Ometači prijenosa signala u bežičnim komunikacijskim mrežama

Benčević, Zvonimir

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

Sveučilišni studij

OMETAČI PRIJENOSA SIGNALA U BEŽIČNIM KOMUNIKACIJSKIM MREŽAMA

Završni rad

Zvonimir Benčević

Osijek, 2019.

SADRŽAJ

1. UVOD

U današnje vrijeme svatko uz sebe ima barem jedan uređaj koji koristi neku vrstu bežične tehnologije. Bio to mobilni telefon, tablet, laptop, bežične slušalice ili ključ od automobila. Da se zaključiti da su bežične mreže u širokoj upotrebi. Bežično povezivanje ne zahtijeva fizičku infrastrukturu kao što su kablovi i pristupne točke koje će omogućiti pristup vezi jer se signal slobodno širi prostorom. Takva vrsta prijenosa signala ranjiva je i nesigurna te može doći do ugrožavanja privatnosti korisnika, krađe podataka i u konačnici financijske štete ukoliko se adekvatno ne zaštiti. Važno je poznavati principe prijenosa, ali i ometanja prijenosa signala u bežičnim mrežama kako bi podatke mogli zaštiti i sigurno prenositi.

U poglavlju „Bežične mreže“ obrađene su osnove bežičnih mreža, spomenuto je kakve sve vrste bežičnih mreža postoje te kako bežične mreže funkcioniraju. Također je objašnjen princip prijenosa informacija putem bežičnih mreža. Glavno poglavlje, „Ometanje prijenosa signala bežičnih mrežama“, obrađuje tematiku ometanja signala te raznih tehnika koje se koriste kako bi se signal ometao. U tom je poglavlju objašnjeno namjerno i nenamjerno ometanje signala. Poglavlje „Zaštita od ometanja prijenosa signala bežičnim mrežama“ opisuje moguće načine zaštite od ometanja koji će omogućiti siguran prijenos informacija. Poglavlje „Izrada uređaja za ometanje signala“ prikazuje što je sve potrebno za izradu uređaja za ometanje signala te analizu izrađenog signala.

1.1. Zadatak završnog rada

U okviru završnog rada zadatak je proučiti princip rada bežičnih mreža. Budući da je naglasak rada na tematici ometanja prijenosa signala, potrebno je dati pregled načina ometanja prijenosa signala, obraditi načine namjernog i nenamjernog ometanja prijenosa signala te proučiti različite načine ometanja i zaštite od ometanja prijenosa signala. Također je potrebno izraditi odabrani uređaj za ometanje određenog tipa bežičnog signala (mobilna mreža, WI-FI mreža, TV mreža) i analizirati primljeni signal uz ometanje i bez ometanja.

2. BEŽIČNE MREŽE

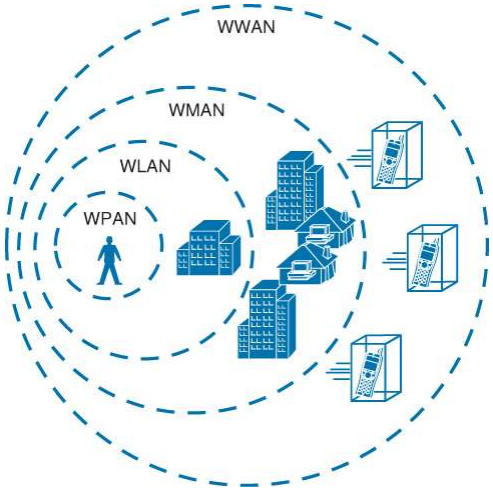
Bežične mreže su komunikacijske mreže u kojima se kao medij preko kojeg se šalju podatci koriste radio valovi. Koriste se u slučajevima kada žičanu mrežu nije moguće uspostaviti ili je isplativija nego žičana. Bežične mreže u odnosu na žične nude prednosti kao što su jednostavnost i brzina spajanja, mobilnost te lakše proširivanje. U bežične mreže spadaju sve mreže koje koriste radio valove kao medij za prijenos podataka kao na primjer Wi-Fi, Bluetooth, mobilni signal, tv signal, satelitski signal i mnogi drugi[1].

2.1. Princip rada bežičnih mreža

Do sada nije realizirana idealna tehnologija koja bi zadovoljila zahtjeve svih korisnika u pogledu brzine, pokrivenosti, sigurnosti i kvalitete usluga. Da je razvoj bežičnih mreža vrlo dinamičan dokazuje nam često uvođenje novih komunikacijskih protokola, tehnologija i standarda. Prema [2] trenutno postoji nekoliko vrsta telekomunikacijskih mreža koje su radi razvoja sustava prešle sa fiksnih tehnologija na bežične tehnologije:

- Bežična osobna mreža – WPAN(Wireless Personal Area Network)
- Bežična lokalna mreža - WLAN(Wireless Local Area Network)
- Bežična velegradska mreža - WMAN(Wireless Metropolitan Area Network)
- Bežična širokopojasna mreža - WWAN(Wireless Wide Area Network)

Ove bežične mreže su pojedinačno modificirane tako da svaka od njih zadovolji zahtjeve korisnika u tom području za koje je namijenjena. Zahtjevi za svaku pojedinačnu namjenu baziraju se na parametrima kao što su: potrebna širina opsega, brzina prijenosa, potrebna udaljenost, snaga, lokacija korisnika, ponuđene usluge[3].



Slika 2.1 Grafički prikaz vrsta bežičnih mreža

Princip rada bežičnih mreža je dosta sličan. Kod širokopojasnih telekomunikacijskih mreža pošiljatelj obavi poziv, pošalje SMS, sliku ili video drugom korisniku. Analogni podaci postaju digitalni nakon što dođu uređaja pošiljatelja te potom dolazi do njihove kompresije. Komprimirani podaci dijele se na malene segmente, tzv. 'pakete' koji se povezuju s adresom primatelja i daljnji put nastavljaju zasebno. Najbliža bazna stanica prikuplja te podatke te ih prosljeđuje dalje u ovisnosti gdje se nalazi primatelj. U slučaju da je primatelj blizu, bazna stanica će poslati tu poruku odmah primatelju. U slučaju da je primatelj na drugom kontinentu tada će podatci otići do sljedeće mobilne stanice pa do glavne centrale. Pošto su podatci namijenjeni za međunarodni prijenos, moraju ići do telekomunikacijskog tornja pa se šalju do zemaljske satelitske postaje. Ovisno o mogućnostima, podatci se dalje šalju preko satelita ili prekooceanskim kablom do drugog kontinenta i cijeli proces se odvija unatrag dok konačno podatci ne dođu do primatelja[4].

Bežične lokalne mreže, kao na primjer WLAN, mogu biti povezane i konfigurirane od strane korisnika koji žele komunicirati bez potrebe za infrastrukturom ili kao infrastrukturalne mreže. U režimu rada gdje je mreža konfigurirana od strane korisnika, uređaji su direktno povezani jedan s drugim dok u infrastrukturalnom režimu postoji pristupna točka koja je spojena na pružatelja usluge bežične mreže te se na tu pristupnu točku spajaju korisnici.

Razvoj novih bežičnih tehnologija zasnovan je na principu pristupa bežičnim uređajima pomoću instaliranja malih ćelija ili pristupnih čvorova, koji su povezani u grupe bržim sustavom komunikacije, a pri tome se ostvaruje suradnja unutar grupe kako bi se zajednički upravljalo resursima. S obzirom na to u kojem smjeru idu mobilne telekomunikacijske mreže, koncept "ćelijske" organizacije mreže će biti zamijenjen "kooperativnim" mrežama, pri čemu će najveći dio infrastrukture baznih stanica biti zamijenjen povezanim podmrežama malih ćelija.

2.2. Frekvencijski opseg

Frekvencijski opseg je raspon frekvencija koje se koriste za komunikaciju u području za koje su namijenjene.

Kratica	Naziv	Raspon frekvencije	Valna duljina	Primjena
ELF	Ekstremno niska frekvencija	3 Hz do 30 Hz	100 mm do 10 mm	Komunikacija podmornica
SLF	Superniska frekvencija	30 Hz do 300 Hz	10.000 km do 1.000 km	Komunikacija podmornica
ULF	Ultraniska frekvencija	300 Hz do 3 kHz	1.000 km do 100 km	Komunikacija u rudnicima
VLF	Jako niska frekvencija	3 kHz do 30 kHz	100 km do 10 km	Komunikacija podmornica, geofizika, bežični EKG monitori
LF	Niska frekvencija	30 kHz do 300 kHz	10 km do 1 km	Navigacija, AM odašiljanje
MF	Srednja frekvencija	300 kHz do 3 MHz	1 km do 100 m	AM odašiljanje
HF	Visoka frekvencija	3 MHZ do 30 MHz	100 m do 10 m	Amaterski radio, vojne komunikacije
VHF	Vrlo visoka frekvencija	30 MHz do 300 MHz	10m do 1m	FM odašiljanje, televizija
UHF	Ultra visoka frekvencija	300MHz do 3GHz	1 m do 10 cm	Televizija, mobilna telefonija, bežične LAN mreže, Bluetooth
SHF	Supervisoka frekvencija	3 GHz do 30 GHz	10 cm do 1 cm	Bežične LAN mreže, radar
EHF	Ekstremno visoka frekvencija	30 GHz do 300 GHz	1 cm do 1 mm	Radioastronomija, mikrovalni radio visokih brzina

Tablica 2.1. Raspodjela frekvencijskog opsega.

2.3. Širina kanala

Širina kanala je razlika između gornje i donje frekvencije u kontinuiranom frekvencijskom pojasu. Obično se mjeri u Hertzima(Hz), a ovisno o kontekstu, može se posebno odnositi na propusnost propusnog opsega ili propusnost osnovnog pojasa. Propusnost propusnog opsega je razlika između gornje i donje granične frekvencije, na primjer, filtra za pojasnu propusnost, komunikacijskog kanala ili spektra signala. Širina pojasa za osnovni pojas primjenjuje se na filtar niskih prolaza ili signal osnovnog pojasa; širina pojasa jednaka je njegovoj gornjoj graničnoj frekvenciji. Frekvencijska širina kanala određena je svojstvima informacije i modulacijskim postupkom, a kod digitalnih sustava i metodom kompresije (npr. govor do 10 kHz, prenosi se od 300 do 3400 Hz, TV signal do 5 MHZ x 3 signala boje)[5].

2.4. Prijenos informacija

Da bi se informacije prenosile komunikacijskim kanalom potrebno je prvo prilagoditi signal koji se želi prenositi. To se radi pomoću modulacije. Prema [6] modulacija je postupak kojim se električni signal koji sadrži informacije prilagođava prijenosu željenim medijem. To podrazumijeva mijenjanje jednog ili više parametara prijenosnog signala u ovisnosti o signalu informacije. Mijenjati se mogu amplituda, faza i frekvencija. Modulacijom se informacija iz svog osnovnog opsega frekvencija transponira u viši frekvencijski pojas jer je lakše izraditi antene čije su dimenzije proporcionalne valnoj duljini zračenog signala te je analogno tome zračenje efikasnije.

Kada se govori o prijenosu signala pomoću radiovalova, tada imaju dvije opcije modulacije a to su analogna i diskretna. Analogne modulacije su Amplitudna modulacija(AM), Frekvencijska modulacija(FM) i Fazna Modulacija(PM). Bežične mreže većinom koriste digitalne modulacije signala. Kada bi se slao digitalni signal pomoću analogne modulacije, recimo amplitudne modulacije tada bi se moralo definirati koja promjena u amplitudi se odnosi na bit „1“ a koja promjena se odnosi na bit „0“. Drugim riječima, koju promjenu amplitude bi trebalo dodijeliti kojem bitu. Tako bi nastala digitalna amplitudna modulacija odnosno diskretna modulacija amplitude.

Za prijenos informacija putem modernijih bežičnih mreža koristi se kvadraturna diskretna modulacija amplitude(QAM) jer se tom modulacijom može razmjenjivati nekoliko bita po simbolu. QAM je kombinacija diskretne modulacije faze(PSK), konkretno kvaternarne diskretne modulacije faze(QPSK) i diskretne modulacije amplitude(ASK).

3. OMETANJE PRIJENOSA SIGNALA BEŽIČNIM MREŽAMA

Ometanje signala bežičnih mreža je ništa drugo nego emitiranje posebnog radio signala koji će stvoriti interferenciju sa signalom kojeg se želi ometati i smanjiti odnos signal/šum pod određenim uvjetima. Signal koji ometa mora biti na istoj frekvenciji kao i signal koji se želi ometati, modulacija tih signala mora biti ista te signal koji ometa mora biti jači, tj. mora imati veću snagu od signala kojeg se želi ometati[7].

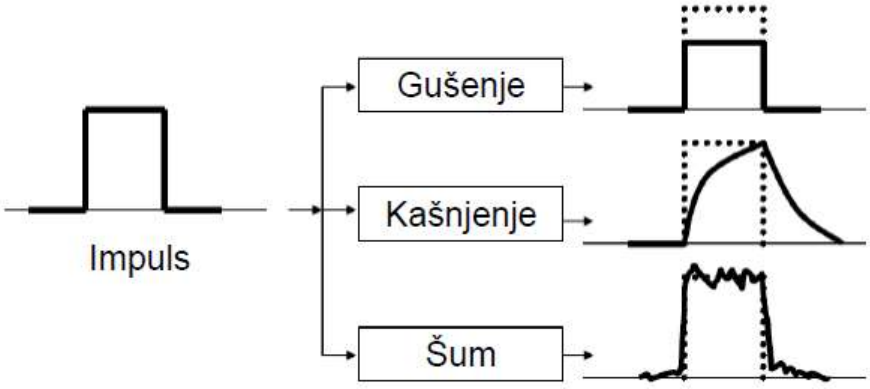
Kada govorimo o ometanju signala tada se javljaju različiti interesi i razlozi zbog kojih se neki signal ometa. Poznato je da je ometanje mobilnog i tv signala ilegalno jer svatko ima pravo pristupa javnom emitiranju signala te je zabranjeno ometati mobilni i tv signal. Moguće je korištenje uređaja za ometanje signala u svrhu osobne sigurnosti kao na primjer uređaj za ometanje signala GPS signala u slučaju da negdje postoji uređaj za praćenje zbog kojeg ste zabrinuti. Poznato je da su uređaji za ometanje signala također korišteni u svrhu krađe automobila i to u smislu da blokiraju signal ključa koji bi trebao dati informaciju automobilu da se zaključa.

Povijest ometanja signala seže još u početke komunikacijskih sustava u Drugom svjetskom ratu. Tada je interes bio ometati komunikaciju neprijatelja te na taj način utjecati na spremnost vojske. I tada su se razvijale tehnike koje bi spriječile ometanje. Mijenjale bi se frekvencije emitiranja, snaga bi se pojačavala i radile bi se usmjerene antene. Nisu se ometale samo vojne komunikacije nego i civilni radio kako bi se spriječio neželjeni protok informacija unutar i van država.

3.1. Nenamjerno ometanje prijenosa signala bežičnim mrežama

Do nenamjernoga ometanja signala može doći ako emitiramo signal na nekoj frekvenciji koju nismo prethodno provjerili koristi li se ili ne. Na prijenos signala i kvalitetu prijema utječu atmosferske prilike i prepreke poput zidova, zgrada i drveća. Smetnje se mogu pojaviti i kao posljedica loših atmosferskih prilika. Razni uređaji također mogu nenamjerno ometati prijenos signala, kao na primjer mikrovalna pećnica. Vibracije automobila i općenito prometa mogu također prouzrokovati smetnje kod prijenosa signala.

Do smetnje može doći tako što nastanu neželjene pojave u komunikacijskom kanalu. Može doći do šuma, gušenja kanala(atenuacije) i kašnjenja signala. Prema [8] šum se može objasniti kao spontane električne fluktuacije. Može se pojaviti na većini komponenata u komunikacijskom sustavu. Na ulazu u prijemnik može se naći šum iz prirodnih izvora i umjetno generirani šum. U prijemniku postoje izvori šuma koji dodatno povećavaju snagu ukupnog šuma. Na odašiljačkoj strani postoji kvantizacijski šum u postupku digitalizacije. Gušenje se manifestira tako što se jačina signala smanji. Razina gušenja ovisi o vrsti prijenosnog medija i o frekvenciji signala – gušenje je intenzivnije s porastom frekvencije. Kompenzaciju gušenja vršimo uporabom pojačala. Zbog različitog vremena kašnjenja spektralnih komponenti signala nastaju izobličenja. Izobličenja nastala zbog djelovanja komunikacijskog kanala ispravljaju se uporabom ekvalizatora.



Slika 3.1. Utjecaj smetnje na impuls.

3.2. Namjerno ometanje prijenosa signala bežičnim mrežama

Namjernim ometanjem prijenosa signala smatra se nekakav aktivan napad na ciljanu komunikaciju. Kao ishod ometanja signala pojavljuju se smetnje u radu uređaja i općenito smetnje u održavanju komunikacije. Namjerno ometanje signala se , u ovisnosti o namjeri, može postići na nekoliko načina. Ako se želi samo ometati prijenos signala bez namjere za otkrivanjem sadržaja, to se može učiniti emitiranjem signala koji će se interferirati sa signalom kojeg se želi ometati. U slučaju da se želi saznati neka informacija iz signala tada je potrebno spojiti se na željeni signal te određenim napadima oslabiti zaštitu i u konačnici otkriti informacije[9].

Većina tehnika za ometanje prijenosa signala mogu u nekoj mjeri ometati signal, a mogu i potpuno onemogućiti prijenos signala. Potpuno onemogućavanje prijenosa signala naziva se *DoS*(eng. Denial of Service) napad. *DoS* napad se svodi na to da se signal zatrpa mnoštvom signala ili jednim jakim signalom koji će onemogućiti komunikaciju. Kada bi dvije osobe stajale same u praznom prostoru na udaljenosti od nekoliko koraka tada bi mogle normalno razgovarati bez poteškoća, no ako bi prostorija bila puna ljudi koji žele uspostaviti razgovor s jednom osobom tada bi se to mogao nazvati *DoS* napad na tu osobu. Ometanje pomoću šuma jedan je od jednostavnijih načina ometanja prijenosa signala. Količina ometanja koju će proizvesti taj šum ovisi o snazi emitiranoga šuma. Dovoljno jaki šum može potpuno nadjačati bežični signal i tako izvesti *DoS* napad. Ako se želi ometati neki signal koji prenosi zvučne informacije tada se mogu emitirati glasovi i zvukovi koji će ometati prijenos signala. Ishod ometanja pomoću zvukova također ovisi o jačini signala koji se emitira.

3.3. Zaštita od ometanja prijenosa signala bežičnim mrežama

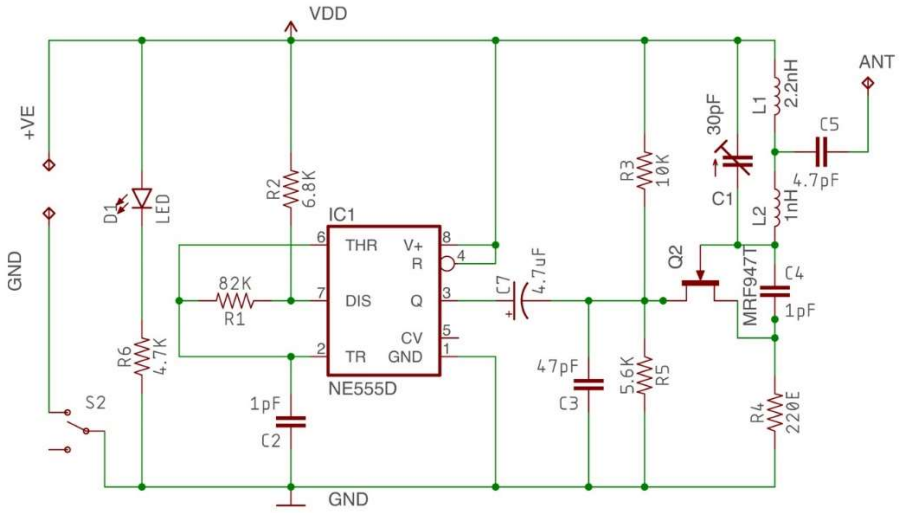
U realnim uvjetima prijenosa, ne može se utjecati na sve smetnje. Neke se mogu ukloniti dok neke ne mogu primjerice smetnje u kanalu. Zato postoje različiti postupci kojima se može povećati zaštita komunikacijskog sustava od smetnji. Vrste zaštite nisu identične za analogne i diskretne sustave. Kod analognih sustava se smetnje mogu smanjiti ponavljanjem informacije, smanjenjem veličine informacije te također i promjenama nekih parametara kao što su snaga odašiljača i indeks modulacije. Za diskretne sustave vrijede iste metode kao i za analogne sustave, ali postoje i dodatne metode. Informacija koja se prenosi se može organizirati u kanalne kodove koji su prilagođeni vrsti informacije i prijenosnom mediju. Također se kod diskretnih sustava mogu dodavati različiti algoritmi šifriranja i kodiranja signala.

Davatelji bežičnih usluga kao što su mobilni signal, tv signal i radio signal mogu utjecati na ometanje signala tako što će osigurati dobru pokrivenost signalom. Ako se nalazimo na velikoj udaljenosti od odašiljača signala, tada možemo utjecati na smetnje tako što ćemo spojiti antenu s adekvatnim dobitkom s obzirom u kakvom se području nalazimo. Kako bi se korisnik zaštitio od ometanja signala i krađe podataka u privatnim mrežama kao što je Wi-Fi treba koristiti najjači mogući sustav enkripcije. Moguće je ograničiti snagu signala kako taj signal ne bi bio vidljiv izvan zone u kojoj se koristi.

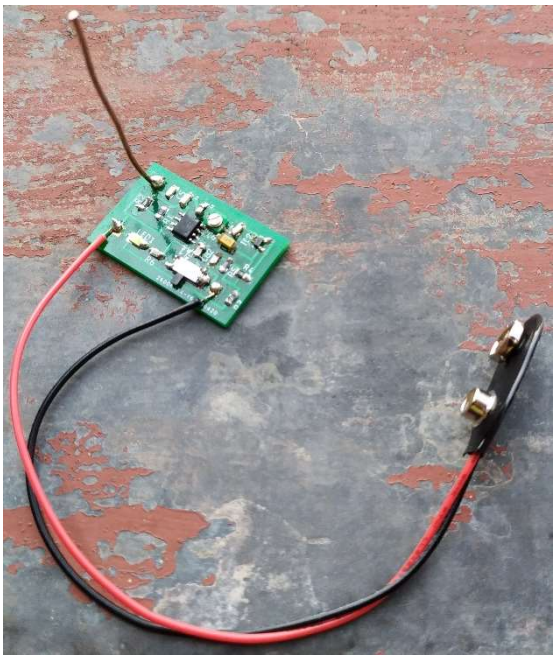
4. IZRADA UREĐAJA ZA OMETANJE SIGNALA

U sklopu završnog rada izrađen je uređaj za ometanje signala na frekvenciji 1550 MHz. Takav uređaj za ometanje signala se uz minimalne preinake može pomaknuti na frekvenciju 4G signala(1800 MHz), ali u radu to nije napravljeno kako se ne bi ometao 4G signal jer je to protuzakonito. Uređaji za ometanje signala se smiju upotrebljavati isključivo iz razloga nacionalne sigurnosti i obrane. Prema [10] potrebne komponente za izradu sklopa uređaja za ometanje signala su:

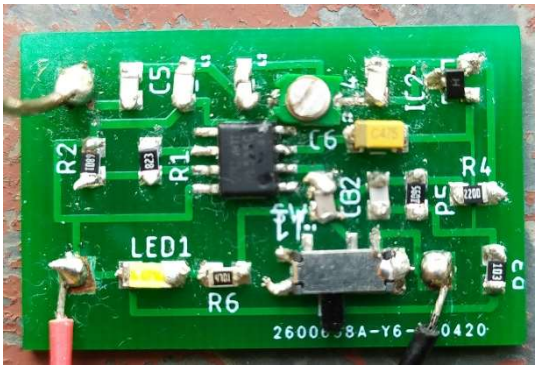
1. Integrirani krug NE555
2. Tranzistor MRF947
3. 4.7µF tantal kondenzator
4. 2.2 nH zavojnica
5. 1nH zavojnica
6. 6.8K Ω otpornik
7. 82K Ω otpornik
8. 4.7K Ω otpornik
9. 5.6K Ω otpornik
10. 220 Ω otpornik
11. 10K Ω otpornik
12. 2 x 1pF keramički kondenzator
13. 47pF keramički kondenzator
14. 4.7pF keramički kondenzator
15. SMD prekidač pod pravim kutom, 7 pinski
16. Bijela LED Dioda
17. 30pF promjenjivi kondenzator
18. Tiskana pločica
19. Konektor za bateriju
20. 9 V baterija
21. Antena



Slika 5.1. Shematski prikaz uređaja za ometanje signala.



Slika 5.2. Igled sklopa uređaja za ometanje signala.

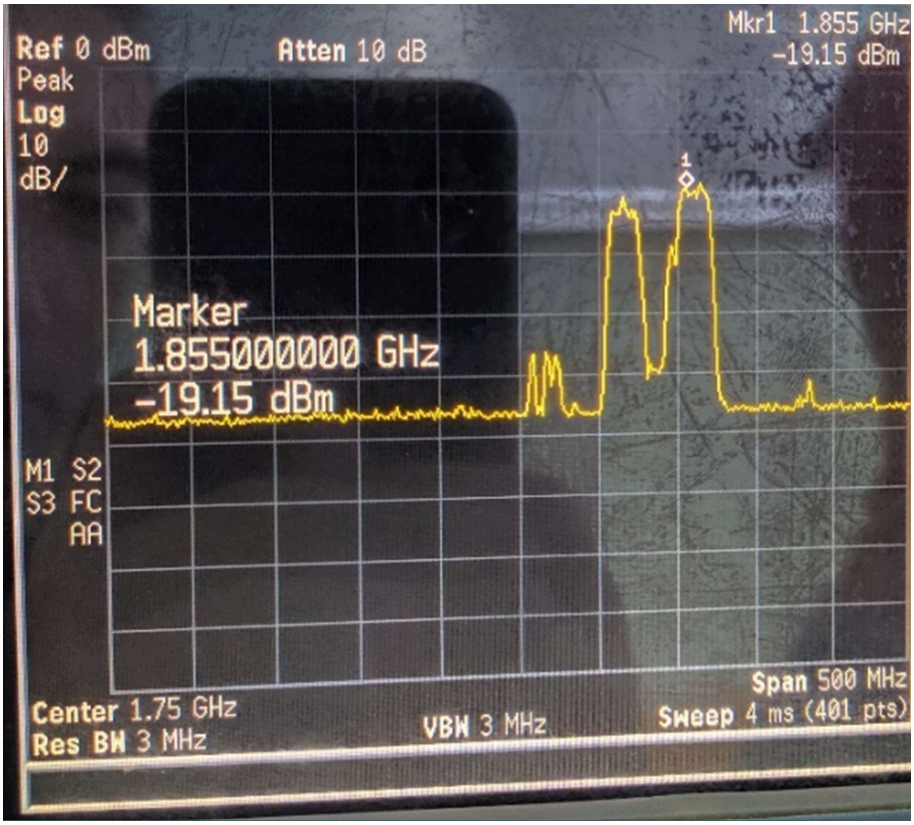


Slika 5.3. Detaljan izgled sklopa uređaja za ometanje signala.

5.1. Analiza uređaja za ometanje signala

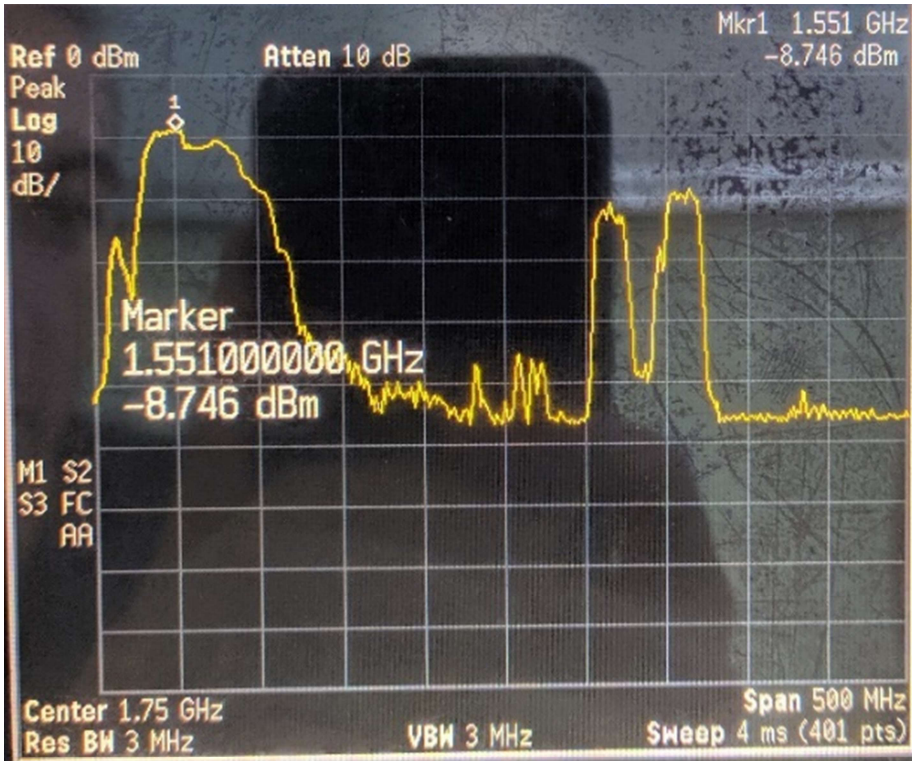
Mjerenja su provedena u laboratoriju sa spektralnim analizatorom „Agilent E4402B“ koji može analizirati spektar u rasponu od 100 Hz do 3 GHz. Provedena su dva mjerenja, prvo mjerenje je bilo sa isključenim uređajem za ometanje signala dok je drugo bilo sa uključenim uređajem za ometanje signala. Frekvencija na kojoj se koristi 4G mreža u hrvatskoj je 1800 MHz.

Prvo mjerenje je pokazalo 4G signal te se jasno vidi kako se signal dijeli na uzlaznu vezu(eng. Uplink: 1710 MHz – 1785 MHz) i silaznu vezu (eng. Downlink: 1805 MHz – 1880 MHz), odnosno da se koristi jedna frekvencija za komunikaciju od mobilnog uređaja ka odašiljaču i druga frekvencija za suprotnu komunikaciju od odašiljača ka mobilnom uređaju (Sl.5.4.). Maksimalna snaga 4G signala bila je na strani silazne veze, na frekvenciji od 1.855 GHz te je iznosila -19.15 dBm.



Slika 5.4. Rezultati mjerenja sa isključenim uređajem za ometanje signala.

Drugo mjerenje pokazuje signal koji emitira uređaj za ometanje signala (Sl.5.5.). Može se primjetiti da je signal koji emitira uređaj za ometanje signala jači od 4G signala te ima veći raspon frekvencije. Maksimalna snaga signala koji emitira uređaj za ometanje signala bila je na frekvenciji od 1.551 GHz te je iznosila -8.476 dBm. Da se zaključiti da bi uređaj za ometanje signala uspješno ometao 4G signal kada bi bio napravljen za frekvenciju od 1800 MHz.



Slika 5.5. Rezultati mjerenja sa uključenim uređaj za ometanje signala.

5. ZAKLJUČAK

Tehnologije bežičnog prijenosa signala se razvijaju u toj mjeri da se čitave kuće i svi uređaji u njima mogu kontrolirati putem bežične mreže. Svakim danom nastaju nove bežične mreže i svijet ide u tome smjeru da sve bude povezano. Električna prijevozna sredstva, dronovi, autonomni roboti i svi ostali električni uređaji omogućili su čovječanstvu napredak i lakši život. Svim tim uređajima je bitna sigurnost kako ih se ne bi zloupotrebljavalo. Korištenje najbolje moguće zaštite bežičnih mreža pruža sigurnost prijenosa informacija. Iako je ilegalno ometati signale u javnoj uporabi, svatko s malo znanja i iskustva može izraditi uređaj za ometanje signala za bilo koju frekvenciju. Takav uređaj za ometanje signala može uspješno ometati signal te napraviti problem za sigurnost ljudi. Zbog toga je bežično povezivanje ranjivo u smislu ometanja signala i krađe podataka. Kako se razvijaju sigurniji načini prijenosa podataka tako se i ometanje signala razvija. U radu je prikazano kako se izvodi ometanje nekoga signala najjednostavnijom metodom *DoS* (eng. Denial of Service) napadom. Tom metodom se ne kradu informacije niti se direktno šteti korisniku nego se samo onemogućava pristup nekoj mreži.

LITERATURA

[1] Centar Informacijske Sigurnosti, Ometanje signala bežičnih mreža, FER, Zagreb, lipanj 2011, dostupno na: https://www.cis.hr/files/dokumenti/CIS-DOC-2011-08-023.pdf (17.9.2019.)

[2] Bežične mreže, Wikipedia, 2014, dostupno na: https://sh.wikipedia.org/wiki/Be%C5%BEi%C4%8Dne_mre%C5%BEe (17.9.2019.)

[3] G.Šišul, Odabrana poglavlja elektroničkih komunikacija - fizički sloj, FER, Zagreb, 2017, dostupno na: www.fer.unizg.hr/predmet/elekom/materijali# (17.9.2019.)

[4] N.Chandler, How 4G Works, howstuffworks, 2014., dostupno na: https://electronics.howstuffworks.com/4g.htm (17.9.2019)

[5] WNDW, Wireless Networking in the Developing World, dostupno na: http://wndw.net (17.9.2019)

[6] E. Zentner, Antene i radiosustavi, Školska knjiga , Zagreb, 2001.

[7] Radio jamming, Wikipedia, 2019, dostupno na: https://en.wikipedia.org/wiki/Radio_jamming (17.9.2019.)

[8] H.Domitrović, K.Jambrošić, A.Petošić, Prijenos zvuka, Element, Zagreb, 2015.

[9] G. Wollenhaupt, How Cell Phone Jammers Work, howstuffworks, 2005, dostupno na: https://electronics.howstuffworks.com/cell-phone-jammer.htm (17.9.2019.)

[10] Creative Science, How to Make 4G-LTE Cell Phone Signal Jammer, Youtube, 2019, dostupno na: https://www.youtube.com/watch?v=WVO0wboKhA0&t=42s (17.9.2019.)

SAŽETAK

Bežične mreže su komunikacijske mreže u kojima se kao medij preko kojeg se šalju podatci koriste radio valovi. To ih čini ranjivim na ometanje i neželjeni pristup. Koriste se u slučajevima kada žičanu mrežu nije moguće uspostaviti ili je isplativija nego žičana. Ometanje signala bežičnih mreža je ništa drugo nego emitiranje posebnog radio signala koji će stvoriti interferenciju sa signalom kojeg se želi ometati. Pošto su bežične mreže u današnje vrijeme u širokoj upotrebi, često se događaju krađe informacija koje se šalju tim putem. U sklopu završnog rada izrađen je i analiziran uređaj za ometanje signala. Rezultati mjerenja su pokazali da uređaj za ometanje signala može nadjačati mobilni 4G signal te ga tako ometati.

Ključne riječi: prijenos signala, bežične mreže, uređaj za ometanje signala, ometanje signala,

ABSTRACT

SIGNAL JAMMERS IN WIRELESS COMMUNICATION NETWORKS

Wireless networks are communication networks where radio waves are used as the medium through which data is transmitted. This makes them vulnerable to interference and unwanted access. They are used in cases where the wired network cannot be established or is more cost effective than the wired. Interfering with wireless signals is nothing more than transmitting a special radio signal that will interfere with wanted signal. Because wireless networks are in widespread use these days, information theft is common. As part of the final paper, a signal jammer was designed and analyzed. Measurement results showed that the signal jammer can override the 4G signal and thus interfere with it.

Keywords: signal transmission, wireless networks, signal jammer, signal interference,

ŽIVOTOPIS

Zvonimir Benčević rođen je 10. travnja 1997. godine u Slavonskom Brodu. Završio je Osnovnu školu Đuro Pilar te Srednju tehničku školu u Slavonskom Brodu, smjer elektrotehnika. Trenutno je redovan student 3.godine preddiplomskog studija na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija Osijek. Tečno govori engleski jezik.