. In the advertising state, the device sends packets containing useful data to others who receive and process it. Once the connection is established, the way in which one of the devices, the server, presents its data to the client, which is ATT and the format of the service, and their characteristics, which is GATT, is defined. Security in BLE technology is managed by Security Manager (SM) which defines protocols and algorithms for generating and exchanging keys between two devices. In 2017, the Bluetooth SIG introduced the Bluetooth mesh standard, where multiple devices can send messages to each other.

**Keywords**: Bluetooth Low Energy (BLE), central device, advertising, peripheral device, scanning

# ŽIVOTOPIS

Stjepan Flisar rođen je u Požegi 05.12.1993. godine. Pohađao je Osnovnu školu „Antun Kanižlić“ u Požegi. Nakon završene osnovne škole upisuje Tehničku školu u Požegi, smjer Tehničar za računalstvo. Srednje strukovno obrazovanje završava 2012. godine, nakon čega iste godine upisuje Stručni studij elektrotehnike, smjer informatika, na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, tadašnji Elektrotehnički fakultet, na Sveučilištu J.J. Strossmayera. Nakon završetka stručnog studija elektrotehnike, 2016. godine stječe akademski naziv prvostupnik (lat. baccalaureus) inženjer elektrotehnike. 2017. godine upisuje Razlikovnu godinu na istom fakultetu. 2019. godine upisuje diplomski sveučilišni studij Elektrotehnike, smjer komunikacije i informatika, izborni blok Mrežne tehnologije u Osijeku.