Mogućnosti primjene Bluetooth-a u IoT okruženju s naglaskom na sigurnosne aspekte

Damjanović, Ana-Marija

Master's thesis / Diplomski rad

2021

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

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:635549

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

SVEUČILIŠNI STUDIJ

MOGUĆNOST PRIMJENE BLUETOOTH-A U IOT OKRUŽENJU S NAGLASKOM NA SIGURNOSNE ASPEKTE

Diplomski rad

Ana-Marija Damjanović

Osijek 2021.

SADRŽAJ

1. UVOD

Internet of Things ili *IoT* kako se češće naziva u svakidašnjoj upotrebi, nova je vrsta umrežene paradigme sastavljene od žičnih i bežičnih mreža, te je pomoću interneta proširena diljem svijeta. Svrha *IoT-a* je povezati mnoštvo heterogenih uređaja, nazvanih „stvari“ (engl. *things*) korištenjem različitih komunikacijskih tehnologija te omogućiti krajnjim korisnicima korištenje različitih aplikacija [1].

IoT sa sobom donosi dobre i loše stvari za cijeli eko-sustav. U to se podrazumijevaju napredak u društvenom razvoju, ekonomski dobici, ali također sa sobom nosi i povoljnije uvjete za napadače koji narušavaju sigurnost sustava.

Ova paradigma se može susresti s brojnim napadačima gledano sa sigurnosnog aspekta, a sigurnost samih IoT aplikacija najviše ovisi o bežičnoj infrastrukturi.

Bluetooth predstavlja jedan od oblika bežične tehnologije temeljene na IEEE 802.15.1 standardu. Kao takav koristi se za razmjenu podataka između fiksnih i mobilnih bežičnih uređaja unutar kratkog pojasa (engl. *short-range*) i WPAN-a (engl. *Wireless Personal Area Networks*). Bluetooth je proizvod telekomunikacijske tvrtke Ericsson te se smatra bežičnom alternativom koja se može koristiti umjesto RS-232 kabela [1].

BLE je tehnologija široke primjene i kratkog dometa te je zahvaljujući svojoj jednostavnosti, niskoj potrošnji energije i višestrukoj primjeni pridobio poziciju u razvoju IoT paradigme [2]. Razlika između standardnog Bluetooth-a i BLE je u količini podataka koja se može razmijeniti korištenjem jedne od dviju tehnologija te o količini energije koja se troši prilikom korištenja jedne od dviju tehnologija unutar IoT projekta.

Mogući su brojni sigurnosni napadi prilikom korištenja bežičnih tehnologija, te se tako i BLE susreće s brojnim napadima, prijetnjama i izazovima. Potrebno je pronaći moguća rješenja kako povećati razinu sigurnosti, tehnologije kojima će se omogućiti veća sigurnost na osnovu dobivenih testnih rezultata.

1.1. Zadatak diplomskog rada

IoT (engl. *Internet of Things*) podrazumijeva modernu komunikacijsku platformu koja primjenom različitih komunikacijskih tehnologija omogućava povezivanje i međusobnu interakciju različitih heterogenih uređaja i sustava. Bluetooth je jedna od komunikacijskih tehnologija koja svoju primjenu pronalazi unutar IoT okruženja. Potrebno je sustavno analizirati mogućnosti i primjere primjene Bluetooth tehnologije u IoT okruženju, s posebnim naglaskom na aspekte sigurnosti i privatnosti. Bluetooth komunikaciju unutar IoT-a analizirati u testnom okruženju, te komentirati dobivene rezultate, te naglasiti smjernice za povećanje razine sigurnosti i privatnosti.

2. BLUETOOTH LOW ENERGY TEHNOLOGIJA

Bluetooth Low Energy (BLE) je bežična tehnologija koja je još u uvijek u procesu nastajanja, razvijena od strane *Bluetooth Special Interest Group* (SIG) za komunikaciju kratkog dosega. Za razliku od prethodnih Bluetooth ogranaka, BLE je dizajniran kao nisko-energetsko rješenje za kontrolne i upravljačke aplikacije. BLE je potomak Bluetooth v4.0 [7].

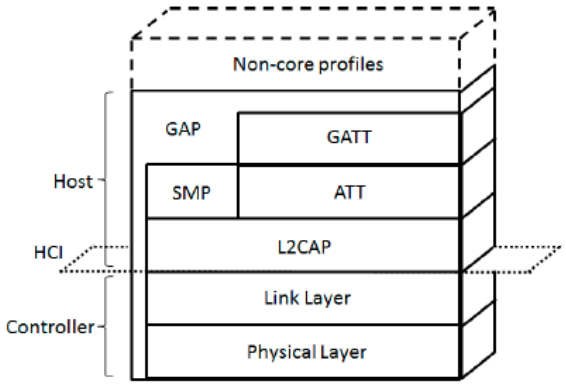
BLE predstavlja jednokratno rješenje primjenjivo na različite prostore upotrebe u područjima kao što su zdravstvo, potrošačka elektronika, pametna energija i sigurnost. Raširenost korištenja Bluetooth tehnologije (na primjer u mobilnim telefonima, prijenosnim računalima, automobilima itd.) mogu dovesti do usvajanja BLE, zašto što je implementacija slična onoj od klasičnog *Bluetooth*-a [7].

BLE standardi su *Bluetooth* tehnologija koja je dizajnirana kako bi omogućila jednostavno uparivanje Bluetooth uređaja slanjem njihove Bluetooth MAC adrese na kanale. Tako bi se korisnik na udaljenosti od samo nekoliko metara od uređaja mogao lako povezati s protokolom te na taj način dobiti svoj jedinstveni identifikator [8].

2.1. Pregled protokolnog stoga BLE-a

Bluetooth Low Energy, također poznat pod nazivom *Bluetooth Smart*, pojavljuje se kao glavna bežična tehnologija niske snage. Iskoristivši dizajn koji može ponovno koristiti klasične Bluetooth sklopove u velikoj mjeri, BLE je stekao dominantan položaj u pametnim telefonima. To omogućava nisku potrošnju energije komunikacije između kasnijih uređaja kao što su senzori, aktuatori, nosivi elementi i mnogi drugi [9].

BLE definira cjelovitu protokolnu arhitekturu čija je svrha omogućavanje komunikacije male snage između uređaja. Arhitektura mrežnog stoga se sastoji od dva glavna dijela, a to su: kontroler, koji obavlja zadatke radijskog sučelja, te host-a, koji nudi višu funkcionalnost slojeva te podržava aplikacije. Kontroler se sastoji od fizičkog sloja i sloja linka, dok se host sastoji od protokola logičke kontrole linka i prilagodbe (L2CAP), *Atribute* protokola (ATT), *Generic Attribute* profila (GATT), sigurnosnog upravljačkog protokola (engl. *Security Manager Protocol*, SMP), te *Generic Access* profila (GAP). Host i kontroler komuniciraju preko sučelja koje se naziva *Host Controller Interface* (HCI) [9]. Na slici 2.1. prikazana je arhitektura mrežnog stoga, koju, kao što je već navedeno čine kontroler i host, te su također slikovito prikazani i protokoli.



Slika 2.1. Protokolni stog BLE-a [9]

2.1.1. Fizički sloj

Buetooth Low Energy radi u pojasu širine 2.4 GHz (ISM) te definira 40 kanala radijske frekvencije (RF) s pojasom širine od 2MHz. Postoje dvije vrste BLE radijskih kanala: kanali za oglašavanje i podatkovni kanali. Kanali za oglašavanje (engl. *Advertising channels*) se koriste za pronalaženje uređaja, uspostavljanje veze te prijenos emitiranja, dok se podatkovni kanali koriste za dvosmjernu komunikaciju između povezanih uređaja. Tri kanala definirana su kao kanali za oglašavanje. Ovim su kanalima dodijeljene središnje frekvencije koje minimaliziraju preklapanje s IEEE 802.11 kanalima 1, 6 i 11. Prilagodljivi mehanizam skakanja frekvencije koristi se na vrhu podatkovnih kanala kako bi se suočio sa smetnjama i problemima bežičnog širenja, poput *fading*-a i višestrukog prolaska. Ovaj mehanizam odabire jedan od 37 dostupnih podatkovnih kanala za komunikaciju tijekom određenog vremenskog intervala. Svi fizički kanali koriste Gaussovu modulaciju frekvencijskog pomaka (engl. *Gaussian Frequency Shift Keying,* GFSK), koja je jednostavna za primjenu. Indeks modulacije je u rasponu između 0,45 i 0,55, što omogućuje smanjenu vršnu potrošnju energije. Brzina prijenosa podataka na fizičkom sloju je 1 Mbps [7].

2.1.2. Sloj linka

U BLE-u, kada uređaj samo treba emitirati podatke, on ih putem oglašivačkih kanala prenosi u oglašivačkim paketima. Bilo koji uređaj koji prenosi oglašivačke pakete naziva se oglašivač. Prijenos paketa putem kanala oglašavanja odvija se u vremenskim intervalima koji se nazivaju oglašivački događaji. Unutar oglašivačkog događaja, oglašivač uzastopno koristi svaki oglašivački kanal za paketni prijenos. Uređaji kojima je cilj samo primanje podataka putem oglašivačkih kanala nazivaju se skeneri [7].

Dvosmjerna podatkovna komunikacija između dva uređaja zahtjeva njihovo međusobno povezivanje. Stvaranje veze između dva uređaja se predstavlja kao asimetrična procedura pri kojoj oglašivač oglašava preko svojih kanala da postoji uređaj na koji se može povezati, dok drugi uređaj, koji je predstavljen kao inicijalizator povezivanja, čeka na obavijest o mogućem povezivanju. Kada inicijalizator pronađe oglašivača, šalje mu poruku sa zahtjevom za povezivanje, čime se stvara *point-to-point* veza između dva uređaja. Nakon što su povezani, ti uređaji mogu komunicirati preko fizičkih kanala. Pakete koji se šalju ovim putem moguće je identificirati pomoću nasumično generiranog 32-bitnog pristupnog koda [7].

BLE definira dvije uloge uređaja na *Link Layer-u* za stvorenu vezu: *master* i *slave*. To su uređaji koji djeluju kao pokretači i oglašivači tijekom stvaranja veze. *Master* može upravljati s više istovremenih veza s različitim *slave*-vovima, dok se svaki *slave* može povezati samo s jednim *masterom*. Dakle, mreža koju čine *master* i njegovi *slave-vovi,* a koja se naziva pikonet, slijedi topologiju zvijezde. BLE uređaj može pripadati samo jednom pikonetu. Kako bi uštedjeli energiju, *slave*-vovi su prema zadanim postavkama u stanju mirovanja i povremeno se bude kako bi osluškivali moguće prijeme paketa od *mastera*. *Master* određuje trenutke u kojima su *slave*-vovi potrebni kako bi slušali, i na taj način koordinira pristup mediju koristeći shemu vremenske podjele višestrukog pristupa (TDMA). *Master* također pruža pomoćnom uređaju informacije potrebne za algoritam preskakanja frekvencije (uključujući mapu podatkovnih kanala koji će se koristiti) i za nadzor veze. Parametri povezani s upravljanjem vezom prenose se u poruci koja sadrži zahtjev za povezivanje i mogu se ažurirati tijekom veze iz različitih razloga (npr. upotrebom nove mape podatkovnih kanala tijekom promjene uzoraka smetnji). Nakon što je stvorena veza između *mastera* i *slave*-a, fizički kanal se dijeli na jedinice koje se ne preklapaju, a koje se nazivaju događaji veze (engl. *connection events*). Unutar događaja veze, svi paketi se prenose istom frekvencijom podatkovnog kanala. Svaki događaj veze započinje prijenosom paketa od strane *master*-a. Ako *slave* primi paket, mora ga u odgovoru poslati *masteru* [7].

Povezivanja na sloju linka koriste *stop-and-wait* kontrolni mehanizam toka podataka koji se temelji na kumulativnim priznanjima, koji u isto vrijeme omogućuju mogućnost oporavka od pogrešaka. Svako zaglavlje paketa podatkovnog kanala se sastoji od dva jednobitna polja koji se nazivaju *Sequence Number* (SN) i *Next Expected Sequence Number* (NESN). SN bit identificira paket, dok NESN ukazuje koji će idući paket primiti od ravnopravnog uređaja. Ako uređaj uspješno zaprimi paket podatkovnog kanala, NESN bit njegovog idućeg bita će se

povećati te će taj paket služiti kao priznanje. U slučaju da uređaj primi paket s neispravnom CRC provjerom, NESN bit primljenog paketa će biti nevažeći [7].

2.1.3. L2CAP

L2CAP koji se koristi u BLE-u je optimizirani i pojednostavljeni protokol koji je temeljen L2CAP-u klasičnog Bluetooth-a. Glavna karakteristika BLE L2CAP-a je multipleksiranje podataka triju viših protokola: ATT-a, SMP-a i kontrolne signalizacije sloja linka na vrhu konekcije sloja linka. L2CAP na najbolji način upravlja podacima unutar ovih servisa bez korištenja retransmisije i mehanizama kontrole toka [7].

2.1.4. ATT

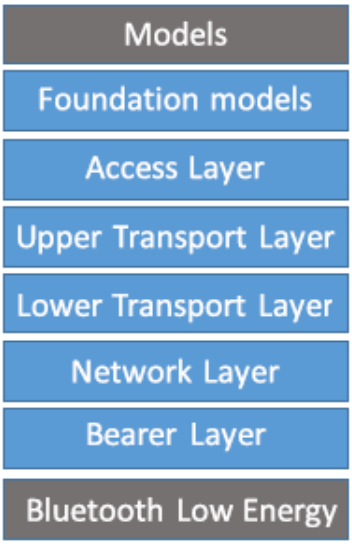
ATT definira komunikaciju između dva uređaja, gdje jedan ima ulogu klijenta, a drugi ima ulogu poslužitelja. Poslužitelj održava skup atributa. Atribut je struktura podataka koja pohranjuje informacije kojima upravlja GATT, protokol koji djeluje na vrhu ATT-a. Ulogu klijenta ili poslužitelja određuje GATT i neovisna je o podređenoj ili glavnoj ulozi. Klijent može pristupiti atributima servera slanjem zahtjeva, koji potiče slanje odgovora od strane poslužitelja. Kako bi se postigla veća učinkovitost, poslužitelj može poslati klijentu dvije vrste neželjenih poruka koje sadrže sljedeće atribute: (i) obavijesti, koje su nepotvrđene; te (ii) indikacije, koje od klijenta zahtijevaju slanje potvrde. Klijent također treba poslati naredbu poslužitelju kako bi se zabilježile vrijednosti atributa. Zahtjev/odgovor te indikacija/potvrda također slijede obilježja *stop-and-wait* sheme [7].

2.1.5. GATT

GATT definira okvire rada koje koristi ATT za pronalaženje servisa i razmjenu karakteristika od jednog uređaja ka drugome. Karakteristika je set podataka koji uključuju vrijednosti i svojstva. Podaci koji se vezuju za servise i karakteristike su pohranjeni u atributima [7].

2.2. Slojevi mrežne arhitekture Bluetooth-a

Mrežna arhitektura Bluetooth-a je dizajnirana slojevito korištenjem BLE 4.x, kojeg karakterizira povratna kompatibilnost. Tako je stvoren način da svi certificirani Bluetooth Smart i Smart Ready uređaj mogu međusobno komunicirati s Bluetooth mrežom nakon što su na njihovom softveru primijenjene prikladne promjene [2].



Slika 2.2. Slojevi mrežne arhitekture BLE-a [2]

Na slici 2.2. prikazan je slojeviti stog. Glavna karakteristika standarda je da je on izgrađen na vrhu kompletnog BLE stoga (na fizičkom sloju i sloju linka). Podaci se uzastopno prenose na kanalima 37,38, te je kanal 39 rezerviran za sva stanja nepovezanosti, te se koristi kod beskonekcijskih oglašavanja, kao i kod neusmjerenih oglašavanja koje nije moguće skenirati, s nekim prilagodbama. Na vrhu ovog mrežnog stoga je implementirana aplikacija, koja predstavlja najvažniju ulogu unutar BLE mrežne strukture pri standardizaciji specifikacija ponašanja uređaja u skladu s paradigmom modela. Arhitektura Bluetooth mreže slijedi arhitekturu ISO-OSI standarda, te time sadržava sve slojeve od aplikacijskog do fizičkog. Pitanja kojima se bavi BLE mrežni stog su: kako definirati i implementirati spomenute modele; kako adresirati podatke i poslati ih kroz mrežu na odredište; kako izdvojiti fundamentalne slojeve jezgre BLE specifikacija [2].

2.2.1. Sloj modela

Sloj modela sadrži implementaciju modela kao što je implementacija temeljnih funkcionalnosti čvorova (ponašanje, stanja, poruke itd.) u specifičnim i standardiziranim aplikacijskim scenarijima kao što su rasvjeta i senzori. Svaki model je dio aplikacije i skupa s njom i osnovnim slojem tvori cijeli prikaz aplikacije [2].

2.2.2. Osnovni sloj modela

Ovaj sloj je odgovoran za implementaciju onih modela čija je zadaća konfiguracija i upravljanje mrežom [2].

2.2.3. Pristupni sloj (engl. Access Layer)

Pristupni sloj definira na koji način aplikacije viših slojeva mogu koristiti više nižih tehničkih slojeva (viši transportni sloj). Ovim slojem se određuje format aplikacijskih podataka, definira i kontrolira enkripciju aplikacijskih podataka kojima upravljaju različiti parametri. BLE mrežna struktura podržava transmisiju neusvojenih i usvojenih poruka [2].

2.2.4. Viši transportni sloj (engl. Upper Transport Layer)

Viši transportni sloj šifrira, dešifrira i autentificira aplikacijske podatke te je dizajniram kako bi podržavao pouzdanost kod pristupnih poruka [2].

2.2.5. Niži transportni sloj

Niži transportni sloj definira segmentiranje i ponovno sastavljanje poruka višeg sloja u više protokolnih podatkovnih jedinica nižeg sloja (PDU) [2].

2.2.6. Mrežni sloj

Mrežni sloj definira kako su adresirane poruke transportnog sloja prema jednom ili više elemenata. Definira također format mrežne poruke koji dozvoljava prijenos PDU preko nosilačkog sloja. Mrežni sloj odlučuje hoće li se poruke proslijediti dalje, prihvatiti ili odbiti. Zbog tog se *relay* i *proxy* poruke implementiraju u mrežni sloj [2].

2.2.7. Nosilački sloj

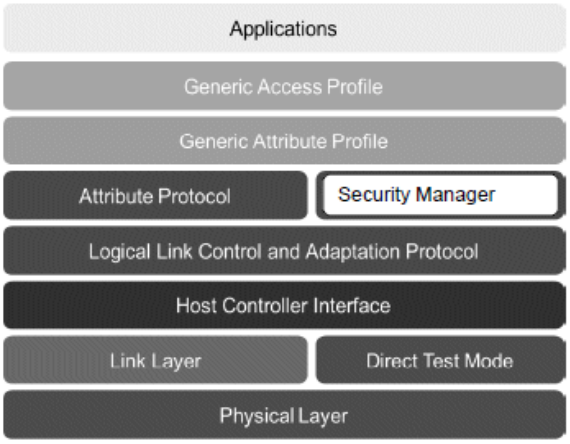
Nosilački sloj definira mehanizme prijenosa poruke. Trenutno postoje dva dostupna nosioca u posljednjoj BLE 5 mrežnoj specifikaciji, među kojima su oglašivački nosioci i GATT nosioci [2].

3. SIGURNOSNE ZNAČAJKE BLUETOOTH TEHNOLOGIJE

Sigurnost je od najveće važnosti u IoT mrežama, s obzirom na utjecaj koji takve mreže imaju na aktivnosti u fizičkom obliku. Međutim, sigurnost je trenutno izazov u BLE mrežama. Budući da SMP servisi nisu dostupni preko oglašivačkih paketa, šifrirani su samo oni paketi koji su preneseni preko podatkovnih kanala. Autentifikacija se izvršava samo unutar veze. Tako, usmjeravanje i podatkovni paketi koji se prenose putem oglašivačkih kanala nisu zaštićeni osim ako aplikacijski sloj pruži neko sigurnosno rješenje [9].

Za razliku od klasičnog Bluetootha, BLE senzori i uređaji implementiraju upravljanje ključem (engl. *key managment*) i upravitelj sigurnosti na hostu umjesto na kontroleru. SMP koji se izvodi na *host*-u brine se za generiranje i distribuciju ključeva. Ovaj pristup uveden Bluetooth specifikacijom omogućuje *host*-u veću fleksibilnost i smanjuje cijenu i složenost LE-kontrolera [11].

Bluetooth podržava SM (*Security menager*) kako bi se zaštitio prijenos podataka. SM definira proces uparivanja, metodu razmjene ključeva te sigurnosne alate korištene za sigurnost Bluetooth-a [6].



Slika 3.1. Security Manager [11]

Kao takav, *security menager* je odgovoran za sve implementacije sigurnosti i privatnosti BLE stoga, poput generiranja i spremanja različitih ključeva, generiranja slučajnih adresa i razlučivosti adresa za značajku privatnosti. Upravitelj sigurnosti koristi usluge koje pruža sloj L2CAP za upravljanje sigurnošću. Svaki uređaj može generirati vlastiti ključ bez ikakvog vanjskog utjecaja, a snaga ključa proporcionalna je algoritmu implementiranom u uređaj [11].

Postoje različiti važni ključevi i funkcije kod Bluetooth-a niske snage. Među tim ključevima su:

a) Privremeni ključ TK (eng. *Temporary Key)* – 128-bitni privremeni ključ se koristi za generiranje kratkoročnog ključa (STK) u procesu uparivanja
b) Kratkoročni ključ STK (eng. *Short Therm Key*) – 128-bitni ključ koji se koristi prilikom šifriranja veze nakon uparivanja
c) Dugoročni ključ LTK (eng. *Long Therm Key*) -128-bitni ključ koji se koristi za šifriranje veze nakon što je završen korak prijenosa distribucije specifičnog ključa.

Funkcije koje se koriste su: funkcija c1 koja se koristi za generiranjem potvrdne vrijednosti, te funkcija s1 koja se koristi za generiranje STK [6].

3.1. BLE sigurnosni modovi (engl. Security modes)

Bluetooth sigurnosni zahtjevi uređaja i usluga izraženi su u načinima zaštite i razinama zaštite. Svaka usluga i uređaj mogu imati zasebne sigurnosne zahtjeve. Fizička veza između dva uređaja uvijek djeluje u jednom sigurnosnom modu. Širokim usvajanjem specifikacija 4.2, sigurne jednostavne metode uparivanja postale su „*de facto*“ uvjet LE uređaja kako bi se osigurala sigurnost [11].

3.1.1. LE sigurnosni mod 1 (engl. *LE security mode 1*)

Postoje četiri sigurnosne razine unutar LE sigurnosnog moda 1. To su:

1) Bez sigurnosti (bez autentifikacije, bez šifriranja)
2) Neautentificirano uparivanje sa šifriranjem
3) Autentificirano uparivanje sa šifriranjem
4) Autentificirano LE sigurnosno povezivanje uparivanjem sa šifriranjem uz korištenje 128-bitnog jakog enkripcijskog ključa [12].

Sigurnosne razine 1 i 2 podržavaju LE komunikaciju bez sigurnosti i šifriranja, odnosno bez uparivanja. Razina 3 i razina 4 pružaju više sigurnosti sustavu nego prethodne razine. LE sigurna veza (razina-4) predstavljena u specifikacijama Bluetooth SIG 4.2, donosi visoku sigurnost LE komunikaciji putem tehnike kriptografije javnog ključa *Elliptic Curve Diffie-Hellman* (ECDH) [11].

3.1.2. LE sigurnosni mod 2 (engl. *LE security mod 2*)

Postoje dvije sigurnosne razine unutar LE sigurnosnog moda 2. To su:

1) Neautentificirano uparivanje s potpisivanjem podataka
2) Autentificirano uparivanje s potpisivanjem podataka [12].

Uređaji u skladu sa sigurnosnim modom rada-2 podržavaju autentificirano i neautentificirano uparivanje zajedno s obveznim potpisivanjem podataka. Podaci se mogu potpisati različitim tehnikama, uključujući kriptografiju javnog ključa, kako bi se osigurala cjelovitost i sigurnost podataka [11]. LE sigurnosni mod 2 se jedino koristi za potpisivanje podataka koje se temelji na povezanosti (slanje podataka između dva nešifrirano povezana uređaja) [12].

3.1.3. Miješani sigurnosni mod (engl. *Mixed Security mode*)

Uređaji kojima su potrebna oba sigurnosna moda, i sigurnosni način 1 i 2, koriste mješoviti mod zaštite. Takav mod omogućuje uređajima korištenje kombinacija višestrukih sigurnosnih načina, kao što su potpisivanje podataka zajedno s ECDH-om kako bi pružili ogromnu sigurnost pametnim uređajima [11].

3.1.4. Način sigurne veze (engl. *Secure Connection Only mode*)

Kada LE pametni uređaji djeluju u načinu sigurne veze, trebali bi koristiti autentificirano povezivanje i uparivanje sa šifriranjem. Uređaj prihvaća samo odlazne i dolazne veze za usluge koje koriste sigurnosni način-1, razine 4. Uz ovo ograničenje, uređaji koji rade u ovom načinu trebaju koristiti ECDH, uveden u specifikacijama 4.2 [11].

		Pairing	Encryption	Data Integrity	Layer
LE Security Mode 1	**Level 1**	No	No	No	Link Layer
	Level 2	Unauthenticated	Yes	Yes	
	Level 3	Authenticated	Yes	Yes	
LE Security Mode 2	**Level 1**	Unauthenticated	No	Yes	ATT layer
	Level 2	Authenticated	No	Yes	

Slika 3.2. LE Security mod-ovi [7]

3.2. Bluetooth LE uparivanje (engl. *Bluetooth LE pairing*)

Uparivanje je proces pronalaženja i izmjenjivanja privremenih ključeva s Bluetooth uređajem. Ovakav privremeni ključ se koristi za šifriranje povezivanja. Razmjena ključeva između klijenta i poslužitelja određuje koja će se metoda uparivanja koristiti [12].

Udruživanje se odvija u tri faze, što uključuje razmjenu mogućnosti uređaja, generiranje LTK za sigurnu vezu i distribuciju ključa specifičnog za transport. Za naslijeđene uređaje umjesto LTK koristi se STK [11].

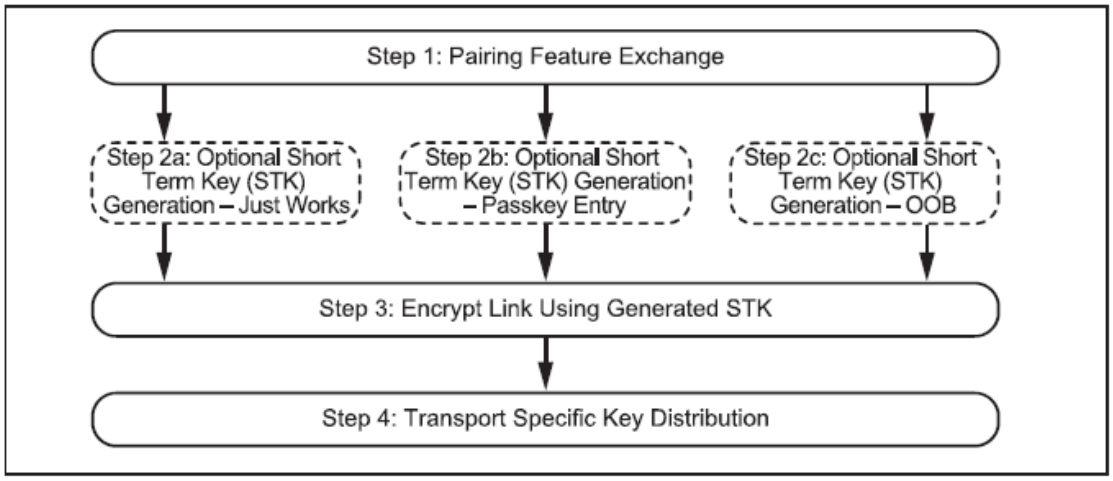
Uparivanje je proces koji se odvija u 3 faze. Unutar prve faze, dva uređaja koja sudjeluju u procesu uparivanja šalju zahtjeve za uparivanje i odgovore zajedno s parametrima uparivanja, koji uključuju mogućnosti uređaja i sigurnosne zahtjeve. Nakon toga oba uređaja odabiru metodu uparivanja na temelju vrijednosti iz razmijenjenih parametara [4].

Faza 2 bavi se provjerom autentičnosti uređaja i šifriranjem veze. Ova faza uspostavlja okruženje koje jamči sigurnost od pasivnog prisluškivanja i MITM (*Man in the middle*) napada [4].
Odabir metode uparivanja ovisi o mogućnostima razmijenjenim u fazi 1. Kratkoročni ključevi (STK) generiraju se na temelju odabrane metode uparivanja, kao što su *Just Works*, *Pass Key Entry* i *Out Of Band*. Generirani sigurni parovi ključeva (STK) koristit će se za uspostavljanje sigurnog kanala između uređaja koji sudjeluju. U *Just Works* metodi, nije obavezna razmjena ključeva između uređaja, kao ni interakciju između korisnika. Ova je metoda vrlo prikladna ako barem jedan od uređaja koji sudjeluju u komunikaciji nema korisničko sučelje. Ako oba uređaja koja sudjeluju u BLE vezi imaju zaslon i barem imaju tipku Da / Ne, tada se može koristiti numerička metoda usporedbe. Na svakom će se uređaju prikazati 6-znamenkasti nasumično generirani kod. Korisnik mora pritisnuti Da / Ne nakon ručne provjere prikazane tipke [11]. Kada jedan ili više uređaja imaju izlazni i ulazni uređaj, mogu koristiti BLE *Passkey Entry* metodu uparivanja. Uređaj treba prikazati šesteroznamenkasti broj između 000000 i 999999. Nakon toga, korisnik treba unijeti isti broj u svoj uređaj [12].

Out of band (OOB) metoda koristi sučelje koje nije Bluetooth za razmjenu podataka o uparivanju. Ova metoda je sigurnija od *Passkey* metode te od *Just Works* metode. Međutim, sučelje oba uređaja mora biti međusobno kompatibilno [6].

U posljednjoj fazi 3, uređaji šifriraju komunikaciju koristeći generirani STK ključ. Zadnji korak je napraviti ključeve koji će koristiti ponovnom povezivanju u budućnosti [6].

Bluetooth Low Energy (BLE) uređaji koriste 48-bitnu adresu. Ako je moguće dekodirati ovakvu adresu koristeći neki drugi uređaj, taj uređaj može pratiti aktivnost uređaja. BLE nepouzdanim uređajima otežava mogućnost praćenja kontinuiranim promjenama adrese. Adrese se frekventno mijenjaju korištenjem ključa koji se zove *Identity Resolving Key* (IRK) koji je dostupan samo pouzdanim uređajima. IRK se razmjenjuje između pouzdanih uređaja prilikom procesa uparivanja nakon što je dovršena enkripcija linka. Nakon toga se pohranjuje u internu memoriju kao dio procesa povezivanja. Takva adresa se naziva *Resolvable Private Adress* (RPA). RPA se sastoji od dvije komponente, a to su: 24-bitna „*hash*-a“ i 24-bitnog „*prand*-a“. Hash je funkcija IRK ključa, a *prand* je sastavljen od 22-bitnog nasumičnog broja i dva najznačajnija bita (MSBs, engl. *most significant bits)* [4].



Slika 3.3. Proces uparivanja [6]

3.3. BLE lijepljenje (engl. *BLE bonding*)

Lijepljenje (engl. *bonding*) je postupak stvaranja dugoročnog pouzdanog odnosa između uređaja na temelju ključa veze stvorenog tijekom postupka uparivanja. Dugoročni ključevi (engl. *Long Term Key*, LTK) generiraju se i pohranjuju i na pokretaču i na odgovoru. Ovi LTK-ovi moraju se koristiti za svu sljedeću komunikaciju između istih uređaja kako bi se osigurala sigurnost podataka [12].

3.4. Sigurnosni nedostaci, prijetnje i izazovi u BLE IoT okruženju

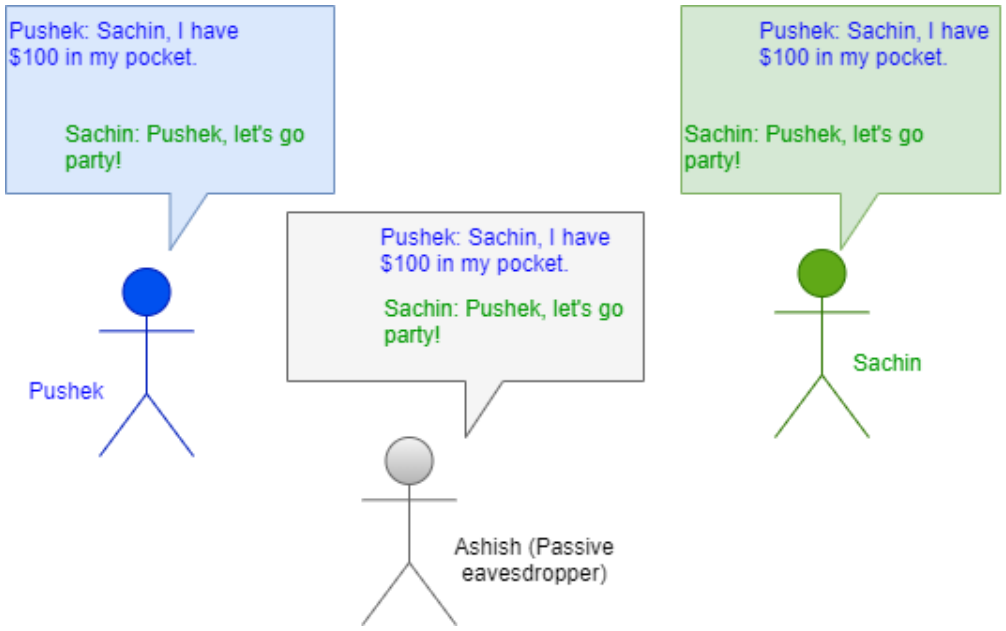
Jedan od najvećih izazova prilikom dizajniranja *Internet of Things* (IoT) aplikacija je sigurnost. Budući da IoT uređaji komuniciraju putem bežične veze, moguće je javno izložiti kontrolne i statusne informacije, kao i privatne korisničke podatke. [4]

Kao i svaka druga bežična tehnologija, BLE nije iznimka od sigurnosnih prijetnji. Iako Bluetooth LE svjetionici donose puno potencijala u dizajnu IoT-a, sigurnosne prijetnje znatno se povećavaju. BLE uređaji dizajnirani su za emitiranje MAC-a, UUID-a i servisnih podataka u unaprijed definiranom intervalu. Zbog kontinuiranog oglašavanja, hakeri mogu jednostavno pratiti uređaj i dešifrirati emitirajuće informacije pomoću *sniffer*-a ili čak pametnog telefona. Uz hakiranje i *cyber* kriminal koji se prijavljuju u cijelom svijetu, ljudi su izuzetno zabrinuti zbog privatnosti. Osjetljivi podaci koji dolaze u ruke pogrešnih ljudi bez pristanka korisnika mogu dovesti do značajne štete. Primjerice, ako se takvi uređaji s ozbiljnim sigurnosnim nedostacima primijene u vojsci, to suparnicima može otkriti tajne [11].

Postoje tri stvari koje je potrebno implementirali kako bi se zaštitili IoT uređaji:

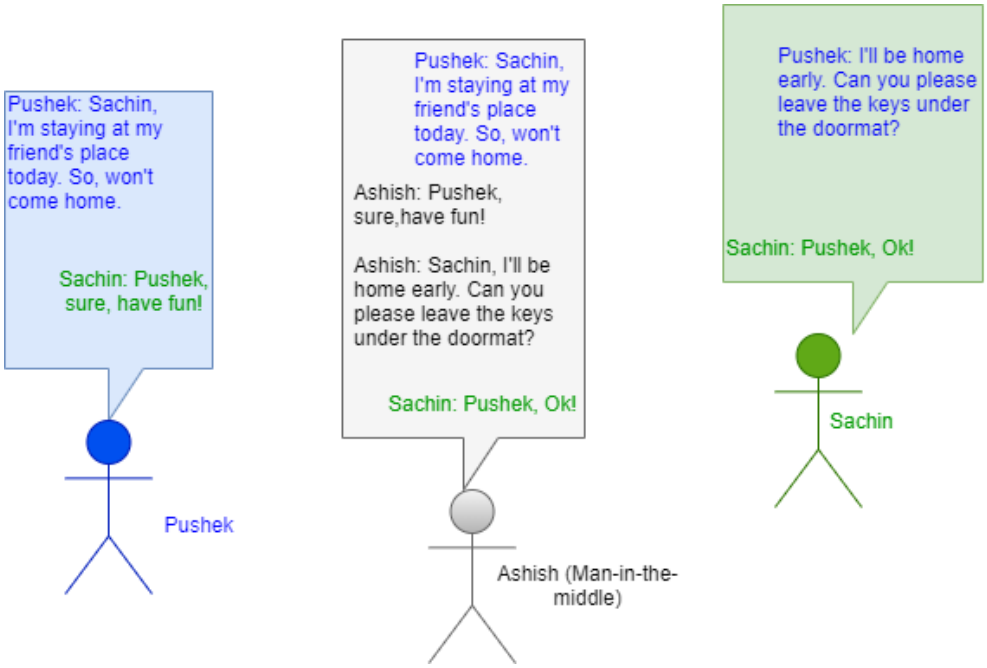
1. Mehanizam sakrivanja identiteta uređaja od neautoriziranog uređaja – zaštita identiteta je ključna kod sigurnosti korisnika u trenucima kada netko pokušava otkriti njegovu fizičku lokaciju. Bez dovoljne zaštite, IoT uređaji dovode korisnika u rizičnu situaciju, gdje može doći do fizičkih ili financijskih prijetnji [4]. Uređaji *Bluetooth Low Energy* 4.0 dizajnirani su za povremeno oglašavanje statusa ili njegovog postojanja. Oglasni paket sadrži MAC adresu emitera i jedinstvenu uslugu. Također sadrži informacije o blizini uređaja u smislu jačine signala. Koristeći javno dostupne podatke i karakteristike oglasa, napadač može izvući veliku količinu informacija koje mu mogu pomoći u praćenju uređaja na temelju tih jedinstvenih podataka [11].
2. Zaštita protiv pasivnog prisluškivanja – pasivno prisluškivanje (engl. *passive eavesdropping*) je proces slušanja privatne komunikacije između dva uređaja. Pasivno prisluškivanje potiho sluša komunikaciju, te ne mijenja podatke [4]. Korištenjem *sniffer*-a kanala od 2,4 GHz može se preslušati sva komunikacija između BLE uređaja bez pristanka komunikacijskih uređaja. Budući da prisluškivanje ne utječe na normalnu komunikaciju između uređaja, šanse da korisnik primijeti pokušaj prisluškivanja izuzetno su malene. Ako se u komunikaciji koriste nešifrirane poruke ili nepotpisane poruke, haker može dobiti izravan pristup svim povjerljivim podacima koje razmjenjuju uređaji. Postupci uparivanja dobro su poznate tehnike za izbjegavanje

problema prisluškivanja i šifriranje poruka prije razmjene. Ali, ako napadač sluša uređaje tijekom samog postupka uparivanja, tada metode uparivanja ne mogu osigurati sigurnost od napada [11].



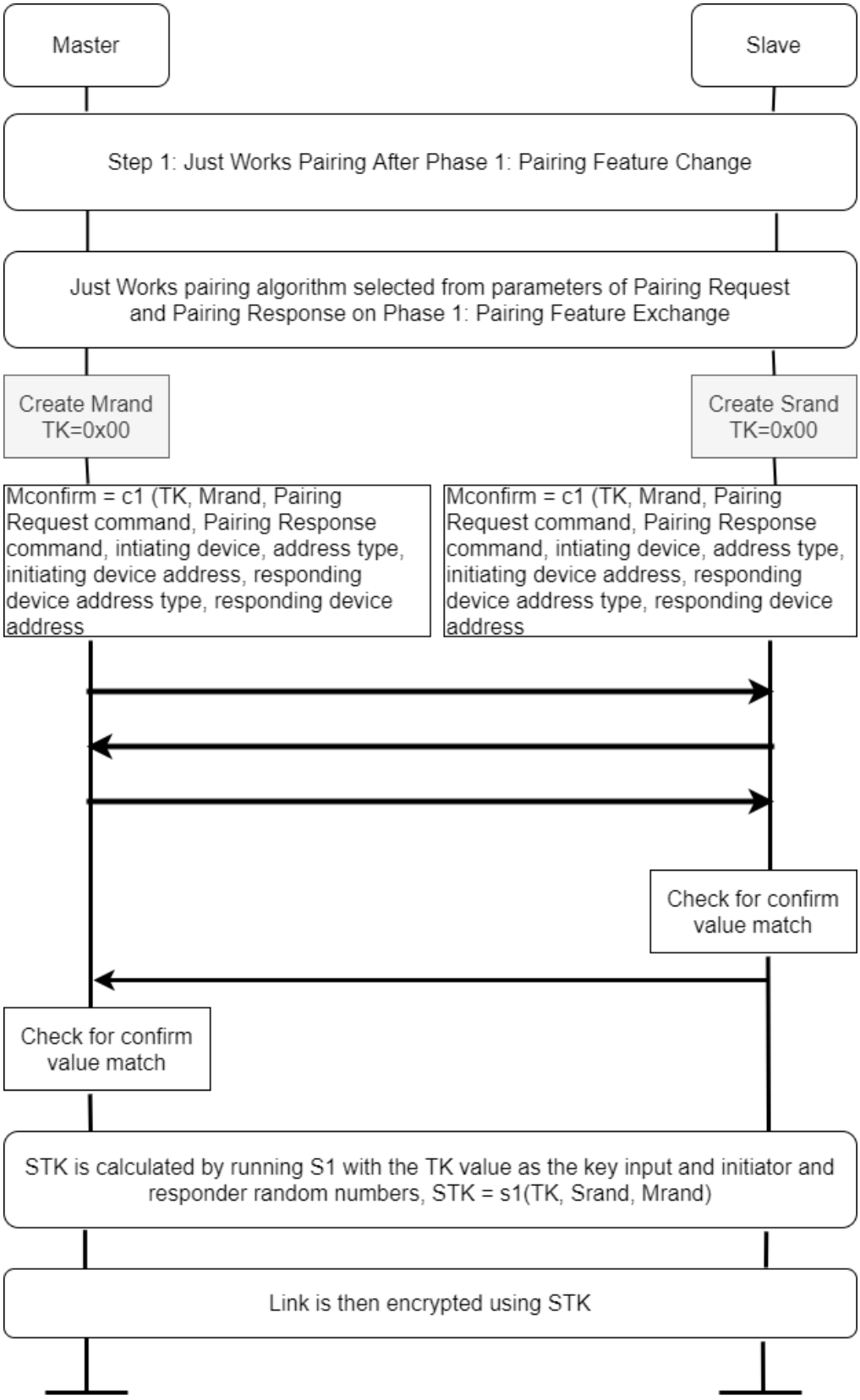
Slika 3.4. Pasivno prisluškivanje (Passive Eavesdropper) [4]

3. Zaštita protiv *man-in-the-middle* napada – *man-in-the-middle* (MITM) napadi su najozbiljniji među sigurnosnim prijetnjama. U ovom slučaju, treći uređaj koji se naziva *MITM* napadač, ne samo da prisluškuje privatnu komunikaciju između dva uređaja, nego se također pretvara da je jedan od uređaja te na taj način izmjenjuje podatke. [4]
   MITM napad je moguć kada se koristi jednostavno uparivanje u *Pass Key* modu. Ako napadač pogodi *Pass Key* koji je prethodno korišten i zna da će se ponovno koristiti u budućem uparivanju, napadač će se moći predstaviti kao obje strane komunikacije.
   To je moguće jer ne postoji način da se provjeri autentičnost i pripadaju li razmijenjeni javni ključevi tijekom druge faze uparivanja pravim entitetima ili ne, jer ne postoji tijelo za ovjeru [1].



Slika 3.5. Man in the middle napad [4]

Tijekom procesa uparivanja, TK se koristi za generiranje STK-a. Zapravo, napadač nikad ne zna TK zato što je to ulazna vrijednost korisnika koja se nikad ne prenosi u paketu. Međutim, duljina TK-a je prekratka te to ujedno znači da ga je moguće predvidjeti. Stoga su moguće fatalne sigurnosne ranjivosti kod BLE-a. *Just works* metoda uvijek koristi predefiniranu vrijednost (0x00) kao TK [6]. Na slici 6. prikazan je proces generiranja ključa.



Slika 3.6. Proces generiranja STK ključa [6]

4. PRIMJENA BLUTOOTH-A U IOT OKRUŽENJU

Bluetooth je jedna od ključnih komponenti koja je potrebna za razvoj bežične komunikacije. Uz Bluetooth, preciznije uz BLE, vežu se mnoge pozitivne osobine zbog kojih je zauzeo mjesto u razvoju IoT paradigme, a neke od njih su jednostavnost, niska potrošnja energije, isplativost i robusnost. Primjena BLE u IoT-u je veoma široka, te se može pronaći u telefonima, slušalicama, medicinskim uređajima kao i u mnogim drugim napravama.

Za razliku od nekih drugih bežičnih tehnologija kao što su WiFi ili ZigBEE , BLE nije posjedovao mogućnost ispreplitanja mreža. Isprepletene mreže omogućuju prijenos podataka između čvorova u dinamičnom i nehijerarhijskom načinu. Čvorovi surađuju i šalju poruke drugim uređajima. Iz tog razloga postojala je sve veća potreba razvijanja takve funkcionalnosti i kod Bluetooth-a [2].

Isprepletene mreže kod Bluetooth-a, u usporedbi s drugim mrežama koje koriste protokole usmjeravanja (engl. *routing protocols*), koriste *flooding* protokole. Svaki od ovih protokola ima svoje prednosti i nedostatke. Prednosti protokola usmjeravanja su robusnost i niska potrošnja energije, no s druge strane su moguća velika kašnjenja te pojavljivanje velikih izazova prilikom pronalaženja najkraćeg puta. Prednosti *flooding* protokola su jednostavnost, redundancija kao i to što ne zahtjeva izračunavanje tablica usmjeravanja. Svaka poruka se šalje preko višestrukih čvorova. Međutim, broj čvorova treba biti ograničen i postavljen tako da omogućuje kontrolu zagušenja, što može dovesti do gubitka paketa [2].

Najčešća primjena *flooding*-a temeljenog na BLE standardu je u aplikacijama u kojima se kontrolira rasvjeta, zbog jednostavnosti implementacije kod takvih sustava [2].

BLE može imati koristi od široke upotrebe Bluetooth tehnologije, jer se BLE lako integrira u klasične Bluetooth sklopove, pa je stoga vjerojatno da će budući Bluetooth uređaji biti uređaji s dvostrukim načinom rada. Prema objavljenim prognozama, očekuje se da će se BLE u bliskoj budućnosti koristiti u milijardama uređaja. S obzirom na važnu ulogu koju BLE može igrati u Internetu stvari, IETF 6LoWPAN WG razvija specifikaciju kako bi omogućio IP *end-to-end* komunikaciju za BLE uređaje. Na primjer, pametni telefoni opremljeni BLE-om mogu djelovati kao IP usmjerivači za senzore i pokretače s omogućenim BLE-om. IP povezivanje može dramatično povećati potencijalni prostor usluga i dodanu vrijednost za BLE uređaje [7].

Bluetooth se može koristiti u beskonekcijskim primjenama, kao što su mobilno plaćanje, plaćanje ulaznica ili kontrola pristupa [7].

4.1. Primjena Bluetooth-a u medicini

Zdravstvo, wellness i sport čine područje primjene u kojem je klasični Bluetooth već korišten, a za koji BLE predstavlja poboljšanje [7]. Bežična tehnologija obećava različite dobrobiti u primjeni medicinskog nadzora, kako pacijenti više ne bi morali biti priključeni na žice. Takvo bežično nadgledanje pacijenata, naročito starijih, omogućilo bi im oporavljanje kod kuće, a da pritom i dalje budu pod stručnim nadzorom liječnika. Od svih dostupnih bežičnih tehnologija, *Bluetooth low energy* je pogodan za sve medicinske zahtjeve i propise koje bi aplikacije trebale podržavati, a to su na primjer: interoperabilnost, mala potrošnja snage, elektronička kompatibilnost, siguran prijenos podataka te direktna komunikacija s baznom stanicom i internetskom infrastrukturom. Bežični medicinski nadzor uz korištenje BLE-a najprije je za cilj imao razviti aplikaciju za mjerenje razine šećera u krvi, a zatim za primjene kao što su mjerenje tjelesne temperature, krvnog tlaka, pulsa te otkucaja srca [23].

4.2. Primjena Bluetooth-a u poljoprivredi

U poljoprivredi BLE također nalazi svoju primjenu, gdje je potrebno uspostaviti komunikaciju između senzora koji se nalaze u poljoprivrednom okruženju kao što su na primjer njive i ostale obradive površine. U radu [24] rađene su simulacije i mjerenja na otvorenom polju. Rezultati simulacije su pokazali da je prijenos podataka u ovakvom tipu okruženja bio najbolji na udaljenosti do 100m, te se prijenos povremeno odvijao na udaljenostima do 200m. Mogućnosti povećanja dometa u ovom se slučaju ovisi o količini okolne interferencije te usmjerenosti antene korištenog modula. Pretpostavlja se da bi domet bio veći u slučaju korištenja BLE modula jače snage odašiljanja i manjeg pojasa osjetljivosti. Istraživanja u ovome radu su pokazala da su na čvorove senzora najviše utjecale biljke smještene između prijemnika i odašiljača, što je dovelo do zaključka da bi komunikacija bila učinkovitija ukoliko bi senzori bili postavljeni iznad usjeva. Kod senzora koji su postavljeni ispod zemlje primijećen je očigledan pad signala, međutim kada bi se senzor postavio ispod betona, efekt prigušenja bio bi mnogo manji te je bio dostupan na udaljenostima do 20m.

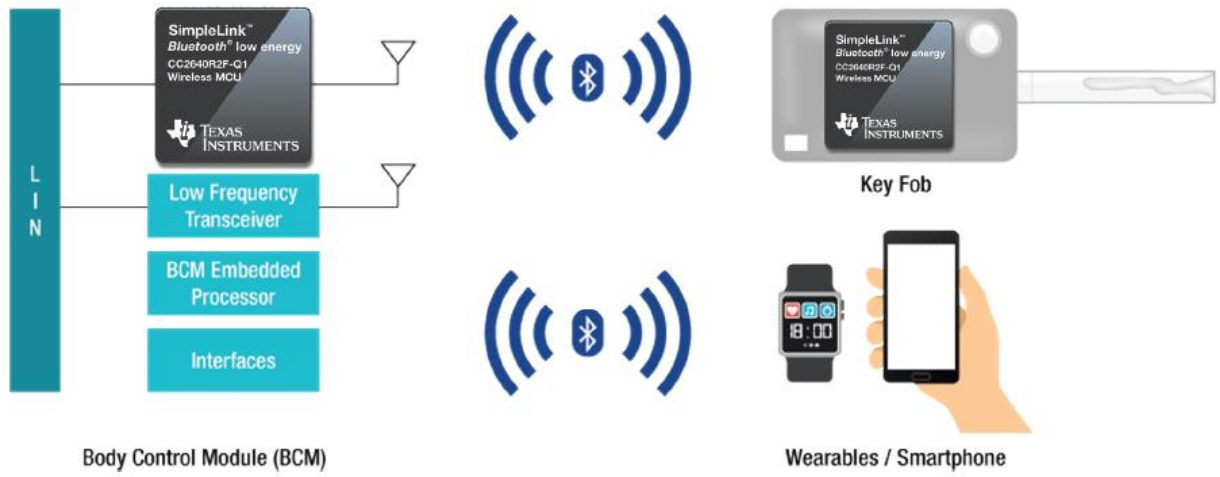
4.3. Primjena Bluetooth-a u automobilskoj industriji

Iako BLE nije primarno dizajniran za automobilsku komunikaciju, njegovi brzi i jednostavni mehanizmi za uspostavu i održavanje povezanosti, čine ga poželjnom tehnologijom u razvoju i uspostavi komunikacije automobilske tehnologije. U koriste tome ide mogućnost održavanja komunikacije u statičnom i pokretnom scenariju, uz pritom nisku potrošnju energije i malo kašnjenje [26].

Ugrađen u moderne pametne telefone, prijenosne uređaje i tablete, Bluetooth low energy omogućava korisnicama interakciju između njihovih osobnih mobilnih uređaja s uređajima s omogućenim BLE načinom rada. Bluetooth low energy je pogodan za automobilsku primjenu zbog sposobnosti za rad na sveprisutnim pametnim telefonima.

Primjeri primjene BLE-a kod automobila posredstvom korištenja pametnih telefona su:

- Pristup pametnom vozilu – vozačev pametni telefon ima funkciju virtualnog ključa, gdje su informacije osigurane na način da prilikom prepoznavanja „ključa“ vozilo dopušta neke od radnji kao što su zaključavanje, otključavanje, uključivanje vozila. Dvosmjerna komunikacija između telefona i automobila omogućena je preko Bluetooth-a.
- *Car sharing* – pristup pametnom vozilu korištenjem dinamičnog virtualnog ključa olakšava siguran i prikladan način za posuđivanje i iznajmljivanje auta. Mobilna aplikacija prima kod koji je potreban za pristup dogovorenom vozilu, BLE autentificira kod na pametnom telefonu te tako omogućava korisniku pristup željenim funkcijama.
- Podaci o dijagnostici vozila – podaci o dijagnostici vozila kao što su tlak u gumama, količinu ulja, status baterije i temperatura se mogu poslati direktno s vozila, ili u nekim slučajevima uz pomoć standardnog ključa, na mobilni uređaj pomoću BLE-a
- Pomoć i personalizacija vozača – vozilo može automatski prepoznati mobilni uređaj približavanjem vozača vozilu, aktiviranjem unutarnje i vanjske rasvjete, personaliziranje položaja sjedišta, postavljanjem ventilacije i klimatizacije.
- Potpomognuto/ daljinsko parkiranje – nakon što vozač napusti vozilo, uz pomoć pametnog telefona aktivira aplikaciju te se automobil sam odveze na mjesto gdje se vozač želi parkirati. Ovakva metoda je učinkovita u situacijama kada je parkirno mjesto jako usko, te se na njega teško parkirati zbog prostornih ograničenja. Komunikacija između automobila i pametnog telefona putem Bluetooth-a može aktivirati i nadzirati proces parkiranja [25].



Slika 4.1. Blok dijagram pristupa automobilu korištenjem BLE aplikacije [25]

4.4. Primjena Bluetooth-a za nadzor u društvenim mrežama

Društvene mreže imaju veliku ulogu u zdravlju pojedinca kroz razne zdravstvene propagande koje se šire preko društvenih mreža. Korištenje uređaja s omogućenim Bluetooth-om za mjerenje povezanosti na društvenim mrežama je jedna od alternativa za prikupljanje podataka u bazu. Korištenjem Bluetooth low energy protokola, koji su prisutni na korisnikovom uređaju, odrađena su mjerenja društvene povezanosti. Aplikacija koja prati prisutnost korisnika na društvenim mrežama je konfigurirana na način da simultano oglašava prisutnost slušalica preko BLE-a, te su preko slušalica skenirani okolni uređaji. MAC adresa slušalica je korištena kako bi jedinstveno identificirala sve slušalice i korisnike. U radu [27] inicijalno testiranje je uključivalo korištenje svih slušalica u tri stanja: *foreground* (kada je aplikacija prikazana korisniku u prvom planu, te kad je zaslon aktivan), *background* (kada je aplikacija pokrenuta u pozadini, početni zaslon je aktivan i upaljen) i kada je zaslon zaključan (aplikacija je pokrenuta u pozadini, početni zaslon je aktivan, zaslon aplikacije je ugašen). Korištene su tri kombinacije uređaja za svako stanje kako bi se testirala međusobna komunikacija, a to su Android i Android, Android i iOS, te iOS i iOS. Nakon provedene analize, zaključeno je da u slučaju kada se uspostavlja veza između iOS i iOS pametnog telefona pri zaključanom zaslonu, nije moguće međusobno skeniranje uređaja.

4.5. Primjena Bluetooth-a i kod unutarnjeg lociranja (engl. *Indoor location*)

Unutarnje lociranje (engl. *Indoor location*) predstavlja jednu od zanimljivijih tema u sustavu temeljenom na IoT-u. BLE tehnologija ima svojstvo širenja koje dopušta određivanje vrijednosti blizine i udaljenosti, s određenom količinom pogreške u zatvorenim prostorima. U zatvorenim prostorima, postoje različiti fizički efekti koji mogu ugroziti radijalno širenje

signala, kao što su *multipath* efekt, raspršivanje te kompleksnost i dinamičnost unutarnjih struktura [28]. BLE dopušta direktno mjerenje snage signala. Bluetooth adapteri šalju RSSI (engl. *Received Signal Strength Indication*) izvješća za svaki skenirani odgovor koji primaju od Bluetooth oznake (engl. *tag*). Vrijednost RSSI je izravno povezana sa snagom signala te s udaljenošću oznake od prijemnika [29]. U eksperimentu u radu [29] postavljeno je nekoliko prijemnika koji su montirani na fiksnim mjestima u stanu. Prijemnici su sastavljeni od Raspberry Pi pločice te Bluetooth USB prijemnika. Raspberry Pi sadrži Ethernet konektor. U slučaju da je poželjna bežična komunikacija, dodan je USB WiFi adapter. Prijemnici šalju detektirane signale i njihove snage u centralnu jedinicu za procjenu lokacije (engl. *location estimation unit*). U centralnoj jedinici su se procesirala RSSI očitanja svih BLE prijemnika. Cilj eksperimenta bio je omogućiti očitavanje lokacije uređaja koji u sebi imaju ugrađene BLE *beacon*-e u svrhu povezivanja pametnih telefona i takvih uređaja, te njihovog lociranja u unutarnjoj okolini.

5. BLUETOOTH IOT UREĐAJ

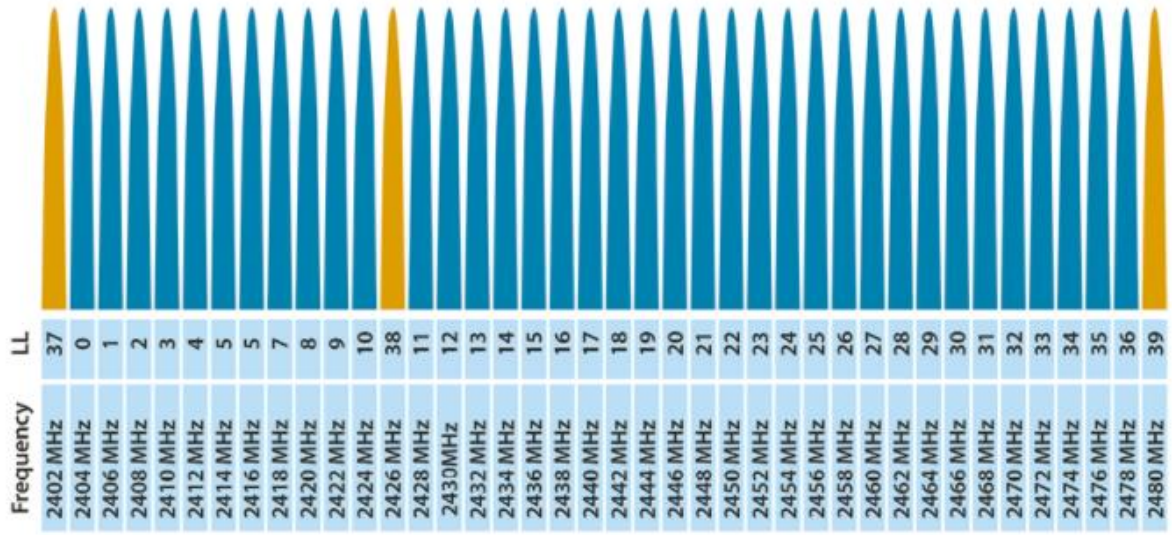
Moguće je uspostaviti komunikaciju između različitih BLE uređaja. Pritom se misli na uspostavu komunikacije između BLE modula i pametnog telefona, komunikaciju između više BLE modula, te komunikaciju između više pametnih telefona i jednog BLE modula. Prilikom testiranja potrebno je obratiti pozornost na enkripciju, te na parametre koje je moguće mijenjati. Platforma koja će biti korištena je *Waspmote* te odgovarajući BLE modul.

5.1. Waspmote

Waspmote je bežična *open-source* platforma senzora posebno usmjerena na implementaciju načina rada s malom potrošnjom koja omogućuje čvorovima senzora ("*motes*") da budu potpuno autonomni i napajani baterijom, nudeći promjenjiv životni vijek između 1 i 5 godina ovisno o radnom ciklusu korištenja [13]. Arhitektura *Waspmote*-a se temelji na Atmel ATmega1281 mikrokontroleru [14].

5.2. Waspmote Bluetooth Low Energy modul

Bluetooth 4.0 standard, poznat i kao Bluetooth Low Energy (BLE), radijska je tehnologija kratkog dometa, optimizirana za aplikacije izuzetno male snage. Razlikuje se od klasičnog Bluetootha (BR / EDR), ali s istim blagodatima poput robusnosti, interoperabilnosti, naknade bez naknade ili povezivosti sa pametnim telefonima i osobnim računalima. BLE moduli koriste opseg 2,4 GHz (2402 - 2480 MHz). BLE modul ima 37 podatkovnih kanala i 3 reklamna kanala, s razmakom od 2 MHz i GFSK modulacijom [15].



Slika 5.1. Distribucija kanala kod BLE standarda [15]

BLE modulom upravlja UART te se može povezati na *Waspmote*-ov SOCKET0 i SOCKET1. Osnovne značajke BLE 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 se mogu obavljati pomoću BLE modula su:

- Slanje *broadcast* reklama (iBeacon)
- Povezivanje s ostalim uređajima kao *master/slave*
- Povezivanje s pametnim telefonima i tabletima
- Postavljanje automatskih ciklusa mirovanja/prijenosa
- Izračunavanje udaljenosti korištenjem RSSI vrijednosti
- Savršeno za unutarnje lokalne mreže (RTLS)
- Skenira uređaje s maksimalnim vremenom upita
- Skenira uređaje s maksimalnim brojem čvorova
- Skenira uređaje koji traže određenog korisnika prema njegovoj MAC adresi.

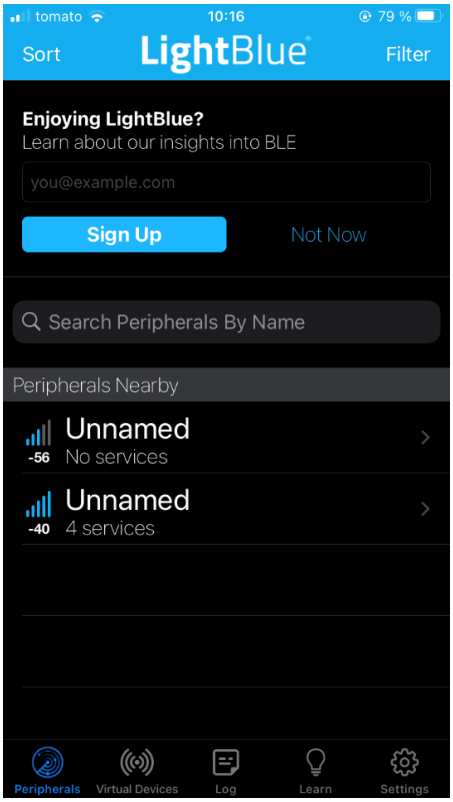
Slika 5.2. BLE modul

5.3. Povezivanje BLE uređaja

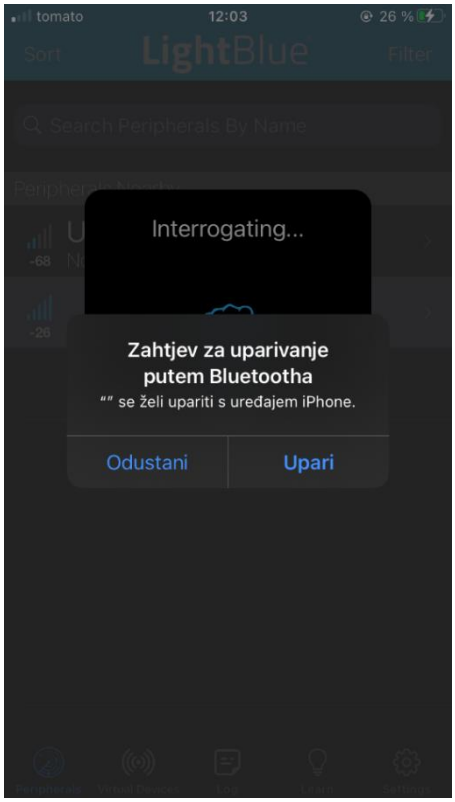
U starijim Bluetooth standardima, korisnik se morao upariti s upravljačkim uređajem prije povezivanja. Kod Bluetooth 4.0 standarda korisnik se može povezati s ostalim uređajima bez procesa uparivanja. Također i korisnici imaju mogućnost korištenja oglasa za slanje neke količine podataka. Međutim, ti procesi nisu sigurni.

Bluetooth 4.0. standard koristi AES-128 enkripciju sloja linka. Enkripcija se može koristiti u konekcijskim procesima kako bi se oni osigurali. Enkripcija veze se može započeti korištenjem funkcije *encryptConnection*(), pružajući rukovatelja uspostavljene veze. Rukovatelj je najčešće nula, osim ako je dopušteno povezivanje [17].

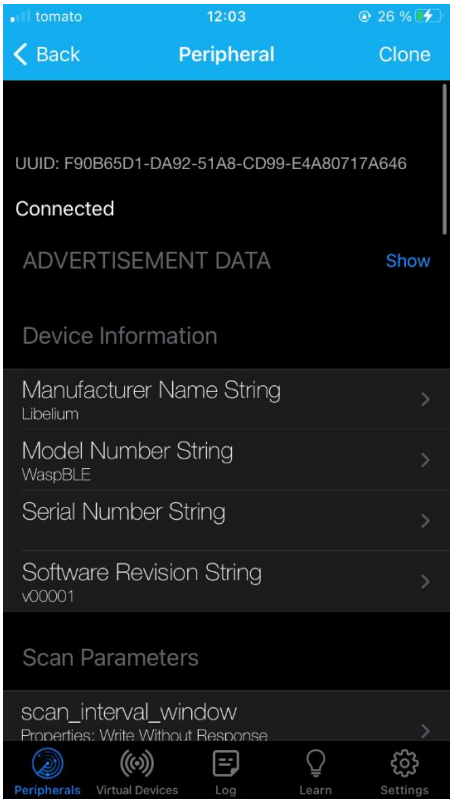
Nakon povezivanja, *waspmote* uređaj ima ulogu *slave*-a. Pomoću *master*-a, koji je u ovom slučaju pametni telefon, mogu se upisivati nove vrijednosti, ukoliko je to dozvoljeno. Upisivanjem novih vrijednosti, *output*-u se pojavljuje vrijednost zastavice *flag* = 8. Kada se prekine veza, zastavica ima vrijednost *flag* = 15. Na slikama 5.3. , 5.4., 5.5., 5.6., 5.7., 5.8., 5.9. i 5.10. prikazani su zasloni aplikacije *LightBlue* uz pomoć koje je ostvarena interakcija između pametnog telefona i BLE modula. Pri ulasku u aplikaciju moguće je skenirati raspoložive BLE uređaje. Nakon skeniranja, prikazuju se uređaji s kojima je moguća povezivost, te njihova snaga. Nakon što je predan zahtjev za uparivanje sa željenim BLE uređajem, moguće je iščitati svojstva uređaja s kojim je telefon povezan, poput njegove MAC adrese, proizvođača itd. Također je moguće i upisivati nove vrijednosti, ukoliko je dozvoljeno pri odabiru nekog od svojstava, odnosno ukoliko stoji opcija *write* uz svojstvo.



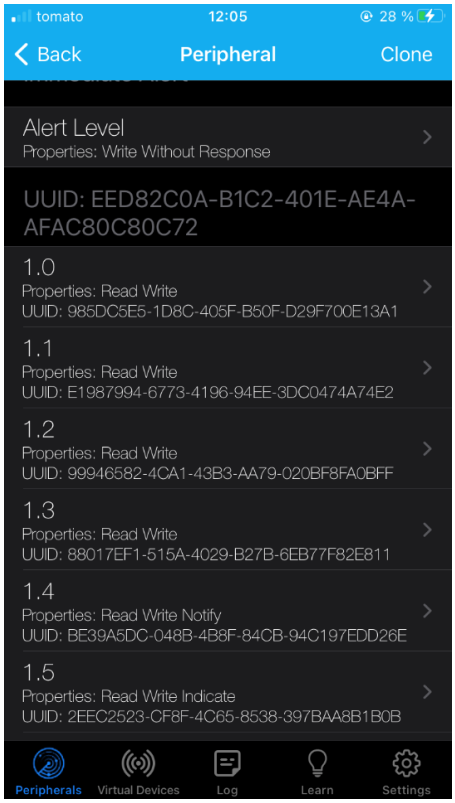
Slika 5.3. Početni zaslon aplikacije LightBlue



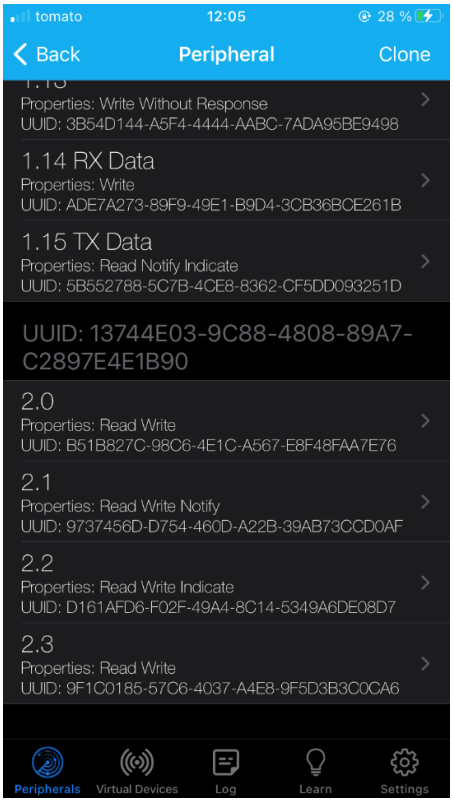
Slika 5.4. Uparivanje uređaja



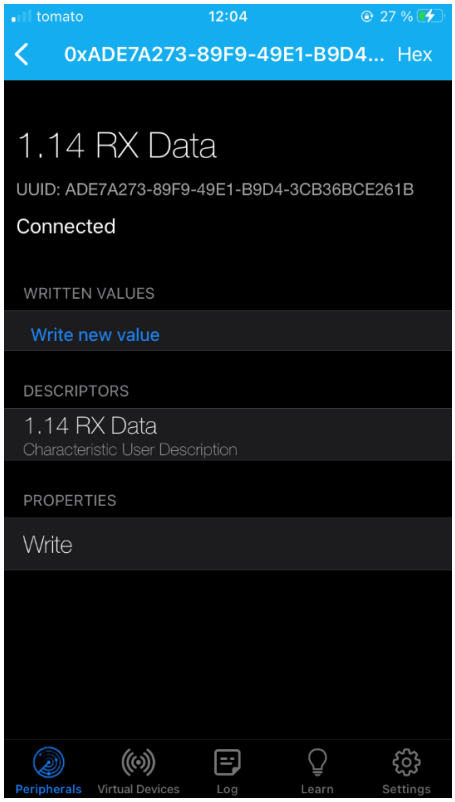
Slika 5.5. Prikaz općih podataka o uparenom uređaju



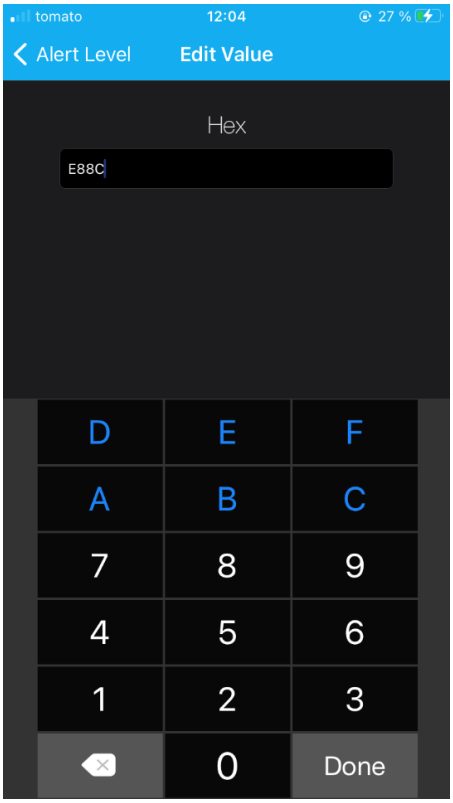
Slika 5.6. Svojstva waspmote-a



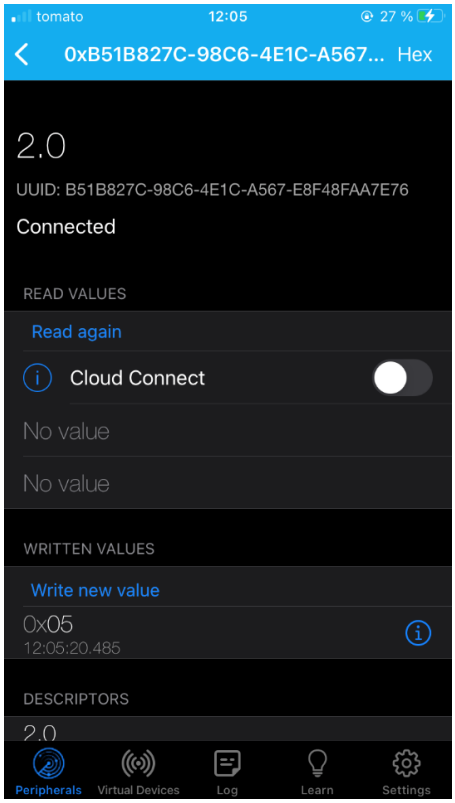
Slika 5.7. Svojstva RX i TX podataka



Slika 5.8.Zaslon RX podataka



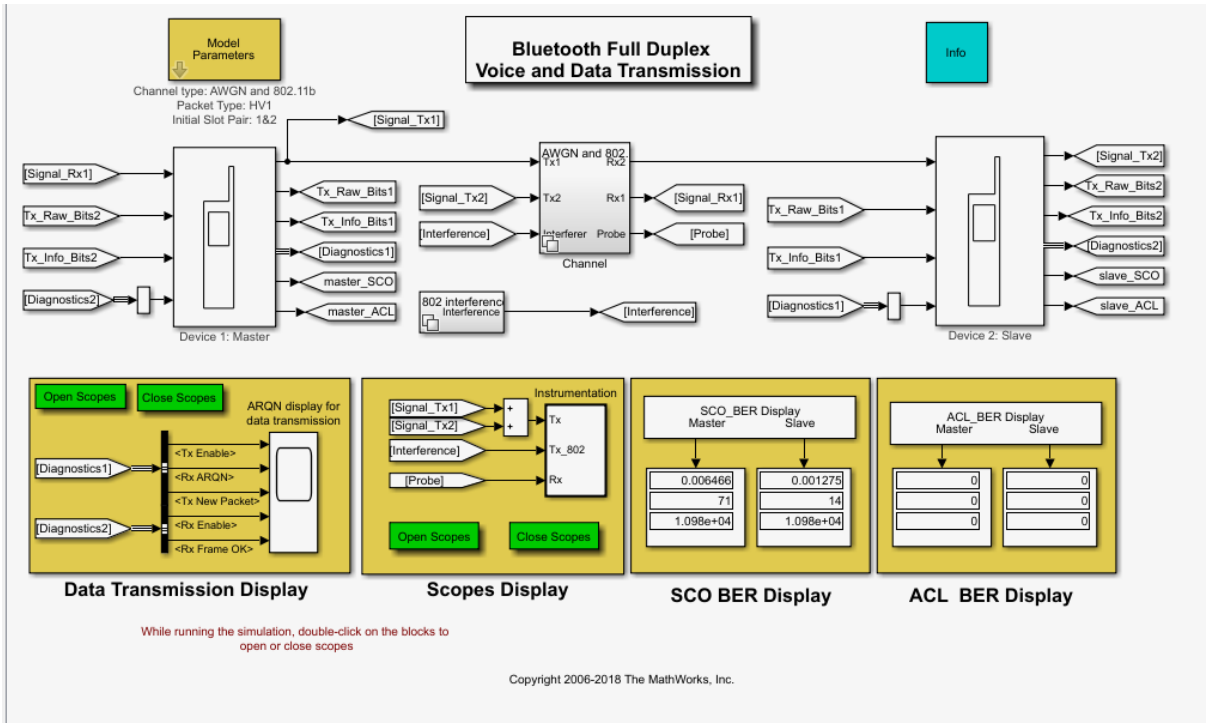
Slika 5.9. Upisivanje nove vrijednosti



Slika 5.10. Prikazan upisanih vrijednosti

5.4. Simulacija dvosmjernog prijenosa glasa i podataka putem Bluetooth-a

Pomoću izvorne simulacije sa službene stranice Matlab-a, odrađen je eksperimentalni dio u kojem se promatra promjena amplitude u ovisnosti koji tip glasovnog paketa (HV1, HV2, HV3 i SCORT) je korišten, te korištenjem podatkovnog paketa DM1.



Slika 5.11. Model prikaza u simulinku

Na slici 5.11. nalazi se model kojim je prikazana full-duplex komunikacija između dva Bluetooth uređaja. Moguće je slanje paketa između uređaja, kako glasovnih tako i podatkovnih. Vrste podržanih glasovnih paketa su:

- HV1, HV2, HV3, SCORT, a podatkovni paket koji je podržan je DM1 [18].

Model prikazan na slici 5.11. uključuje CVSD kodiranje govora, HEC, *payload* CRC za DM1, FEC, uokvirivanje, *frequency hopping*, GFSK modulaciju, generaciju skoka sekvence, 802.11b signal interferencije, valnu datoteku I/O, BER mjerač, spektar, vrijeme te spektrometar.

Odašiljač se u ovom primjeru sastoji od:

- Kontrolnog bloka
- *Payload*-a i FEC bloka
- Okvirnog bloka
- Radio bloka.

Prijemnik se sastoji od:

- Radio bloka
- Bezokvirnog bloka
- Kontrolnog bloka,

Sljedeći podsustavi su izgrađeni u *Bluetooth Full Duplex* biblioteci:

- AWGN kanal
- AWGN kanal te 802.11b interferencija
- Ništa.

Blokovi koji su korišteni u ovom modelu su:

- CPM modulator osnovnog pojasa – koristi se za implementaciju GFSK (engl. *Gaussian frequency shift keying*). Bluetooth radio modul koristi GFSK, gdje je binarna jedinica predstavljena pozitivnom frekvencijskom devijacijom, a binarna nula je predstavljena negativnom frekvencijskom devijacijom.
- MFSK modulator osnovnog pojasa – koristi se za implementaciju frekvencijskih skokova (engl. *frequency hopping*-a) u Bluetooth radiju. Bluetooth radio ostvaruje spektar širenja korištenjem 79 frekvencijskih skokova, svaki pomaknut za 1 MHz, počevši od 2.402GHz i završavajući na 2.480GHz.
- Blok gubitka putanje slobodnog prostora (engl. *The Free Space Path Loss block*) – zajedno s AWGN blokom i 802.11b interferencijskim podsustavom prikazuje konstrukciju prijenosnog kanala.
- *The General CRC Generator* – ovaj blok se koristi za izračun CRC-a prenesenih podataka.

Osim navedenih blokova, također se koriste M-FSK demodulator, *General CRC Syndrome Detector block* te implementacija 1/3 i 2/3 *rate*-a kod FEC-a [18].

Signali između dvaju uređaja u ovom slučaju su:

- Tx_Raw_Bits1 – *master* uređaj generira informacijske podatke slučajnim odabirom, obavlja CRC i FEC skupa korisnih informacija te ih pakira prema definiranom Bluetooth formatu. Isto to predstavlja i Tx_Raw_Bits2 za *slave* uređaj.
- Signal_Tx1 – *master* uređaj uzima Tx_Raw_Bits1 te ga modulira prema određenom Bluetooth standardu. Signal_Tx1 se prenosi kroz kanal (isto vrijedi i za Signal_Tx2 kod *slave* uređaja).

- Signal_Rx1 – signal oštećen zbog pristutnosti aditivnog bijelog šuma i interferencije. Signal_Rx1 se dovodi do *master* uređaja kako bi se izvršila demodulacija i detekcija (isto vrijedi i za Signal_Rx2 za *slave* uređaj).
- Tx_Info_Bits1 – informacijski podaci generirani od strane *master* uz korištenje CRC-a. Koriste se za SCO BER provjeru na strani *slave*-a. (Isto vrijedi za Tx_Info_Bits2 kod *master* uređaja).
- Diagnostics2 – skup okvira i paketa informacija koji se koriste za ACL BER provjeru na *master* strani. (Diagnostics1 se koristi kod *slave* uređaja).
- master_SCO – SCO BER informacija za prikaz kod *master* uređaja (slave_SCO kod *slave* uređaja).
- master_ACL – ACL BER informacija za prikaz kod *master* uređaja (slave_ACL kod *slave* uređaja).
- Interference – signal interferencije generiran 802.11b kanalom [18].

Bluetooth tehnologija koristi kombinaciju tehnologija kruga i prebacivanja podataka kako bi upravljala podatkovnim prometom. Kanal s kružnom komutacijom je kanal koji pruža redovito rezerviranu širinu pojasa. Audio uživo zahtijeva od kružne komutacije zagarantirano regularno dostavljanje glasovnih informacija – kodeks primanja zahtijeva regularnu pohranu informacija kako bi pružio dobru kvalitetu izlaznog signala. Kanali s kružnom komutacijom su sinkronizirano konekcijski orijentirani linkovi, odnosno oni zauzimaju fiksne *slot*-ove koji su dodijeljeni od strane *master*-a prilikom prvotnog postavljanja linka [19].

Kanal s komutacijom paketa je aktivan samo kada je potreban prijenos podataka, te ne posjeduje rezervirani pojas širine. Kanali s komutacijom paketa u Bluetooth sustavu predstavljaju asinkrone bezkonekcijske linkove. Ako se glasovi šalju preko ACL linkova, ne postoji garancija regularne širine pojasa, te može doći do oštećenja primljenog signala [19].

Raznovrsni paketi korišteni na SCO linkovima omogućuju jednak simetrični prijenos od 64Kbps između *master*-a i *slave*-a. Svaki tip paketa se šalje u periodično rezerviranim *slot*-ovima, ali različiti tipovi zahtijevaju različito rastojanje između rezerviranih *slot*-ova. Svaki SCO tip paketa koristi različito kodiranje korisne nosivosti podatka. SCO paketi su definirani na sljedeći način:

- HV1 prenosi 1.25 milisekunde glasa unutar 10 bajta. 1/3 FEC-a (eng. *Forward Error Correction*) dodaje 2 bita korekcije pogreške za svaki bit podatka, te tako povećava

veličinu korisnog paketa na 30 bajta. HV1 glasovni paketi se šalju i primaju u obliku jednostrukih *slot*-ova u svakom paru *slot*-a.

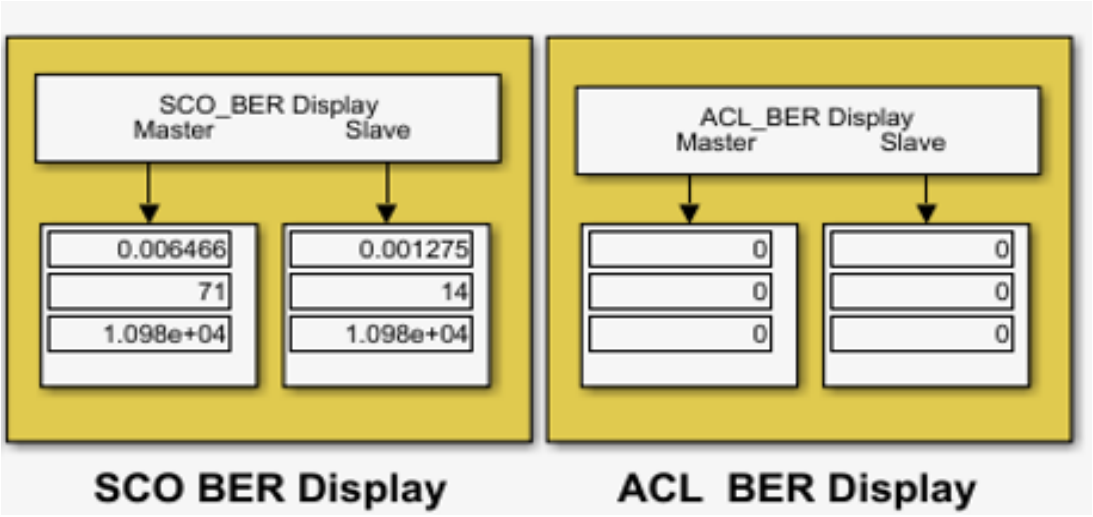
- HV2 nosi 2.5 milisekunde glasova u 20 bajta. 2/3 FEC dodaje jedan bit korekcije pogreške na svaka 2 bita podatka, te se time povećava veličina korisnog tereta na 30 bajta. HV2 paketi se šalju kao jednostruki *slot* paketi u dva uzastopna *slot*-a od svaka četiri *slot*-a.
- HV3 prenosi 3.75 milisekundi glasa unutar 30 bajtova. Nema korekcije pogreške na korisnom teretu. HV3 paketi se šalju kao jednostruki *slot*-ovi paketa unutar dva uzastopna *slot*-a unutar svakog od šest *slot*-ova.

Svi SCO paketi su jednostruki i nijedan od njih ne prenosi CRC. U okruženju u kojem postoji šum, ne događa se retransmisija paketa unatoč postojanju pogrešaka, ali pomoću FEC-a moguće je zaštititi 80% uzoraka, te se istovremeno osigurava viša kvaliteta zvuka. Međutim, FEC kodiranje zauzima prostor unutar korisnog tereta, stoga pakete koji nose veću zaštitu od pogrešaka treba češće slati. U okruženju bez pogrešaka, FEC daje nepotrebne troškove koji smanjuju protok [19]. Na slici 5.12. pokretanjem simulacije, u kojemu su poslani paketi SCO tipa, prikazan je BER u okruženju aditivnog bijelog šuma i 802.11b signala u kojemu su poslani HV1 glasovni paketi.

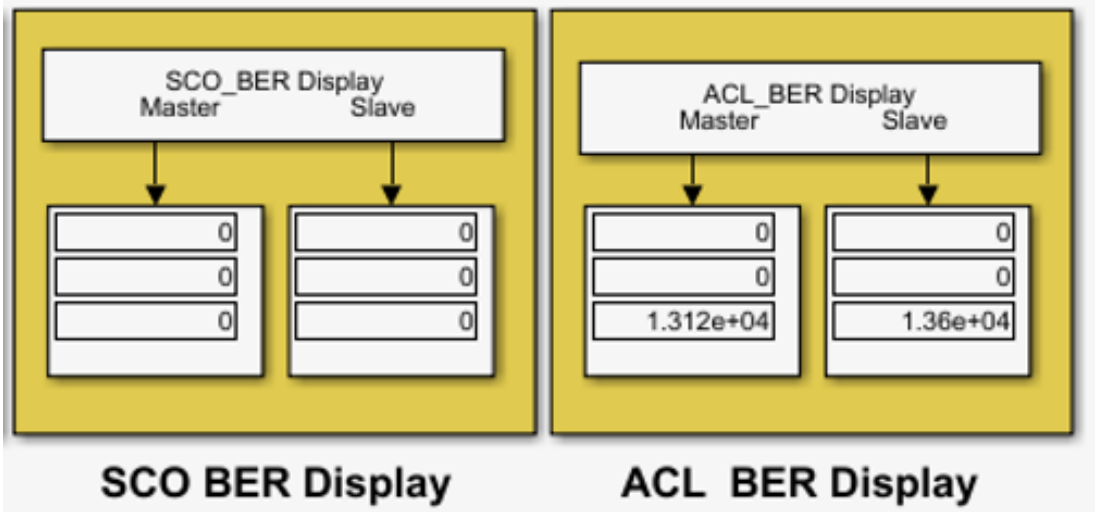
Sinkronizirano orijentirana veza (SCO) s ponavljajućom retransmisijom paketa (engl. *Synchronous Connection-oriented with Repeated Transmission – SCORT*) postiže veću korisnost prijenosa zamjenjujući *bit-level* redundanciju s *packet-level* redundancijom. SCORT nema korekcija pogrešaka, te se prenosi u svakom drugom vremenskom *slotu*. Ako je prijenos uništen interferencijom unutar prvog *slot*-a, još uvijek postoje tri ostala *slot*-a, ili prilike za uspostavu komunikacije s paketom [16].

Asinkroni beskonekcijski link je *point-to-point* veza između *master*-a i aktivnih *slave*-ova u pikonetu. Automatski ponavljajući zahtjev (engl. *Automatic Repeat Request*) se primjenjuje kod ACL paketa te se zahtjevi ponavljaju sve dok primatelj ne primi pozitivni ACK, odnosno potvrdu. Pozitivni ACK se nalazi u zagljavlju bez autoriziranog pristupa (engl. *piggy-backed*). ARQN se postavlja na vrijednost „0“ ili „1“ ovisno o tome je li prethodni paket uspješno primljen ili nije [22]. Na slici 5.13. prikazan je iznos BER-a prilikom zaustavljanja pokrenute simulacije gdje se DM1 paketi šalju u okruženju aditivnog bijelog šuma i interferirajućeg signala.

Jedan od ACL tipova paketa je DM1. Ovakav paket prenosi samo podatkovne informacije. Informacija i ciklička provjera redundancije (CRC) bitova kodirane su korištenjem 2/3 FEC-a. DM1 paket zauzima jednostruki vremenski *slot* [21].



Slika 5.12. Rezultati BER-a pri prijenosu SCO paketa



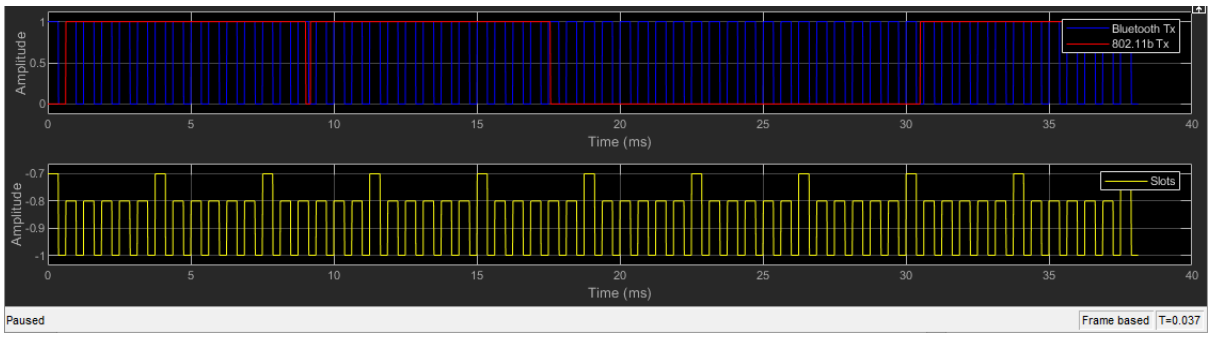
Slika 5.13. Rezultati BER-a pri prijenosu ACL paketa

5.5. Rezultati simulacije u Matlab-u

Nakon pokrenute simulacije u Matlab-u prikazuju se dva izlazna zaslona. Na jednom je prikazan vremenski dijagram primljenog signala, a na drugom je prikazan spektrogram signala šuma i interferirajućeg signala. Simulacija je izvedena u različitim uvjetima, odnosno korišteni su različite vrste glasovnih paketa, kao i jedan podatkovni paket. Simulacija je izvedena u okruženju bez šuma, u okruženju gdje je prisutan aditivni bijeli šum, te u okruženju gdje je osim bijelog šuma prisutna i interferencija uz korištenje 802.11b. Kombiniranjem različitih tipova *slot*-ova, šumova i vrsta paketa, izvedene su različite simulacije čiji se signali razlikuju. Na samom modelu moguće je očitati vrijednost BER-a.

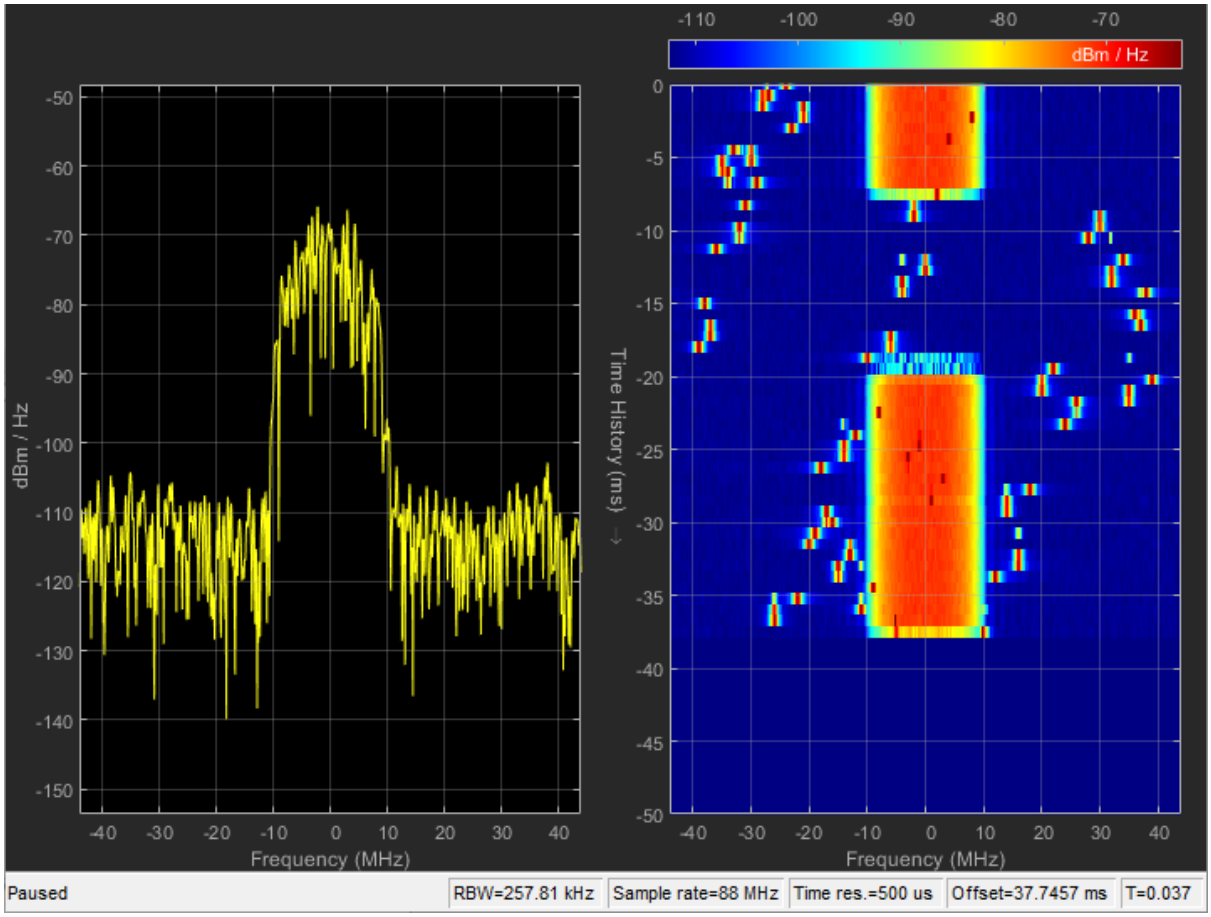
5.5.1. Rezultati simulacije uz prisutnost AWGN&802.11b

Kod prvog primjera korišten je HV1 glasovni tip podatka, a u okruženj u kojemu je izvršena transmisija glasa je prisutan Gaussov bijeli šum ili AWGN, te je također prisutrna intereferncija omogućena 802.11b standardom. Početni par *slot*-a je 1&2.



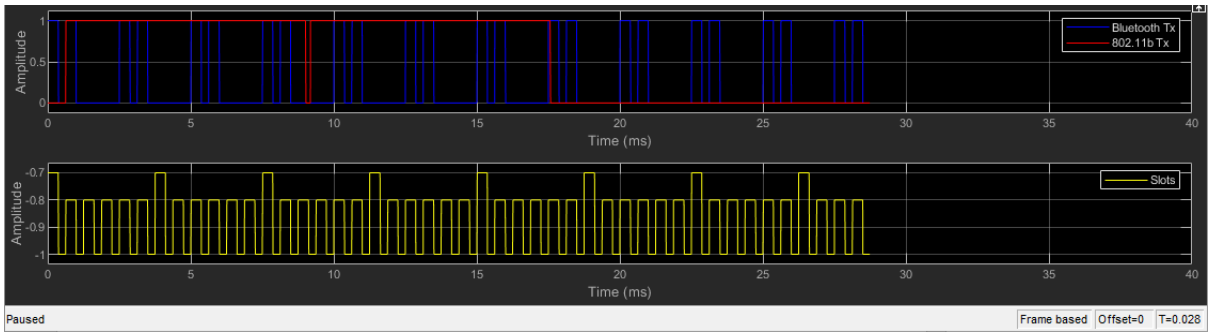
Slika 5.14. Vremenski dijagram primljenog signala HV1/AWGN&802.11b/1&2

Na slici 5.14. prikazan je vremenski dijagram primljenog signala. Plavom bojom označen je Bluetooth signal, a crvenom bojom je označen 802.11b signal koji je prisutan do cca. 18ms, zatim se zbog smetnji prekida do cca. 31ms. Bluetooth signal je kontinuiran, odnosno nema vremenskih prekida. Budući da je korišten HV1 signal, moguće je uvidjeti da se svakih 1.25 milisekundi mijenja amplituda, te da se svaki glas prenosi uzastopno po svakome *slot*-u. Izlazni signal *slot*-ova prikazan je žutom bojom.



Slika 5.15. Spektar primljenog signala te spektrogram kanala HV1/AWGN&802.11b/1&2

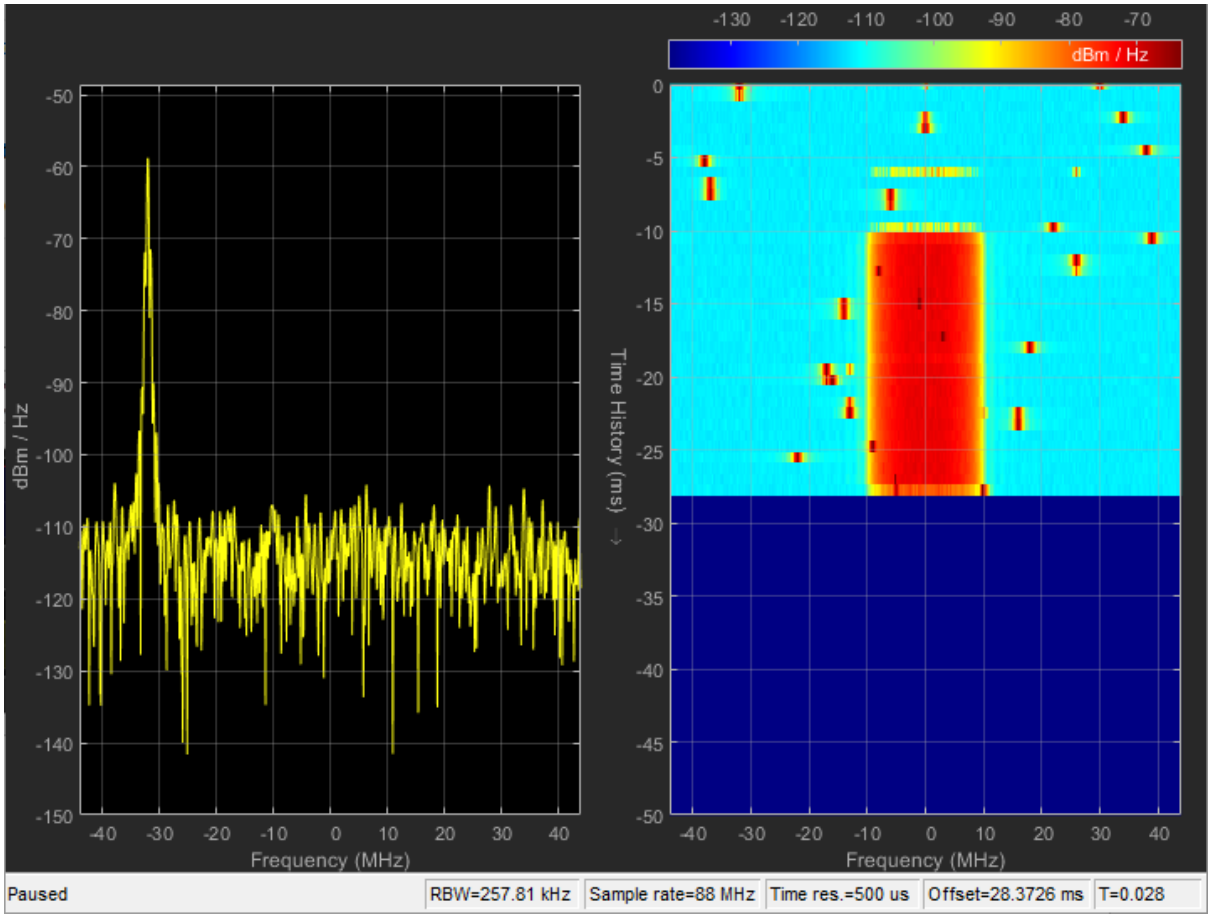
Na slici 5.15. prikazan je spektar primljenog signala s lijeve strane, te spektrogram kanala. Na lijevoj strani je prikazana snaga primljenog signala na određenoj frekvenciji, te se može zaključiti kako snaga primljenog signala i snaga signala 802.11b postižu najvišu vrijednost u istom frekvencijskom pojasu.



Slika 5.16. Vremenski dijagram primljenog signala HV2/AWGN&802.11b/1&2

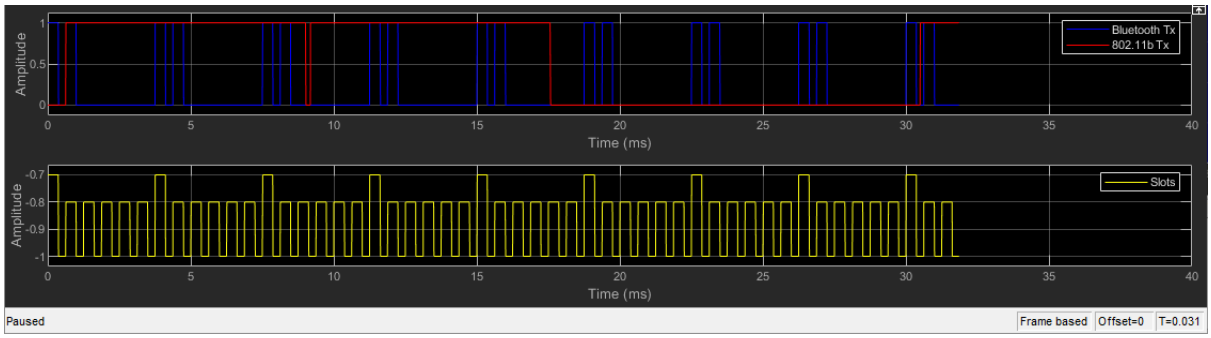
Slika 5.16. prikazuje slanje odnosno primljeni signal slanja glasovnih paketa tipa HV2, što samim time znači da se vrijednosti amplitude „1“ i „0“ izmjenjuju svakih 2.5 ms, kao što se može vidjeti i iz signala označenog plavom bojom. Budući da se u ovom primjeru slanje odvija u okruženju u kojemu su prisutni aditivni bijeli šum te signal 802.11b, također se može vidjeti

kako se promjena amplitude signala 802.11b odvija nakon 17 ms, te je ukupni period trajanja 30 ms. Paketi se šalju kao jednostruki *slot* paketi u dva uzastopna *slot*-a od svaka četiri *slot*-a



4.17. Spektar primljenog signala te spektrogram kanala HV2/AWGN&802.11b/1&2

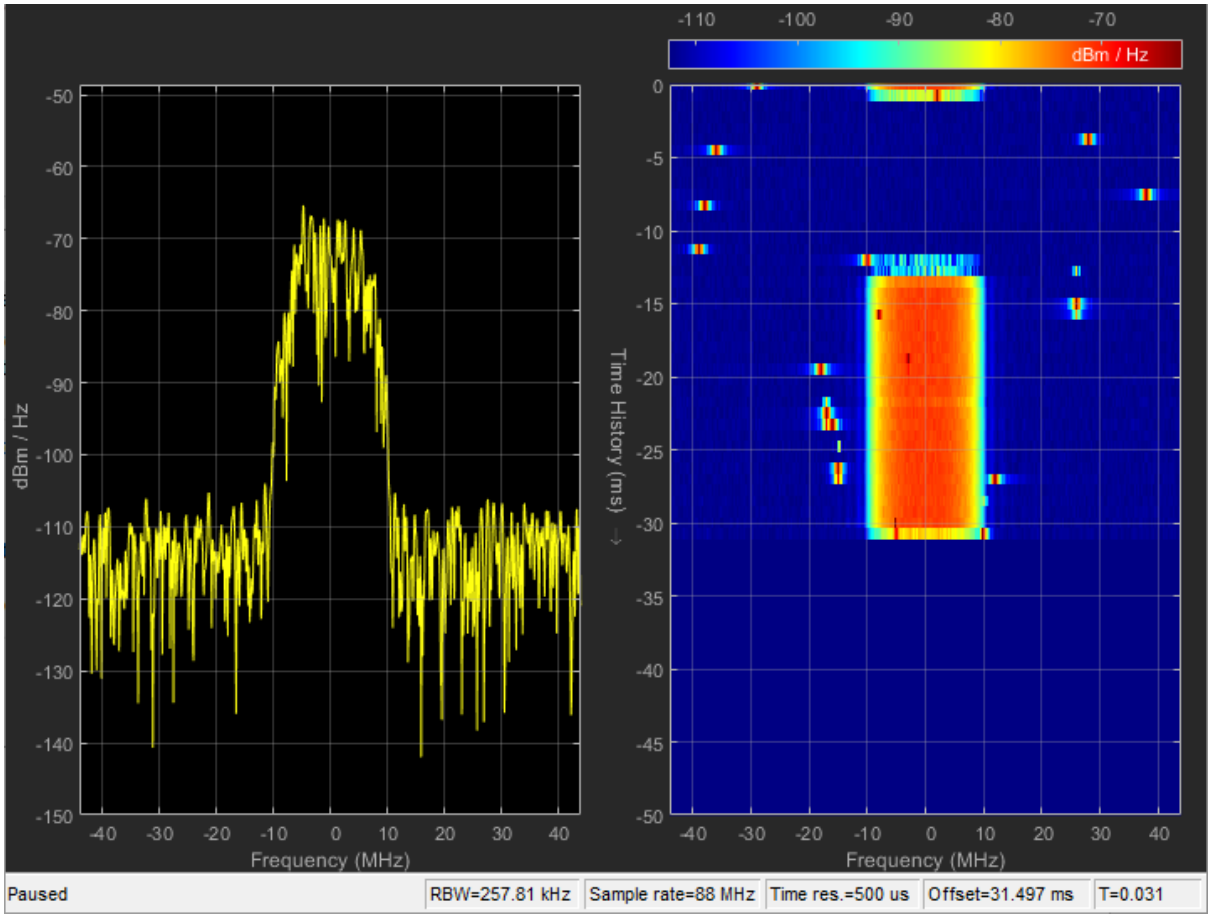
Prema spektru primljenog signala te spektrogramom kanala prikazanom na slici 5.17. vidi se kako maksimalna snaga primljenog signala u ovom primjeru nema isti frekvencijski opseg kao maksimalna snaga 802.11b. Na desnom prikazu na ovoj slici se također može uočiti period trajanja „jedinice“ koji iznosi 17 ms, od -27ms do -10 ms.



Slika 5.18. Vremenski dijagram primljenog signala HV3/AWGN&802.11b/1&2

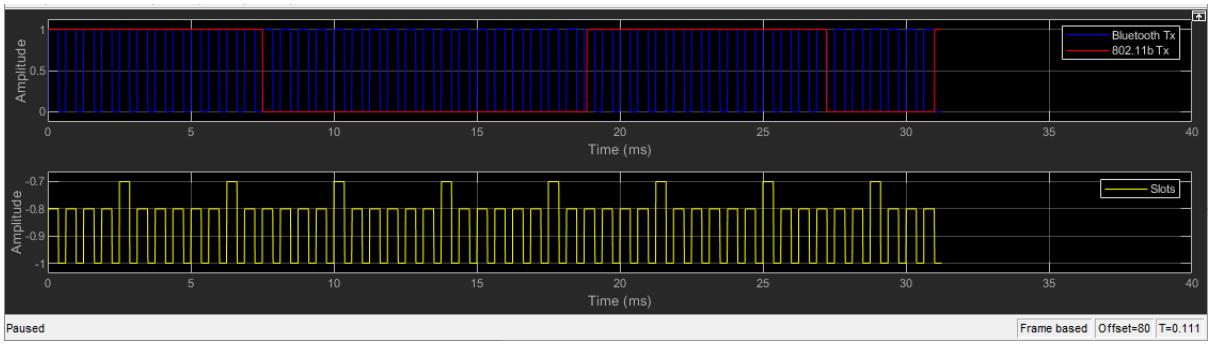
Slika 5.18. prikazuje vremenski dijagram u okruženju u kojem je uključen i šum i interferirajući signal. Šalju se glasovni paketi tipa HV3. Period u kojem interferirajući signal ima vrijednost

amplitude jednaku jedinici je cca. 17.5ms. Amplituda je jednaka nuli cca. 13.5 ms. Ukupni period interferirajućeg signala je stoga 31ms.



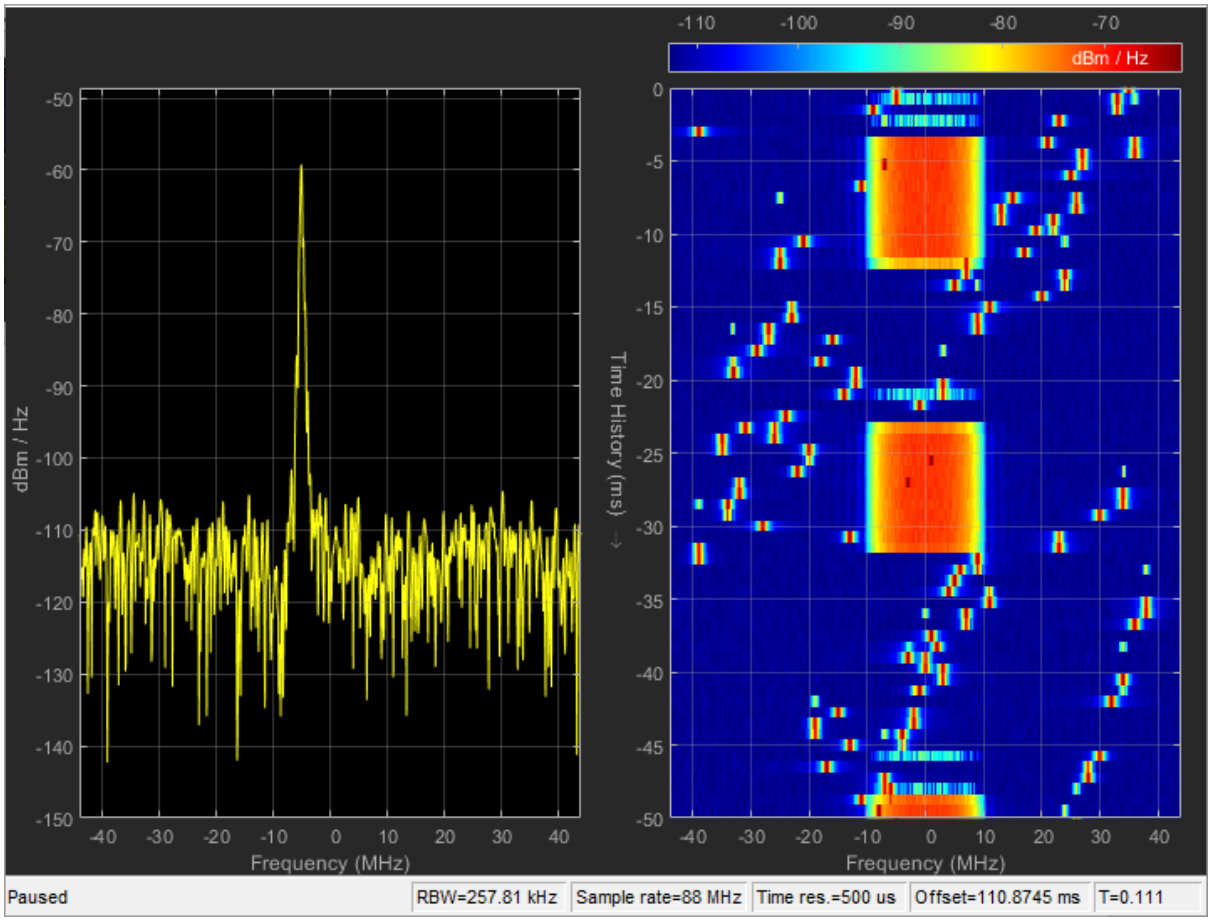
Slika 5.19. Spektar primljenog signala te spektrogram kanala HV3/AWGN&802.11b/1&2

Na dvodimenzionalnom prikazu na lijevoj strani slike 5.19. nalazi se graf koji prikazuje snagu primljenog signala pri određenom frekvencijskom opsegu. Najviša vrijednost snage je -65dBm/Hz. Može se primijetiti kako graf interferirajućeg signala na desnoj strani prikazuje kako je snaga i ovoga signala u istom frekvencijskom opsegu najviša. Također se može iščitati period trajanja u kojem je snaga interferirajućeg signala najviša, a to je 17.5 ms.



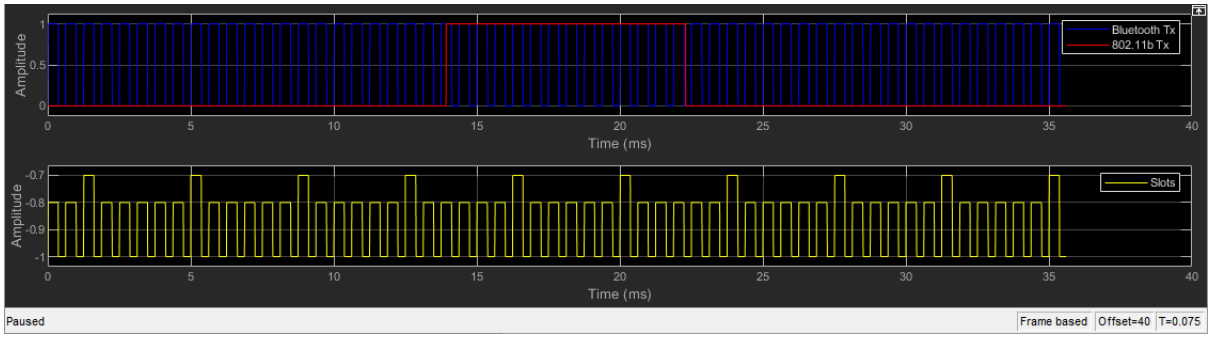
Slika 5.20. Vremenski dijagram primljenog signala DM1/AWGN&802.11b/1&2

Na slici 5.20. prikazan je primljeni signal podatkovnog tipa paketa DM1. Iz priloženog grafa može se zaključiti kako je period prijenosa jednog podatkovnog tipa paketa preko bluetooth veze jednak periodu prijenosa HV1 glasovnog tipa paketa. Interferirajući signal ima period trajanja iznosa 20 ms. Amplituda je jednaka nuli cca. 12.5 ms, a amplituda ima vrijednost „1“ ostalih 7.5 ms periode. DM1 tip paketa zauzima jedan vremenski *slot*.



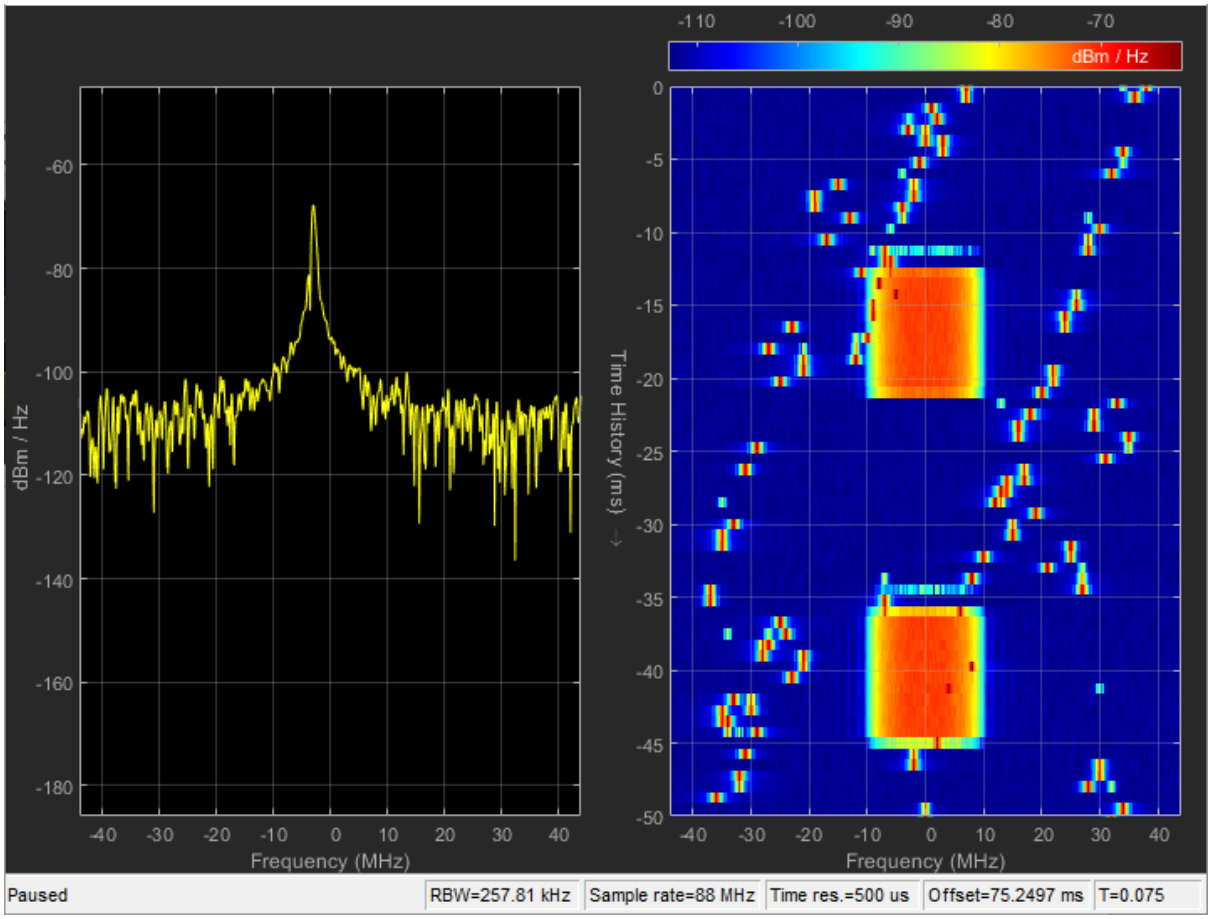
Slika 5.21. Spektar primljenog signala te spektrogram kanala DM1/AWGN&802.11b/1&2

Na slici 5.21. na lijevoj strani prikazan je graf primljenog signala gdje je tip paketa koji se prenosi preko Bluetooth veze DM1. Signal je izobličen zbog prisutnosti aditivnog bijelog šuma. Najviša snaga koji signala doseže je cca. -60dBm/Hz. Na desnoj strani slike prikazan je trodimenzionalni graf interferirajućeg 802.11b signala. Na grafu se vidi njegov period trajanja, te je period trajanja u kojem snaga signala doseže najvišu vrijednost cca. 9 ms.



Slika 5.22. Vremenski dijagram primljenog signala SCORT/AWGN&802.11b/1&2

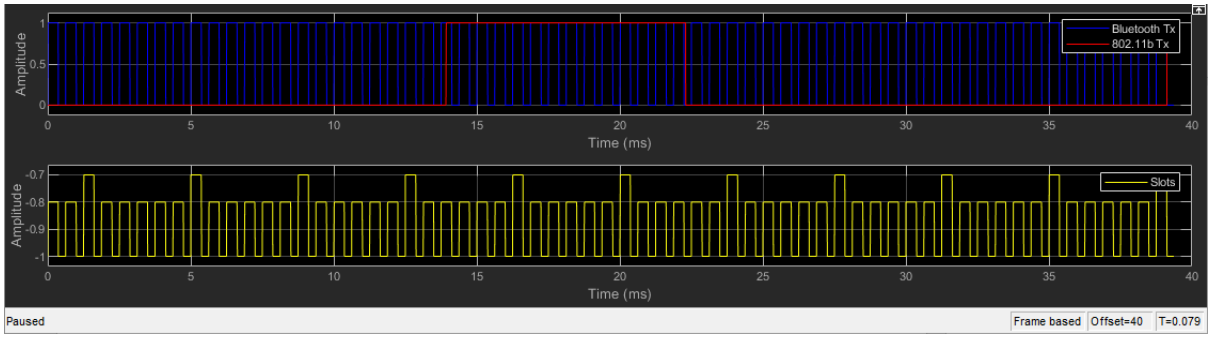
Vremenski dijagram na slici 5.22. prikazuje graf primljenog signala Bluetooth veze gdje se prenosi SCORT tip glasovnog paketa. Period ponavljanja primljenog signala je 1.25 ms. SCORT prema ovom grafu zauzima jedan par *slot*-a. Interferirajući signal ima period od 22 ms. Amplituda je jednaka nuli do 14. ms, a zatim do kraja trajanja perioda je jednaka jedinici.



Slika 5.23. Spektar primljenog signala te spektrogram kanala SCORT/AWGN&802.11b/1&2

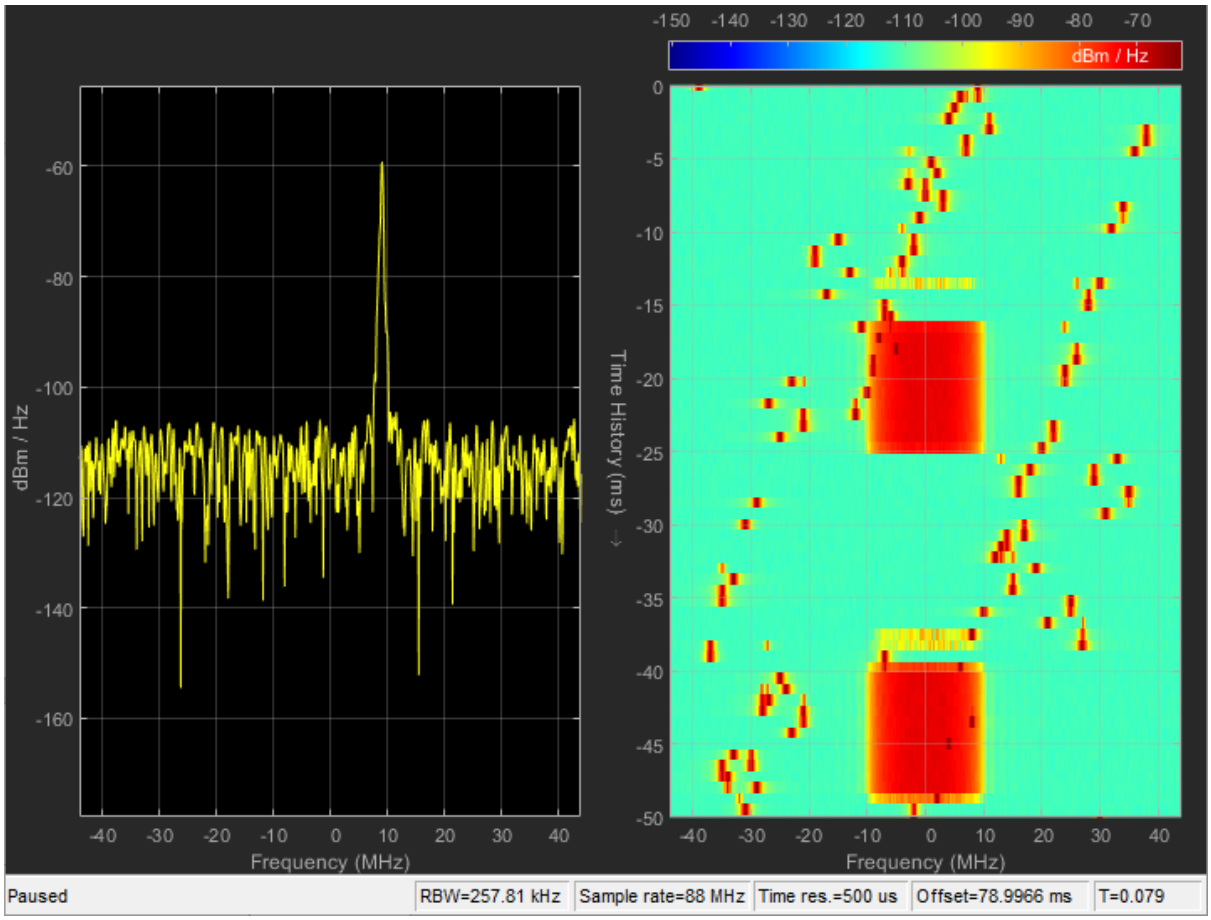
Spektar primljenog signala na lijevoj strani slike 5.23. ima najvišu vrijednost snage čiji je iznos cca. -55dBm/Hz. Signal ima izobličen oblik zbog okruženja u kojem se nalazi, odnosno zbog prisutnosti aditivnog bijelog šuma i interferirajućeg signala. Na desnoj strani prikazan je

trodimenzionalni grad interferirajućeg signala. Period trajanja u kojem je snaga interferirajućeg signala najviša je 9 ms.



Slika 5.24. Vremenski dijagram primljenog signala HV1/AWGN&802.11b/3&4

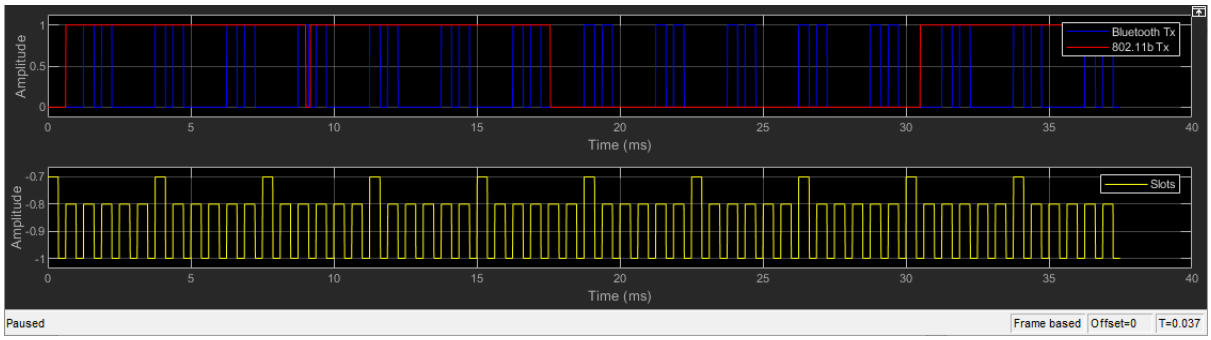
Na slici 5.24. prikazan je primljeni Bluetooth signal gdje se amplituda izmjenjuje od nule do jedinice svakih 1.25 ms. Interferirajući signal prikazan crvenom bojom prema grafu ima amplitudu 0 do 13.5 ms, te u tom trenutku prelazi u jedinicu do 23.5 ms, što ukazuje da je period interferirajućeg signala 23.5 ms. Inicijalni par *slot*-a je 3&4.



Slika 5.25. Spektar primljenog signala te spektrogram kanala HV1/AWGN&802.11b/3&4

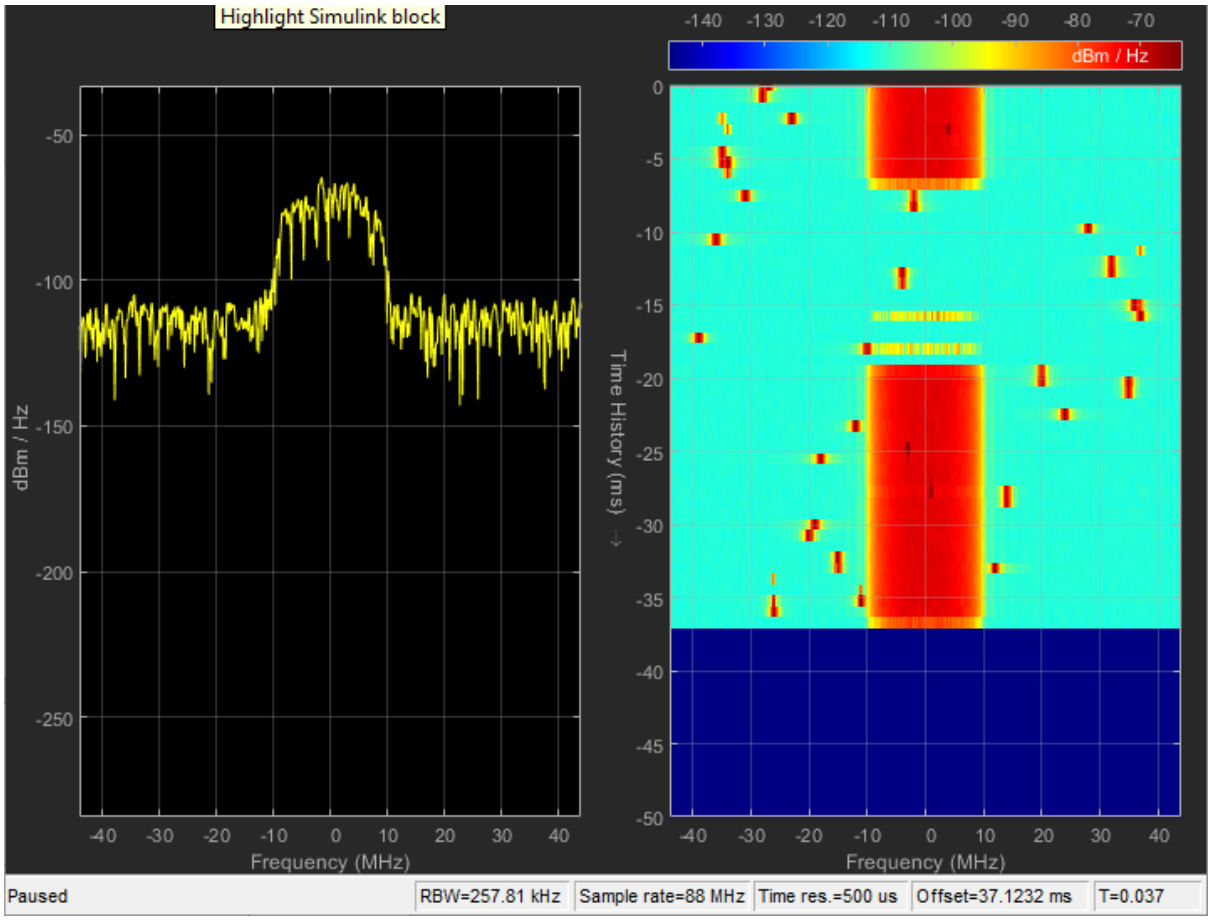
Na lijevom dvodimenzionalnom prikazu na slici 5.25. vidi se graf primljenog signala. Najviša vrijednost snage primljenog signala je -60dBm/Hz. Na desnoj strani slike nalazi se

trodimenzionalni prikaz (Frequency/Time History/ dBm/Hz) na kojemu se vidi interferirajući signal. Period u kojemu je prisutan interferirajući signal je 9ms, zatim se signal ponovno pojavljuje nakon 14.5 ms.



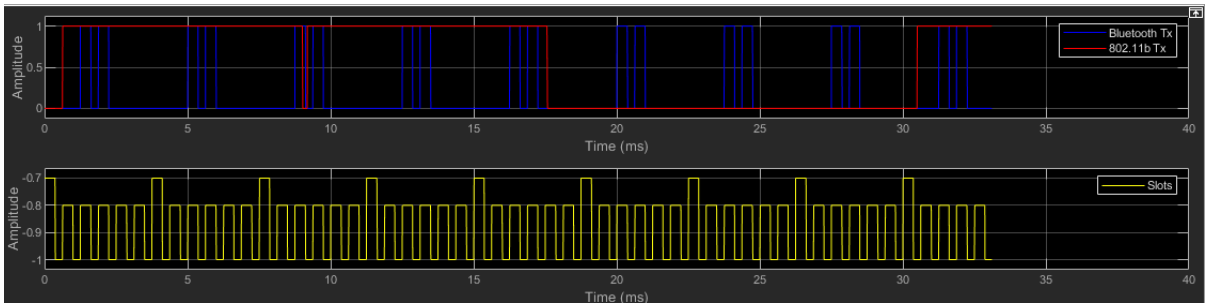
Slika 5.26. Vremenski dijagram primljenog signala HV2/AWGN&802.11b/3&4

Na slici 5.26. na vremenskom dijagramu primljenog signala se vidi da se primljeni Bluetooth signal periodički ponavlja svakih 2.5 ms. Amplituda je jednaka jedinici u vremenu trajanja od 1.25 ms, te isto toliko traje i nula. Zatim se periodički izmjenjuju. Crvenom linijom označen interferirajući signal ima period trajanja jedinice od 17 ms, a amplituda je jednaka nuli u vremenu od 13 ms, te se također periodički ponavlja.



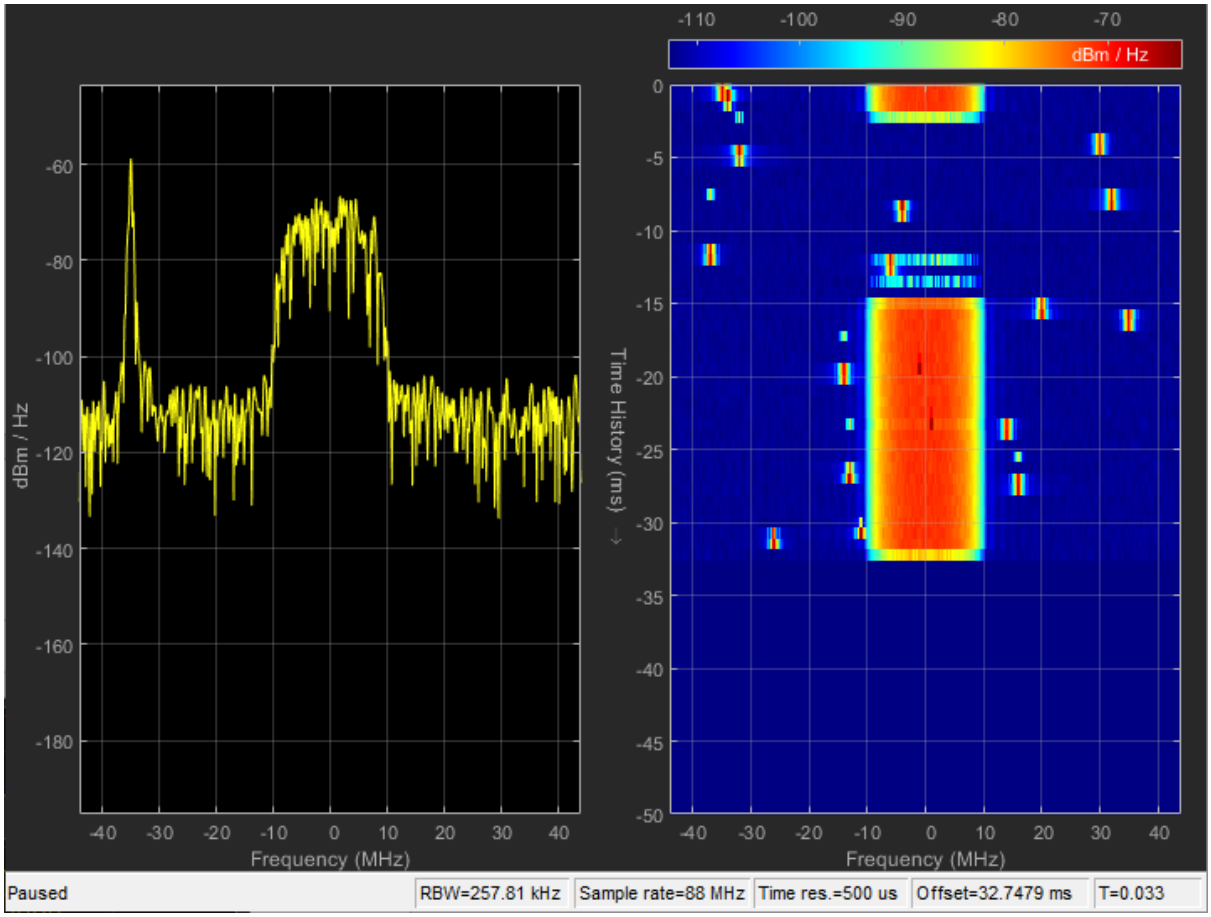
Slika 5.27. Spektar primljenog signala te spektrogram kanala HV2/AWGN&802.11b/3&4

Na slici 5.27. s lijeve strane je prikazan spektar primljenog signala. Uzimajući u obzir i lijevi grafički prikaz, može se zaključiti da je pri istom frekvencijskom opseg snaga oba signala najviša. S desne strane prikazan je spektrogram kanala gdje je prisutan interferirajući signal. Iz desne strane prikaza se također vidi da interferirajući signal ima najveći snagu unutar 17 ms. Signala nema idućih 13 ms, te se ponovno pojavljuje.



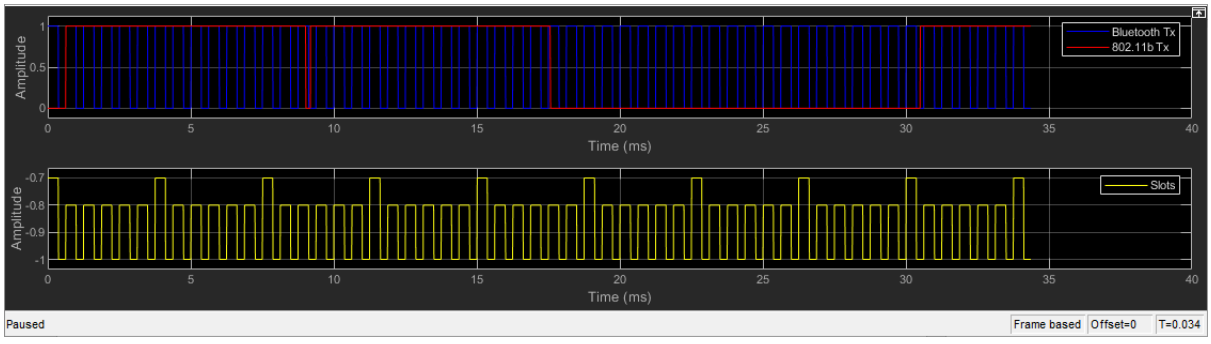
Slika 5.28. Vremenski dijagram primljenog signala HV3/AWGN&802.11b/3&4

Na slici 5.28 prikazan je primljeni Bluetooth signal. Vremenski period trajanja u kojem je amplituda jednaka jedinici je 1.25 ms. Period u kojem je vrijednost amplitude nula traje 2.5 ms. Period nakon koga se signal ponavlja je 3.75 ms. Interferirajući signal 802.11b ima vrijednost amplitude „1“ u vremenu trajanja od 17 ms, dok je iznos amplitude jednak „0“ u vremenu od 13 ms, što znači da period ponavljanja interferirajućeg signala iznosi 30 ms.



Slika 5.29. Spektar primljenog signala te spektrogram kanala HV3/AWGN&802.11b/3&4

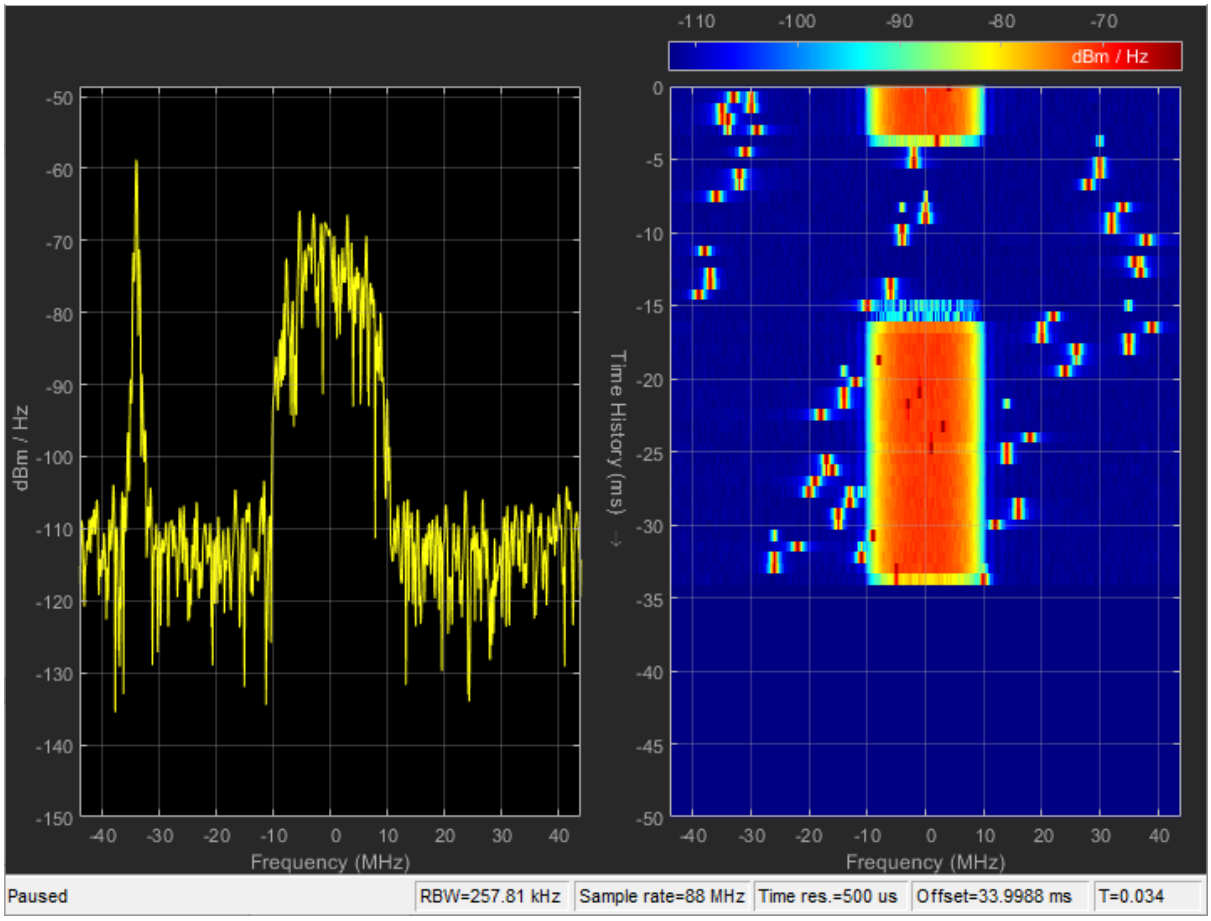
Na slici 5.29. na dvodimenzionalnom prikazu gdje se nalazi graf primljenog signala mogu se primijetiti oscilacije koje su izazvane prisutnošću aditivnog bijelog šuma. Na desnom trodimenzionalnom grafu prikazan je interferirajući signal. Period trajanja interferirajućeg signala je 30 ms. Signal ima najvišu snagu 17 ms. Ostalih 13 ms, signala nema, amplituda mu je „0“,



Slika 5.30. Vremenski dijagram primljenog signala DM1/AWGN&802.11b/3&4

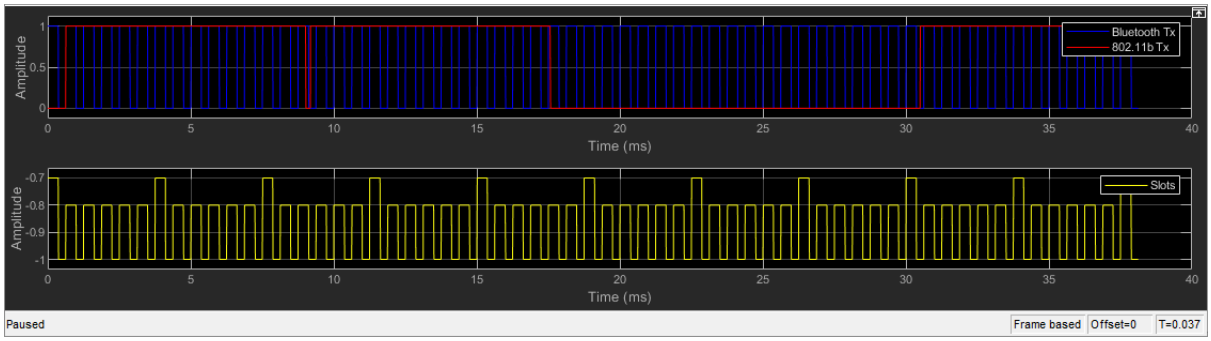
Vremenski dijagram prikazan na slici 5.30. prikazuje primljeni signal Bluetooth veze kojom se u ovom slučaju prenose paketi podatkovnog tipa DM1. Period trajanja prijenosa jednog paketa

je 1.25 ms, što odgovara trajanju jednog para *slot*-a. Interferirajući signal ima period iznosa 30 ms. Amplituda je jednaka jedinici u prvom dijelu perioda, te je njezino vrijeme trajanja 17 ms.



Slika 5.31. Spektar primljenog signala te spektrogram kanala DM1/AWGN&802.11b/3&4

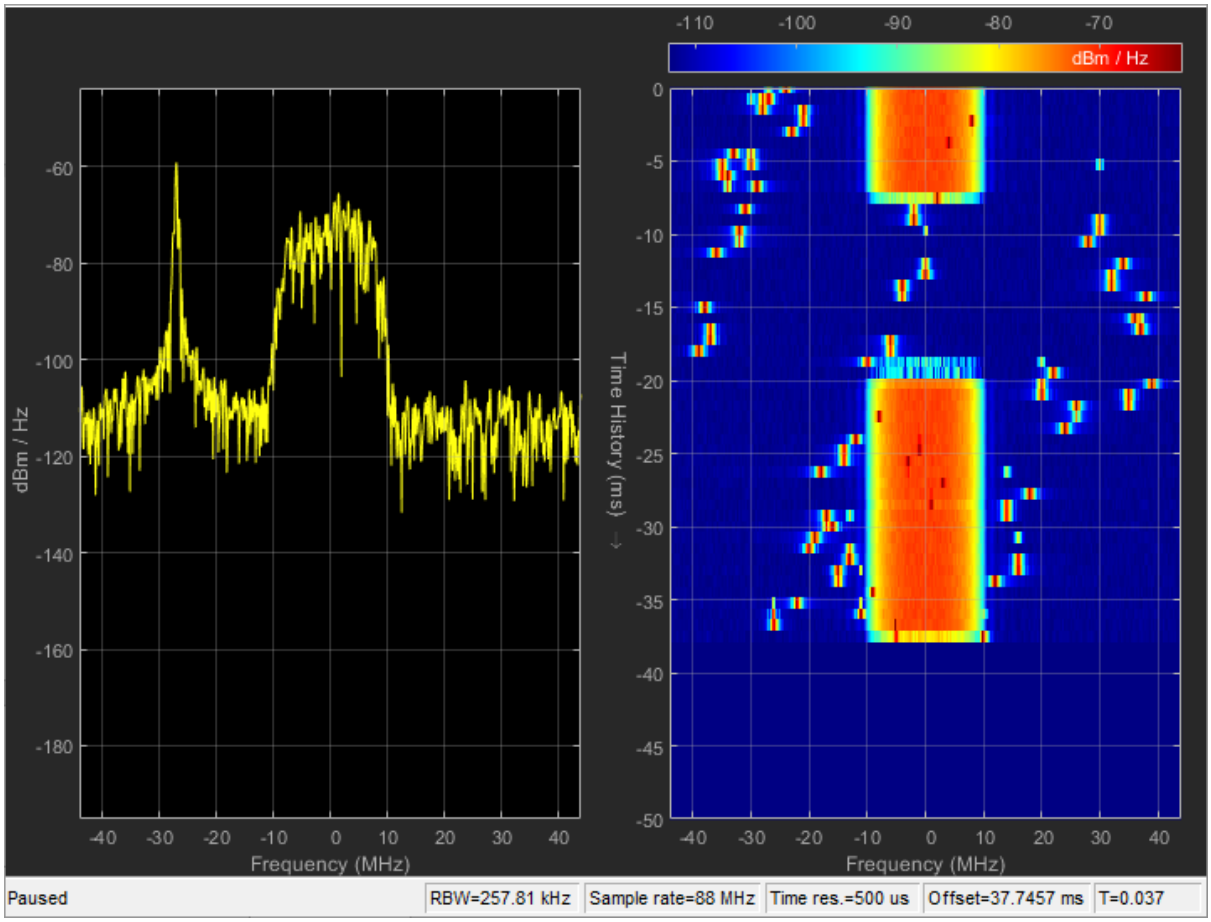
Spektar primljenog signala na lijevoj strani slike 5.31. je izobličen zbog prisutnosti smetnji. Na trodimenzionalnom prikazu na desnoj strani nalazi se interferirajući signal. Može se zaključiti kako period u kojem je snaga interferirajućeg signala najviša iznosi 17 ms, te je taj period jednak trajanju amplitude vrijednosti 1.



Slika 5.32. Vremenski dijagram primljenog signala SCORT/AWGN&802.11b/3&4

Primljeni signal na vremenskom dijagramu prikazanom na slici 5.32. ima period trajanja1.25 ms. Nakon tog se ponavlja. Period trajanja SCORT tipa glasovnog paketa u ovom slučaju

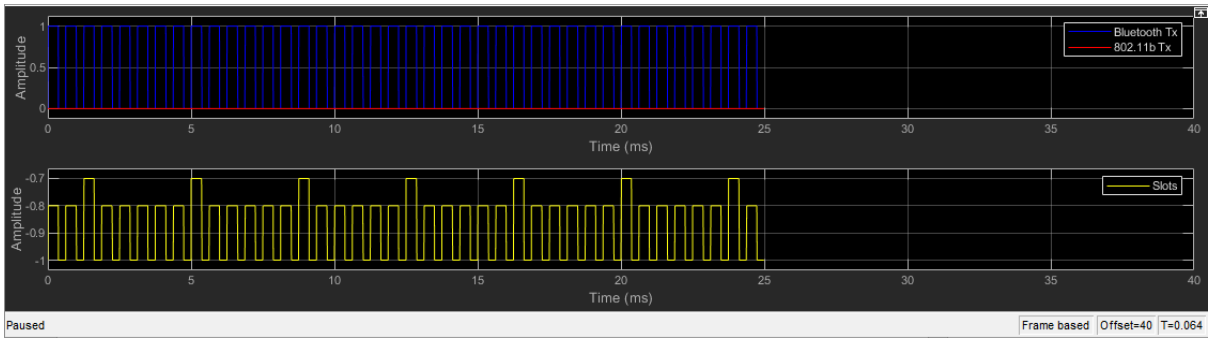
odgovara trajanju jednog para vremenskog *slot*-a. Interferirajućem signala odgovara perioda od 30 ms. U prvom dijelu perida amplituda ima vrijednost „1“, te ona traje 17 ms, dok je vrijednost amplitude jednaka „0“ ostalih 13 ms.



4.33. Spektar primljenog signala te spektrogram kanala SCORT/AWGN&802.11b/3&4

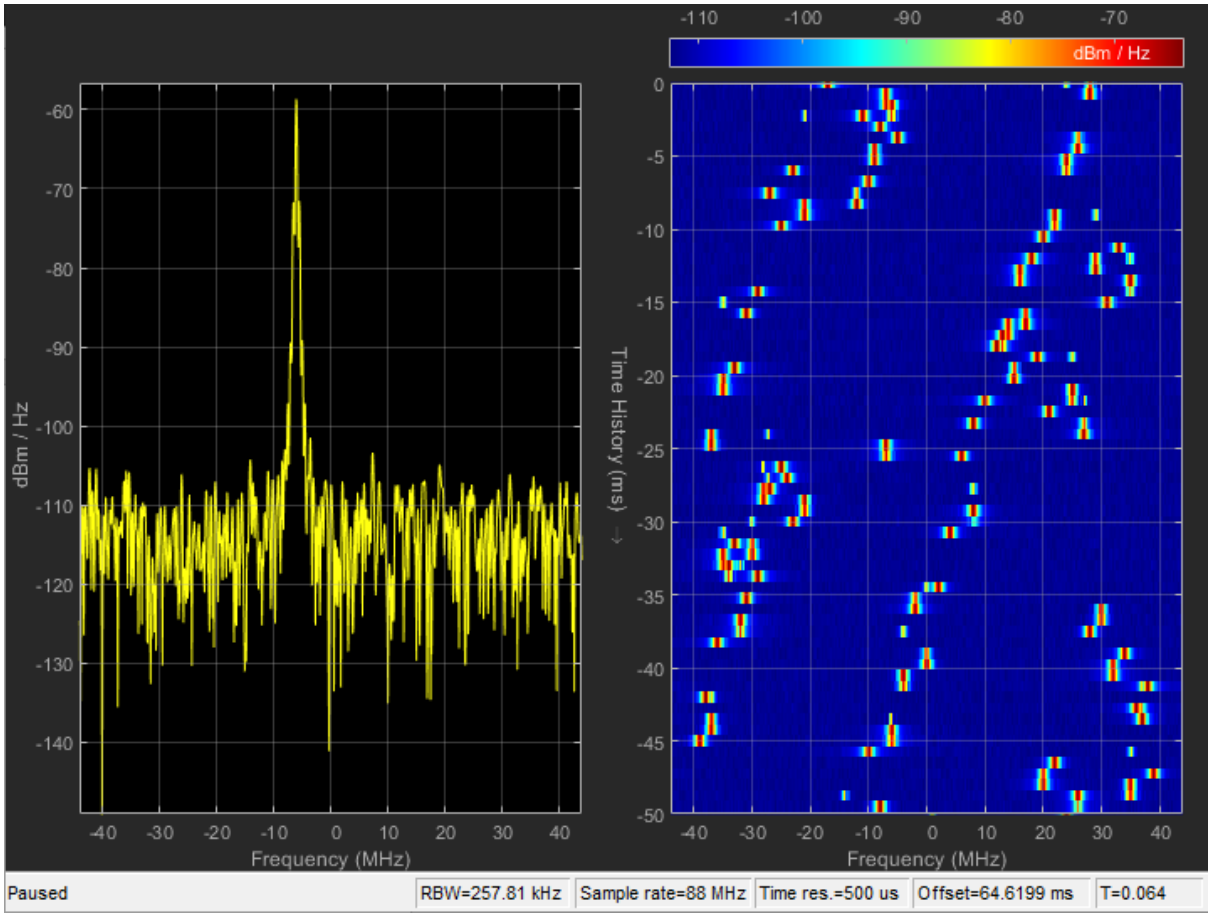
Zbog prisutnosti aditivnog bijelog šuma te interferirajućeg signala, spektar primljenog Bluetooth signala je izobličen što se može vidjeti na dvodimenzionalnog prikazu na slici 5.33. Na lijevom trodimenzionalnom prikazu vremenski period u kojem je snaga interferirajućeg signala najviša odgovara periodu u kome je vrijednost amplitude „1“, te on iznosi 17 ms. Ostalih 13 ms perioda je interferirajući signal odsutan, nakon čega se ponovno pojavljuje.

5.5.2. Rezultati simulacije u okruženju AWGN šuma



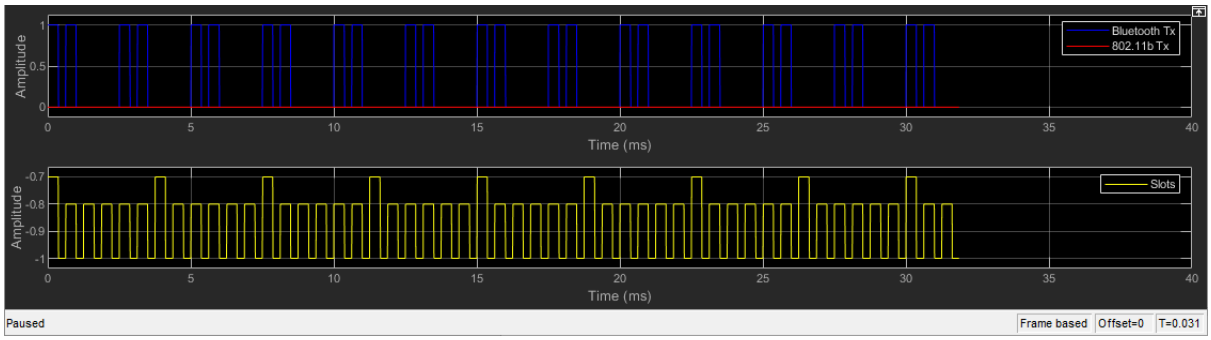
Slika 5.34. Vremenski dijagram primljenog signala HV1/AWGN/1&2

Slika 5.34. prikazuje vremenski dijagram primljenog signala gdje je glasovni tip podatka HV1, prijenos je ometan aditivnim bijelim šumom te se prenosi u inicijalnom paru *slot*-a 1&2. Budući da u ovom primjeru nema interferencije signalom 802.11b, njegova amplituda kroz cijeli period je jednaka nuli. Kao i u prošlom primjeru, budući da je glasovni tip podatka HV1, amplituda Bluetooth signala se izmjenjuje svakih 1.25 ms. HV1 glasovni paketi se šalju i primaju u obliku jednostrukih *slot*-ova u svakom paru *slot*-a.



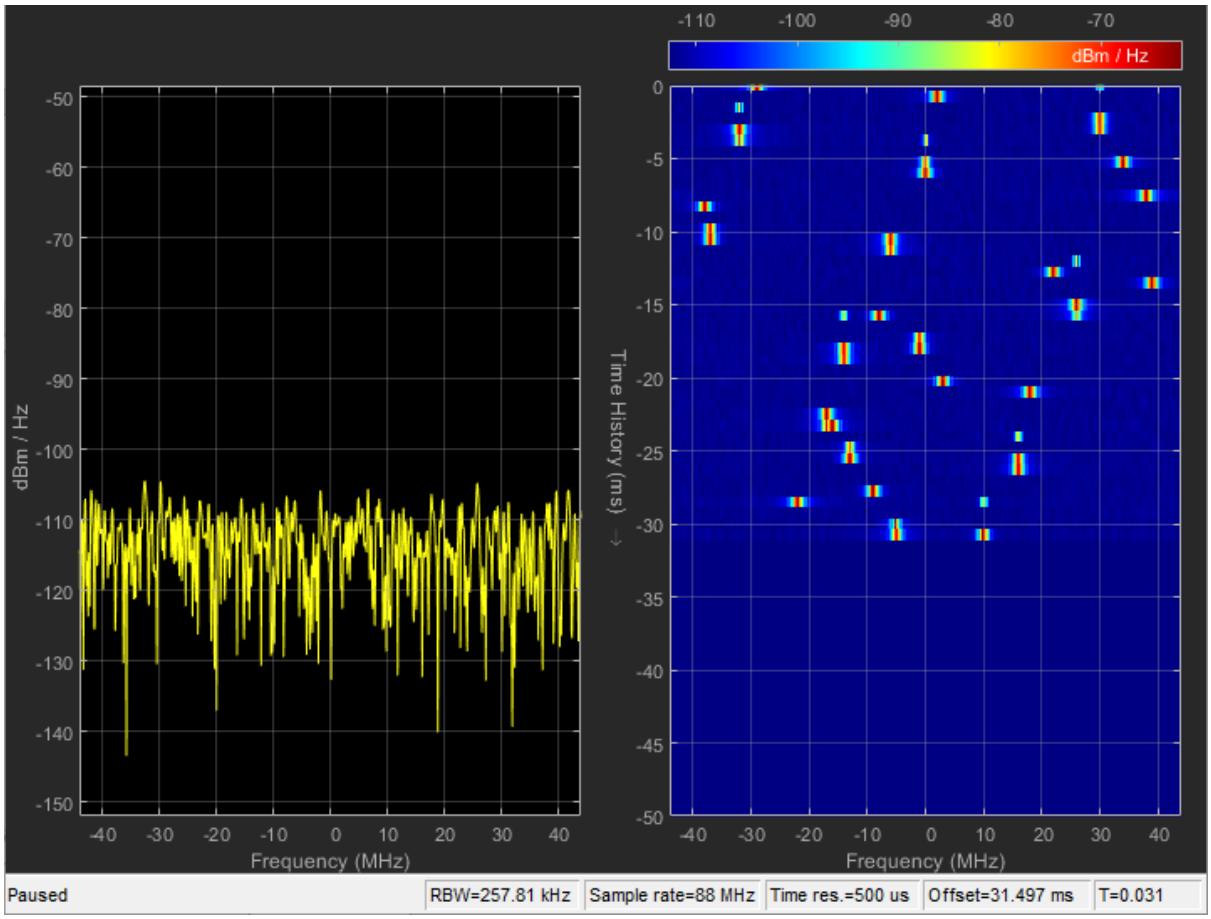
Slika 5.35. Spektar primljenog signala te spektrogram kanala HV1/AWGN/1&2

Na slici 5.35. je vidljiva prisutnost aditivnog bijelog šuma, ali ne i signala 802.11b. Zbog prisutnosti aditivnog bijelog šuma, primljeni Bluetooth signal je izobličen. Najviša dosegnuta vrijednost snage signala je cca. -55dBm/Hz.



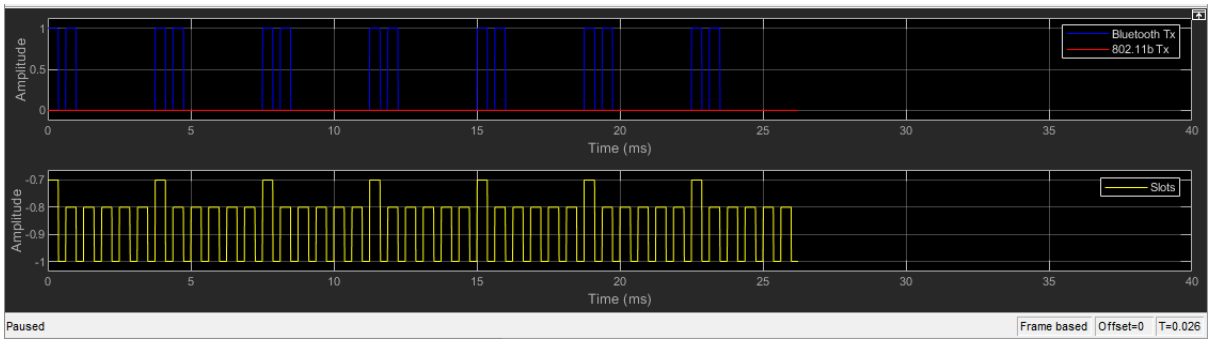
Slika 5.36. Vremenski dijagram primljenog signala HV2/AWGN/1&2

Na slici 5.36. , gdje je prikazan primljeni signal glasovnog paketa HV2 u okruženju aditivnog bijelog šuma, ima period trajanja 2.5 ms, što odgovara vremenu trajanja glasa koji se prenosi unutar 20 bajta, odnosno period trajanja primljenog signala odgovara trajanju dva para vremenskog *slot*-a. Signal prikazan prikazan crvenom linijom kroz cijeli period trajanja ima amplitudu jednaku nuli, budući da je u ovom primjeru prilikom pokretanja simulacije odabrano okruženje bez interferirajućeg 802.11b kanala. S



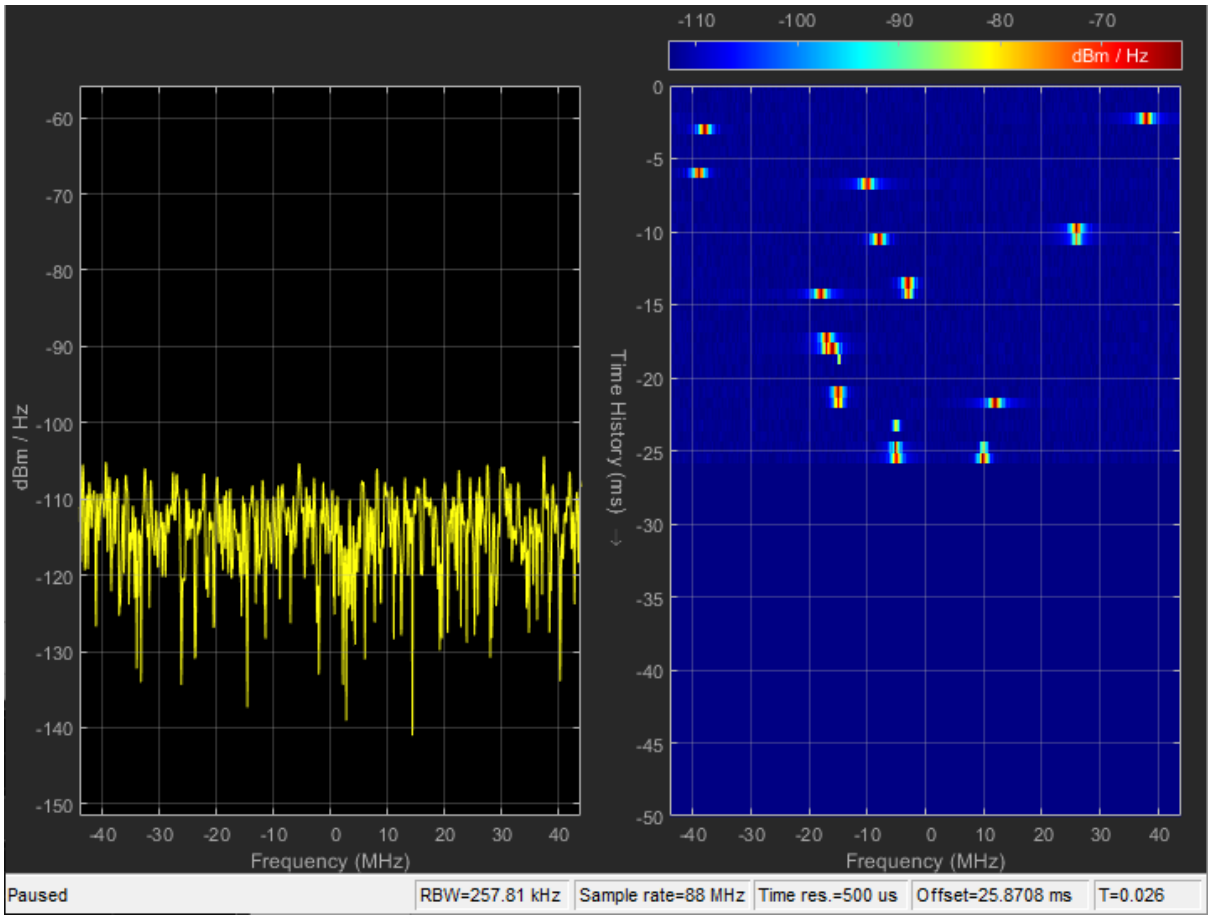
Slika 5.37. Spektar primljenog signala te spektrogram kanala HV2/AWGN/1&2

Na slici 5.37. prikazan je s lijeve strane graf primljenog signala. U trenutku zaustavljanja simulacije, budući da je u okruženju prisutan šum, primijećene su oscilacije. S desne strane slikovitog prikaza nalazi se graf koji prikazuje odsutnost 802.11b signala.



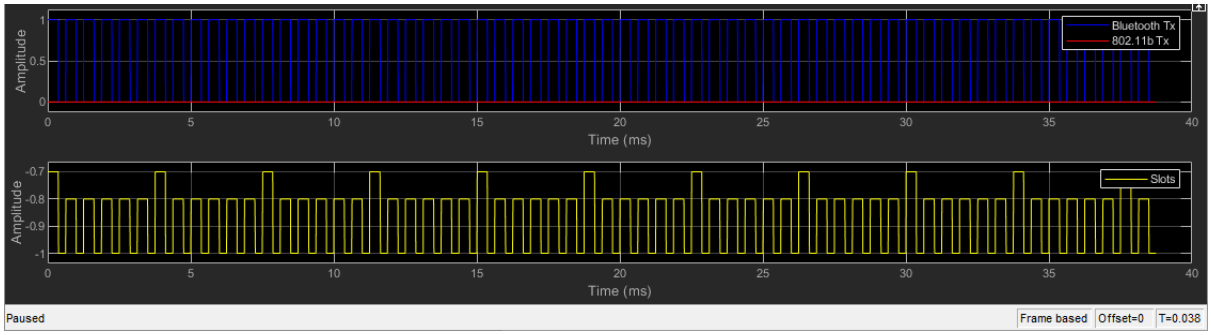
Slika 5.38. Vremenski dijagram primljenog signala HV3/AWGN/1&2

Na vremenskom dijagramu na slici 5.38. prikazan je primljeni signal u okolini u kojoj je prisutan šum, bez interferirajućeg signala. Period trajanja primljenog signala je 3.75 ms, što odgovara prijenosu glasova unutar 30 bajtova. Nakon šestog uzastopnog *slot*-a se ponavlja primljeni signal, tj. nakon 3 para vremenskih *slot*-ova.



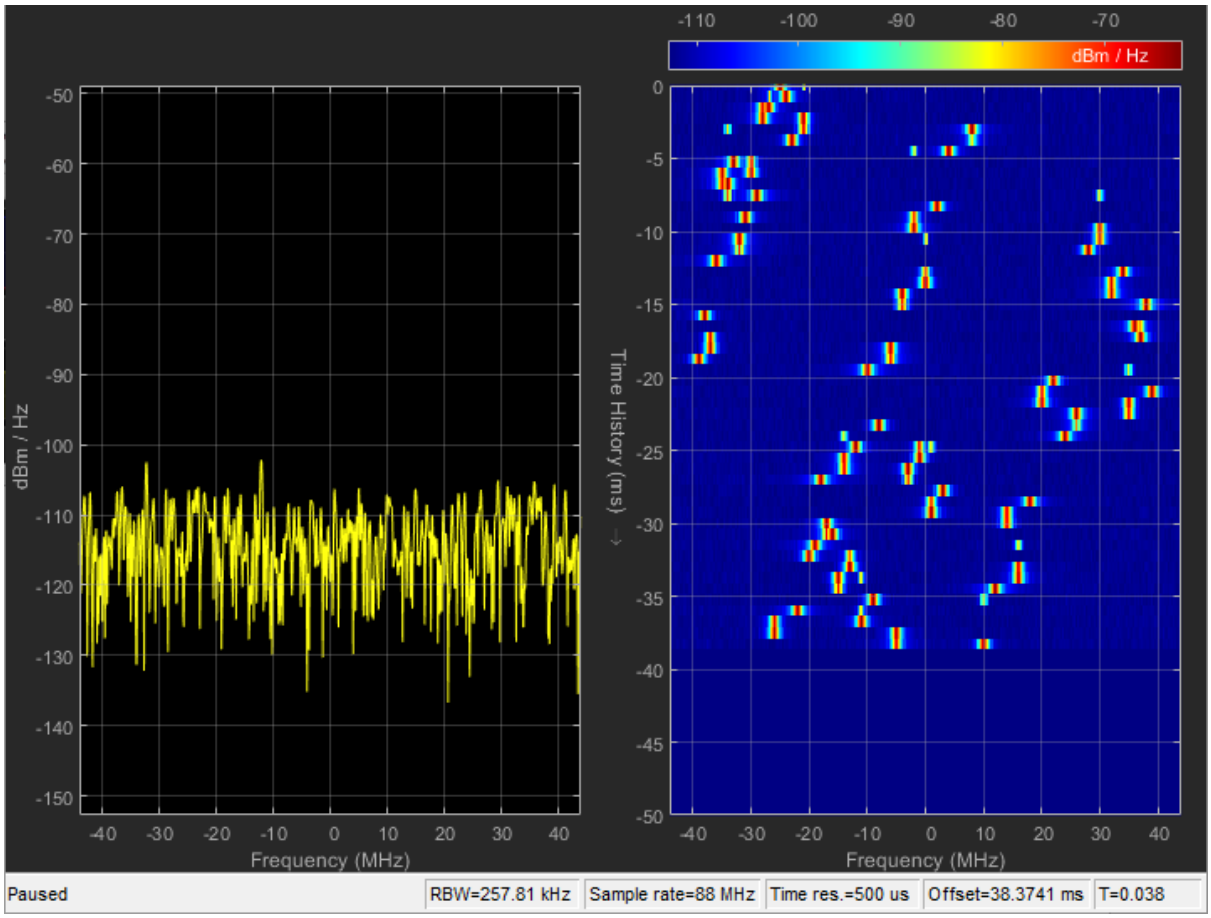
Slika 5.39. Spektar primljenog signala te spektrogram kanala HV3/AWGN/1&2

Na slici 5.39. vidljivo je da graf koji prikazuje primljeni signal kojemu najviša vrijednost snage -105 dBm/Hz. Interferirajućeg signala nema.



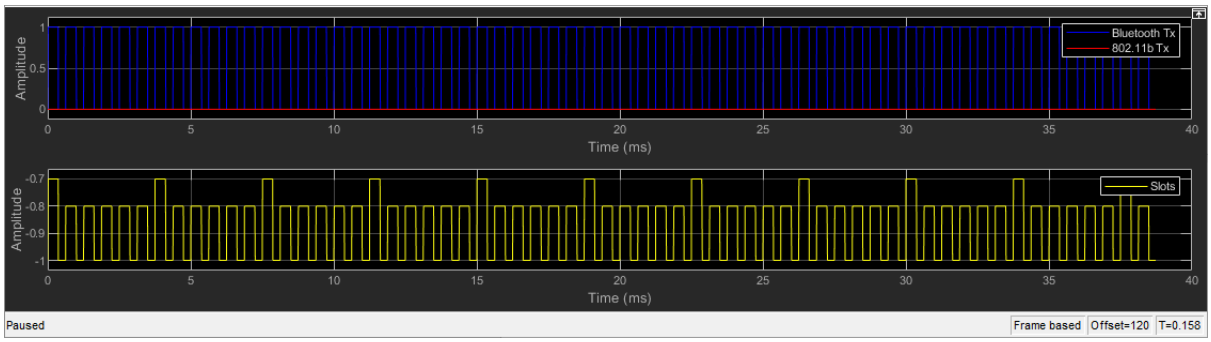
Slika 5.40. Vremenski dijagram primljenog signala DM1/AWGN/1&2

Na slici 5.40. prikazan je vremenski dijagram primljenog signala Bluetooth veze u kojem su poslani paketi podatkovnog tipa DM1 u okruženju gdje je prisutan šum, u kojoj nema interferirajućeg signala. Period prijenosa jednog glasovnog paketa je 1.25 ms, stoga se paket prenosi unutar jednog para vremenskog *slot*-a.



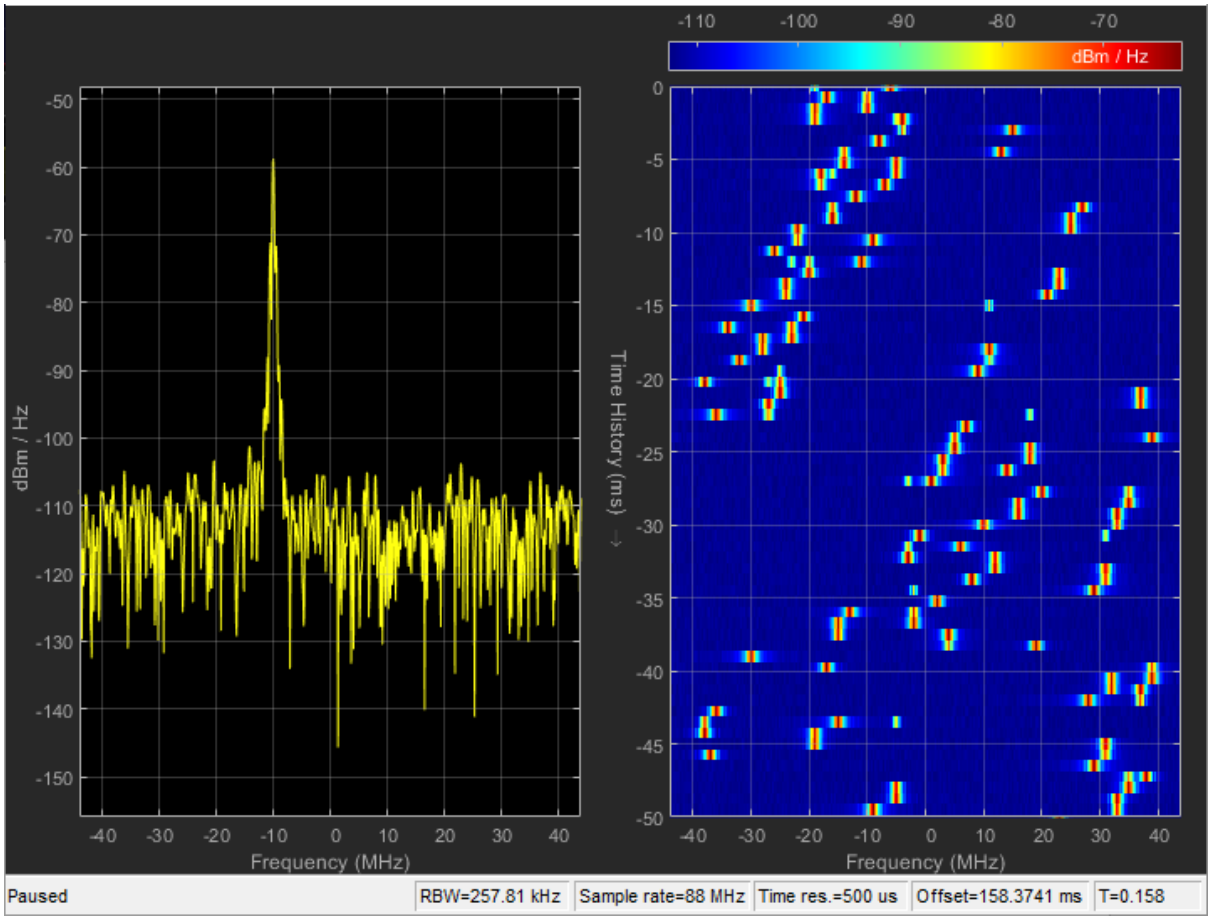
Slika 5.41. Spektar primljenog signala te spektrogram kanala DM1/AWGN/1&2

Zbog prisutnosti šuma, signal na dvodimenzionalnom prikazu na slici 5.41. je izobličen, odnosno ne odgovara izvornom signalu Bluetooth veze. U trenutku zaustavljanja simulacije, najviša vrijednost snage primljenog signala je -102 dBm/Hz.



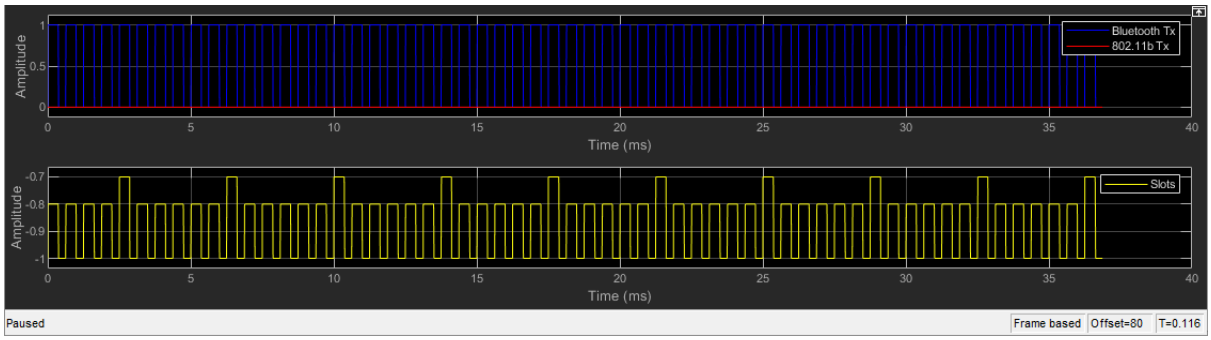
Slika 5.42. Vremenski dijagram primljenog signala SCORT/AWGN/1&2

Na slici 5.42. prikazan je primljeni signal, odnosno njegov vremenski dijagram. Plavom označen je Bluetooth signal kojim su slani SCORT paketi. Period trajanja slanja jednog glasovnog paketa je 1.25 ms koji odgovara trajanju jednog para vremenskog slot-a. Signal interferencije je kroz cijeli period predstavljen ravnom linijom, budući da u ovom slučaju nije prisutna interferencija nego samo aditivni bijeli šum.



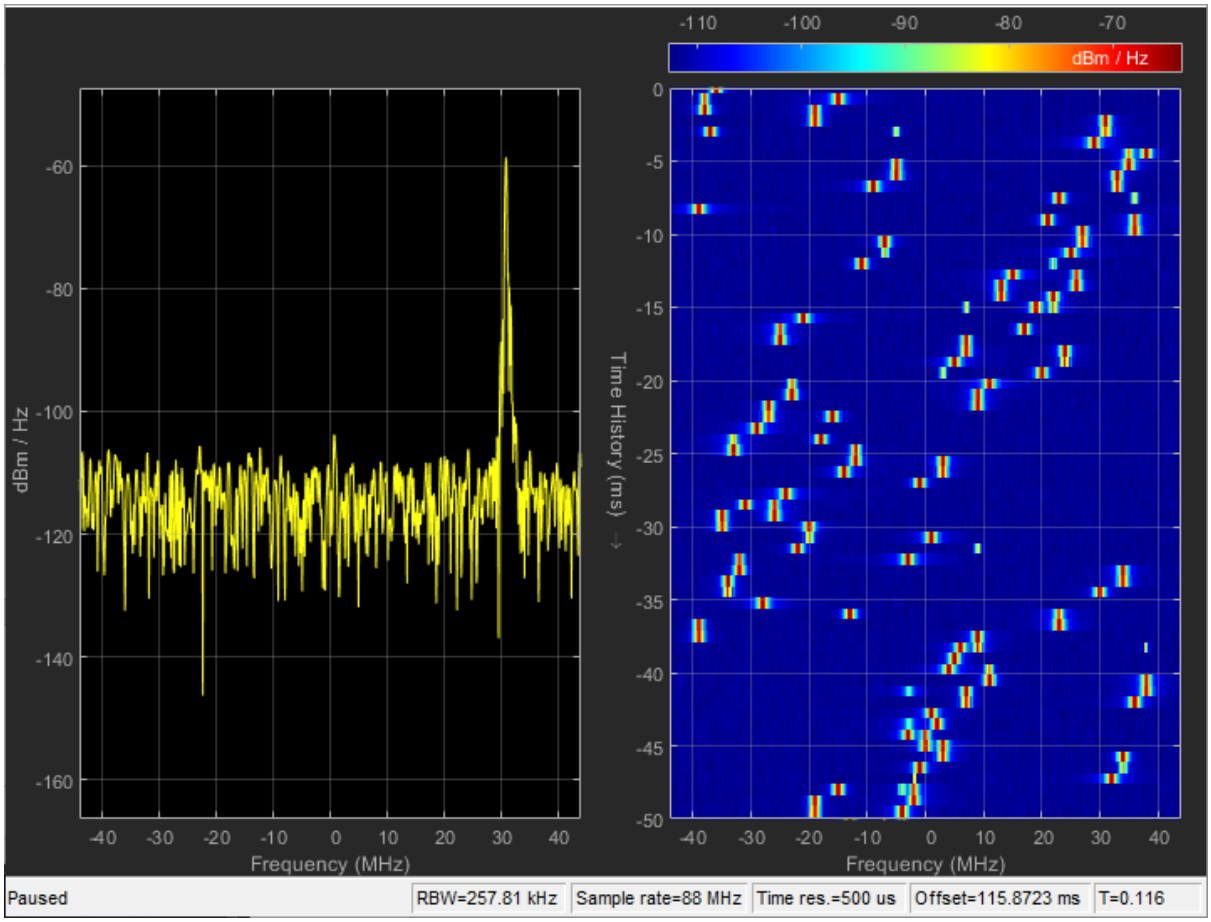
4.43. Spektar primljenog signala te spektrogram kanala SCORT/AWGN/1&2

Spektar primljenog signala prikazan na dvodimenzionalnom grafu na slici 5.43. je izobličen u odnosu na Bluetooth signal koji se šalje u okruženju bez prisustva ikakvih smetnji. Najviša vrijednost snage iznosi -58 dBm/Hz.



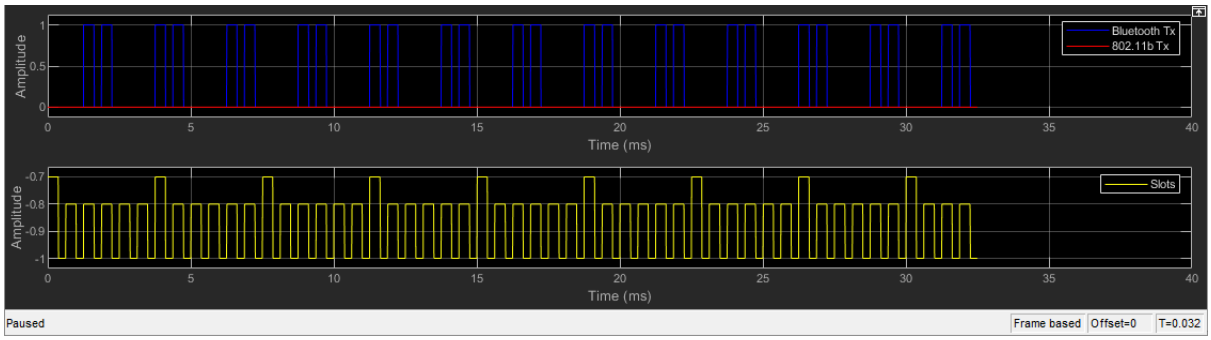
Slika 5.44. Vremenski dijagram primljenog signala HV1/AWGN/3&4

Na slici 5.44. prikazan je vremenski dijagram primljenog signala poslanog preko Bluetooth veze. Glasovni paket koji je poslan je HV1, te je period slanja jednog paketa 1.25 ms. Time se podrazumijeva da se glasovni paketi prenosi unutar jednog para vremenskog *slot*-a. Kod interferencijskog signala nema promjene amplitude budući da se paketi šalju u okruženju u kojem je izostavljen 802.11b.



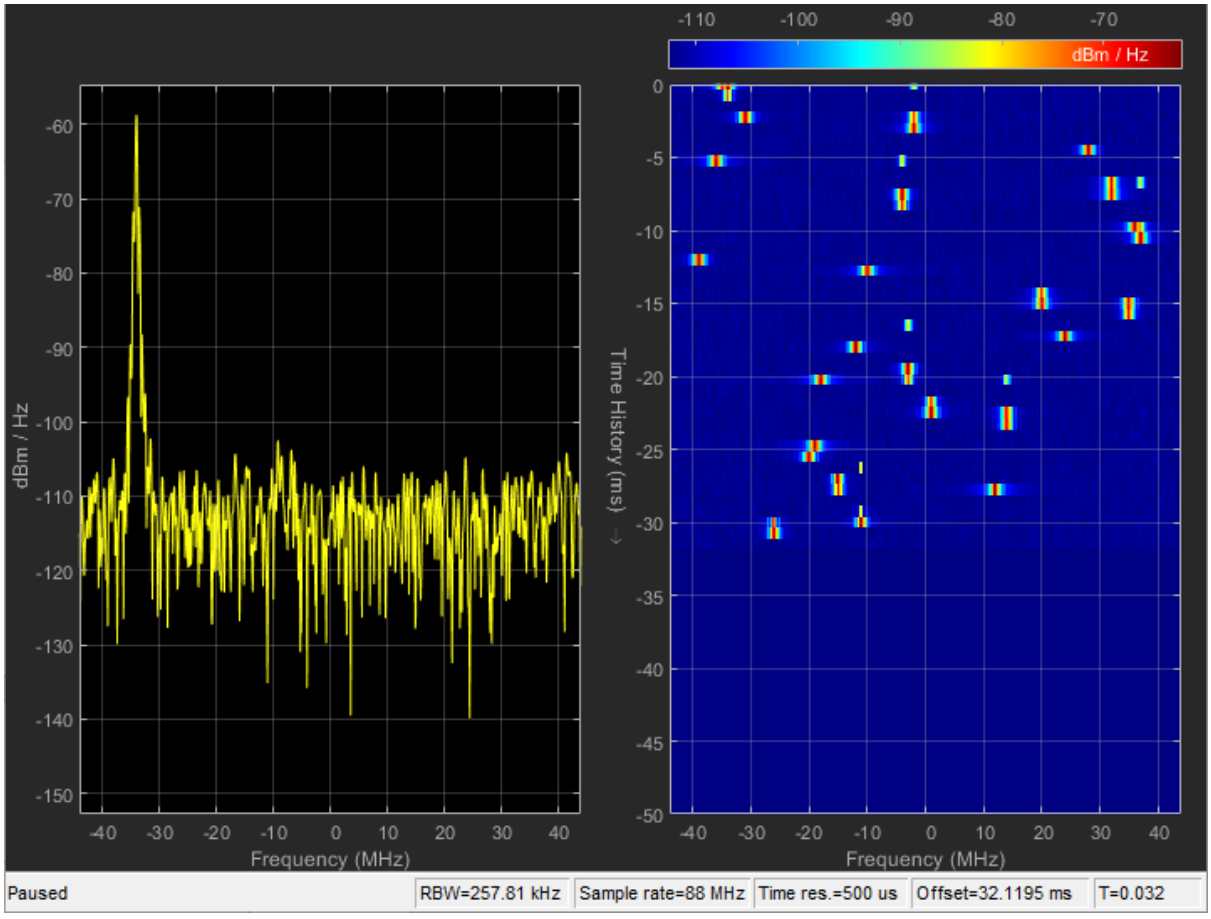
Slika 5.45. Spektar primljenog signala te spektrogram kanala HV1/AWGN/3&4

Spektar primljenog signala u okruženju s aditivnim bijelim šumom prikazan na dvodimenzionalnom prikazu slike 5.45. prikazuje izobličeni signal, što je posljedica samog okruženja u kojem se odvija slanje glasovnih paketa.



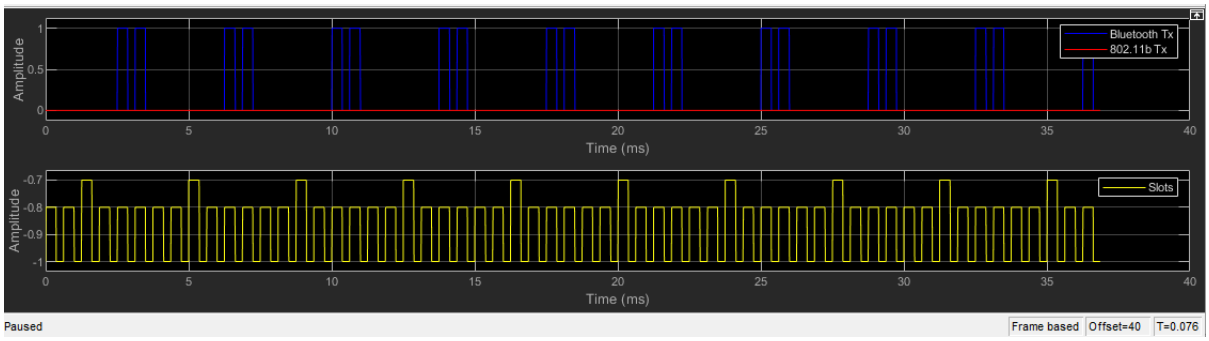
Slika 5.46. Vremenski dijagram primljenog signala HV2/AWGN/3&4

Na vremenskom dijagramu primljenog signala na slici 5.46. može se vidjeti kako je period slanja jednog paketa glasovnog tipa HV2 2.5 ms. Trajanje perioda odgovara vremenskom trajanju dvaju parova vremenskog *slot*-ova, odnosno ponavljaju četiri uzastopna *slot*-a. Budući da je paket poslan u okruženju u kojem je isključen interferencijski signal, amplituda spomenutog signala je kroz cijeli period jednaka nuli.



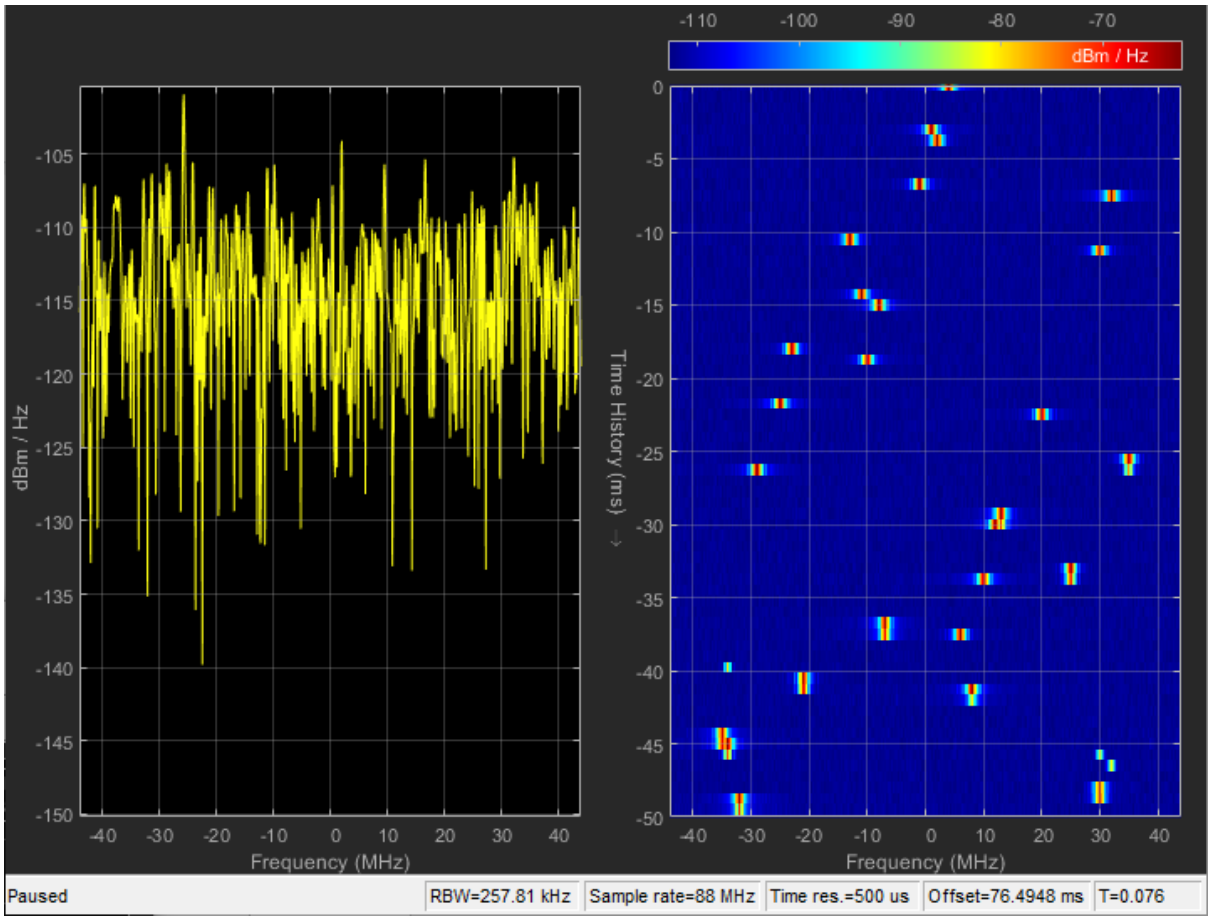
Slika 5.47. Spektar primljenog signala te spektrogram kanala HV2/AWGN/3&4

Spektar primljenog signala u okruženju aditivnog bijelog šuma je izobličen u odnosu na Bluetooth signal koji se nalazi u okruženju bez smetnji, što se može vidjeti iz dvodimenzionalnog grafa prikazanog na slici 5.47.



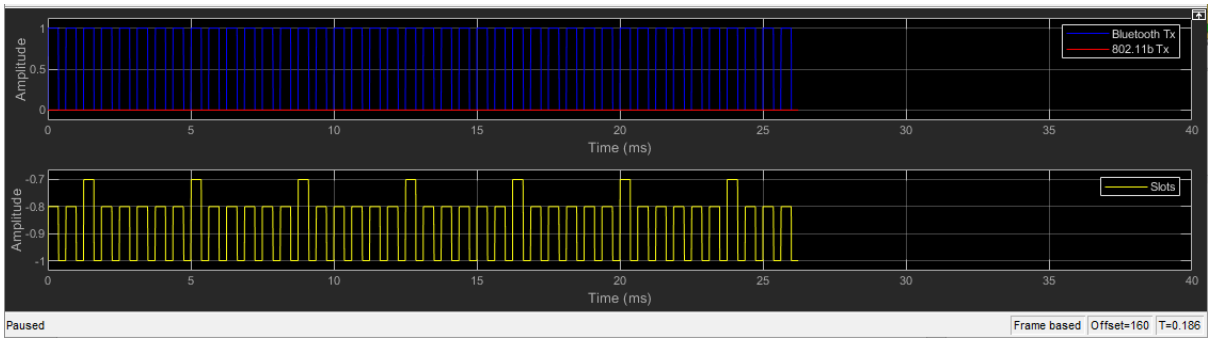
Slika 5.48. Vremenski dijagram primljenog signala HV3/AWGN/3&4

Prema slici 5.48. može se zaključiti da je period slanja jednog glasovnog HV3 paketa 3.75 ms. Vremensko trajanje slanja jednog glasovnog paketa odgovara trajanju 6 uzastopnih vremenskih *slot*-ova, odnosno trajanju triju parova vremenskih *slot*-ova. Amplituda signala interferencije je kroz cijeli period jednaka „0“.



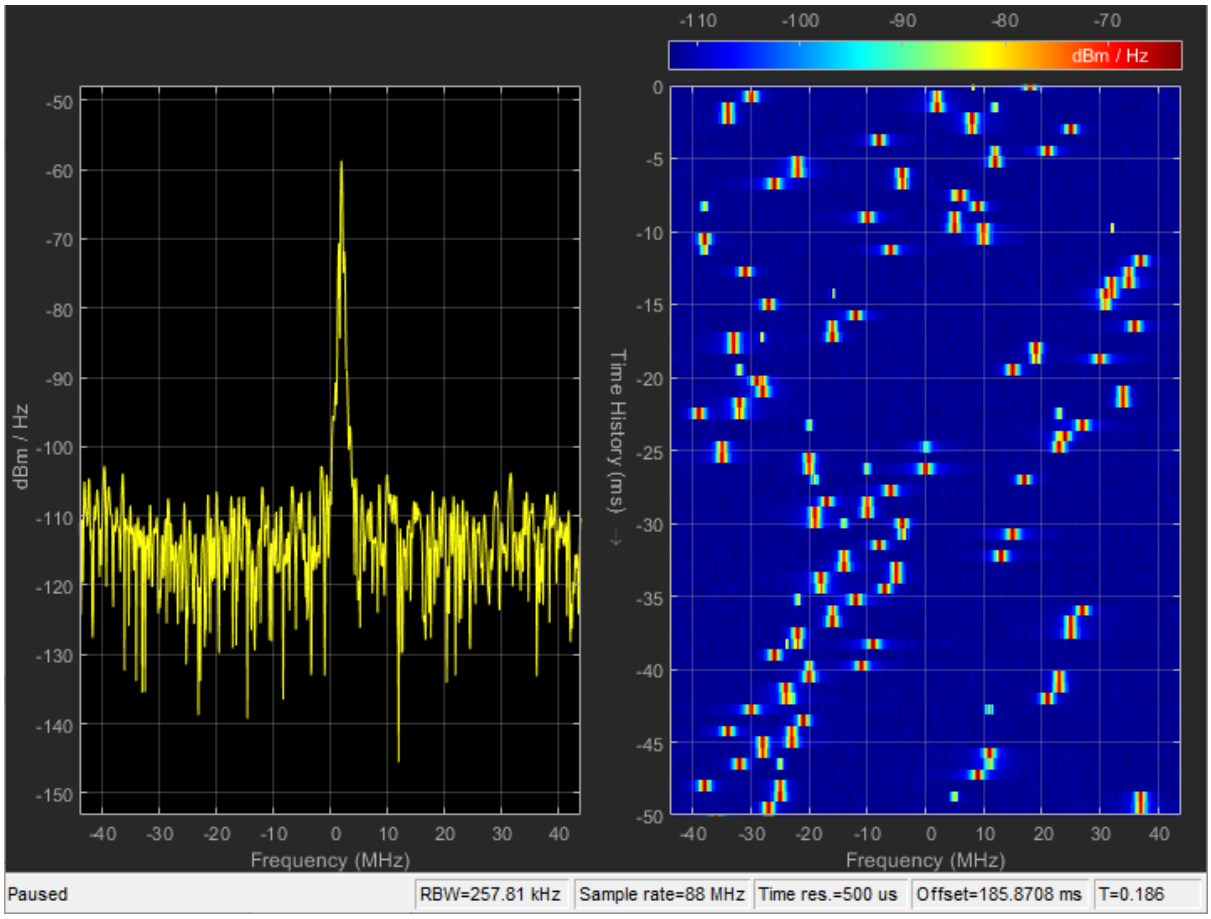
Slika 5.49. Spektar primljenog signala te spektrogram kanala HV3/AWGN/3&4

Na slici 5.49. se na spektru primljenog signala mogu uočiti oscilacije u cijelom frekvencijskom opsegu zbog prisutnosti aditivnog bijelog šuma u okruženju.



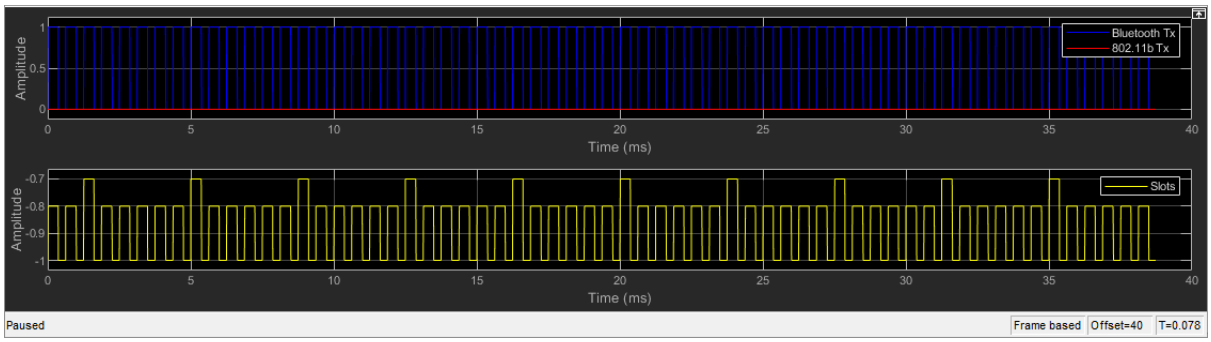
Slika 5.50. Vremenski dijagram primljenog signala DM1/AWGN/3&4

Na slici 5.50. nalazi se prikaz vremenskog dijagrama primljenog Bluetooth signala. U ovome slučaju preko Bluetooth konekcije poslan je podatkovni tip paketa DM1 koji ima period trajanja prijenosa jednog paketa 1.25 ms. Stoga vrijeme trajanja jednog paketa odgovara vremenu trajanja dvaju uzastopnih vremenskih *slot*-ova, odnosno jednom paru vremenskog *slot*-a.



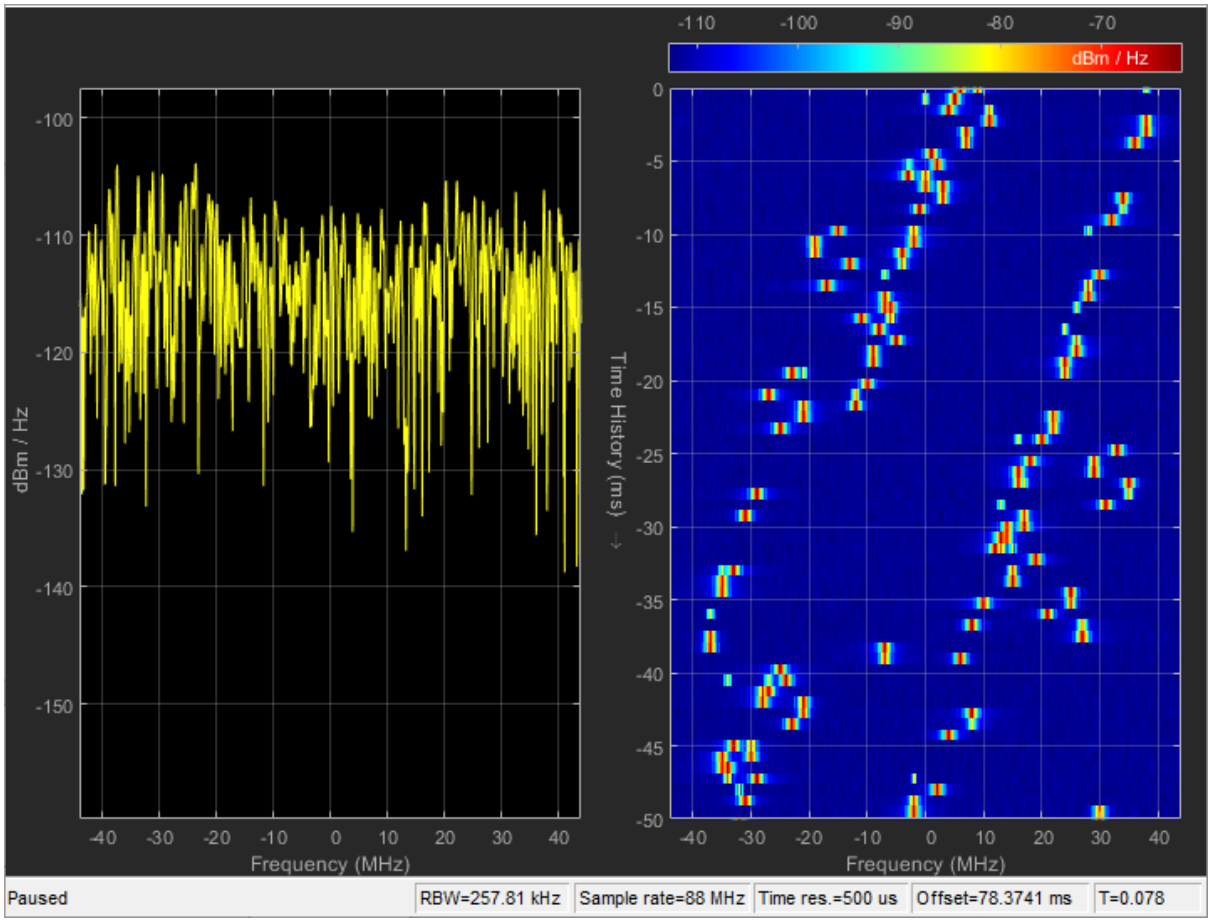
Slika 5.51. Spektar primljenog signala te spektrogram kanala DM1/AWGN/3&4

Na spektrogramu na slici 5.51. može se vidjeti kako je smetnjama uzrokovanim šumom izobličen primljeni Bluetooth signal. Na trodimenzionalnom prikazu može se uvidjeti da nema prisutnosti interferencijskog signala.



Slika 5.52. Vremenski dijagram primljenog signala SCORT/AWGN3&4

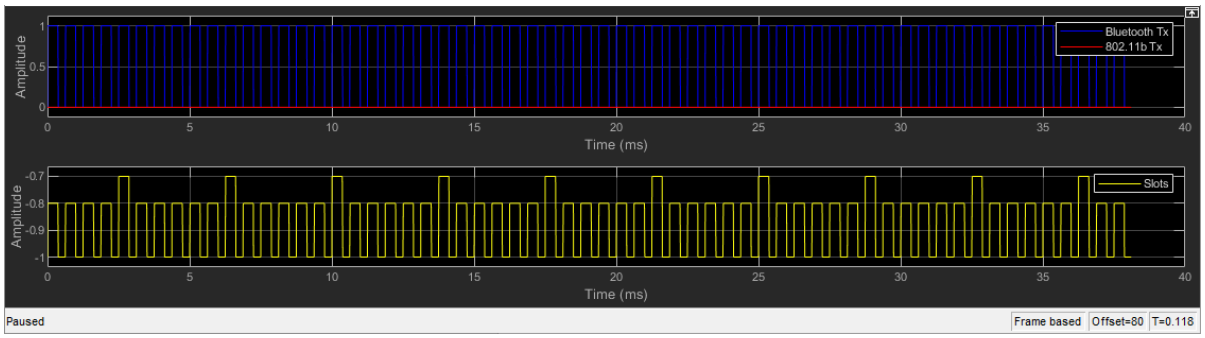
Vremenski dijagram primljenog signala na slici 5.52. prikazan je primljeni Bluetooth signal gdje su preko Bluetooth veze poslani SCORT glasovni paketi. Njihov period je 1.25 ms. Nakon toga se signal periodički ponavlja. Jedan par vremenskog slota odgovara vremenu potrebnom za slanje jednog glasovnog paketa. Interferencijskog signala nema, odnosno amplituda mu je nula kroz cijeli period.



Slika 5.53. Spektar primljenog signala te spektrogram kanala SCORT/AWGN/3&4

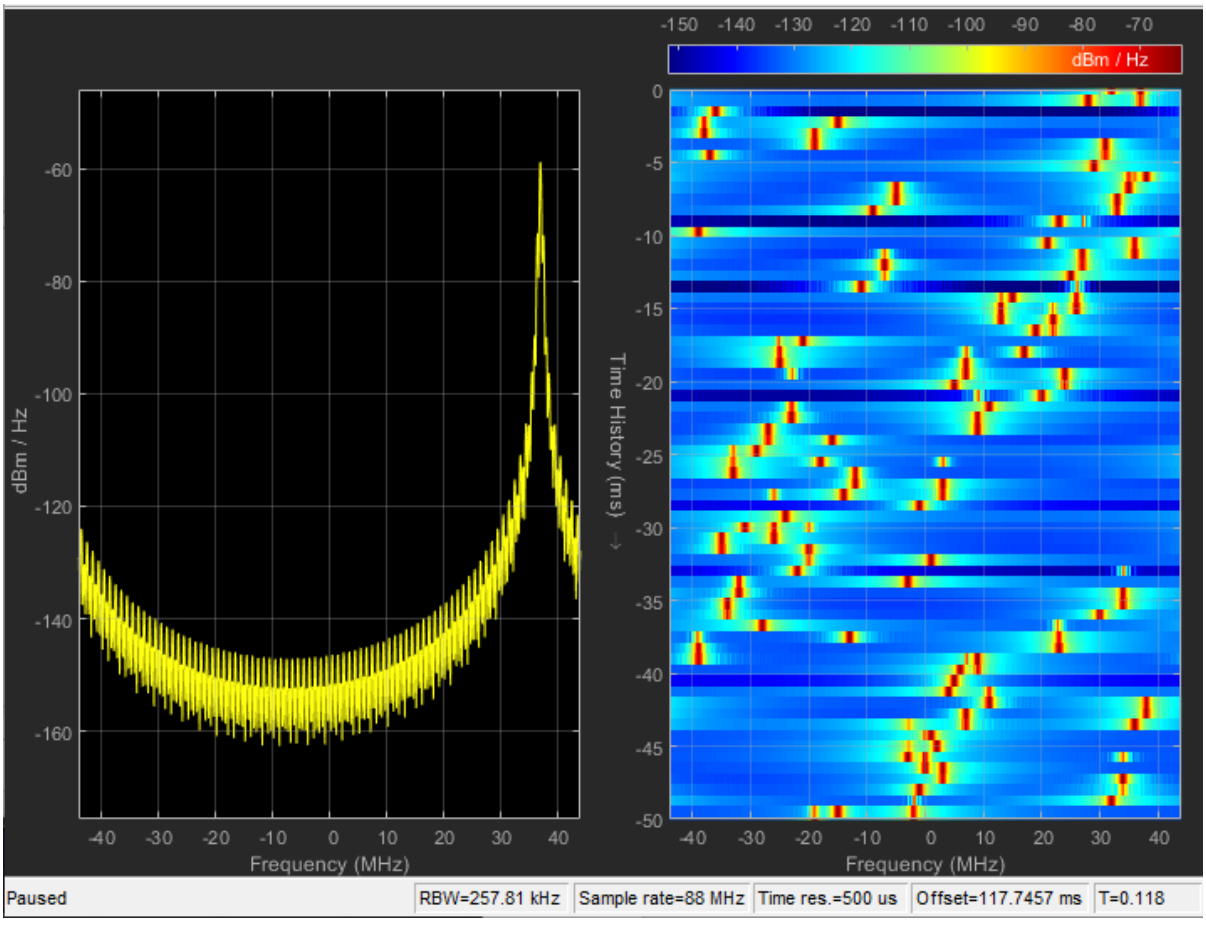
Na dvodimenzionalnom prikazu spektra primljenog signala na slici 5.53. vidljivo je postojanje šuma u okruženju slanja glasovnih paketa preko Bluetooth veze.

5.5.3. Rezultati simulacije u okruženju bez smetnji



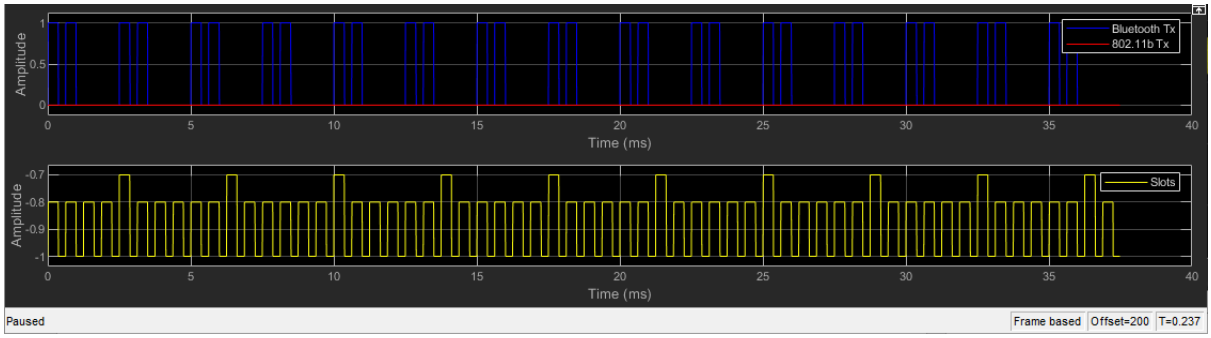
Slika 5.54. Vremenski dijagram primljenog signala HV1/None/1&2

Vremenski dijagram na slici 5.54. prikazuje primljeni signal u okruženju u kojem nije prisutan niti šum niti signal 802.11b. Amplituda signala 802.11b jednaka je nuli kroz cijeli period ponavljanja, a amplituda Bluetooth signala prelazi iz vrijednosti 1 u 0 svakih 1.25 ms. Kao i u prethodna dva primjera, korišten je HV1 tip glasovnog paketa. U svakom paru *slot*-a šalje se jednostruki uzastopni slot koji predstavlja glasovni paket.



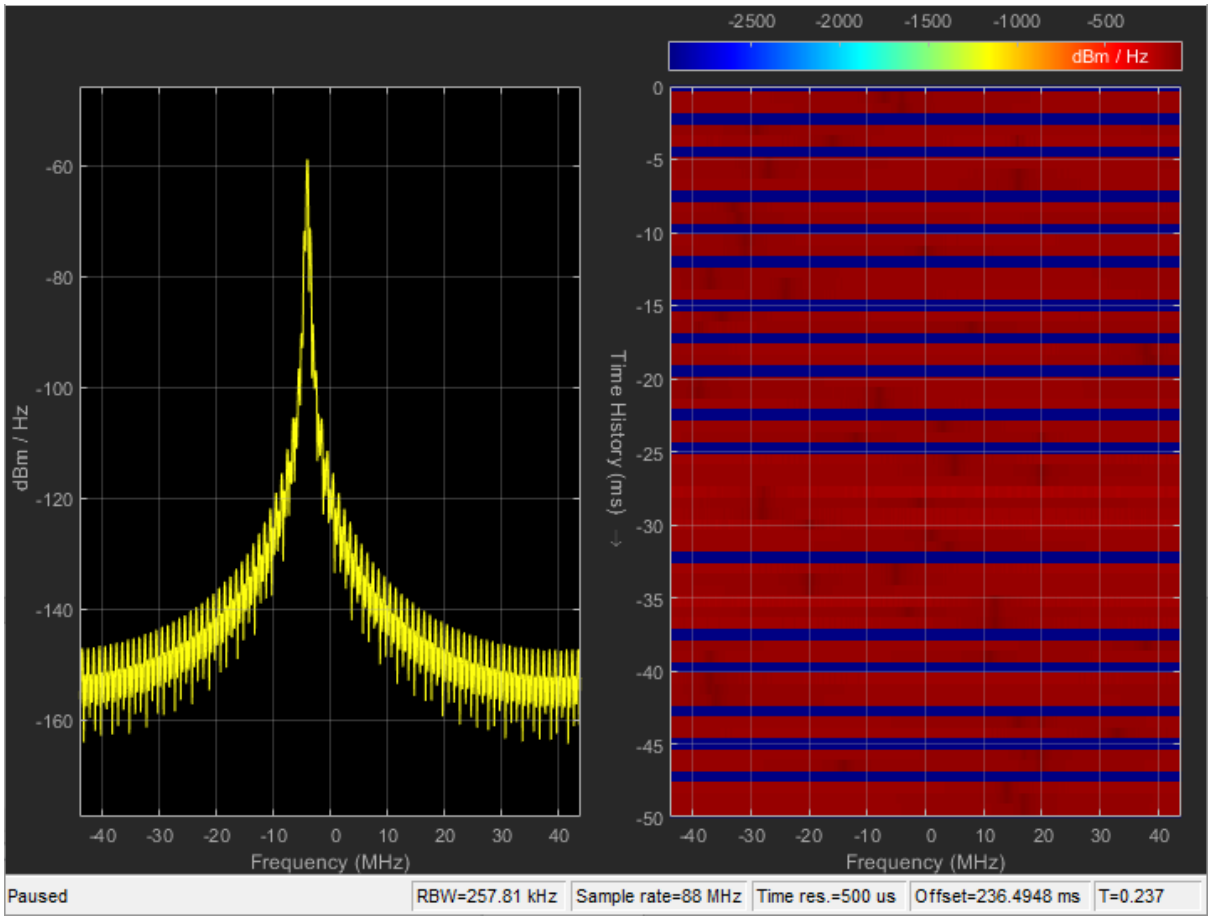
Slika 5.55. Spektar primljenog signala te spektrogram kanala HV1/None/1&2

Na grafovima prikazanima na slici 5.55. jasno se vidi kako u okruženju nema šuma ni drugog ometajućeg signala, što je posljedica odabranog okruženja prilikom pokretanja simulacije – bez smetnji. Primljeni signal na lijevoj strani slike je u svom izvornom obliku, a na desnoj strani nalazi se trodimenzionalni prikaz interferirajućeg internetskog signala, koji u ovome slučaju nije prisutan.



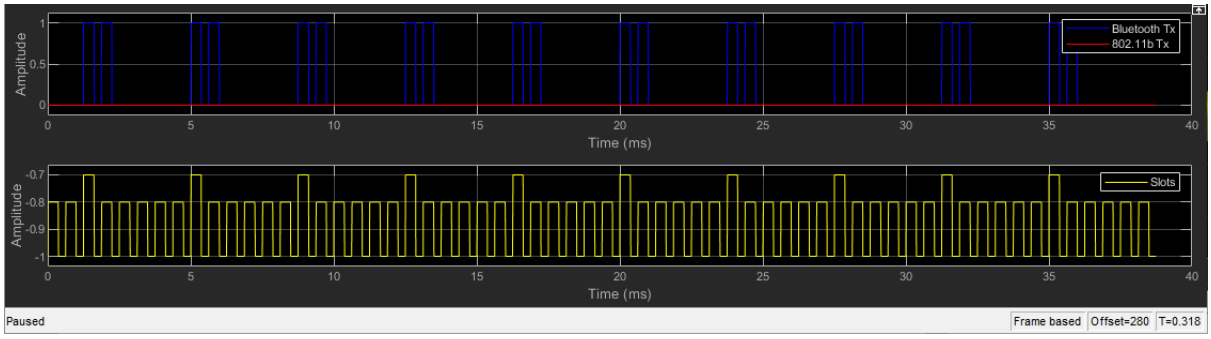
Slika 5.56. Vremenski dijagram primljenog signala HV2/None/1&2

Na slici 5.56. se vidi da se primljeni Bluetooth signal pojavljuje u obliku bitova čiji je period 2.5 ms. Signal slota prikazuje kako se Bluetooth signal ponavlja nakon četiri uzastopna *slot*-a, odnosno nakon dva para vremenskih *slot*-ova.



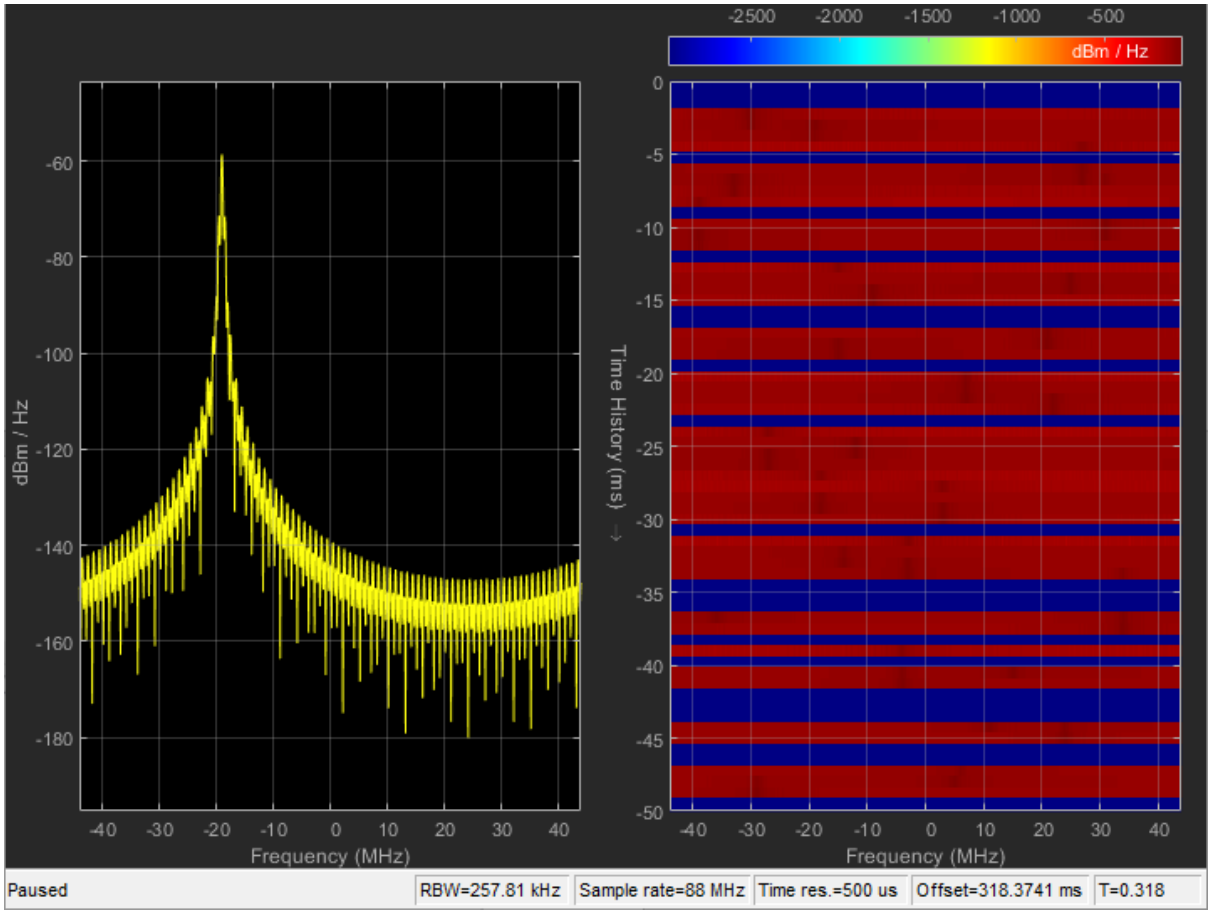
Slika 5.57. Spektar primljenog signala te spektrogram kanala HV2/None/1&2

Signal s lijeve strane na slici 5.57. je predstavljen ravnom linijom, što označava da se radi o okolini u kojoj su isključeni šumovi – aditivni bijeli šum. S desne strane je graf koji označava odsutstvo interferirajućeg signala 802.11b. Slanje i primanje signala se odvija bez smetnji.



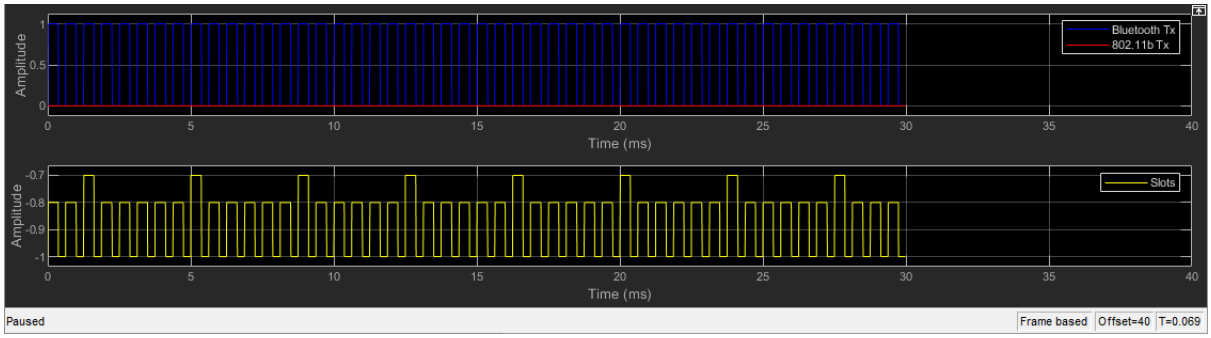
Slika 5.58 Vremenski dijagram primljenog signala HV3/None/1&2

Grafovi na slici 5.58. prikazuju primljeni signal koji je poslan u okruženju u kojemu su odsutni aditivni bijeli šum i interferirajući signal. Period u kojem se prenosi glas je 3.75 ms. Period trajanja jednog bita ponavlja se nakon šest uzastopnih *slot*-ova.



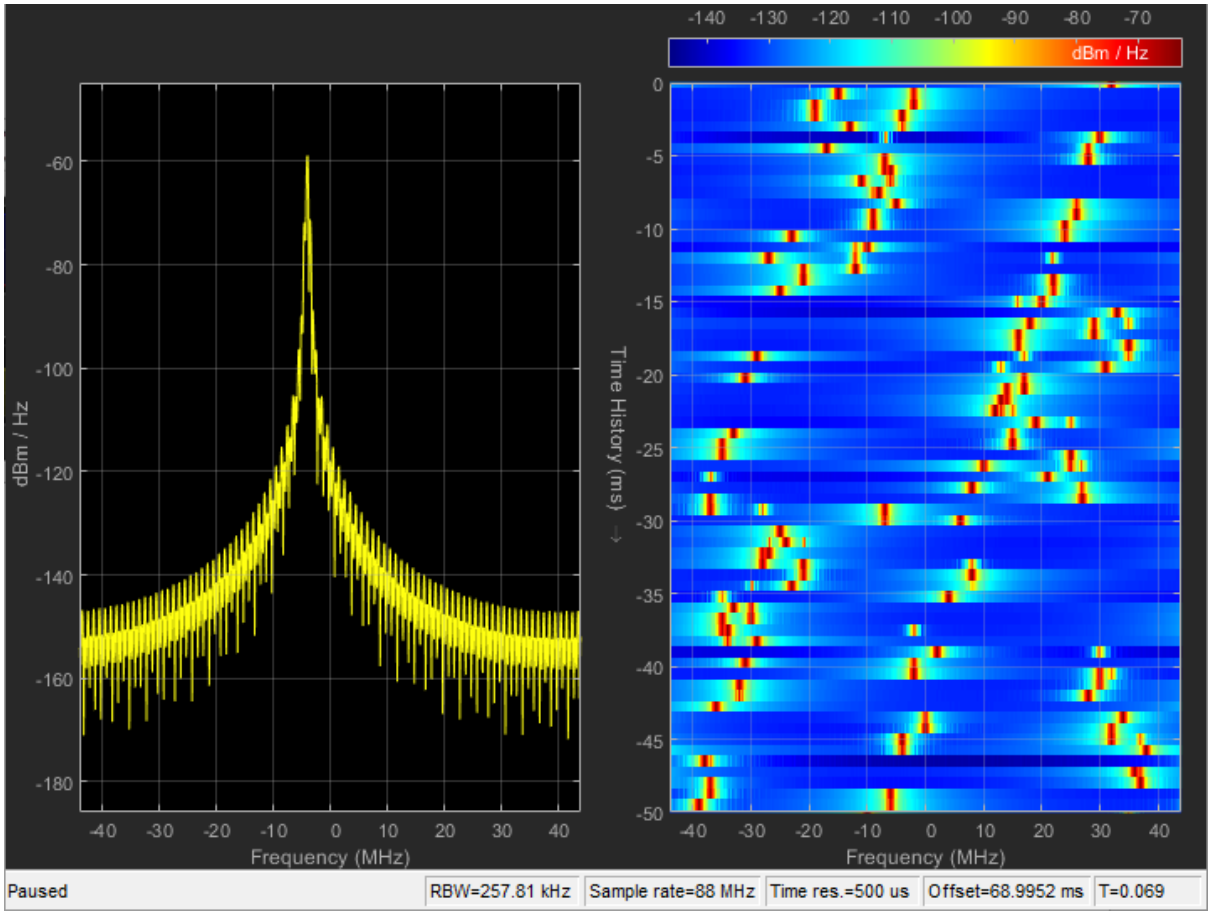
Slika 5.59. Spektar primljenog signala te spektrogram kanala HV3/None/1&2

Slika 5.59. prikazuje spektar primljenog Bluetooth signala u okruženju u kojem je izostavljen interferencijski signal, kao i aditivni bijeli šum. Budući da su paketi poslani u okruženju bez smetnji, na dvodimenzionalnom grafu je jasno vidljivo kako je Bluetooth signal prikazan u svom izvornom obliku.



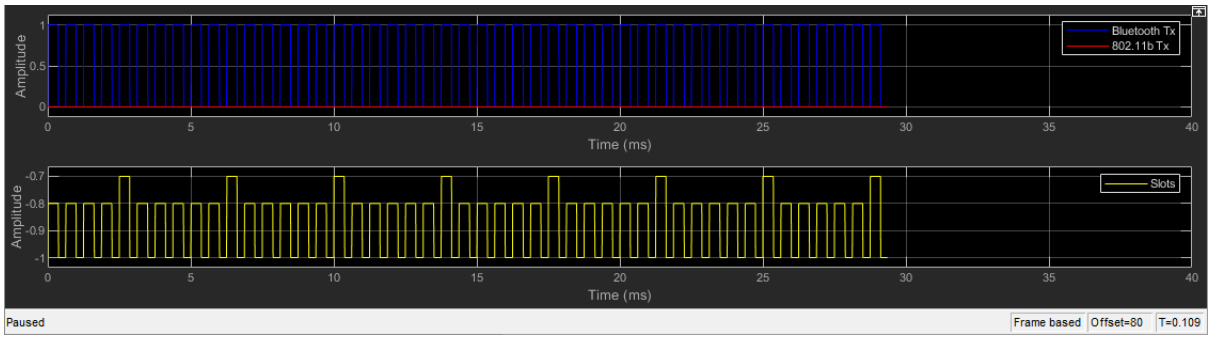
Slika 5.60. Vremenski dijagram primljenog signala DM1/None/1&2

Vremenski dijagram na slici 5.60. prikazuje primljeni Bluetooth signal u okruženju bez smetnji gdje su poslani paketi podatkovnog tipa DM1. Amplituda signala se periodički mijenja nakon 0.625 ms, što znači da je period slanja paketa 1.25 ms. Taj period odgovara vremenskom trajanju jednog para vremenskih *slot*-ova.



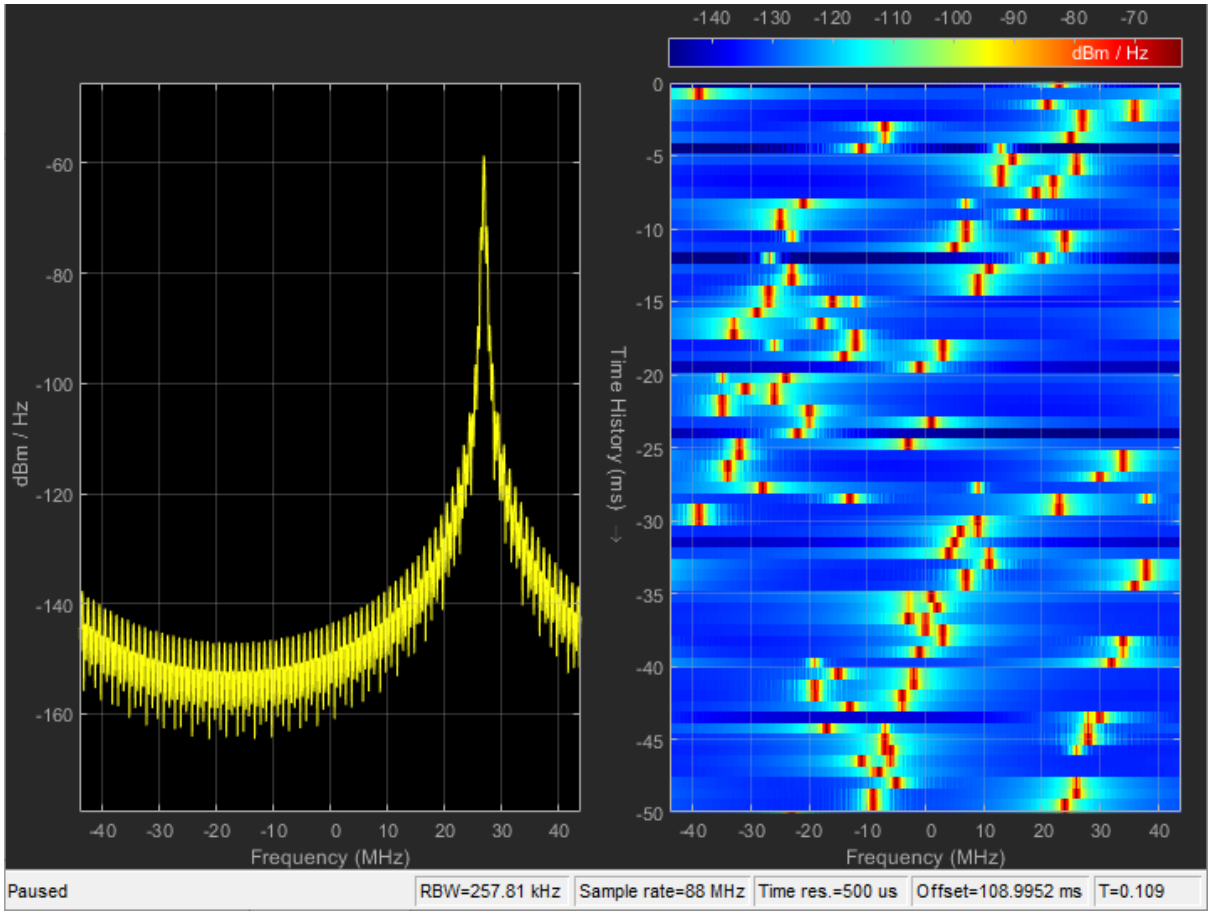
Slika 5.61. Spektar primljenog signala te spektrogram kanala DM1/None/1&2

Spektar primljenog signala na slici 5.61. prikazan je u okruženju bez šuma i interferencije. Nema izobličenja, te tako graf pokazuje izvorni spektar Bluetooth signala. Na trodimenzionalnom prikazu je vidljivo kako nema pojave interferencije uzrokovane 802.11b standardom.



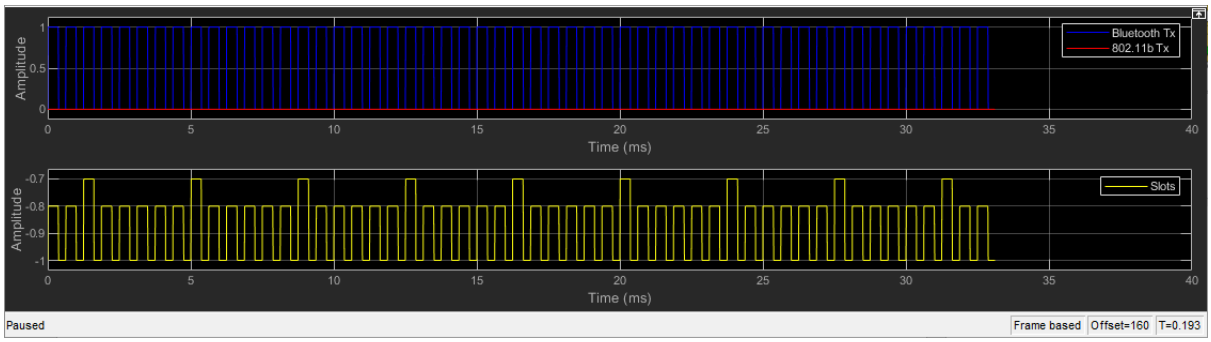
Slika 5.62. Vremenski dijagram primljenog signala SCORT/None/1&2

Prema vremenskom dijagramu na slici 5.62. može se zaključiti kako se amplituda periodički mijenja nakon 0.625 ms. Tako je period ponavljanja slanja jednog glasovnog paketa tipa SCORT 1.25 ms. Trajanje prijenosa jednog glasovnog paketa odgovara vremenskom periodu jednog para vremenskih *slot*-ova.



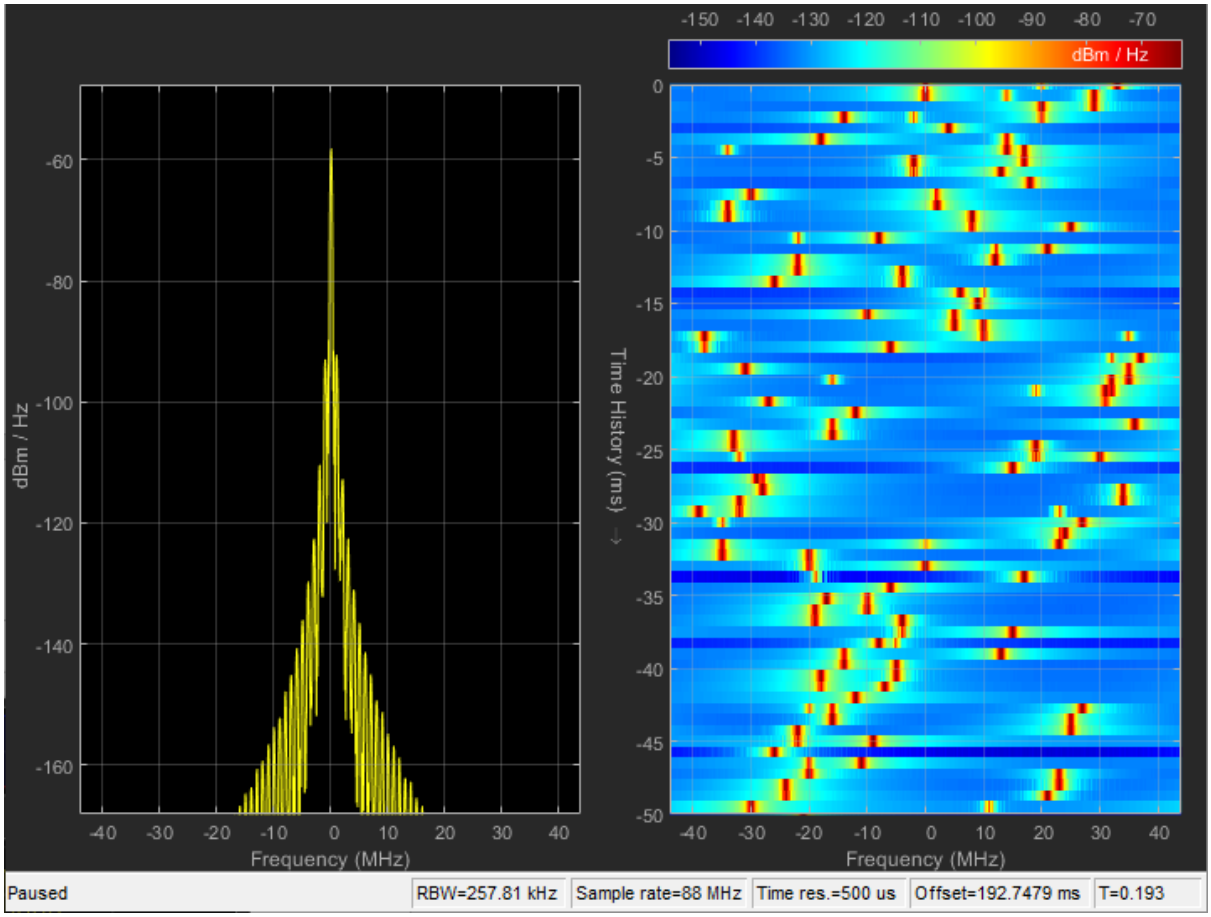
Slika 5.63. Spektar primljenog signala te spektrogram kanala SCORT/None/1&2

Promatranjem spektra primljenog signala na slici 5.63. može se uočiti da se primljeni signal nalazi u standardnom obliku. Nema odstupanja od izvornog oblika, zato što su iz okoline izvođenja simulacije isključeni aditivni bijeli šum i signal interferencije.



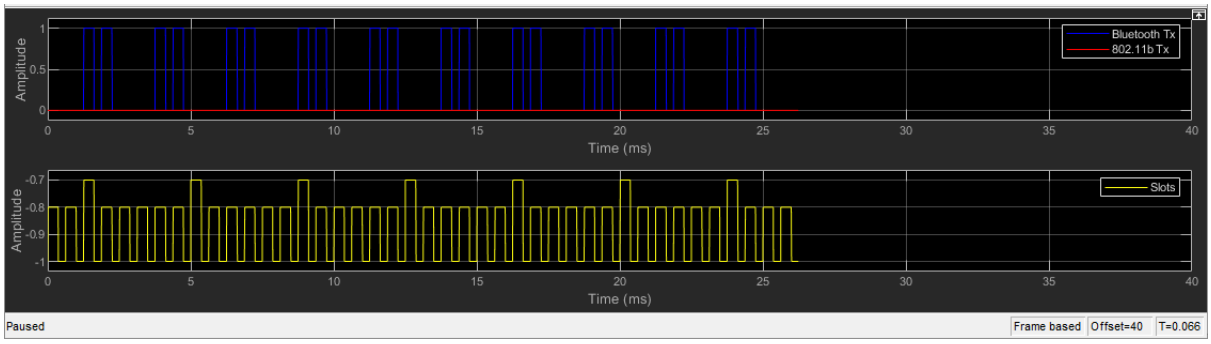
Slika 5.64. Vremenski dijagram primljenog signala HV1/None/3&4

Vremenski dijagram primljenog signala na slici 5.64. prikazuje Bluetooth signal kojim se prenose glasovni paketi HV1 u okolini bez smetnji. Može se primijetiti kako se amplituda mijenja svakih 0.625 ms, te stoga period slanja jednog paketa iznosi 1.25 ms. Taj period odgovara trajanju jednog para vremenskog *slot*-a.



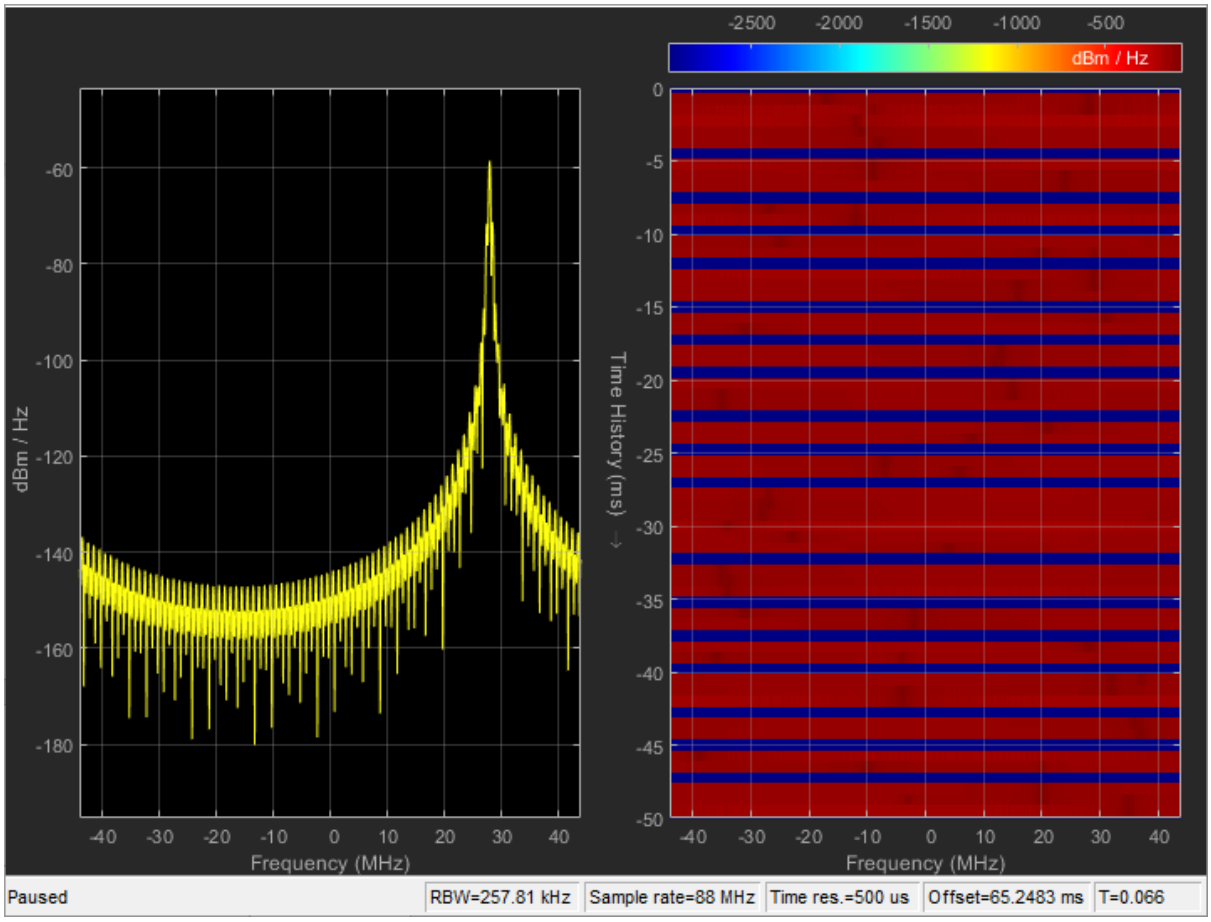
Slika 5.65. Spektar primljenog signala te spektrogram kanala HV1/None/3&4

Grafički prikaz na slici 5.65. prikazuje Bluetooth signal koji je također i u ovome slučaju u svom izvornom obliku.



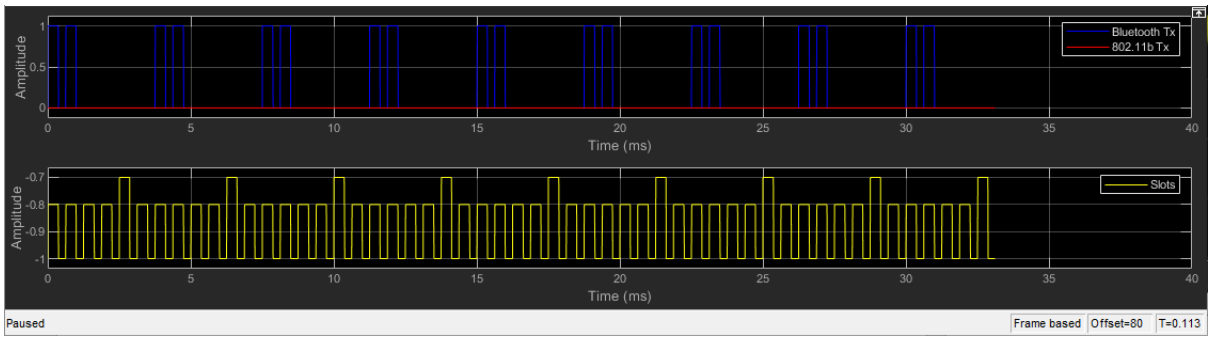
Slika 5.66. Vremenski dijagram primljenog signala HV2/None/3&4

Vremenski dijagram na slici 5.66. prikazuje primljeni signal u slučaju kada su slani glasovni paketi tipa HV2. Uspoređujući primljeni signal i signal slot-a, može se primijetiti kako je period slanja jednog paketa jednak vremenu trajanja četiriju uzastopnih vremenskih slot-ova.



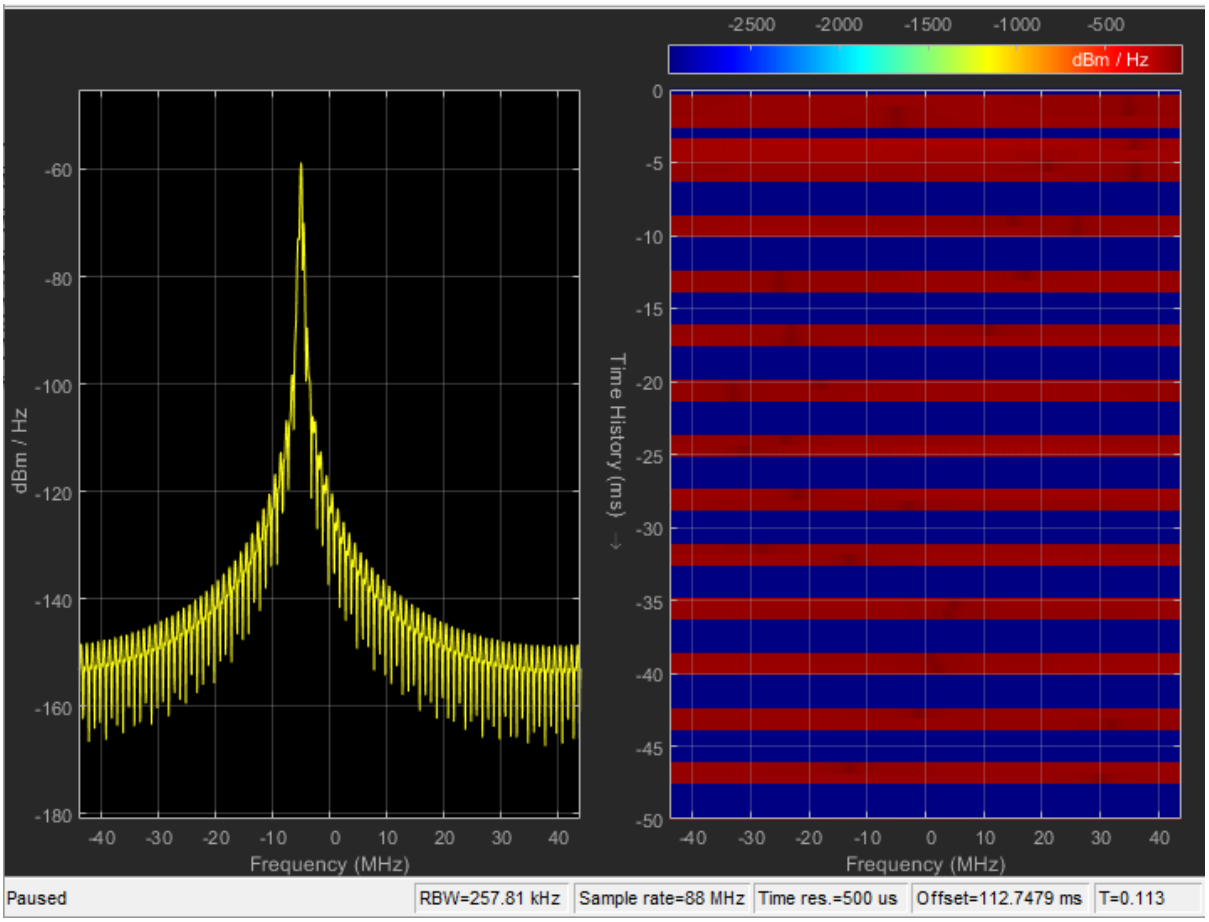
Slika 5.67. Spektar primljenog signala te spektrogram kanala HV2/None/3&4

Budući da se slanje odvija u okolini bez smetnji, na dvodimenzionalnom prikazu na slici 5.67. se ne mogu primijetiti nikakva odstupanja kod primljenog signala.



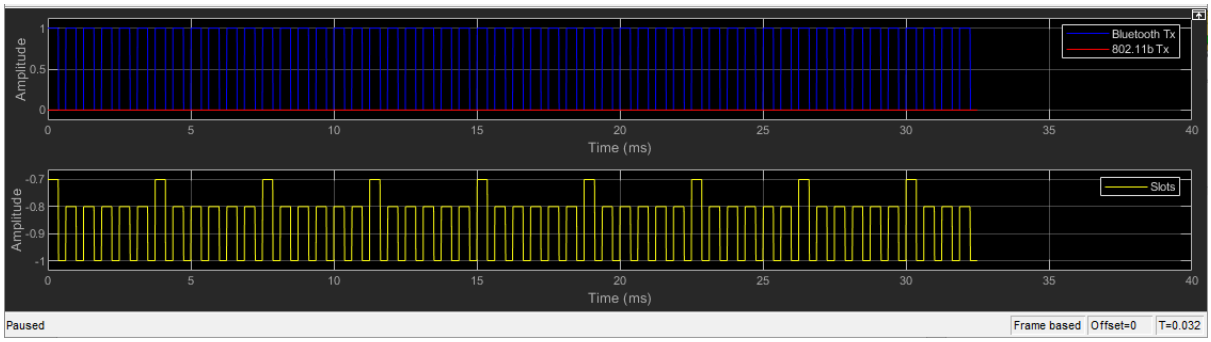
Slika 5.68. Vremenski dijagram primljenog signala HV3/None/3&4

U slučaju kada se šalju glasovni paketi tipa HV3, u okruženju bez smetnji, promatranjem slike 5.68. može se primijetiti kako se glasovni paket šalje u periodu koji odgovara vremenu trajanja šest uzastopnih *slot*-ova, te je stoga period slanja jednog paketa u ovome slučaju 3.75 ms. Amplituda ima vrijednost jedan u trajanju od 1.25 ms, što znači da je amplituda jednaka nuli u periodu od 2.5 ms.



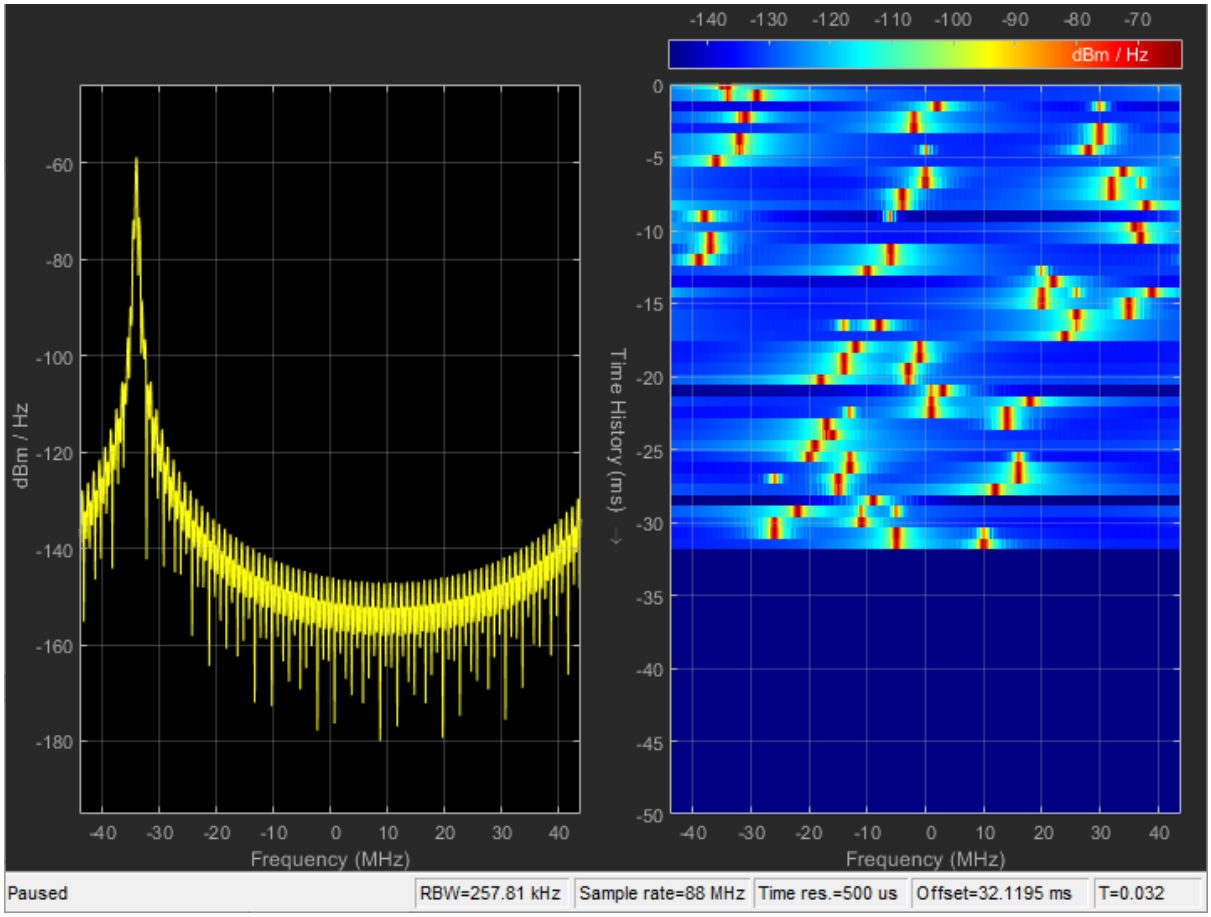
Slika 5.69. Spektar primljenog signala te spektrogram kanala HV3/None/3&4

Na slici 5.69. spektar primljenog signala nema nikakvih izobličenja. Najviša vrijednost snage je -58 dBm/Hz.



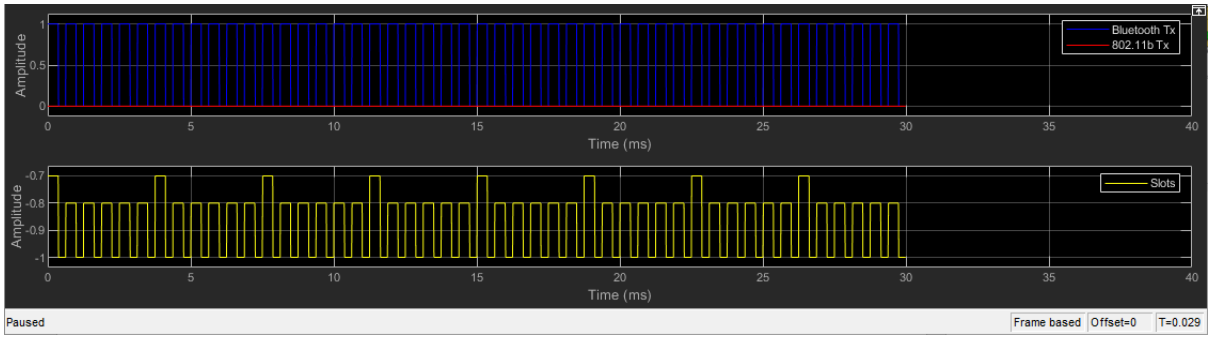
Slika 5.70. Vremenski dijagram primljenog signala DM1/None/3&4

Primljeni signal prikazan na vremenskom dijagramu na slici 5.70. ima period slanja podatkovnog paketa 1.25 ms. To znači da se za slanje jednog paketa koriste dva uzastopna vremenska *slot*-a, odnosno jedan par *slot*-ova.



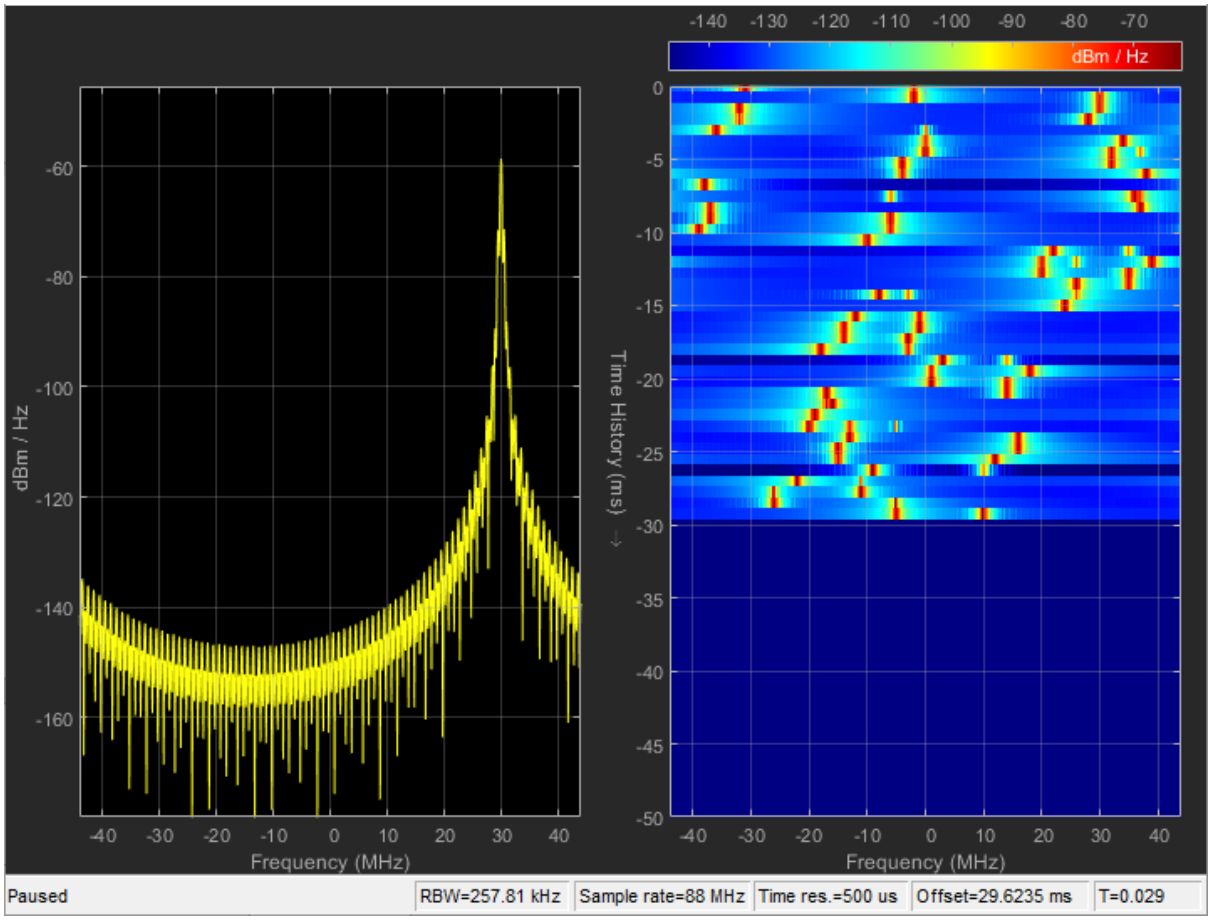
Slika 5.71. Spektar primljenog signala te spektrogram kanala DM1/None/3&4

Budući da se na spektru primljenog signala na slici 5.71. ne vide izobličenja, signal se nalazi u svom izvornom obliku, što i odgovara okruženju u kojem se šalju podatkovni paketi preko Bluetooth veze.



Slika 5.72. Vremenski dijagram primljenog signala SCORT/None/3&4

Promatranjem vremenskog dijagrama primljenog signala sa slike 5.72. , može se uvidjeti da je period prijenosa jednog paketa jednak vremenskom trajanju jednog para *slot*-a. Interferencijski signal kroz cijeli period ponavljanja ima vrijednost amplitude jednaku „0“, budući da je spomenuti signal isključen prilikom pokretanja simulacije.



Slika 5.73. Spektar primljenog signala te spektrogram kanala SCORT/None/3&4

Spektar signala prikazan na slici 5.73. nema nikakvih izobličenja, što i odgovara okruženju u kojemu je pokrenuta simulacija slanja SCORT paketa preko Bluetooth veze. Najviša vrijednost snage signala je, kao i u svim slučajevima, -58 dBm/Hz.

6. ZAKLJUČAK

Bluetooth, kao tehnologiju koja je još uvijek u procesu nastajanja, pronašli široku primjeni u raznovrsnim životnim krugovima, poslovima, gospodarstvima kao cjelini. Bluetooth je dizajniran kao niskoenergetsko rješenje za kontrolne i upravljačke aplikacije, te za uspostavljanje komunikacije male snage i potrošnje između različitih uređaja. Bluetooth ima slojevitu mrežnu arhitekturu. Jedno od najvažniji značajki Bluetooth-a je sigurnost, ali i svih ostalih IoT mreža, budući da IoT ima veliku važnost u skoro svim aktivnostima današnjeg čovječanstva. Postoje različiti *mod*-ovi kojima se garantira sigurnost prijenosa Bluetooth vezom, ali postoje tri stvari koje je najpotrebnije implementirati kako bi se zaštitili IoT uređaji, a to su: mehanizam sakrivanja identiteta uređaja od neautoriziranog korisnika, zaštita protiv pasivnog prisluškivanja, te zaštita protiv *man-in-the-middle* napada.

Radi svojstava kao što su jednostavnost, niska potrošnja energije, isplativost i robusnost, BLE je pronašao široku primjenu te se može pronaći u telefonima, slušalicama, medicinskim uređajima i dr.

Prilikom analiziranja praktičnog dijela izvedenog u Matlab-u, može se zaključiti kako okruženje u kojemu se odvija prijenos podataka, najviše utječe na Bluetooth signal, odnosno najveće razlike se zapažaju na dvodimenzionalnim prikazima spektra primljenog Bluetooth signala. Promatrajući vremenske dijagram prijenosa paketa preko uspostavljene Bluetooth konekcije, za svaki tip podatka, bez obzira odvija li se prijenos u okruženju u kojemu je prisutan šum ili uz njega i interferencijski signal, vrijeme potrebno da se prenese jedan glasovni ili podatkovni paket ostaje dosljedno teorijskom vremenu.

SAŽETAK

Internet of things ili IoT je nova vrsta umrežene paradigme koja je pomoću interneta proširena diljem svijeta. Glavni cilj je povezati mnoštvo heterogenih uređaja korištenjem različitih komunikacijskih tehnologija. IoT sa sobom nosi mnoštvo dobrih stvari kao što su napredak u društvenom razvoju i ekonomski dobici.

Jedan od glavnih oblika bežične tehnologije koja se koristi u razvoju IoT-a je Bluetooth. Jedna od glavnih primjena Bluetooth-a je razmjena podataka između fiksnih i mobilnih bežičnih uređaja unutar kratkog dometa. Bluetooth Low Energy standardi su Bluetooth tehnologija koja je dizajnirana kako bi se omogućilo što jednostavnije uparivanje uređaja.

Cilj ovoga rada je istraživanje sigurnosti i sigurnosnih nedostataka Bluetooth-a, kakva poboljšanja pruža šifriranje i razmjena ključeva, te analiziranje ponašanja Bluetooth signala u okruženjima u kojemu se generiraju smetnje različitog tipa.

Ključne riječi: Bluetooth, Bluetooth Low Energy (BLE), Internet stvari, Simulacija dvosmjernog prijenosa glasa i podataka putem Bluetooth-a

ABSTRACT

The Internet of Things or IoT is a new kind of networking paradigm that has been expanded around the world using the Internet. The main goal is to connect a mulitple of heterogeneous devices using different communication technologies. The IoT carries with it a various of good things such as progress in social development and economic gains.

One of the main forms of wireless technology used in the development of IoT is Bluetooth. One of the main applications of Bluetooth is the exchange of data between fixed and mobile wireless devices within short range. Bluetooth Low Energy standards are Bluetooth technology designed to make pairing as easy as possible.

The aim of this paper is to investigate the security and security flaws of Bluetooth, what improvements are provided by encryption and key exchange, and to analyze the behavior of Bluetooth signals in environments in which different types of interference are generated.

Keywords: Bluetooth, Bluetooth Low Energy (BLE), Internet of Things, Full Duplex transmission

ŽIVOTOPIS

Ana-Marija Damjanović je rođena 5.9.1996. u Vinkovcima, Republika Hrvatska. Pohađala je Osnovnu školu fra Ilije Starčevića u Tolisi, te je nakon završene osnovne škole upisala Opću gimnaziju u Školskom centru fra Martina Nedića Orašje koju je završila 2015. godine. Nakon završene srednje škole upisuje preddiplomski sveučilišni studij elektrotehnike na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, te se na drugoj godini opredjeljuje za smjer Komunikacije i informatika. Godine 2018. završava sveučilišni preddiplomski studij, te iste godine upisuje diplomski studij smjer Mrežne tehnologije.

LITERATURA

[1] K. Lounis, M. Zulkernine, „Attacks and Defenses in Short-Range Wireless Technologies for IoT", IEEE Access, April 2020.

[2] Á. Hernández Solana et al., „Bluetooth Mesh Analysis, Issues, and Challenges", IEEE Access, March 26, 2020.

[3] Angela M. Lonzetta, Peter Cope, Joseph Campbell, Bassam J. Mohd and Thaier Hayajneh, „Security Vulnerabilities in Bluetooth Technology as Used in IoT", Journal of sensor and actuator networks, July, 2018. Dostupno na: https://www.mdpi.com/2224-2708/7/3/28

[4] P. Madaan, S. Gupta, „Implementing BLE Security in IoT Applications", Electronic Design. Dostupno na: https://www.electronicdesign.com/industrial-automation/document/21807085/implementing-ble-security-in-iot-applications-pdf-download:

[5] Albert F. Harris III, Vansh Khanna, Güliz Tuncay, Roy Want, and Robin Kravets

[6] Giwon Kwon, Jeehyeong Kim, Jaewon Noh, Sunghyun Cho, Department of Computer Science and Engineering, Hanyang University, Ansan, Republic of Korea, „Bluetooth Low Energy Security Vulnerability and Improvement Method", IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 2016

[7] Carles Gomez , Joaquim Oller, Josep Paradells, „Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology", Universitat Politècnica de Catalunya, December, 2012

[8] Are all bluetooth security device secure?, dostupno na: https://www.infoguardsecurity.com/are-all-bluetooth-security-device-secure/, pristupljeno: 20.1. 2021.

[9] Seyed Mahdi Darroudi, Carles Gomez ,Department of Network Engineering, „Bluetooth Low Energy Mesh Networks: A Survey", Universitat Politècnica, 22 June, 2017

[10] Muhammad Rizwan Ghori, Tat-CheeWan, Gian Chand Sodhy, „Bluetooth Low Energy Mesh Networks: Survey of Communication and Security Protocols",

[11] Security Considerations For Bluetooth Smart Devices, dostupno na: https://www.design-reuse.com/articles/39779/security-considerations-for-bluetooth-smart-devices.html, pristupljeno: 22.1.2021.

[12] Introduction to BLE security for IoT, dostupno na: https://www.simform.com/iot-bluetooth-security-vulnerabilities/, pristupljeno: 20.1.2021.

[13] Waspmote - Wireless Sensor Networks Open Source Platform, dostupno na: https://www.cooking-hacks.com/documentation/tutorials/waspmote.html, pristupljeno: 20.4.2021.

[14] Architecture and system, dostupno na: https://development.libelium.com/waspmote-technical-guide/architecture-and-system, pristupljeno: 20.4.2021.

[15] Introduction - BLE Networking Guide, dostupno na: https://development.libelium.com/ble-networking-guide/introduction, pristupljeno: 3.5..2021.

[16] Anil Mathew, Nithin Chandrababu, Khaled Elleithy, and Syed Rizvi, IEEE 802.11 & Bluetooth Interference: Simulation and Coexistence, Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT 06604

[17] Connecting Waspmote to other BLE devices, dostupno na: https://development.libelium.com/ble-networking-guide/connecting-waspmote-to-other-ble-devices?fbclid=IwAR1ljdUtsunAsRvYuhwkSGXX2OG-fKJhCACyQhSE9QEBfxgHoJLw0lqtitk, pristupljeno: 3.5.2021.

[18] Bluetooth Full Duplex Voice and Data Transmission, dostupno na: https://www.mathworks.com/help/comm/ug/bluetooth-full-duplex-voice-and-data-transmission.html, pristupljeno 15.6.2021.

[19] Choosing an HV Packet Type, dostupno na: https://www.fishercom.xyz/bluetooth-technology/choosing-an-hv-packet-type.html, pristupljeno: 20.6.2021.

[21] Packet Settings:Packet Type Property, dostupno na: https://zone.ni.com/reference/en-XX/help/373431L-01/lvbtanalysisprop/attr3/, pristupljeno 25.6.2021.

[22] Radosveta Sokullu, Engin Karatepe, Adaptive packet selection algorithm for bluetooth data packets, Department of Electrical and Electronics Engineering, Ege University, 35100 Bornova, Izmir, Turkey, April 15-17, 2007

[23] Alf Helge Omre, Bluetooth Low Energy: Wireless Connectivity for Medical Monitoring, Journal of Diabetes Science and Technology, March 2010

[24] Jonathan Bjarnason, Evaluation of Bluetooth Low Energy in Agriculture Environments ,An empirical analysis of BLE in precision agriculture, Department of Computer Science and Engineering, Spring 2016

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

[26] Christian Poellabauer, Pramita Mitra , Using Bluetooth Low Energy for Dynamic Information-Sharing in Vehicle-to-Vehicle Communication, SAE International Journal of Passenger Cars - Electronic and Electrical Systems, March 2017

[27] Samuel Townsend, Mark E. Larsen, Tjeerd W. Boonstra, Helen Christensen,Using Bluetooth Low Energy in smart phones to map social networks, Black Dog Institute, University of New South Wales, Sydney, Australia

[28] Marco Terán, Juan Aranda and Henry Carrillo, Diego Mendez and Carlos Parra, IoT-based System for Indoor Location using Bluetooth Low Energy, Escuela de Ciencias Exactas e Ingeniería Universidad Sergio Arboleda - Bogotá, Colombia, Pontificia Universidad Javeriana - Bogotá, Colombia, IEEE, 2017

[29] Cosero, Find My Keys! Object Localization and Retrieval Using Bluetooth Low Energy Tags, dostupno na: https://link.springer.com/chapter/10.1007/978-3-319-18615-3_16, pristupljeno 10.7.2021.