S V E U Č I L I Š T E U S P L I T U

FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

POSLIJEDIPLOMSKI DOKTORSKI STUDIJ ELEKTROTEHNIKE I INFORMACIJSKE TEHNOLOGIJE

KVALIFIKACIJSKI ISPIT

OBRADA SIGNALA U SVRHU OTKLANJANJA INTERFERENCIJE U PRIJAMNICIMA SUSTAVA GNSS

Katarina Radoš

Split, rujan 2023.

Sadržaj

Popis slika

Popis skraćenica

AGC	Automatic Gain Control
BPSK	Binary Phase Shift Keying
C/A	Coarse Acquisition Code
C/N	Carrier to Noise Ratio
DOP	Dilution of Precision
ESA	European Space Agency
Galileo	European Global Navigation Satellite System
GAN	Generative Adversarial Network
GCC	Galileo Control Center
GCS	Ground Control Segment
GDOP	Geometric Dilution of Precision
GEO	Geosynchronous Equatorial Orbit
GLONASS	Navigazionnaya Sputnikovaya Sistema
GMS	Ground Mission Segment
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HDOP	Horizontal Dilution of Precision
IGSO	Inclined Geosynchronous Orbit
KNN	K-Nearest Neighbors
LHCP	Left-Hand Circular Polarization
LOS	Line of Sight
MEO	Medium Earth Orbit
ML	Machine Learning
MP	Multipath
NAVSTAR	Navigation System with Time and Ranging
NLOS	Non Line of Sight
NMEA	National Marine Electronics Association

PDOP	Position Dilution of Precision
PVT	Position, Velocity and Time
P(Y)	Precision/secure Code
RHCP	Right-Hand Circular Polarization
RINEX	Receiver Independent Exchange Format
SQM	Signal Quality Monitoring
SVM	Support Vector Machine
SVR	Support Vector Regression
TDOP	Time Dilution of Precision
URE	User Range Error
USRP	Universal Software Radio Peripheral
VDOP	Vertical Dilution of Precision

1. Uvod

Aplikacije za navigaciju i pozicioniranje su postale svakodnevnica bilo da negdje putujemo, nešto tražimo ili radimo svoj posao vozača autobusa, kamiona, taksija, posade brodova i aviona. Stabilna i precizna sinkronizacija je od ključne važnosti u mobilnim mrežama za uspješno povezivanje baznih postaja i prijenos podataka u stvarnom vremenu te za usluge navigacije i pozicioniranja. Mobilne mreže moraju biti sinkronizirane tako da bazne postaje, čija se prekrivanja preklapaju ne ometaju jedne druge uzrokujući pad poziva ili pogoršanje usluge. Zbog gubitka sinkronizacije dolazi do pogoršanja kvalitete mobilnog prijenosa te pada u broju uspješnih poziva i smanjenja broja korisnika. Jedan od značajnih izvora referentnog signala za sinkronizaciju i pružanje usluga navigacije i pozicioniranja je globalni navigacijski satelitski sustav GNSS (*Global Navigation Satellite Systems*). Sustav GNSS (*Global Navigation Satellite Systems*) čine četiri globalna navigacijska sustava: GPS (*Global Positioning System*), GLONASS (*Navigazionnaya Sputnikovaya Sistema*), Galileo (*European Global Navigation Satellite System*) i BeiDou (*Chinese Global Navigation Satellite System*). Stalnim unaprjeđivanjem postojećih sustava osigurava se bolja preciznost. Međutim, zbog sve veće upotrebe satelitskih navigacijskih sustava, javlja se sve više rizika i opasnosti kao što je korištenje ovih sustava u neke zlonamjerne svrhe [1].

Glavne interferencije u prijamnicima sustava GNSS su: napad lažiranjem GNSS signala (*spoofing*), višestazno prostiranje GNSS signala (*multipath*) i ometanje GNSS signala (*jamming*). Za izvođenje napada lažiranjem, prije je trebalo veliko znanje i skupa oprema. Međutim, danas ove napade može izvesti gotovo svatko zbog jeftine opreme i dostupnosti različitih uputa za samo izvođenje. Najčešće korišteni uređaj za izvođenje ovih napada je jeftini softverski definirani radio npr. USRP, HackRF One, LimeSDR, itd. Uređaji koji su najosjetljiviji na napade lažiranjem su mobilni telefoni koji se danas najviše koriste za usluge navigacije.

Refleksija signala u gradskim sredinama uzrokuje pojavu višestaznog prostiranja signala GNSS sustava, a to je prijam GNSS signala preko više različitih staza. Nastaje kada dio signala sa satelita stigne do prijamnika nakon jedne ili više refleksija ili raspršenja od tla, zgrade ili dru-

gog reflektirajućeg objekta. Reflektirani signali imaju puno manju snagu u odnosu na izvorni signal i po tome ih se može razlikovati. Višestazno prostiranje predstavlja jedan od ključnih izvora smetnji u prijemu signala GNSS sustava. Stoga je otklanjanje utjecaja višestaznog prostiranja u središtu istraživačkih aktivnosti. Najizazovnija sredina u kojoj se javlja višestazno prostiranje signala je urbani kanjon.

Ometanje signala je namjerno ili nenamjerno odašiljanje signala visoke radiofrekvencije koja je jednaka ili bliska frekvencijama na kojima rade GNSS prijamnici. Komercijalni uređaji koji se koriste za ometanje signala su jeftini i lako dostupni.

Napad lažiranjem korištenjem softverski definiranog radija se odvija na način da predajnik (softverski definirani radio) odašilje lažne GNSS signale koji imaju veću snagu nego autentični signali te su prijemnici prisiljeni uzeti lažne signale. Utjecaj napada lažiranjem na neki GNSS prijamnik se ogleda u preuzimanju navigacijskog sustava i lažiranju lokacije prijamnika. Ovakvi napadi su posebno opasni iz sigurnosnog aspekta kada se koriste u vojne svrhe ili za preusmjeravanje aviona, brodova, automobila itd. Stoga je potrebno unaprijediti već postojeće metode za detekciju ovakvih napada te razviti nove učinkovite metode. Postojeća rješenja pokazuju da metode strojnog učenja imaju vrlo visoku točnost za detekciju napada lažiranjem. Kako tehnološki napredak čini GNSS uređaje sve pristupačnijima u svakodnevnom životu, potreba za preciznim pozicioniranjem i vremenom u svrhu automatizacije, učinkovitosti i sigurnosti postaje sve veća. Usporedno s tim raste i važnost sigurnosnih aspekata u primjeni GNSS sustava. Korištenje GNSS prijamnika koji su otporni na ometanje i lažiranje je ključno za sigurno pozicioniranje, navigaciju, vrijeme i sinkronizaciju.

Ovaj rad je podijeljen na pet poglavlja. U prvom poglavlju dan je uvod i motivacija rada. Drugo poglavlje opisuje osnovne značajke i način rada sustava GNSS te strukturu GNSS signala. U trećem poglavlju opisane su ključne interferencije u prijamnicima sustava GNSS, a to su napad lažiranjem GNSS signala, višestazno prostiranje GNSS signala i ometanje GNSS signala. Navedene su i vrste napada lažiranjem: pojednostavljeni napad, napad lažiranjem srednje razine složenosti te sofisticirani napad lažiranjem. Prikazano je i izvođenje napada lažiranjem pomoću softverski definiranog radija, stanje u literaturi te sva oprema i detalji potrebni za sami napad. Nadalje, detaljno je prikazan koncept višestaznog prostiranja te parametri po kojima se može prepoznati. Metode za detekciju interferencija u prijamnicima sustava GNSS prikazane su u četvrtom poglavlju. Konačno, u zadnjem poglavlju je dan zaključak.

2. Globalni navigacijski satelitski sustav GNSS

GNSS sustavi su nevidljivi dijelovi tehnologije na koje se ljudi svakodnevno oslanjaju npr. korištenje mobilnih navigacijskih aplikacija. Svrha navigacijskih satelitskih sustava je pružanje usluga pozicioniranja i navigacije u realnom vremenu bilo kada i bilo gdje. Osnovne značajke sustava GNSS su opisane u ovom poglavlju.

2.1. Osnovne značajke sustava GNSS

Pod pojmom GNSS sustav podrazumijeva se bilo koja konstelacija satelita koja pruža usluge pozicioniranja, navigacije i mjerenja vremena. GNSS se temelji na konstelaciji satelita koji odašilju signale iz svemira prema zemaljskoj površini. Signali prenose podatke o položaju i vremenu na GNSS prijamnik te prijamnik koristi te podatke za određivanje položaja odnosno pozicioniranje.

2.1.1. Satelitski sustav GPS

Ovaj radionavigacijski sustav je u najširoj civilnoj upotrebi danas. Poznat je i kao NAVSTAR (*Navigation System with Time and Ranging*) te je prvotno razvijen u vojne svrhe od strane Ministarstvoa obrane SAD-a. Američki kongres je dozvolio i civilnu upotrebu. Prvi satelit lansiran je 1978. godine, a puna konstelacija je ostvarena 1995. godine. GPS sateliti konstantno odašilju dva signala nosioca u L pojasu (L1 i L2). Signali nosioci vrlo su važni jer na Zemlju donose informacije sa satelita koje prijamniku omogućuju da utvrdi točnu lokaciju [2].

Osnovni segmenti satelitskog navigacijskog sustava GPS su sljedeći:

1. svemirski,
2. kontrolni,
3. korisnički.

Svemirski segment GPS sustava sastoji se od 24 do 32 satelita, ravnomjerno raspoređena u 6 orbitalnih ravnina, koji svakih 12 sati obiđu Zemlju na udaljenosti od približno 20 200 kilometara. Osnovna zadaća ovog segmenta je odašiljanje radio signala pomoću kojih se mjere udaljenost te pružanje točnih informacija o položaju i vremenu korisnicima bilo gdje u svijetu. Orbitalne ravnine ne rotiraju u odnosu na udaljene zvijezde i centrirane su na Zemlji. Orbite su raspoređene tako da je najmanje šest satelita uvijek vidljivo sa svih strana Zemljine površine. Od 2019. godine 31 satelit se nalazi u GPS konstelaciji te je devet satelita vidljivo u bilo kojem trenutku s bilo kojeg mjesta na Zemlji. Dodatni sateliti poboljšavaju preciznost mjerenja.

Kontrolni segment odnosi se na zemaljske postaje smještene u cijelom svijetu u blizini ekvatora. Koriste se za praćenje, kontrolu i slanje informacija svakom GPS satelitu. Glavni zadatak kontrolnog ili zemaljskog segmenta je praćenje satelita u svrhu određivanja orbita i vremena, sinkronizacija vremena satelita te odašiljanje poruka satelitima. Kontrolni ili zemaljski segment sastoji se od: glavne kontrolne stanice, alternativne glavne kontrolne stanice, četiri dodijeljene zemaljske antene i šest dodijeljenih nadzornih stanica. Glavna kontrolna stanica nalazi se u bazi zračnih snaga u Colorado Springsu u SAD-u i odgovorna je za cjelokupno upravljanje lokacijama daljinskog nadzora i prijenosa. Osim toga, zadaće su joj i praćenje GPS satelita, nadziranje njihovih prijenosa, prikupljanje podataka nadzornih stanica, sinkronizacija vremena i prosljeđivanje podataka zemaljskim stanicama. Šest nadzornih stanica provjerava točnu visinu, položaj, brzinu i ukupno stanje satelita u orbiti. Kontrolni segment koristi mjerenja prikupljena od strane nadzornih stanica za predviđanje ponašanja orbite i sata svakog satelita. Podaci o predviđanjima prenose se korisnicima satelitima za prijenos. Kontrolni segment osigurava da orbite i satovi GPS satelita ostanu unutar prihvatljivih granica. Stanica može pratiti do 11 satelita istovremeno. Ova provjera obavlja se dva puta dnevno za svaku stanicu, nakon što sateliti završe svoje putovanje oko Zemlje. U slučaju da se zapaze nekakvi problemi, proslijedi ih se glavnoj kontrolnoj stanici. Četiri zemaljske antene nadziru i prate satelite od horizonta do horizonta. Osim toga, satelitima prenose informacije o korekcijama.

Korisnički segment uključuje bilo koga tko koristi/ima GPS prijamnik. Ovaj se segment sastoji od stotina tisuća američkih i savezničkih vojnih korisnika usluge preciznog pozicioniranja i desetaka milijuna civilnih, komercijalnih i znanstvenih korisnika usluge standardnog pozicioniranja [2].

2.1.2. Satelitski sustav Galileo

Galileo je europski navigacijski satelitski sustav nastao kao zajednička inicijativa Europske svemirske agencije *(European Space Agency - ESA)* i Europske komisije, koji pruža vrlo točan, zajamčeni servis globalnog pozicioniranja u stvarnom vremenu s preciznošću od metra pod civilnom kontrolom. Prvi Galileo testni satelit GIOVE-A, lansiran je 2005. godine, a prvi satelit koji je kasnije postao dio operativnog sustava lansiran je 2011. Do srpnja 2018. godine, 26 od planiranih 30 satelita, uključujući i rezervne, bili su u orbiti. Potpuno raspoloživi Galileo sustav sastoji se od 24 operabilna satelita plus 6 rezervnih u orbiti, smještenih u 3 krušne orbite na 23 222 km visine iznad Zemlje.

Sustav Galileo sastoji se od svemirskog segmenta (sateliti u svemiru), zemaljskog segmenta na nekoliko lokacija te korisničkog segmenta. Svemirski segment sustava Galileo definiran je kao 24/3/1 Walker konstelacija. To predstavlja 24 satelita nominalne srednje Zemljine orbite *(Medium Earth Orbit - MEO)* raspoređena u 3 orbitalne ravnine. Konstelaciju je moguće nadopuniti pomoćnim Galileo satelitima koji zauzimaju orbitalne utore koji nisu dio osnovne konstelacije. Zemaljski Galileo segment sastoji se od dva Galileo kontrolna centra *(Galileo Control Center - GCC)* smještena u Oberpfaffenhofeu u Njemačkoj i u Fucinu u Italiji. Svaki Galileo kontrolni centar upravlja kontrolnim funkcijama koje podržava Segment zemaljske kontrole *(Ground Control Segment - GCS)* i funkcijama misije koje podržava Segment zemaljske misije *(Ground Mission Segment - GMS)*. Segment zemaljske kontrole nadzire i kontrolira satelite i bazira se na Galileo kontrolnom centru u Oberpfaffenhofenu, a povezan je s telemetrijskim, pratećim i telekomunikacijskim postajama u Kiruni (Švedska) i Kourou (Francuska Gvajana). Segment zemaljske misije nalazi se u drugom Galileo kontrolnom centru (Fucino) i osigurava najsuvremenije navigacijske performanse Galilea. Galileo korisnički segment sastoji se od svih kompatibilnih prijamnika i uređaja koji prikupljaju Galileo signale i izračunavaju svoju lokaciju. Postoje različite korisničke zajednice ovisno o primjeni te pokrivaju širok raspon, od prijevoza do aplikacija za mjerenje vremena. Galileo sateliti odašilju tri signala: E1 (1575.42 MHz), E5 (1191.795 MHz) koji se sastoji od E5a (1176.45 MHz) and E5b (1207.14 MHz), te E6 (1278.75 MHz) [3].

2.1.3. Satelitski sustav GLONASS

GLONASS je ruski satelitski navigacijski sustav. Prvi GLONASS satelit odaslan je 1982. godine, a sustav je 1993. godine proglašen potpuno operativnim. Postojalo je razdoblje u kojem su performanse GLONASS-a opale te se Rusija obavezala dovesti sustav na potreban minimum od 18 aktivnih satelita. Trenutno GLONASS ima punu raspodjelu od 25 satelita u konstelaciji. Dizajn GLONASS sustava sličan je dizajnu GPS sustava i sastoji se od tri dijela: kontrolni segment, svemirski segment, korisnički segment, koja su definirana na vrlo sličan način kao i segmenti sustava GPS. Konstelacija GLONASS-a, ovisno o lokaciji, omogućava vidljivost različitog broja satelita. Potrebna su barem četiri satelita u vidokrugu kako bi GLONASS prijamnik mogao izračunati svoju poziciju u tri dimenzije te kako bi se sat prijamnika sinkronizirao sa satom sustava. Geometrija GLONASS konstelacije ponavlja se otprilike jednom svakih osam dana. Satelitski signal GLONASS identificira satelit i uključuje: podatke o pozicioniranju, brzini i ubrzanju za izračunavanje satelitskih lokacija, informacije o "zdravstvenom" stanju satelita te odmaku GLONASS vremena od UTC vremena. Svaki GLONASS satelit odašilje na nešto različitim L1 i L2 frekvencijama, s P-kodom, na L1 i L2 te s C/A-kodom na L1 (svi sateliti) i L2 (većina satelita). GLONASS sateliti odašilju isti kod na različitim frekvencijama [4].

2.1.4. Satelitski sustav BeiDou

Satelitski sustav BeiDou kineski je navigacijski satelitski sustav. Sastoji se od dvije odvojene satelitske konstelacije. BeiDou trenutno ima 44 operabilna satelita. Prvi BeiDou sustav, poznat i kao BeiDou-1, sastojao se od tri satelita koji su nudili ograničenu pokrivenost i navigacijske usluge, uglavnom za korisnike u Kini i susjednim regijama. Druga generacija sustava, BeiDou-2, imala je djelomičnu konstelaciju od 10 satelita u orbiti. TreÄ‡a generacija BeiDou navigacijskog satelitskog sustava osigurava globalnu pokrivenost za mjerenje vremena i navigaciju te može poslužiti kao alternativa američkom GPS-u, ruskom GLONASS-u i europskom Galileu. BeiDou-1 bio je eksperimentalni regionalni navigacijski sustav koji se sastojao od tri radna i jednog rezervnog satelita. Sateliti su bili bazirani na kineskom geostacionarnom komunikacijskom satelitu DFH-3 i svaki je imao težinu lansiranja od 1 tone. Za razliku od prethodno opisanih satelitskih sustava, BeiDou-1 je koristio satelite u geostacionarnoj orbiti što znači da sustav ne zahtijeva veliku konstelaciju satelita, no ipak ograničava pokrivenost područja na

Zemlji odakle su sateliti vidljivi. BeiDou-2 u potpunosti zamjenjuje sustav BeiDou-1, on nije njegovo proširenje. Njegova konstelacija sastoji se od 35 satelita - 5 geostacionarnih satelita i 30 negeostacionarnih satelita koji nude potpunu pokrivenost. Sateliti su odašiljali signale na tri frekvencije B1, B2 i B3. Treća faza razvoja sustava BeiDou uključuje tri GEO *(Geosynchronous Equatorial Orbit)* satelita, tri IGSO *(Inclined Geosynchronous Orbit)* satelita i 24 MEO satelita. Time su uvedene nove frekvencije civilnih signala B1C/B1I/B1A (1575.42 MHz), otvorenih signala B2a/B2b (1191.795 MHz), signala B3I/B3Q/B3A (1268.52 MHz) i Bs signala (2492.028 MHz) za eksperimentalno emitiranje S pojasa. Novi civilni signal B1C odašilje se na novoj frekvenciji 1575,420 MHz kao i signali na L1 u GPS-u. Otvoreni signali B2a (1176,450 MHz) i B2b (1207,140 MHz) odašilju se na frekvencijama koje su identične frekvencijama Galileo signala E5a i E5b, te postoji mogućnost njihove zajedničke obrade (1191,795 MHz). Novi BDS-3 signali omogućuju bolju kompatibilnost i interoperabilnost s drugim GNSS-ima. Sustav omogućuje dvije vrste usluga: otvoreni i autorizirani servis. Otvoreni servis za civilnu upotrebu je besplatan, a osigurava točnost apsolutnog pozicioniranja. Autorizirani servis omogućuje pouzdanije određivanje pozicije, brzine i vremena, te komunikacijski servis i viši stupanj integriteta. Besplatna civilna usluga ima točnost praćenja lokacije od 10 m, dok ograničena vojna usluga ima točnost od 10 cm.

2.2. Način rada sustava GNSS

Pod pojmom GNSS sustav podrazumijeva se bilo koja konstelacija satelita koja pruža usluge pozicioniranja, navigacije i mjerenja vremena. GNSS se temelji na konstelaciji satelita koji odašilju signale iz svemira prema zemaljskoj površini. Signali prenose podatke o položaju i vremenu na GNSS prijamnik te prijamnik koristi te podatke za određivanje položaja odnosno pozicioniranje. GNSS prijamnik se sastoji od antene i jedinice za obradu (prijamnika) [1]. Satelitski signali se prikupljaju pomoću antene, a jedinica za obradu pretvara prikupljene informacije u oblik razumljiv korisniku tj. zemljopisne koordinate. Sami položaj antene određuje stvarna mjerenja, primjerice ako se antena nalazi na nekom teško dostupnom položaju kao što je urbani kanjon, u samim mjerenjima će postojati mnogo reflektiranih signala nastalih višestaznim prostiranjem signala. Postoje različiti GNSS prijamnici koji ne mogu primati sve GNSS signale. Primjerice, GPS prijamnik može primati samo GPS signale dok GLONASS prijamnik može primati samo signale s GLONASS satelita. Također, postoje i složeniji prijamnici koji

mogu primati signale s više satelita tzv. multi-konstelacijski GNSS prijamnici [48].

Za određivanje položaja moraju biti poznati sljedeći elementi:

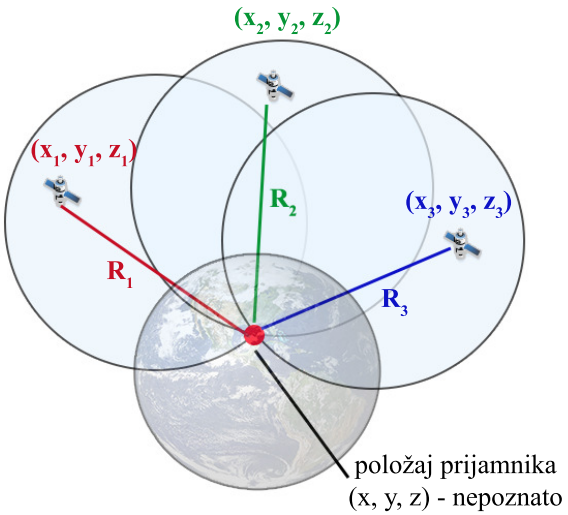
- položaj satelita,
- vrijeme odašiljanja signala,
- vrijeme prijama signala,
- brzina prostiranja signala.

Određivanje položaja temelji se na mjerenju vremena propagacije (širenja) satelitskog radijskog signala od satelitske odašiljačke antene do antene korisničkog prijamnika. GNSS pozicioniranje na visokoj razini jednostavno se temelji na konceptu trilateracije. Kako bismo odredili nepoznati položaj (x,y,z) prijamnika kao što je prikazano na slici 2.1, pretpostavimo da su položaji triju GNSS satelita unaprijed poznati (sateliti šalju prijamniku informacije o položaju preko navigacijske poruke). Kada prijamnik dobije i prati dolazne GNSS signale od tri satelita, može odrediti vrijeme propagacije signala Δt (vrijeme prijenosa minus vrijeme prijema). Pošto su GNSS signali elektromagnetski valovi koji se šire brzinom svjetlosti $c = 3 \times 10^9 m/s$, udaljenosti od prijamnika do tri satelita (R_1, R_2, R_3) se dobiju množenjem c s Δt i te udaljenosti se nazivaju pseudoudaljenosti. Pseudoudaljenost predstavlja pravu udaljenost na koju je dodana mala (pozitivna ili negativna) korekcija udaljenosti uzrokovana pogreškom sata prijamnika. Mjerenje pseudoudaljenosti zahtijeva precizno poznavanje vremena odašiljanja signala sa satelita i vremena prijama signala na prijamniku. Konačno, set trilateracijskih jednadžbi se može postaviti kao

$$c(\Delta t^m) = \sqrt{(x-x^m)^2 + (y-y^m)^2 + (z-z^m)^2}, \quad m = 1,2,3 \tag{2.1}$$

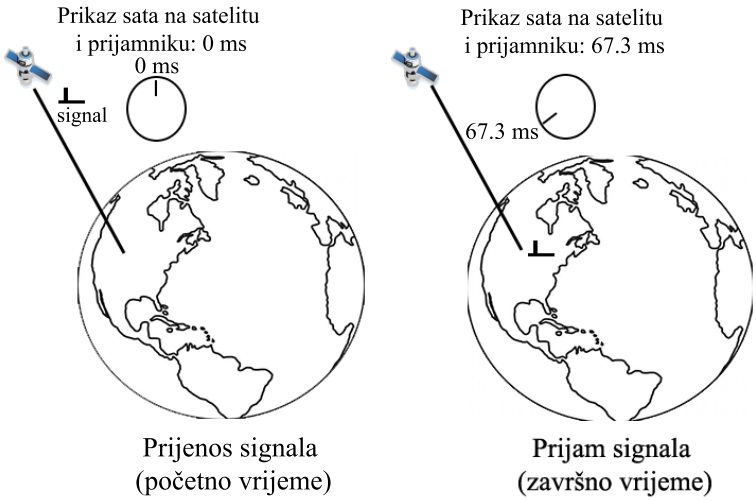
gdje su x_m, y_m i z_m poznate koordinate triju satelita [10]. Nepoznate koordinate prijamnika se određuju rješavanjem triju jednadžbi s tri nepoznanice. Iako su dovoljna samo tri satelita, točnost i preciznost povećat će se s većim brojem satelita, pa se za izračun položaja najčešće koriste četiri satelita.

Preduvjet za određivanje položaja i vremena je sinkronizacija odnosno vremensko usklađivanje svih elemenata (satelit i prijamnik) sustava na zajedničko vrijeme GNSS sustava. Sinkronizacija elemenata sustava omogućuje mjerenje vremena propagacije satelitskog signala na način da satelit označava trenutak odašiljanja signala, a prijamnik trenutak prijama signala. Na



Slika 2.1: GNSS trilateracija [10].

slici 2.2 prikazana je sinkronizacija satova satelita i prijamnika za vrijeme propagacije signala [6].



Slika 2.2: Sinkronizacija satova satelita i prijamnika [6].

Za početno vrijeme propagacije signala prikaz sata na satelitu i prijamniku je 0 ms. Svaki satelit prenosi svoj točni položaj i točno vrijeme do Zemlje s određenom frekvencijom ovisno o frekvencijskom pojasu i vrsti satelitskog sustava. Ovi signali putuju brzinom svjetlosti i prema tome treba približno 67,3 ms da dosegnu Zemljinu površinu neposredno ispod satelita što je prikazano kao završno vrijeme propagacije signala.

Satelitski navigacijski sustavi koriste visoko postavljene satelite na način da se iz bilo koje točke na tlu može povući crta do četiri satelita. Svaki satelit ima do četiri atomska sata (najtoč-

niji sat koji ima najveću grešku od 1 sekunde u 30 milijuna godina). Za još veću preciznost, atomski satovi rade korekciju ili sinkronizaciju iz kontrolne točke na Zemlji. Bez atomskog sata ne bi bio izvediv ni GPS, navigacija bi bila otežana, svemirski letovi se ne bi mogli tako precizno planirati, itd. Atomski sat na bazi cezija je sat koji koristi elektromagnetsko zračenje, koje nastaje kod prijelaza između dviju hiperfinih razina osnovnog stanja atoma cezija -133 na temperaturi od 0 K. I atomski i običan mehanički sat za mjerenje vremena koriste titranje ili osciliranje, ali kod atomskog sata je ono određeno masom jezgre atoma i silom gravitacije, te elektrostatičkom oprugom između pozitivnog naboja jezgre i elektronskog oblaka [7].

Na točnost položaja i vremena utječu dva faktora [44]:

1. Korisnička pogreška udaljenosti URE (*User Range Error*) je razlika između navigacijskih podataka satelita (položaj i sat) i istinitih vrijednosti, projiciranih na vidokrug korisnika. URE je funkcija kvalitete emitiranog signala i podataka.

2. Geometrijsko smanjenje preciznosti GDOP (*Geometric Dilution of Precision*) je mjera kvalitete geometrije (distribucija satelita na nebu)koju definiraju sateliti i prijamnik odnosno opisuje jakost trenutne satelitske konfiguracije ili geometrije na točnost podataka prikupljenih prijamnikom. GDOP je učinak geometrije satelita na pogrešku položaja i grubo se definira kao omjer pogreške položaja i pogreške dometa. GDOP ovisi samo o položaju satelita (broj vidljivih satelita i koliko su visoko na nebu - geometrija). Kada su vidljivi sateliti blizu jedan drugome na nebu, geometrija je slaba, a DOP vrijednost visoka. To potencijalno smanjuje kvalitetu pozicioniranja za nekoliko metara. S druge strane, kada su sateliti međusobno udaljeni, geometrija je jaka, a DOP vrijednost niska što je prikazano na slici 2.3. Što je veći broj satelita, to je bolja vrijednost GDOP-a i obrnuto.

   GDOP se može izraziti kao niz zasebnih komponenti [21]:

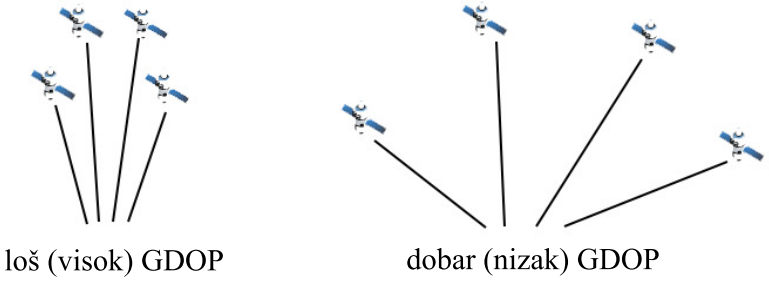
   (a) Horizontalno smanjenje preciznosti HDOP (*Horizontal Dilution of Precision*) je mjera točnosti u 2D položaju (zemljopisna širina i dužina). HDOP vrijednosti su tipično između 1 i 2.

   (b) Položajno smanjenje preciznosti PDOP (*Position Dilution of Precision*) označava mjeru preciznosti položaja (HDOP + VDOP). Sateliti raširenі nebom obično će imati dobru (nižu PDOP vrijednost) geometriju. Sateliti skupljeni čvrsto na određenom dijelu neba obično će imati lošu (veću PDOP vrijednost) geometriju. PDOP

vrijednosti koje se smatraju dobrima za pozicioniranje su male, poput 3. Vrijednosti veće od 7 se smatraju lošima.

(c) Vertikalno smanjenje preciznosti VDOP (*Vertical Dilution of Precision*) je mjera točnosti u 1-D položaju (visina).

(d) Vremensko smanjenje preciznosti TDOP (*Time Dilution of Precision*) je mjera preciznosti vremena. Visoki TDOP uzrokuje pogreške sata prijamnika što rezultira do povećanja pogreški položaja.



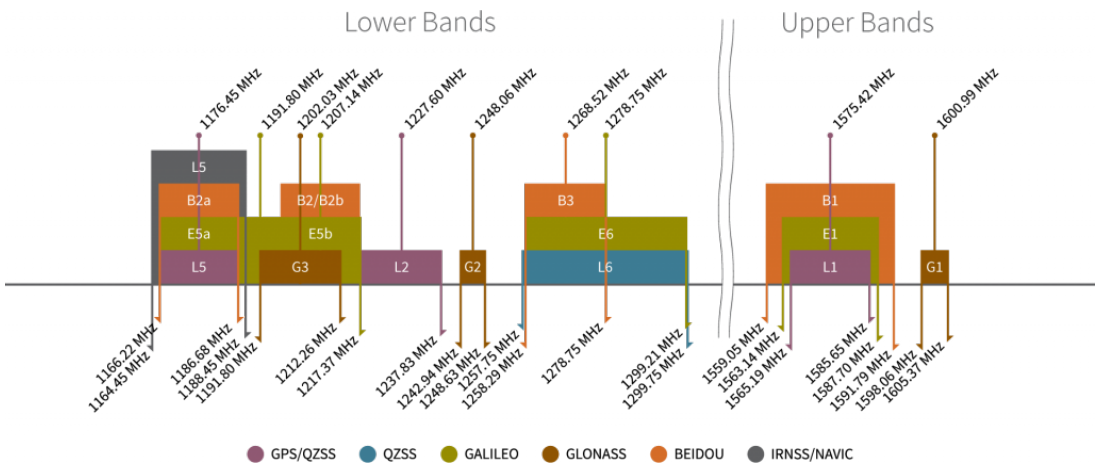
Slika 2.3: Ilustracija dobre i loše geometrije satelita.

2.3. Struktura GNSS signala

Raspon frekvencija GNSS signala je od $1,2-1,6$ GHz (L pojas). Ovi frekvencijski pojasevi koriste se za satelitske sustave iz razloga što imaju manje gubitke s povećanjem udaljenosti i što valovi L pojasa prodiru kroz oblake, maglu, kišu, oluje i vegetaciju te GNSS jedinice mogu primati točne podatke u svim vremenskim uvjetima, danju ili noću. Frekvencijski pojasevi za GNSS sustave su prikazani na slici 2.4. Osobitost svih GNSS signala je modulacija harmonijskog radio signala (signal nosioc) s karakterističnim pseudoslučajnim nizom PRN (Pseudo-random Noise Code). PRN kod je binarni niz brojeva 0 i 1. Ovaj kod se neprekidno ponavlja u intervalima od nekoliko milisekundi do sekunde i olakšava mjerenje vremena propagacije signala. Svaki prijamnik po PRN nizu razlikuje svaki pojedinačni satelit koji emitira na istoj frekvenciji.

GNSS sateliti kontinuirano odašilju signale na dvije ili više frekvencija u L pojasu. Ovi signali sadrže PRN kodove i navigacijske poruke pomoću kojih se računa vrijeme propagacije od satelita do prijamnika i koordinate satelita u bilo kojoj epohi.

Osnovne komponente GNSS signala su [8]:



Slika 2.4: Frekvencijski pojasevi u sustavima GNSS [9].

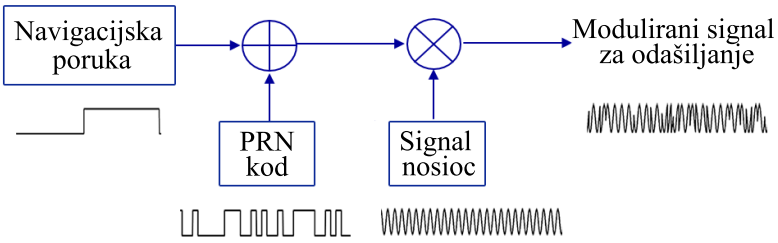
1. signal nosioc - radio frekvencijski sinusoidalni signal na određenoj frekvenciji,

2. kod za mjerenje udaljenosti je binarni niz nula i jedinica dodijeljen svakom satelitu, koji omogućava korisničkom prijamniku da odredi vrijeme propagacije signala od satelita do prijamnika. Ovi kodovi se nazivaju pseudoslučajni kodovi ili PRN kodovi. Generiraju se matematičkim modeliranjem i imaju vrijednost koja omogućava svim satelitima emitiranje na istoj frekvenciji bez da ometaju jedan drugoga. Nadalje, PRN kod omogućava precizno mjerenje udaljenosti satelita. Svaki satelit u GNSS konstelaciji ima jedinstveni PRN kod koji emitira kao dio navigacijske poruke te tako omogućava prijamniku da točno identificira satelit od kojeg prima signal.

3. navigacijska poruka je binarno kodirana poruka koja pruža informacije o satelitskim efemeridama (položaj i brzina satelita), parametrima za usuglašavanje satova, almanahu (raspored satelitskih orbitalnih parametara kako bi prijamnik dobio informaciju o vidljivosti satelita u određenom trenutku), zdravstvenom statusu satelita (aktivni satelit jer prijamnik ne prati satelite koji nisu aktivni) i drugim komplementarnim informacijama. Navigacijske poruke se odašilju brzinom od najmanje 50 bit/s s trajanjem od 20 ms. Bitne satelitske efemeride i parametri sata ponavljaju se svakih 30 s.

Kao primjer, glavne komponente GPS L1 C/A signala su prikazane na slici 2.5.

Svaki GPS satelit odašilje dva različita koda: civilni kod C/A (*coarse acquisition*) i enkriptirani kod P(Y) (*precision/secure*) koji je rezerviran za vojne i ovlaštene civilne korisnike. Svaki C/A kod je jedinstvena sekvenca od 1023 bita i ponavlja se svaku milisekundu. C/A kod se prenosi na jednoj frekvenciji L1 dok se P od prenosi na dvije frekvencije (L1 i L2).



Slika 2.5: Struktura GNSS signala.

Za zbrajanje navigacijske poruke i PRN koda koristi se operacija *xor* tj. zbrajanje po modulu 2. Ako su oba bita 0 ili 1, rezultat je 0. Ako su bitovi različiti (jedan bit 0, drugi 1), rezultat je 1. Ovakav binarni signal se utiskuje (modulira) u signal nosioc postupkom modulacije te nastaje modulirai signal koji se odašilje. Vrsta modulacije koja se najčešće koristi je digitalna modulacija s binarnim faznim pomakom ili BPSK (*Binary Phase Shift Keying*) u kojoj se podaci prenose mijenjanjem ili moduliranjem dviju različitih faza signala nosioca. Bit 0 ostavlja signal nosioc nepromijenjen dok se za bit 1 množi signal nosioc s -1 (ekvivalent za fazni pomak sinusnog signala za 180°). Kada kod prelazi s 0 na 1 ili obrnuto, faza signala nosioca se mijenja za 180°.

3. Interferencije u prijamnicima sustava GNSS

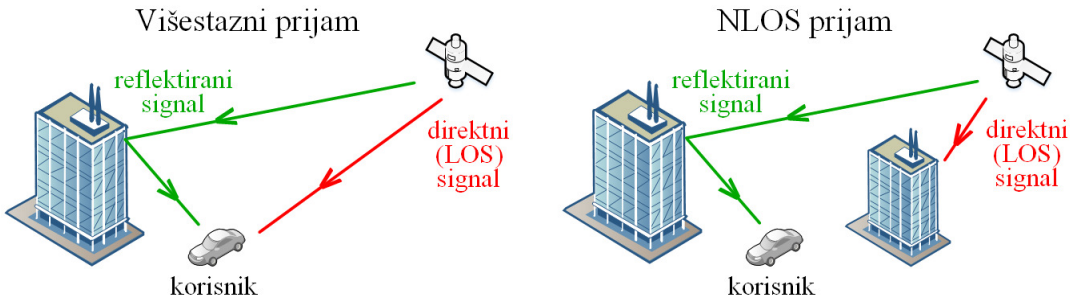
3.1. Višestazno prostiranje signala

Kao što sami naziv kaže, višestazno prostiranje GNSS signala je prijam GNSS signala preko više putanja (staza), a ne putem izravne linije vidljivosti. Nastaje kada dio signala sa satelita stigne do prijamnika nakon jedne ili više refleksija ili raspršenja od tla, zgrade ili drugog reflektirajućeg objekta. Ovi reflektirani signali mogu interferirati sa signalom koji do prijamnika stiže izravno sa satelita i uzrokovati iskrivljenje korelacijskog vrha. Uzrok višestaznom prostiranju je blizina antene reflektirajućim objektima. Budući da se mjere udaljenosti do satelita, što je temelj pozicioniranja u GNSS sustavima, signal koji se odbije od prepreke prije nego što stigne do antene GNSS prijamnika uzrokuje problem. Ako postoji zavoj u signalu, to remeti udaljenost, domet, koji prijamnik mjeri do satelita. Signal se može reflektirati više puta i svakom refleksijom ima manju snagu. Može se reflektirati i od tla. Višestazno prostiranje predstavlja jedan od ključnih izvora smetnji u prijamu signala GNSS sustava. Stoga je otklanjanje utjecaja višestaznog prostiranja u središtu istraživačkih aktivnosti. Postoje različiti pristupi za detekciju višestaznog prostiranja signala u različitim sredinama od kojih je najizazovnija urbani kanjon. Posebno problematično može biti primanje signala sa satelita pod malim kutem elevacije tj. od 15 do 20 stupnjeva [58].

Visoku točnost pozicinirania s GNSS sustavima je teško postići u urbanim područjima zbog refleksije signala. Korištenje reflektiranih GNSS signala za pozicioniranje može rezultirati velikom pogreškom pozicioniranja većom i od 100m.

Iz perspektive prijama signala, GNSS signal se može primiti u tri sljedeća slučaja [59]:

1. LOS (*Line of Sight*) - kada se primaju samo signali izravne linije vidljivosti,
2. NLOS (*Non Line of Sight*) - kada se primaju samo signali koji nemaju izravnu linisju vidljivosti između satelita i prijamnika,
3. LOS + NLOS - kada se istovremeno primaju LOS i NLOS signali.



Slika 3.1: GNSS višestazni i NLOS prijam [60].

Slika 3.1 prikazuje višestazni i NLOS prijam. U slučaju NLOS prijama, direktni (LOS) signal koji ide od satelita do prijamnika je blokiran i primaju se samo reflektirani signali. Kod višestaznog prijama, kao što i samo ime kaže, primaju se signali (direktni i reflektirani) preko više različitih putanja. Unutar GNSS zajednice, uobičajeno je klasificirati NLOS prijam kao višestazni. Međutim, ove dvije pojave nisu iste jer se njihove značajke grešaka razlikuju. Budući da je reflektirani put uvijek duži od direktnog puta, NLOS prijam uvijek rezultira pozitivnom pogreškom dometa koja je neovisna o dizajnu signala i prijamnika. Nasuprot tome, koherentna priroda višestaznih smetnji može proizvesti i pozitivne i negativne pogreške u dometu, a one se razlikuju ovisno o dizajnu signala i prijamnika [60].

Izravni GNSS signal može se matematički prikazati na sljedeći način

$$S_0(t) = A_0 \cdot C(t - \tau_0) \cdot cos(\omega_0 t) \tag{3.1}$$

gdje su A, ω, i τ amplituda, frekvencija signala nosioca i kašnjenje izravnog signala.

U slučaju kada na izravni signal $S_0(t)$ utječe pojedinačni reflektirani signal $S_1(t)$, LOS višestazni signal $S_(LOS)(t)$ se može izraziti kao

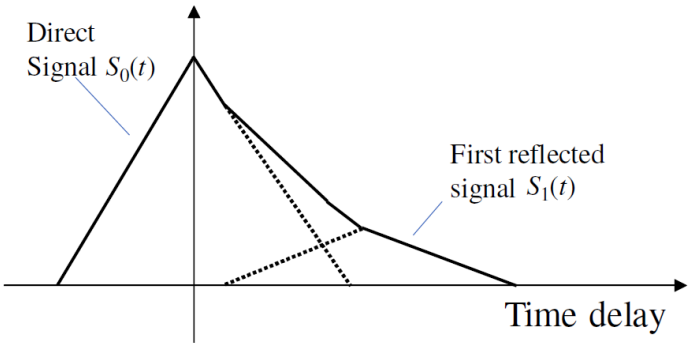
$$S_{LOS}(t) = S_0(t) + S_1(t) = S_0(t) + A_1 \cdot C(t - \tau_1) \cdot cos(\omega_0 t + \Delta\phi_1) \tag{3.2}$$

gdje su A_1, τ_1, i $\Delta\phi_1$ amplituda višestaznog signala, kašnjenje i relativna faza između izravnog i višestaznih signala. Izravni signal je kompozitni signal s višestaznim signalom i na njega utječu tri navedena višestazna parametra.

Odnos amplituda višestaznog signala je glavni čimbenik koji iskrivljuje korelacijsku funkciju LOS višestaznog signala i definiran je kao

$$\alpha_{LOS} = \frac{A_1}{A_0}. \tag{3.3}$$

Što je amplituda reflektiranog ili difraktiranog signala manja u odnosu na izravni signal, manji je utjecaj na korelacijsku funkciju izravnog signala. Reflektirani i difraktirani signali imaju manju amplitudu A_1 od izravnih signala A_0 jer gube energiju tijekom refleksije i difrakcije. Kao rezultat toga, oblik korelacijske funkcije višestaznog LOS signala s izravnim signalom postaje čisti trokutasti oblik sa samo jednim vrhom (slika [86]).



Slika 3.2: Korelacijska funkcija LOS višestaznog signala [86].

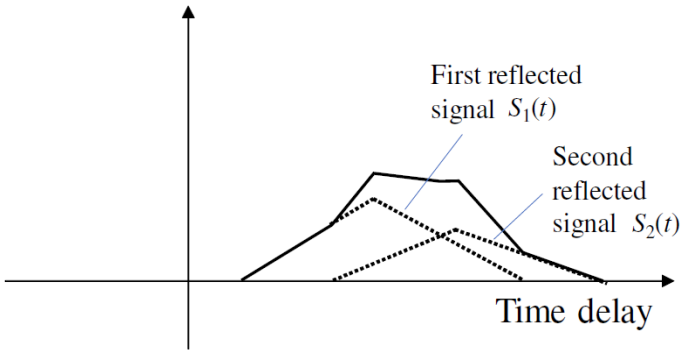
NLOS višestazni signal se može prikazati kao

$$S_{NLOS}(t) = S_1(t) + S_2(t) = S_1(t) + A_2 \cdot C(t - \tau_2) \cdot cos(\omega_0 t + \Delta\phi_2). \tag{3.4}$$

NLOS korelacijska funkcija je kombinacija reflektiranih i difraktiranih signala i nema izravnog signala (slika 3.3). Odnos amplituda kod NLOS signala je definiran

$$\alpha_{NLOS} = \frac{A_2}{A_1}. \tag{3.5}$$

U ovom slučaju, amplituda prvog reflektiranog signala A_1 i drugog reflektiranog signala A_2 ne razlikuju se puno i stoga je odnos amplituda približno jednak 1.



Slika 3.3: Korelacijska funkcija NLOS višestaznog signala [86].

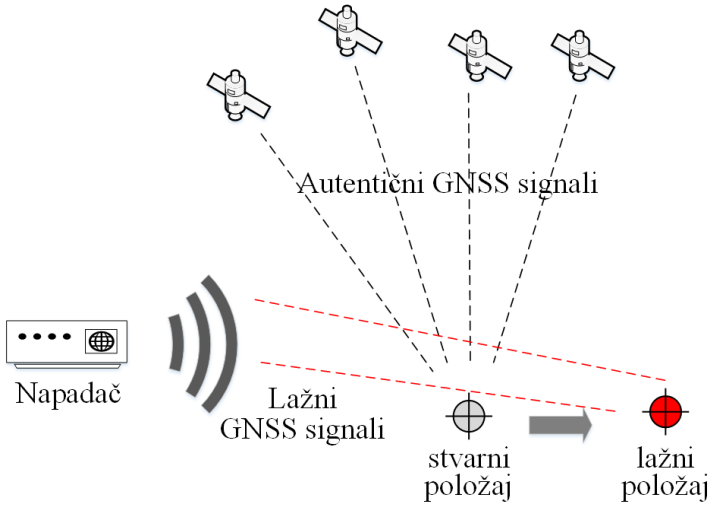
NLOS korelacijska funkcija je osjetljivija na drugi signal u odnosu na LOS korelacijsku

funkciju, što rezultira velikim izobličenjem korelacijske funkcije. Stoga NLOS korelacijska funkcija nema idealan čisti trokutasti oblik.

3.2. Napad lažiranjem u sustavu GNSS

Mobilni telefoni su vrlo osjetljivi na napade lažiranjem lokacije tzv. *spoofing*. Ovakvi napadi se često koriste u vojnim svrhama npr. za preusmjeravanje aviona ili dronova na lažnu lokaciju. Napad lažiranjem predstavlja veliki sigurnosni problem i zato je potrebno razviti nove algoritme i metode za sprječavanje ovih napada te poboljšati postojeće metode.

Pod pojmom napad lažiranjem GNSS signala podrazumijeva se namjerno odašiljanje lažnih GNSS signala s namjerom da prijamnik lažne signale pogrešno protumači kao autentične te u svrhu lažiranja lokacije prijamnika. Osnovne zadaće GNSS prijamnika su primiti i razdvojiti signale sa satelita, izračunati pseudoudaljenosti za svaki satelit na temelju vremena prijama signala, demodulirati navigacijsku poruku kako bi se dobili efemeris podaci te procijeniti PVT rješenje.



Slika 3.4: Napad lažiranjem.

Slika 3.4 prikazuje jednostavan napad lažiranjem. Dakle, napadač (*spoofer*) odašilje lažne signale, koji su veoma slični autentičnim GNSS signalima. Lažni signali imaju veću snagu u odnosu na autentične kako bi se prijamnik zavarao i uzeo te signale. Nakon primanja lažnih signala, prijamnik pokazuje lažnu lokaciju na kojoj se zapravo ne nalazi. U načelu, lažni signal mora imati određene značajke podataka koje odgovaraju onima stvarnog satelitskog signala.

Ove napada je veoma lako izvesti zbog lake dostupnosti jeftinih softverski definiranih radija.

Također, GNSS sustav prisutan je u većini aplikacija za navigaciju i to ga čini još osjetljivijim na napade [12]. GNSS zajednica nije posvećivala dovoljno pozornosti na ovu prijetnju u otvorenoj literaturi sve dok Humphreys i ostali [22] nisu razvili sustav za izvođenje napada lažiranjem GNSS signala te ga uspješno testirali na komercijalnom standardnom prijamniku. U [13] i [40], autori detaljno prikazuju vrste napada lažiranjem i obrambene tehnike koje se razmatraju ili razvijaju. Strategija za detekciju napada lažiranjem na kriptografski zaštićene GNSS signale je prikazana u [55].

Općenito, primljeni GNSS signali se mogu matematički opisati kao kombinacija nekoliko signala [13]

$$y(t) = Re\left\{ \sum_{i=1}^{N} A_i D_i[t-\tau_i(t)] C_i[t-\tau_i(t)] e^{j}[\omega_c t - \phi_i(t)] \right\} \tag{3.6}$$

gdje je N broj GNSS signala, ω_c nominalna frekvencija signala nosioca, A_i amplituda signala, $D_i(t)$ tok podataka signala (navigacijska poruka), $C_i(t)$ PRN kod), $\tau_i(t)$ faza koda, $phi_i(t)$ faza nosioca, za svaki signal i.

Napadač odašilje slične signale, u kojima pokušava reproducirati nosioc i PRN kod te se lažni signal može prikazati kao

$$y_s(t) = Re\left\{ \sum_{i=1}^{N_s} A_{si} D_i[t-\tau_{si}(t)] C_i[t-\tau_{si}(t)] e^{j}[\omega_c t - \phi_{si}(t)] \right\} \tag{3.7}$$

gdje su $\tau_s i(t)$, $phi_s i(t)$ i $A_s i$ faze kodova, faze nosioca i amplitude lažnih signala. Njihove vrijednosti ovise o vrsti napada, i razlikuju se od vrijednosti stvarnih signala. Napadač pokušava što bolje procijeniti tokove podataka koji su označeni s $\hat{D_i}(t)$. Pseudoslučajni nizovi lažnih signala moraju odgovarati stvarnim pseudoslučajnim nizovima kako bi se omogućilo uspješno lažiranje.

Ukupan primljeni signal tijekom napada lažiranjem jednak je

$$y_{tot(t)} = y(t) + ys(t) + v(t) \tag{3.8}$$

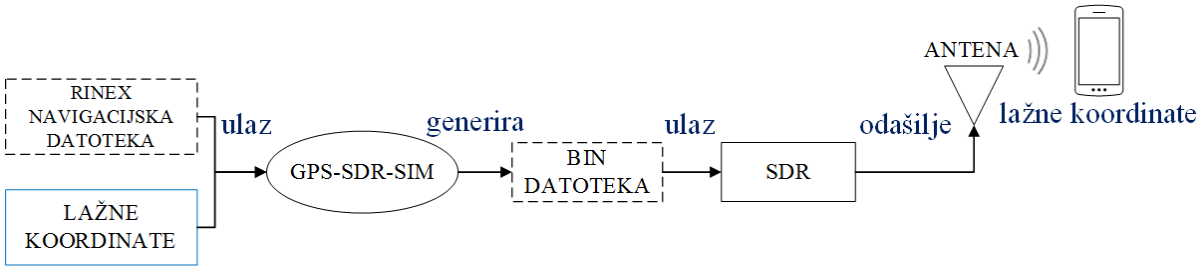
gdje je $v(t)$ primljeni šum. Primljeni šum ponekad može uključivati komponentu šuma koja se dodaje iz napadača. Izvori bijelog šuma u GNSS prijamniku obično se opisuju temperaturnim šumom antene i prijamnika. Temperatura antene modelira šum koji ulazi u antenu s neba, dok temperatura prijamnika modelira toplinski šum zbog gibanja naboja unutar uređaja kao Ľto je prednji dio prijamnika. Ovi izvori šuma određuju gustoću buke. Dodatni šum se javlja prilikom

propagacije signala od antene do prijamnika kao šum aktivne (npr. pojačalo) ili pasivne (kabel) komponente.

3.2.1. Izvođenje napada lažiranjem pomoću softverski definiranog radija

Glavni i najčešće korišteni dio opreme za izvođenje napada lažiranjem je softverski definirani radio. Jedan jeftini SDR može vrlo lako preuzeti navigacijski sustav pametnih telefona i lažirati njihove lokacije što može biti vrlo opasno.

SDR sustavi sastoje se od analogne korisničke aplikacije *(front-end)* i digitalne poslužiteljske aplikacije *(back-end)*. Analogni dio upravlja funkcijama za odašiljanje i primanje.



Slika 3.5: Blok dijagram.

Slika 3.5 prikazuje blok dijagram izvođenja pojednostavljenog napada lažiranjem. Za izvođenje napada potrebno je prikupiti vlastitu RINEX (*Receiver Independent Exchange Format*) navigacijsku datoteku ili istu preuzeti s NASA-ine stranice na linku te definirati lažne koordinate na koje želimo staviti prijamnik ili pametni telefon. RINEX datoteka služi za zapisivanje neobrađenih podataka primljenih sa satelita. Korištenjem navigacijske datoteke i lažnih koordinata kao ulaz za program npr. GPS-SDR-SIM, kreira se bin datoteka koja se odašilje na softverski definirani radio i s njega dalje na prijamnik koji bi ovisno o udaljenosti i snazi predajnika trebao kroz nekoliko sekundi/minuta trebao pokazivati lažnu lokaciju. Predajnik prenosi I/Q modulirane GPS signale na frekvenciji L1 1575.42 MHz.

Na slici 3.6 prikazana je oprema potrebna za izvođenje napada lažiranjem korištenjem softverski definiranog radija: laptop - 1, softverski definirani radio HackRF One koji može primati ili odašiljati signale frekvencija 1 MHz do 6 GHz - 2, antena ANT500 - 3, vanjski oscilator - 4 i pametni telefoni - 5.

Slika 3.6: Oprema za izvođenje napada lažiranjem.

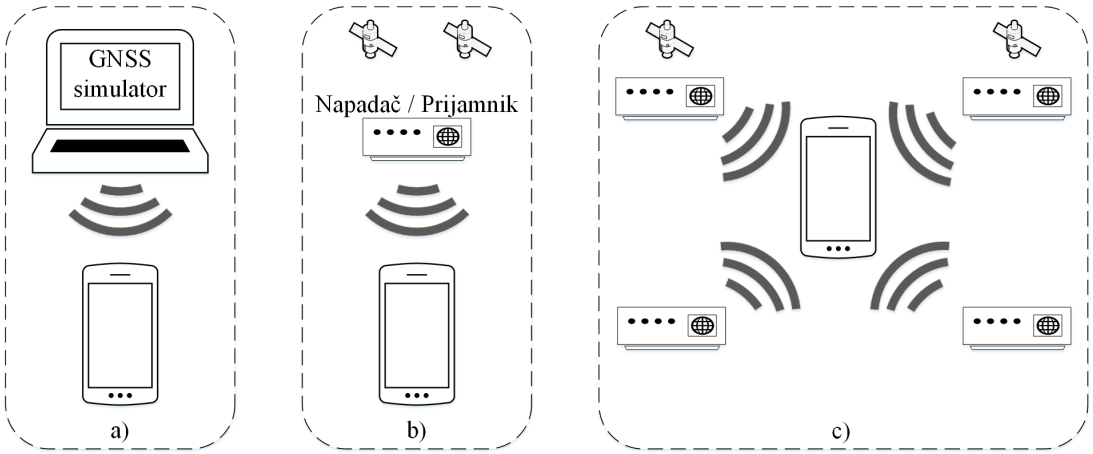
3.2.2. Vrste napada lažiranjem

U novijim istraživanjima, različite vrste napada lažiranjem klasificirane su na temelju kompleksnosti napadača te na poteškoće u detekciji napada lažiranjem sa strane prijamnika.

Iako postoji više vrsta napada, sve se svodi na dva temeljna načina izvođenja napada:

- lažni signali kreiraju se na način da nalikuju autentičnim signalima,
- emitiraju se signali snimljeni negdje drugdje u neko drugo vrijeme.

1. **Pojednostavljeni napad lažiranjem (*simplistic*)** prikazan je na slici 3.7a. Ovaj napad temelji se na korištenju simulatora GNSS signala za kreiranje lažnog signala i njegovo odašiljanje kako bi se zavarao prijamnik. Ovu vrstu napada je veoma lako implementirati jer se koristi jeftina oprema. S druge strane, pojednostavljeni napad je lako detektirati s



Slika 3.7: Vrste napada lažiranjem.

obzirom na to da je potrebna velika snaga lažnog signala kako bi prijamnik zanemario autentični satelitski signal i uzeo lažni, a uz to lažni signal nije sinkroniziran sa satelitskom konstelacijom. Obično se ovi napadi izvode na način da se prvo omete autentični GNSS signal kako bi se prijamnik prisilio na ponovno prikupljanje i zaključavanje na lažni signal. Rezultat pojednostavljenog napada su većinom skokovi u PVT (*Position, Velocity and Time*) izračunima [11].

U [14], autori su pokazali da je lako lažirati lokacije pametnih telefona pomoću pojednostavljenog napada lažiranjem. Predloženi pristup je jednostavan i ekonomičan jer za izvođenje lažnog napada koristi jeftini SDR (HackRF One) [51] i simulator otvorenog pristupa GPS-SDR-SIM [49] koji je distribuiran pod MIT licencom [50]. Lažni signal je kreiran korištenjem simulatora GPS-SDR-SIM na temelju lokacije na koju se lažno želi locirati pametni telefon i navigacijske datoteke. Zatim se lažni kreirani signali prenose na SDR koji ih pretvara u RF signale. Eksperimentalni setup sastoji se od: HackRF One (predajnik koji odašilje GPS L1 signal), pametnog telefona (prijamnik) i ANT 500 antene. Parametri koji su promatrani u ovom eksperimentu su: broj vidljivih satelita, SNR satelita te lokacija pametnog telefona. U provedenim eksperimentima udaljenost između predajnika i prijamnika varira od 1m do 7m. Na udaljenostima do 5m prijamnik dobiva signal dok na udaljenostima većim od 5m prijamnik ne može primiti signal. Eksperimentom je zaključeno da je raspon prijenosa HackRF One 5m. Pametni telefon je uspješno lažno lociran na željenu lokaciju (Mahatma Gandhi Institute of Technology (MGIT)) umjesto svoje stvarne lokacije (Chaitanya Bharathi Institute of Technology (CBIT)). Pokazano je da jeftini setup može lako preuzeti navigacijski sustav pametnog telefona.

Autori u [15] istražuju učinke napada lažiranjem na jedinice za pozicioniranje i navigaciju na masovnom tržištu koje su integrirane u obične Android pametne telefone. Za izvođenje napada se također koriste HackRF One i GPS-SDR-SIM. Pokazano je da pametni telefoni imaju odličnu otpornost na pojednostavljene lažne napade (simplistic) ističući potencijalne slabosti koje treba zaštititi pomoću praktičnih obrambenih mehanizama i protumjera za lažne napade.

2. **Napad lažiranjem srednje razine složenosti (*intermediate*)** ili napad temeljen na prijamniku prikazan je na slici 3.7b. Kod ove vrste napada, napadač ima ugrađen prijamnik koji prati i prikuplja parametre autentičnog satelitskog signala kako bi u skladu s tim signalom generirao lažirani signal te ga odašiljao ciljnom prijamniku. Ova vrsta napada je složena jer lažirani signali trebaju biti sinkronizirani s autentičnim signalima. Izvedivost ovog napada je dokazana kao i mogućnost promjene položaja prijamnika bez podizanja upozorenja ili stvaranja diskontinuiteta u PVT rješenju [22].

3. **Sofisticirani napad lažiranjem (*sophisticated*)** je najsloženija vrsta napada koja je prikazana na slici 3.7c. Ova vrsta napada koristi nekoliko napadača srednje razine koji generiraju i prenose lažne GNSS signale [11]. U ovom slučaju, napad se ne može jednostavno detektirati gledajući kut dolaska signala zbog toga što signali dolaze iz različitih kuteva i od različitih napadača. Međutim, ovi napadi imaju mnogo veću razinu složenosti zbog procesa sinkronizacije i komunikacije između svakog pojedinačnog odašiljača, što ga čini vrlo teškim za realizaciju i neprikladnim za scenarije u realnom vremenu. Također, sofisticirani napad lažiranjem nije isplativ ni što se tiče ekonomske strane jer zahtijeva dodatnu i skupu opremu (nekoliko napadača tj. predajnika i antena) [13].

3.3. Ometanje signala

Ometanje signala može se opisati kao namjerno odašiljanje signala visoke radio frekvencije koja je jednaka ili vrlo bliska frekvenciji uređaja čiji rad se želi spriječiti. Ometanje ima za cilj spriječiti prijamnik u prikupljanju i praćenju GNSS signala te navigaciji pomoćuGNSS signala. Jednostavno rečeno, ometanje se događa zbog prijenosa visokih radiofrekvencija blizu frekvencijskih pojasa L1, L2 i L5 na kojima rade GNSS prijamnici. Frekvencije koje ometaju imaju namjeru preopteretiti prijamnike do te mjere da prijamnici izgube zaključavanje na satelite. S obzirom na obilje uređaja koji odašilju na frekvencijama bliskima GNSS prijamnicima, moguće

je da neki od tih uređaja nenamjerno ometa GNSS signale. Ometanje uzrokuje gubitak točnosti i potencijalno gubitak pozicioniranja. Za razliku od napada lažiranjem, ometanje ne zahtijeva točno rekreiranje signala. Budućida GNSS signali putuju preko velike udaljenosti kako bi došli do prijamnika, imaju malu snagu signala. Stoga su osjetljivi na smetnje, slučajne i namjerne. Kod ometanja se odašiljač koristi za stvaranje radio signala više ili iste frevencije kao GNSS signali kako bi se izazvale namjerne smetnje koje GNSS prijamnicima otežavaju primanje bilo kakvog signala. Ometanje je još problematičnije od napada lažiranjem jer su npr. GPS ometači relativno mnogo jednostavniji i lakši za izradu od uređaja za lažiranje. Čak i mali ometači koji stanu u dlan mogu izazvati ometanja u rasponu od nekoliko metara. Ometač može blokirati sve radijske komunikacije na bilo kojem uređaju koji radi na radio frekvencijama unutar svog dometa i emitirati radiofrekvencijske valove koji sprječavaju ciljani uređaj od uspostavljanja ili održavanja veze [61].

Slika 3.8: GPS ometač (lijevo) i skupi prijenosni GNSS/Wi-Fi/mobilni ometač (desno)[62].

Slika 3.8 prikazuje uređaje za ometanje signala. Ovi uređaji su jeftini i lako dostupni. Lijevi uređaj se naziva GPS ometač za vozila i jednostavno se uključi u bilo koji upaljač za cigarete ili utičnicu za napajanje vozila. Njegov domet je oko 10 m. Desni uređaj je skuplji prijenosni GNSS/Wi-Fi/mobilni ometač koji odašilje radio signale kako bi prekinuo komunikaciju između mobitela i baznih postaja.

Ometajući (interferencijski) signal se može jednostavno opisati kao

$$i(t) = A_I cos(2(f_{RF} + f_I)t + \phi_I) \tag{3.9}$$

gdje su A_I, f_{RF}, f_I i ϕ_I amplituda ometajućeg signala, centralna frekvencija, vremenski promjenjiva frekvencija smetnje i faza ometajućeg signala.

Kao i kod napada lažiranjem, ukupan signal na prijamu jednak je zbroju stvarnog signala koji je sastavljen od različitih komponenti koje dolaze s vidljivih GNSS satelita, ometajućeg signala, mogućeg lažnog signala i šuma.

4. Metode za detekciju interferencija u prijamnicima sustava GNSS

4.1. Metode za detekciju višestaznih signala

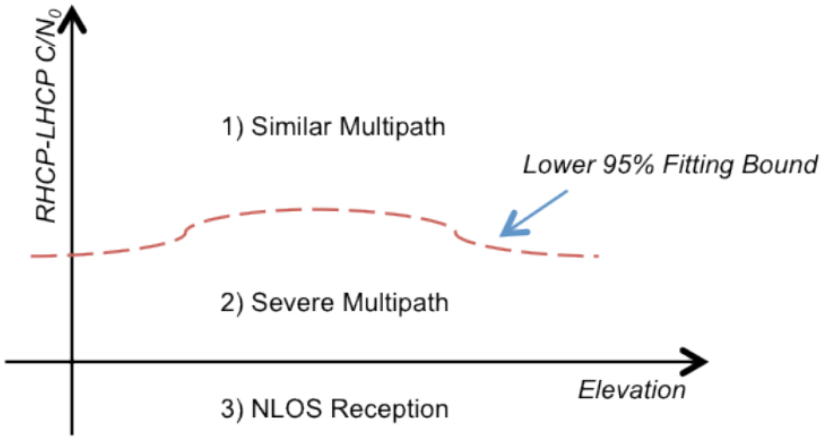
Višestazno prostiranje GNSS signala je najizraženije u urbanim kanjonima u kojima ne postoji izravna vidljivost između satelita i antene prijamnika nego signal različitim putanjama dolazi do prijamnika i na taj način mu se smanjuje snaga, a povećava prijeđeni put odnosno pseudoudaljenost. U urbanim područjima teško je postići visoku točnost pozicinirania s GNSS sustavima jer se signali u mnogim slučajevima reflektiraju od zgrada [63]. Korištenje reflektiranih GNSS signala za pozicioniranje može rezultirati pogreškom pozicioniranja većom od 100m [64].

Postoje različite metode za detekciju višestaznih signala tj. samo NLOS signali ili NLOS i LOS signali istovremeno koji degradiraju performanse. Tradicionalna metoda detekcije višestaznih signala koristi C/N_0 GNSS signala [65], [66], [67]. Definiranjem praga za C/N_0 vrijednosti, signal koji ima C/N_0 veći od praga se klasificira kao LOS signal dok se signal koji ima C/N_0 manji od praga klasificira kao NLOS signal ili NLOS + LOS signal. Osim toga, postoje metode detekcije koje se temelje na hardveru i koje koriste posebne antene ili niz antena [68], dual-polarizacijske antene [78], [79], kamere usmjerene prema nebu (*sky-pointing camera*) [69], [70], metoda koja koristi 3D model grada [71], [72],[73], [74], [75] i algoritme praćenja zraka [71], [76], metoda podudaranja sjeni [84]. Nadalje, najaktualnije metode za detekciju višestaznih signala u današnje vrijeme se temelje na strojnom učenju [89] i na njih je stavljen najveći naglasak u ovom radu.

4.1.1. Klasična metoda temeljena na omjeru snage signala nosioca i šuma

Klasična metoda otkrivanja višestaznih signala koja se temelji samo na promatranju C/N_0 [65], [78]. Vrlo dobar C/N_0 je izmjeren za sve pozitivne vrijednosti kuta elevacije. Što je manji kut elevacije, veća je mogućnost za višestaznim signalima. Razmatrana su tri slučaja:

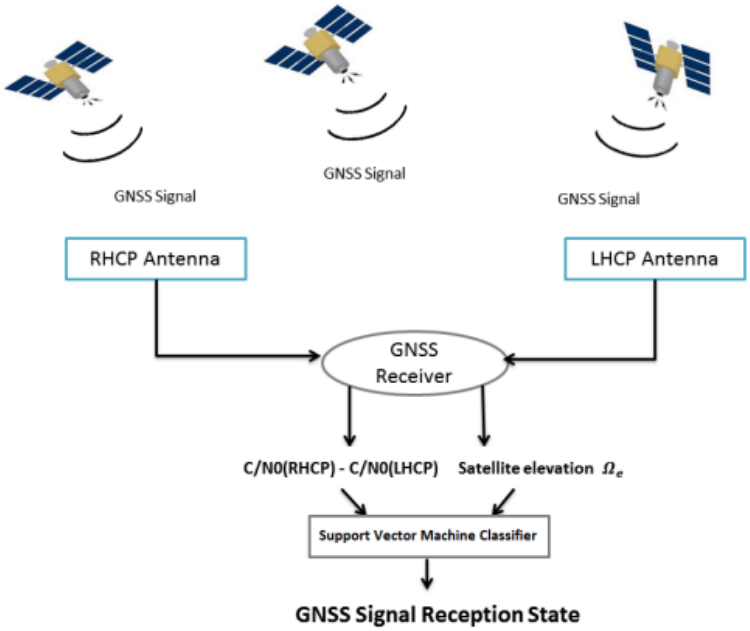
- Niska višestaznost (*similar multipath*) - ako izmjerena C/N_0 razlika leži unutar granica od 95% podešene funkcije, tada se može pretpostaviti da će signal vjerojatno biti podložan niskoj razini višestaznih smetnji.
- Visoka višestaznost (*severe multipath*) - ako je razlika C/N_0 pozitivna, ali leži ispod donje granice podešene funkcije, tada postoji značajna vjerojatnost da je signal podložan visokoj razini višestaznih smetnji.
- NLOS prijam - ako je razlika C/N_0 negativna, tada je vjerojatno da je izravni LOS signal blokiran i da se primaju samo reflektirani signali.



Slika 4.1: Usporedba vrijednosti C/N_0 [70].

4.1.2. Korištenje različitih metoda u kombinaciji sa strojnim učenjem

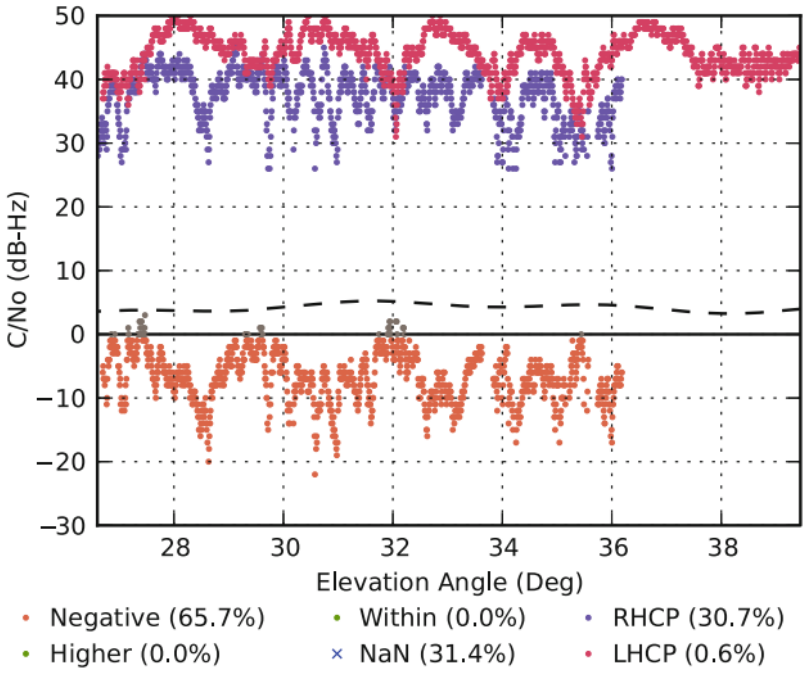
U ovom potpoglavlju prikazane su različite metode detekcije višestaznih signala u kombinaciji sa strojnim učenjem. Navedene metode detekcije koriste dual-polarizacijske antene, 3D modela zgrada, algoritam praćenja zraka, algoritam podudaranja sjeni i korelacijske funkcije.



Slika 4.2: Shema predloženog SVM klasifikatora [79].

Autori u [78] istražuju potencijal dual-polarizacijskih antena za detekciju NLOS signala te provode klasifikaciju signala temeljenu samo na C/N_0. Predložena je nova metoda tzv. C/N_0 diskriminator, koja izračunava $C/N_0 - R - L$ vrijednost tj. razliku C/N_0 mjerenja dobivenih od lijevo kružno polarizirane LHCP (*Left-Hand Circular Polarization*) i desno kružno polarizirane RHCP (*Right-Hand Circular Polarization*) antene. Na slici 4.3 prikazan je primjer prijama NLOS signala koji je identificiran korištenjem pragova temeljenih na C/N_0. Negativna C/N_0 razlika je prikazana narančastom bojom i označena je kao NLOS prijam, a identificirani signal je od satelita s niskim kutom elevacije. U [79], autori se također bave problemom vezanim za detekciju stanja primljenog GNSS signala (LOS, NLOS ili višestazni) u svrhu poboljšanja lokalizacije vozila u urbanim kanjonima. Međutim, njihov predloženi sustav se zasniva na objedinjavanju podataka dobivenih od RHCP i LHCP antene i SVM metodi strojnog učenja koja kao ulazne parametre za klasifikaciju uz $C/N_0 - R - L$ omjer ima i kut elevacije što je prikazano na slici 4.2. Novi klasifikator GNSS signala je predložen u [80]. Ova metoda se zasniva na fuziji podataka dobivenih od RHCP i LHCP antene te metodama strojnog učenja (stablo odlučivanja, SVM i KNN) za inteligentne transportne sustave. Dana je poredbena analiza različitih metoda strojnog učenja i kao najbolja metoda pokazala se stablo odlučivanja uz točnost klasifikacije od 99%.

U [81] razvijen je algoritam za detekciju NLOS signala iz mjerenja pseudoudaljenosti koristeći 3D model zgrada, simulaciju praćenja zraka i poznatu poziciju prijamnika. Nadalje,

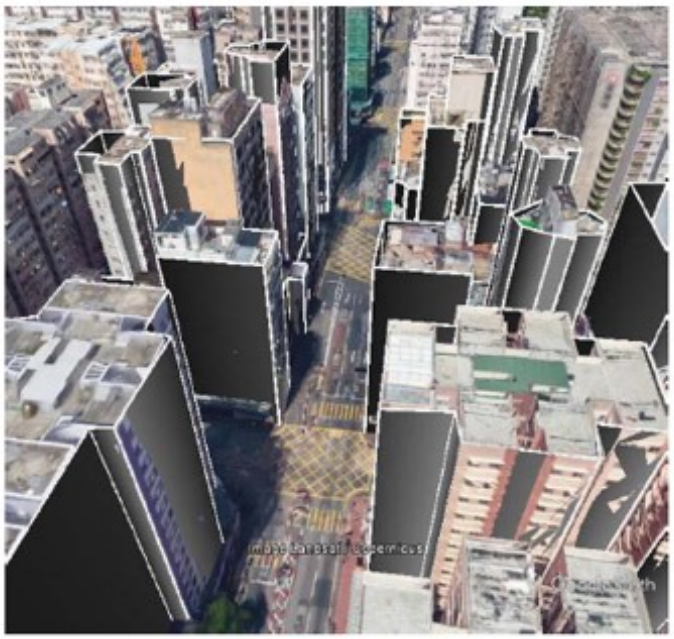


Slika 4.3: Identificirani NLOS prijam [78].

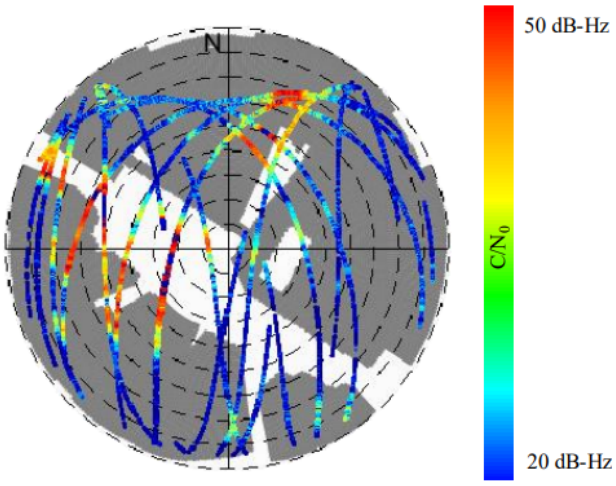
predložen je novi pristup za klasifikaciju LOS/NLOS signala korištenjem stabla odlučivanja (algoritam nadziranog strojnog učenja). Uz dovoljno veliki skup podataka za treniranje, predloženi pristup može predvidjeti status vidljivosti satelita u gustim urbanim područjima s velikom sigurnošću (preko 85%). Autori u [76] predlažu klasifikator koji se temelji na SVM nadziranoj metodi strojnog učenja za klasifikaciju signala u tri kategorije: LOS, NLOS i višestazni koristeći dodatne ulazne parametre (kako bi se naznačila dosljednost između mjerenja pseudoudaljenosti i Dopplerova pomaka). U radu je uspoređena klasifikacija po jednom i više parametara te je pokazano da razlika između delta pseudoudaljenosti i stope dosljednosti pseudoudaljenosti ima pozitivan utjecaj na klasifikaciju. U radu je korišten algoritam praćenja zraka za preciznu simulaciju reflektiranih signala u urbanom okruženju koristeći model urbanog grada (cilj je ući u trag reflektiranim zrakama). 3D model zgrada je konstruiran na temelju Google Earth-a i prikazan je na slici 4.4.

Slika 4.5 prikazuje nebo s okolnim zgradama u urbanom kanjonu u Hong Kongu. Siva boja označava da je blokiran direktan signal dok crvena boja označava veću primljenu snagu signala, a plava manju primljenu snagu signala (manji kut elevacije). Sa slike je vidljivo da LOS signali imaju veću snagu.

Autori u [82] predlažu integraciju algoritma podudaranja sjeni (*shadow matching*) za poboljšano pozicioniranje s LOS/NLOS klasifikatorom. Napravljena je implementacija i uspo-



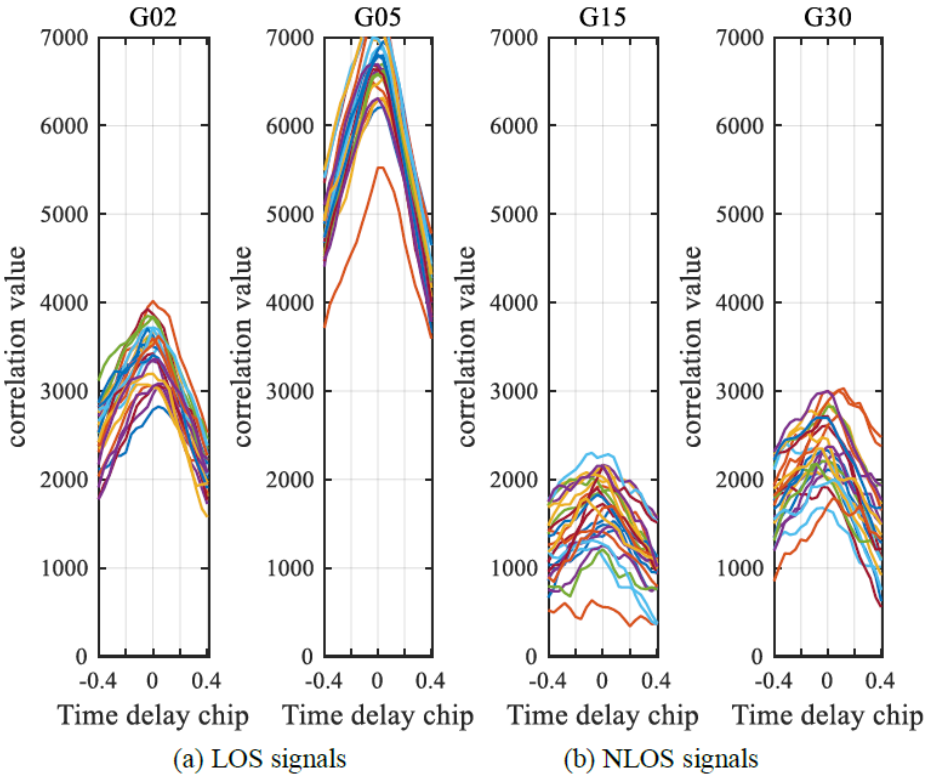
Slika 4.4: 3D model zgrada [78].



Slika 4.5: Prikaz neba s okolnim zgradama u Hong Kongu [76].

redba različitih metoda strojnog učenja npr. KNN, neuralna mreža, SVM, stablo odlučivanja te jednostavni SNR klasifikator. Rezultati su pokazali da većina modela ima veoma dobru točnost kada se uzme u obzir samo SNR dok SVM ima najbolje performanse u različitim urbanim scenarijima. U [83], autori predlažu primjenu SVM metode strojnog učenja za određivanje vidljivosti satelita (LOS/NLOS klasifikacija) na temelju više značajki u urbanim sredinama (Hong Kong). Također, predlažu poboljšanu metodu podudaranja sjena za pozicioniranje korisnika u urbanim sredinama. Metoda podudaranja sjena je poboljšana koristeći dva parametra: procijenjeni početni položaj i vidljivost satelita. Rezultati pokazuju poboljšanu točnost pozicioniranja

te da SVM klasifikacija može doseći točnost od 91.5% u urbanim scenarijima. Poboljšani algoritam podudaranja sjeni koji koristi 3D model grada uz optimiziranu shemu ocjene vidljivosti je prikazan u [84]. Poboljšana je učinkovitost procesa koji se koristi za generiranje mreže granica zgrada koja se koristi za predviđanje satelitske vidljivosti. Podaci su prikupljeni na 22 različite lokacije. Autori u [74] predlažu algoritam za predviđanje i isključivanje višestaznih signala. Predloženi algoritam koristi metodu praćenja zraka (*ray-tracing*) na 3D modelu zgrada i popraćen je isključenjem satelita u slučaju da su NLOS.



Slika 4.6: Izgled korelacijske funkcije za LOS i NLOS signal [85].

U GNSS pozicioniranju, zgrade često ometaju GNSS satellite što dovodi do refleksije i difrakcije signala tj. NLOS signala. Autori u [85] predlažu novi SVM klasifikator koji na temelju korelacijske funkcije signala detektira i eliminira NLOS signale i propušta samo LOS signale koji se onda koriste za pozicioniranje u urbanim okolinama. Eksperimenti pokazuju da je 87% LOS i 99% NLOS signala ispravno klasificirano. Slika 4.6 prikazuje korelacijske izlaze za LOS i NLOS signale. Može se vidjeti da korelacijska funkcija NLOS signala nema jasan vrh u središtu kao što ima LOS signal, a mnogo lokalnih maksimuma postoji u svim drugim točkama osim u vrhu. Nadalje, NLOS signali imaju manji korelacijski vrh od LOS signala, čak i za satelit s istim kutom elevacije. U [86] autori daju poredbenu analizu SVM metode i neuralnih mreža za detekciju NLOS višestaznih signala (koji uzrokuju velike greške pozicioniranja) koja se temelji

na korištenju korelacijskog izlaza GNSS signala. Pokazano je da je metoda neuralnih mreža bila točnija od SVM metode i da je 97,7% NLOS signala ispravno detektirano. U prethodno navedenim radovima setovi podataka za treniranje i testiranje su prikupljeni na istim lokacijama. U radu [90] dana je usporedba različitih metoda strojnog učenja uz korištenje setova podataka za treniranje i testiranje koji su prikupljeni na istim i različitim lokacijama. Pokazano je da je točnost klasifikacije veća u slučaju kada su setovi podataka za treniranje i testiranje prikupljeni na istim lokacijama 82% - 96% dok je u slučaju različitih lokacija točnost 44% - 77%. Kao nastavak ovog rada, model temeljen na stablu odlučivanja za klasifikaciju GPS signala uz korištenje dvostruko polariziranih antena je dan u [91]. Točnost ovog modela je uspoređena s modelom temeljenim na stablu odlučivanja, a koji koristi jednostruko polarizirane antene. Dana je i usporedba setova podataka prikupljenih na istim i različitim lokacijama. Pokazano je da je bolje rješenje korištenje dvostruko polariziranih antena zbog kompaktnijeg oblika.

Slika 4.7: Urbani kanjon - Seoul, Korea [88].

Autori u [88] predlažu model za predviđanje višestaznog prostiranja temeljen na regresiji potpornog vektora SVR (*Support Vector Regression*) kako bi se dobila funkcija elevacije i azimuta za svaki satelit. Generirana je nelinearna višestazna mapa koja na odgovarajući način odražava geometriju zgrade u blizini korisnika. Ovaj model se pokazao učinkovitim u poboljšanju točnosti pozicioniranja u dubokim urbanim područjima (Korea) - slika 4.7. Budući da ovaj nelinearni model koristi samo relativni smjer satelita od korisnika, sve vrste signala i prijamnika mogu uobičajeno koristiti ovaj model bez ikakve klasifikacije signala ili vrsta refleksije. Bez

ikakve pomoći prethodnih informacija o zgradi, višestazna karta modelirana metodom nelinearne regresije odražava točno kako se zgrada vidi s tla.

Višestazno prostiranje signala utječe na performanse navigacije i pozicioniranja. Metoda detekcije višestaznih signala korištenjem konvolucijskih neuralnih mreža za vrlo precizno pozicioniranje je prikazana u [87]. Ova metoda se temelji na činjenici da se značajke višestaznog prostiranja u kontaminiranim podacima mogu naučiti i identificirati od strane konvolucijske neuralne mreže. Predložena metoda je potvrđena sa simuliranim i stvarnim GPS statičkim i kinematičkim podacima.

4.2. Metode za detekciju ometanja i lažnih signala

Metode detekcije lažnih GNSS signala imaju za primarni cilj otkrivanje napada lažiranjem kako bi upozorile prijamnik da podaci o njegovoj lokaciji i vremenu nisu točni. Potrebno je razumjeti svojstva različitih napada kako bi se razvila dobra obrana od samog napada.

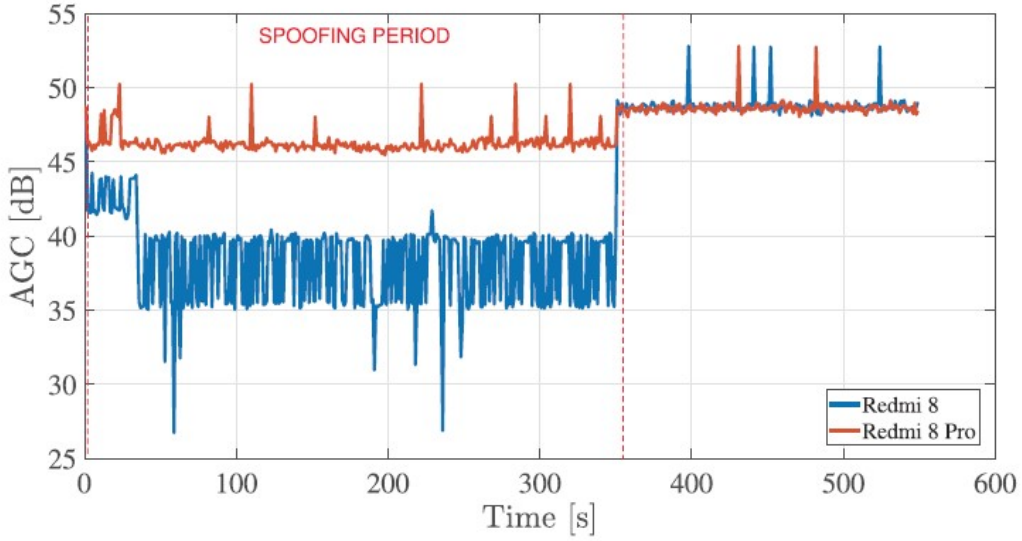
Postoje različite metode detekcije lažnih signala: klasične metode temeljene na promatranju C/N_0, pseudoudaljenosti i različitih parametara, klasične metode koje se temelje na promatranju korelacijskih funkcija signala, metode temeljene na simulatorskom hardveru (npr. simulator poput Spirenta) koje nisu ekonomične [30], metode koje počivaju na korištenju niza antena, metode koje koriste NMEA (*National Marine Electronics Association*) poruke [31] te metode strojnog učenja.

Korisnički uređaj koji prima lažne signale i vjeruje da je autentičan može potaknuti opasno ponašanje zbog pogrešnog položaja ili ispravki vremena. Primjer je spomenut u [12], gdje je lažiranje GPS signala korišteno za krivo usmjeravanje drona u neplanirano ronjenje i za skretanje jahte s kursa. Stoga je obrana od prijevare usmjerena na otkrivanje napada kako bi se napadnuti prijamnik upozorio da su njegov izračunati položaj i pomak sata nepouzdani. Dan je prikaz različitih metoda napada lažiranjem.

4.2.1. Strojno učenje u kombinaciji s promatranjem klasičnih parametara i korištenjem softverski definiranog radija

U [46], autori prikazuju eksperimentalne rezultate osjetljivosti pametnih telefona na pojednostavljeni napad lažiranjem. Učinci osjetljivosti pametnih telefona se očituju kroz neobrađena mjerenja parametara npr. C/N_0, automatsko upravljanje pojačanjem AGC (*Automatic Gain*

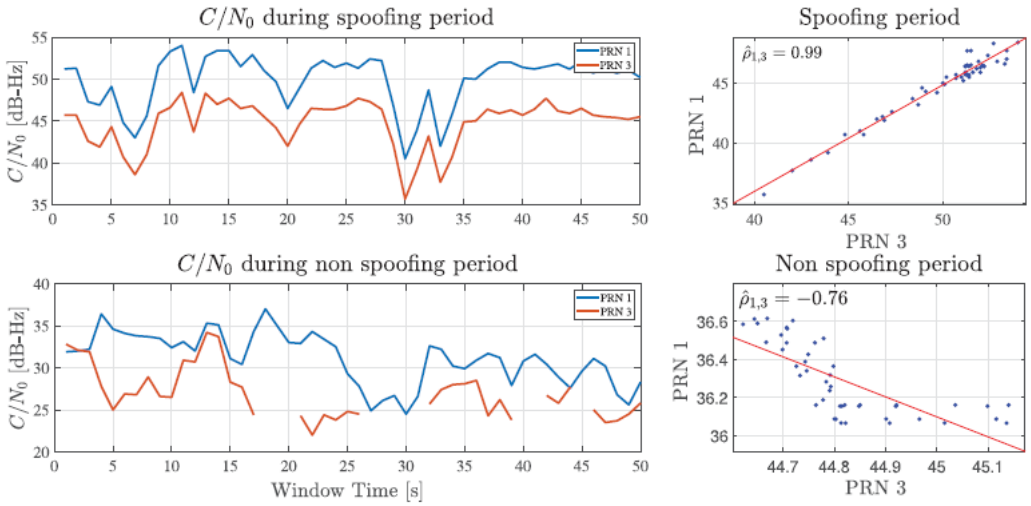
Control), pseudoudaljenosti i procjene pozicije. Autori reproduciraju dva scenarija pojednostavljenog napada lažiranjem.



Slika 4.8: Usporedba AGC parametra između dva Android uređaja prilikom napada lažiranjem [46].

Slika 4.8 prikazuje AGC vrijednosti za dva Android uređaja (Redmi 8 i Redmi 8 Pro) prilikom napada lažiranjem. Napad lažiranjem traje od $0-350s$. U trenutku $t = 350s$ kada napad lažiranjem završava, AGC vrijednost se povećava na svoju početnu razinu kao što se može vidjeti sa slike. Skok u AGC vrijednosti za Redmi8 uređaj može biti posljedica gubitka kačenja na autentične signale i ponovnog praćenja te kačenja na lažne signale. Velika snaga i postojanost lažnog signala mogu biti čimbenik u određivanju praznina u mjerenjima. Primjerice, ukoliko je lažni signal dovoljno snažan i postojan, GNSS prijamnik može izgubiti povezanost odnosno "kačenje" na signale na duži period što rezultira prazninom u GNSS mjerenjima. S druge strane, ako je lažni signal slab i manje postojan, prijamnik može zadržati kačenje na autentične signale i proizvesti kontinuirani izlaz, unatoč prisutnosti lažnih signala. Različiti prijamnici imaju različite osjetljivosti i druge značajke koje utječu na otpornost na napade lažiranjem.

Praćenje snage signala je najjednostavniji način detekcije napada lažiranjem jer je snaga lažnog signala puno veća u odnosu na autentični signal. Osim po većoj snazi signala, lažni signal se može detektirati po konstantnom Dopplerovom pomaku jer se napadač nalazi na istoj lokaciji. Kod stvarnih satelitskih signala, Dopplerov pomak je dinamičan i stalno se mijenja ovisno o kretanju prema ili od satelita. Dodatni parametri po kojima se mogu prepoznati lažni signali su konstantna pseudoudaljenost i konstantni kut elevacije jer napadač odašilje s fiksne



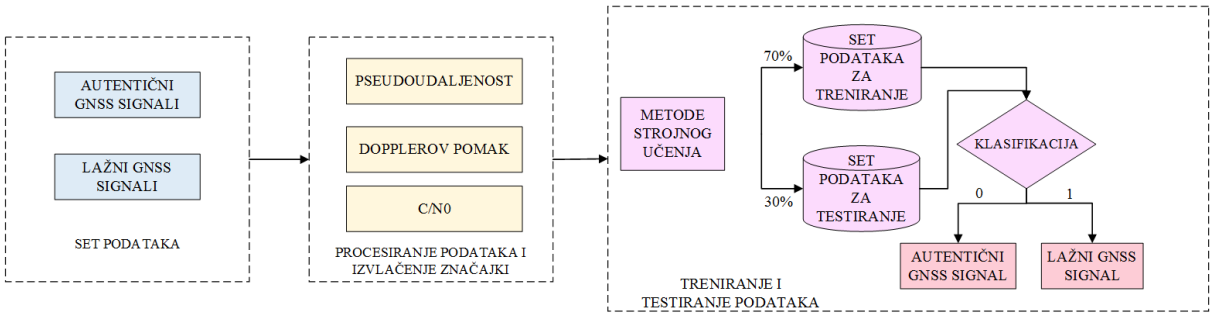
Slika 4.9: Usporedba C/N_0 za različite satelite tijekom i bez napada lažiranjem [46].

lokacije. U slučaju dinamičkog napada, trebalo bi postojati nekoliko lokacija s kojih napadač odašilje i tada bi bilo teže detektirati lažne signale.

Klasična detekcija lažnog signala temeljena na C/N_0 je predložena u [54], gdje je izmjereni C/N_0 primljenih GNSS signala uspoređen s poznatom ili očekivanom vrijenosti. U [15] autori uz C/N_0 za detekciju napada lažiranjem prate i pseudoudaljenosti. S druge strane, autori u [28] skupa s pseudoudaljenostima i snagom signala razmatraju i korelacijsku distorzijsku funkciju. U [36] and [17], lažni GNSS signali su detektirani na temelju korelacijskih vrhova i faznih razlika između lažnih i autentičnih signala. Eksperimentalni rezultati osjetljivosti pametnih telefona na pojednostavljeni napad lažiranjem su prikazani u [46]. Slika 4.9 prikazuje usporedbu C/N_0 vrijednosti za GPS PRN 1 i PRN 3 tijekom (gore) i bez (dolje) napada lažiranjem za Xiaomi Redmi 8. Tijekom napada lažiranjem, C/N_0 za oba satelita je u rangu 35-55 dB-Hz dok je u uvjetima bez napada vidljiva osjetna razlika u kojima C/N_0 ima vrijednosti od 20-40 dB-Hz s laganim trendom opadanja i diskontinuiteta pri nižim vrijednostima. Korelacija između vrijednosti za oba slučaja je potvrđena linearnom regresijom i Pearsonovim koeficijentom korelacije. U slučaju napada lažiranjem, postoji veća korelacija između vrijednosti s koeficijentom 0.99 dok je bez napada niska korelacija s koeficijentom -0.76 zbog diskontinuiteta podataka i različitih trendova. Učinci osjetljivosti pametnih telefona se ogledaju kroz njihova neobrađena mjerenja npr. C/N_0, pseudoudaljenosti i procjene položaja. Utjecaj napada lažiranjem na pametne telefone je analiziran u [53]. Autori predlažu tehnike za povećanje sigurnosti kao što je upotreba jeftinih senzora ubrzanja.

Pojednostavljeni napad lažiranjem je izveden u [52] pomoću softverski definiranog radija.

GPS signali su snimljeni i ponovno odašiljani na pametne telefone. GPS Test aplikacija je korištena za praćenje rezultata napada tj. parametara: dostupni sateliti i njihov C/N_0. U slučajevima u kojima C/N_0 diskriminacija ima ograničenu učinkovitost, prijamnik može mjeriti apsolutnu snagu korelacijskih vrhova, i ova metoda je učinkovita za detekciju i diskriminaciju izvora napada. Autori u [56] pokazuju da praćenje apsolutne snage signala značajno samnjuje područje osjetljivosti prijamnika u usporedbi s praćenjem C/N_0. U [57], autori predlažu metodu za detekciju napada lažiranjem i ometanja signala temeljenu na automatskoj kontroli pojačanja i C/N_0 observacijama. Napad lažiranjem će vjerojatno biti detektiran kada se AGC vrijednost smanji, i C/N_0 je relativno konstantan ili čak povećan. Međutim, AGC nije dovoljan za detekciju prisustva lažnog signala, nego samo za podizanje upozorenja. Stoga bi se AGC trebao koristiti u kombinaciji s C/N_0.



Slika 4.10: Dijagram toka modela strojnog učenja za klasifikaciju signala.

Na slici 4.10 prikazan je dijagram toka modela strojnog učenja za klasifikaciju signala. Prvi korak je prikupljanje seta podataka (autentični i lažni signali). U drugom koraku se izvlaÄŤe parametri po kojima će se vršiti klasifikacija signala. Zadnji korak je primjena metoda strojnog učenja tj. treniranje i testiranje modela na prikupljenim podacima. Kao rezultat model klasificira signale na autentične i lažne na temelju parametara korištenih za treniranje i testiranje.

U [45], autori uspoređuju performanse nekoliko nadziranih modela s onima nenadziranih modela u smislu točnosti, vjerojatnosti otkrivanja, vjerojatnosti pogrešnog otkrivanja, vjerojatnosti lažnog alarma, vremena obrade, vremena obuke, vremena predviđanja i veličine memorije. Rezultati pokazuju da klasifikacijski i regresijski modeli stabla odlučivanja nadmašuju ostale nadzirane i nenadzirane modele u otkrivanju i klasificiranju GPS napada lažiranjem.

U [23] i [24] autori uspoređuju izvedbu nekoliko ML (*Machine Learning*) algoritama u otkrivanju napada lažiranjem GPS signala. Autori u [23] provode K-fold analizu kako bi odabrali najbolji ML algoritam između nekoliko ML algoritama Na temelju njihovih rezultata, metoda potpornih vektora SVM (*Support Vector Machine*) s polinomskom jezgrom nadmašuje ostale

metode. S druge strane, rezultati i analiza ML algoritama u [24] pokazuje da algorimi temeljeni na stablima odlučivanja daju bolje rezultate u odnosu na SVM (linearni i radijalni), K najbližih susjeda i ostale analizirane algoritme.

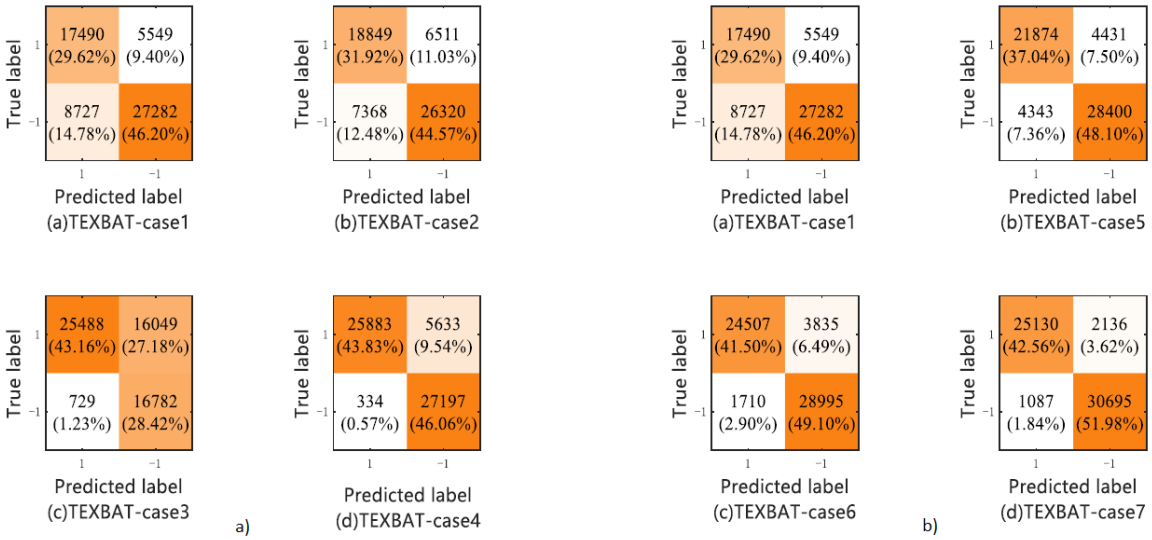
U [18], autori predlažu detekciju lažnih GNSS signala korištenjem SVM metode strojnog učenja uz kombinaciju stvarnih i simuliranih setova podataka za provjeru i validaciju algoritama strojnog učenja. Rezultati pokazuju da je SVM metoda obećavajući pristup za detekciju lažnih signala. Međutim, ovo istraživanje ne analizira razloge za odabir određenih parametara te kombinaciju i sklonost prema odreženim značajkama. Većina postojećih algoritama za otkrivanje napada lažiranjem koristi postojeći set podataka TEXBAT koji je objavilo Sveučilište Texas [19], s relativno fiksnim scenarijima. Albright i ostali iz Nacionalnog laboratorija Oak Ridge, SAD, objavili su još jedan gotovi set podataka OAKBAT [20] koji sadrži lažne signale GPS i Galileo, pružajući više testnih scenarija za istraživanje otkrivanja napada lažiranjem.

Autori u [34] predlažu GNSS više-parametarsku metodu zajedničke detekcije koja se također temelji na SVM metodi obradom i usporedbom setova podataka TEXBAT i OAKBAT. Dobiveni rezultati pokazuju značajno poboljšanje u performansama otkrivanja lažnih signala u usporedbi s tradicionalnim jedno-parametarskim metodama. S druge strane, autori u dijelu I [38] koriste tri sintetički generirana (simulirana) seta podataka lažnih signala sa Spirent simulatorom za treniranje i verifikaciju i dva seta podataka za provjeru valjanosti modela stvorena korištenjem softverski definiranih radija LimeSDR i HackRF. Autori koriste C-SVM metodu nadziranog strojnog učenja za otkrivanje lažnih signala. U dijelu II [39], autori nadopunjuju eksperimente i rezultate dobivene u I. dijelu. Uz laboratorijski generirane setove podataka lažnih signala koji su u dijelu I korišteni za treniranje modela, dodani su setovi podataka lažnih signala u stvarnom vremenu u fazi treniranja C-SVM metode.

Slika 4.11 prikazuje konfuzijsku matricu za detekciju napada lažiranjem uz korištenje različitih parametara - a) i kombinacije različitih parametara b). Sa slika je vidljivo da se točnost SVM metode poboljšala u slučaju sedam, u kojem je korišteno svih devet parametara, sa 75.82% na 95.54%.

U preglednom radu [25], dane su preporuke za istraživače te je zaključeno da su ML metode obećavajući pristup za primjenu u GNSS sustavima.

Budući da su bespilotne zračne letjelice (UAS) vrlo osjetljive na ovu vrstu napada, autori u [26] provode usporedbu nekoliko modela nadziranog strojnog učenja koji se temelje na stablu kako bi otkrili lažne napade i prikupili stvarne GPS signale pomoću SDR-a. U [37], autori



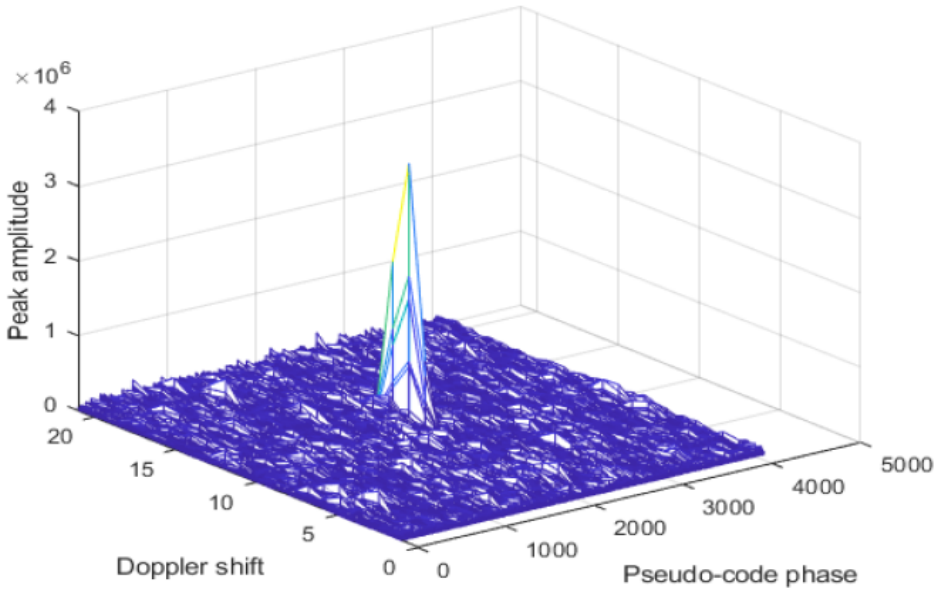
Slika 4.11: Konfuzijska matrica za detekciju napada lažiranjem u TEXBAT setu podataka [34].

vrednuju pet modela strojnog učenja temeljenih na instancama za otkrivanje lažnih GPS signala. Također, autori koriste SDR jedinicu za prikupljanje i izdvajanje značajki satelitskih signala te simuliraju tri vrste napada lažiranjem (pojednostavljeni napad, napad srednje razine složenosti i sofisticirani napad). Rezultati pokazuju da Nu-SVM ima najbolje performanse.

Autori u [28] predlažu navigaciju u okruženju u kojem se događa napad lažiranjem GNSS signala uzimajući u obzir primljenu snagu, funkciju izobličenja korelacije i pseudoudaljenosti. U setu podataka se koriste i stvarna i lažna mjerenja. Strojno učenje prikazuje autentična mjerenja iz dostupnog seta pomoću parametara kao što su primljena snaga i izobličenje korelacijske funkcije. U radu je korišteno nekoliko metoda strojnog učenja za klasifikaciju i detekciju lažnih signala. Kao najbolje metode, pokazale su se neuralne mreže i linearni SVM s točnošću od 98,20%.

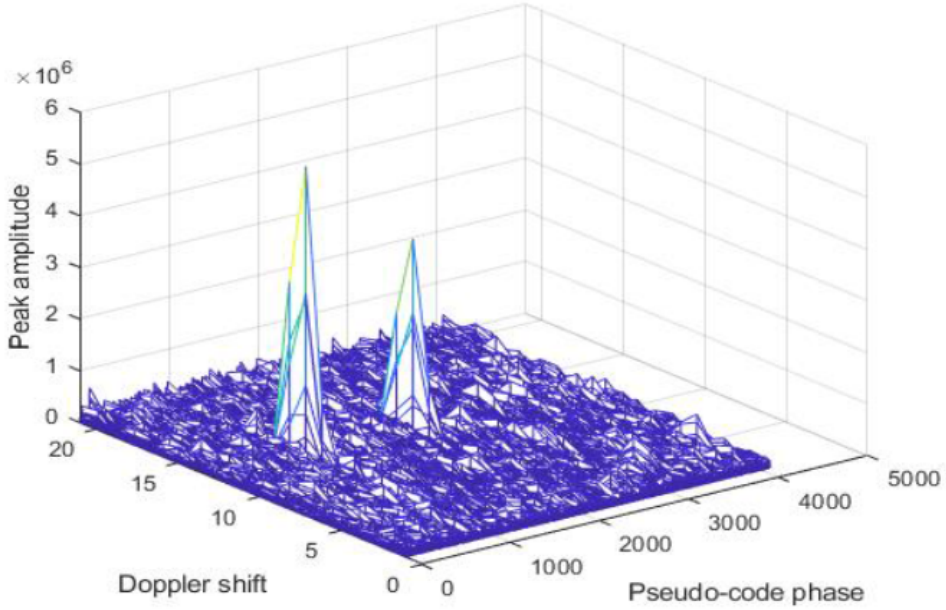
4.2.2. Tradicionalna metoda promatranja korelacijske funkcije - SQM

Metoda detekcije lažnih GNSS signala na temelju korelacijskih vrhova SQM *Signal Quality Monitoring* i fazne razlike između lažnog i autentičnog signala je korištena u [16], [17] i [36]. Rad [16] je fokusiran na detekciju lažnih signala s malim kašnjenjem korištenjem K-najbližih susjeda KNN (*K-Nearest Neighbors*) metode strojnog učenja. Detekcija broja vrhova signala je ključan korak za detekciju lažnog signala. Detekcija se temelji na otkrivanju lažnog signala na način da se procijeni broj vrhova koji prelaze unaprijed postavljeni prag kada prijemnik uhvati signal. Ako u primljenom signalu postoji samo pravi GNSS signal, vrijednost samo jednog



Slika 4.12: Stvarni satelitski signal u fazi snimanja [16].

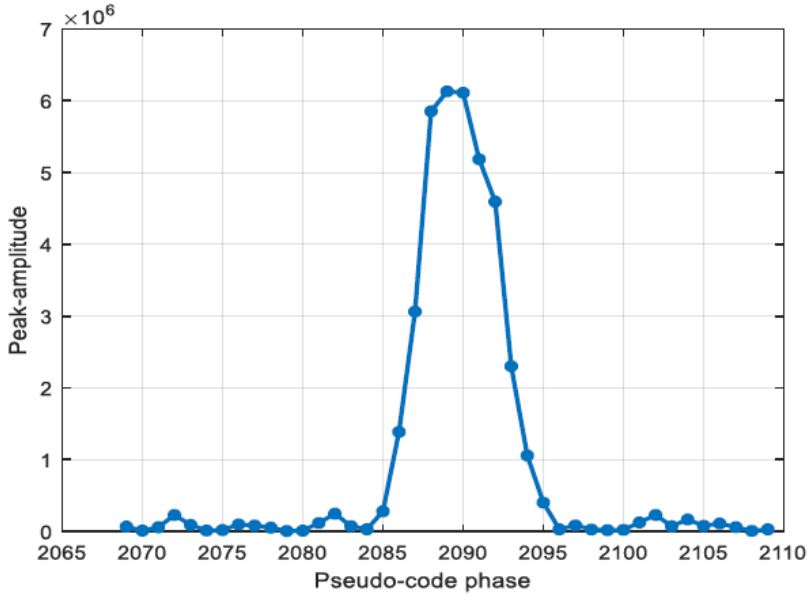
korelacijskog vrha će premašiti unaprijed postavljeni prag što je prikazano na slici 4.12.



Slika 4.13: Lažni signal postoji u fazi snimanja uz kašnjenje od 100 čipova [16].

Kada postoje lažni signali, onda postoje dva ili više korelacijskih vrhova koji su veći od postavljenog praga (4.13) i ovakav način detekcije lažnih signala vrijedi kada je fazna razlika između lažnog signala i stvarnog signala velika tj. veća od 2 čipa. Kada je fazna razlika između stvarnog i lažnog signala manja npr. 1 čip što je slučaj na slici 4.14, broj vrhova je i dalje 1 pa je teško detektirati lažne signale. Eksperimentalni rezultati provedeni u ovom radu su pokazali

da predloženi algoritam može detektirati lažne signale s kašnjenjem većim od 0,6 čipova te da ima visoku točnost. Autori u [17] pokazuju da generativna suparnička mreža GAN (*Generative Adversarial Network*) može doseći više od 98% točnosti kada fazna razlika između lažnog i autentičnog signala prelazi 0,5 čipova i može se primijeniti na situacije u kojima je lažni signal visoko sinkroniziran s autentičnim signalom.



Slika 4.14: Lažni signal postoji u fazi snimanja uz kašnjenje od 1 čip [16].

Autori se u [29] fokusiraju na klasifikaciju GNSS signala i svrstavaju ih u klase: autentični, višestazni, lažni ili ometani. Značajke koje koriste za klasifikaciju signala su prosječna snaga i izobličenje korelacije. Različite metode strojnog učenja su testirane korištenjem testa točnosti i konfuzijske matrice. Lažni i ometani signali lako se razlikuju od autentičnih signala zbog njihove visoke prosječne snage i visokog stupnja izobličenja korelacije. Stoga je u slučaju namjernih ometanja (interferencija) ovakva metoda klasificiranja moćan alat za navigacijske aplikacije koje koriste GNSS prijamnik.

4.2.3. Detekcija pomoću NMEA poruka

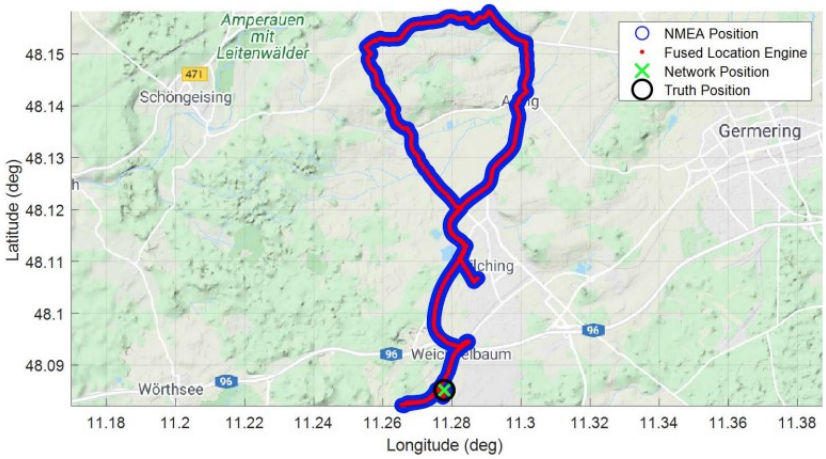
Autori u [31] predlažu pristup temeljen na korištenju NMEA poruka od GNSS prijamnika (pametni telefoni i komercijalni ublox prijamnik) za detekciju i identifikaciju sumnjivih potencijalno lažnih signala. NMEA 0183 poruke sadrže informacije o vidljivim satelitima, položaju prijamnika, brzini i vremenu te za njihovu obradu nije potrebno značajno procesiranje. Korištenjem NMEA poruka zaobiđena su velika proračunska opterećenja koja su potrebna za dobivanje

i obradu neobrađenih mjerenja. Slika 4.15

NMEA Message Type	Description
GSV	GNSS satellites in view PRN, Elevation, Azimuth, C/No
GSA	GNSS DOP and active satellites
GGA	GNSS fix data Time, Position, DOP
RMC	Recommended minimum specific data Time, Position, Velocity
VTG	Track made good and ground speed Velocity, Heading
GRS (not available for smartphones)	Range residuals for active satellites

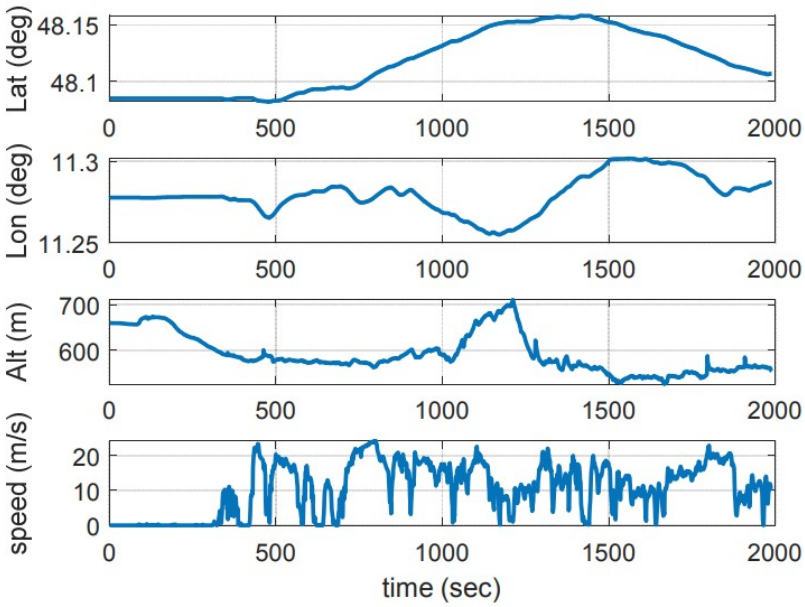
Slika 4.15: Definicija NMEA poruka prikupljenih od strane GNSS prijamnika [31].

Promatrana su tri različita scenarija: u prvom scenariju napadač je emulirao vožnju koja počinje od zgrade i radi petlju oko obližnjeg područja, u drugom scenariju napadač se udaljava od zgrade i vraća na početak i treći sceanrij je isti kao drugi samo što napadač ima dodatno prigušenje. U prvom scenariju, lokacije svih pametnih telefona su uspješno lažirane. Iako su pametni telefoni bili u stacionarnom položaju na stolu unutar zgrade, NMEA poruke su zabilježile da su uređaji u pokretu u okolnom području (slika 4.16).



Slika 4.16: Putanja kretanja uređaja tijekom uspješnog napada lažiranjem.

Za drugi scenarij, napad lažiranjem utjecao je na točnost pozicioniranja, ali potpuno očekivana lažna putanja nije uočena dok je za treći scenarij napad lažiranjem bio uspješan i uočena je očekivana lažna putanja. Slika 4.17 prikazuje položaje i brzine zabilježene od strane pametnih telefona (NMEA poruke za položaj, brzinu i vrijeme). Iako su uređaji u stacionarnom stanju, logovi su zabilježili da su u dinamičnom stanju pod napadom lažiranjem.

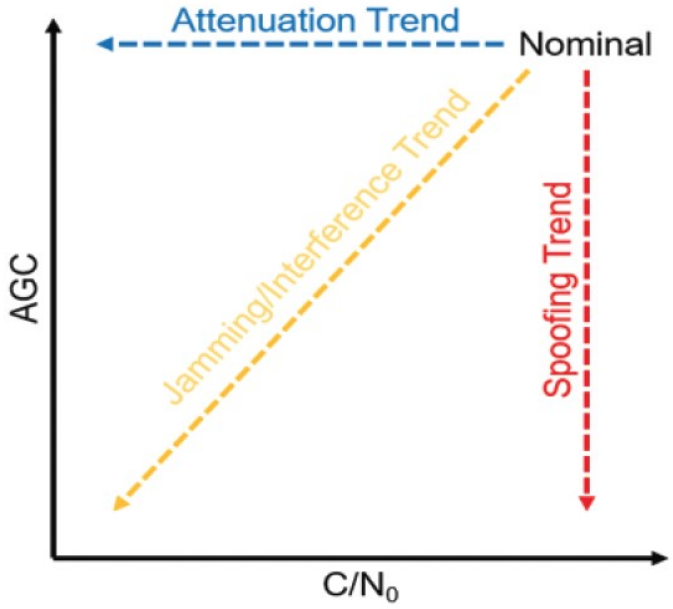


Slika 4.17: Pozicije i brzine prijamnika pametnih telefona.

4.2.4. Metoda detekcije ometanja i lažiranja na temelju parametara pametnih telefona

Ometajući signal se može detektirati kao i lažni signal promatranjem parametara C/N_0 i AGC. Autori u radu [32] opisuju kako se preko prethodno navedenih parametara mogu razlikovati lažni i ometajući signal. Ukoliko se i AGC i C/N_O smanje, vjerojatniji je ometajući signal, a ako se AGC smanji i C/N_0 ostane konstantan, vjerojatniji je lažni signal. Ako je AGC konstantan, onda je malo vjerojatan bilo koji oblik smetnje, a slabi signal se može pripisati prigušenju.

U radu [33], autori predlažu rješenje za detekciju ometanja i napada lažiranjem korištenjem izvornih parametara (između ostalih AGC i C/N_0) lokacije unutar Androida. Ovo rješenje povećava robusnost proračuna pozicije i vremena u Android sustavima i implementirano je u GNSSAlarm Android aplikaciji koja sadrži indikatore za AGC i C/N_0 . Ako AGC padne ispod postavljenog praga i C/N_0 padne na jednak iznos ili više, smetnje su vjerojatne i odgovarajući indikatori postati žuti što je vidljivo na slici. Ako se dogodi isti scenarij, a C/N_0 ne padne proporcionalno, indikatori postaju crveni i upozoravaju na napad lažiranjem što je prikazano na slici 4.18.



Slika 4.18: Očekivani trend za AGC i C/N_0 [33].

5. Zaključak

Aplikacije za navigaciju i pozicioniranje imaju vrlo veliku primjenu u svim aspektima života. Jedan od značajnih izvora referentnog signala za sinkronizaciju i pružanje usluga navigacije i pozicioniranja je globalni navigacijski satelitski sustav GNSS. Od svih satelitskih navigacijskih sustava, najzastupljeniji je GPS. Stalnim unaprjeđivanjem postojećih sustava osigurava se bolja preciznost. Međutim, zbog sve veće upotrebe satelitskih navigacijskih sustava, javlja se sve više rizika i opasnosti kao što je korištenje ovih sustava u neke zlonamjerne svrhe.

Glavne interferencije koje se javljaju u prijamnicima sustava GNSS i koje su detaljno opisane u ovom radu su: napad lažiranjem GNSS signala, višestazno prostiranje GNSS signala i ometanje GNSS signala. Napad lažiranjem i ometanje GNSS signala je vrlo lako izvesti zbog dostupnosti jeftine opreme kao što su softverski definirana radija i ometači. Najosjetljiviji na napade lažiranjem su pametni telefoni koji se najviše koriste za usluge navigacije i pozicioniranja. Utjecaj napada lažiranjem na neki GNSS prijamnik se ogleda u preuzimanju navigacijskog sustava i lažiranju lokacije prijamnika što je jako opasno u slučaju preusmjeravanja aviona, brodova, dronova itd. Višestazno prostiranje GNSS signala se najčešće javlja u urbanim sredinama tzv. urbanim kanjonima kao posljedica refleksije signala od različite reflektirajuće objekte. Stoga je bitno na vrijeme detektirati i otkloniti navedene interferencije.

U ovom radu dan je pregled postojećih rješenja za detekciju navedenih interferencija u prijamnicima sustava GNSS. Većina rješenja za detekciju navedenih interferencija temelji se na kombinaciji strojnog učenja s drugim metodama prikazanima u četvrtom poglavlju rada. Može se zaključiti da metode koje zahtijevaju skupu opremu kao što su simulatori nisu isplative u odnosu na jeftine i lako dostupne softverski definirane radije. Također, visoka točnost u klasifikaciji višestaznih i lažnih signala pokazuje da su metode strojnog učenja učinkovit i pouzdan pristup za detekciju ovih interferencija.

Literatura

[1] Novatel, ”What are Global Navigation Satellite Systems?”, https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss, s Interneta, 15.11. 2022.

[2] ”Global Positioning System”, https://en.wikipedia.org/wiki/Global_Positioning_System#Principles, s Interneta, 5.6.2023.

[3] ”Galileo System”, https://www.gsc-europa.eu/galileo/system, s Interneta, 5.6.2023.

[4] ”GLONASS”,https://novatel.com/an-introduction-to-gnss/chapter-3-\satellitesystems/glonass-global-navigation-satellite-system-russia, s Interneta, 5.6.2023.

[5] ”BeiDou”, https://en.wikipedia.org/wiki/BeiDou, s Interneta, 5.6.2023.

[6] P. J. G. Teunissen, O. Montebruck, “Handbook of Global Navigation Satellite Systems“, Springer International Publishing, August 2017., https://link.springer.com/content/pdf/bfm:978-3-319-42928-1/1.pdf

[7] “Atomic clock“, Wikipedia, https://en.wikipedia.org/wiki/Atomic_clock, s Interneta, 15.12.2022.

[8] J. Sanz Subirana, JM. Juan Zornoza, M. Hernandez-Pajares, “GNSS signal“, Navipedia, 2011., https://gssc.esa.int/navipedia/index.php/GNSS_signal, s Interneta, 1.12.2022.

[9] “GNSS Constellations, Radio Frequencies and Signals“, https://www.tallysman.com/gnss-constellations-radio-frequencies-and-signals/, s Interneta, 5.6.2023.

[10] Y. Peng, W. A. Scales, “Ionospheric Remote Sensing with GNSS,” Encyclopedia, vol. 1, no. 4, pp. 1246–1256, Nov. 2021, MDPI, doi: 10.3390/encyclopedia1040094.

[11] E. Garbin Manfredini, “Signal processing techniques for GNSS anti-spoofing algorithms“, PhD thesis, 2017, doi: 10.6092/polito/porto/2672749.

[12] M. L. Psiaki, T. E. Humphreys and B. Stauffer, “Attackers can spoof navigation signals without our knowledge. Here’s how to fight back GPS lies,“ in IEEE Spectrum, vol. 53, no. 8, pp. 26-53, August 2016, doi: 10.1109/MSPEC.2016.7524168.

[13] M. L. Psiaki and T. E. Humphreys, “GNSS Spoofing and Detection,“ in Proceedings of the IEEE, vol. 104, no. 6, pp. 1258-1270, June 2016, doi: 10.1109/JPROC.2016.2526658.

[14] K. K. Songala, S. R. Ammana, H. C. Ramachandruni and D. S. Achanta, "Simplistic Spoofing of GPS Enabled Smartphone," 2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Bhubaneswar, India, 2020, pp. 460-463, doi: 10.1109/WIECON-ECE52138.2020.9397980.

[15] A. Rustamov, N. Gogoi, A. Minetto and F. Dovis, "Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices," 2020 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 2020, pp. 1-6, doi: 10.1109/ICL-GNSS49876.2020.9115489.

[16] J. Li, W. Li, S. He, Z. Dai and Q. Fu, "Research on Detection of Spoofing Signal with Small Delay Based on KNN," 2020 IEEE 3rd International Conference on Electronics Technology (ICET), Chengdu, China, 2020, pp. 625-629, doi: 10.1109/ICET49382.2020.9119515.

[17] J. Li, X. Zhu, M. Ouyang, W. Li, Z. Chen and Q. Fu, "GNSS Spoofing Jamming Detection Based on Generative Adversarial Network," in IEEE Sensors Journal, vol. 21, no. 20, pp. 22823-22832, 15 Oct.15, 2021, doi: 10.1109/JSEN.2021.3105404.

[18] S. Semanjski, A. Muls, I. Semanjski and W. De Wilde, "Use and Validation of Supervised Machine Learning Approach for Detection of GNSS Signal Spoofing," 2019 International Conference on Localization and GNSS (ICL-GNSS), Nuremberg, Germany, 2019, pp. 1-6, doi: 10.1109/ICL-GNSS.2019.8752775.

[19] T. E. Humphreys, J.A. Bhatti, D.P. Shepard, and K.D. Wesson, “The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques,” Proc. ION GNSS, Nashville, TN, 2012.

[20] A. Albright, S. Powers, J. Bonior, and F. Combs, “Oak Ridge Spoofing and Interference Test Battery (OAKBAT) - GPS“, Oak Ridge National Lab. (ORNL), Oak Ridge, United States: N. p., 2020. doi:10.13139/ORNLNCCS/1664429.

[21] “Global Positioning System Standard Positioning Service Performance Standard“, $5^{(th)}$ edition, Department of Defense, United States of America, 2020, available at: `https://www.gps.gov/technical/ps/`.

[22] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, P. M. Kintner: “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer”, 2008 ION GNSS Conference, 2008.

[23] A. Shafique, A. Mehmood and M. Elhadef, “Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models,“ IEEE Access, vol. 9, pp. 93803-93815, 2021, doi: 10.1109/ACCESS.2021.3089847.

[24] F. Gallardo and A. P. Yuste, "SCER Spoofing Attacks on the Galileo Open Service and Machine Learning Techniques for End-User Protection," in IEEE Access, vol. 8, pp. 85515-85532, 2020, doi: 10.1109/ACCESS.2020.2992119.

[25] A. Siemuri, K. Selvan, H. Kuusniemi, P. Valisuo and M. S. Elmusrati, "A Systematic Review of Machine Learning Techniques for GNSS Use Cases," in IEEE Transactions on Aerospace and Electronic Systems, vol. 58, no. 6, pp. 5043-5077, Dec. 2022, doi: 10.1109/TAES.2022.3219366.

[26] G. Aissou, H. O. Slimane, S. Benouadah and N. Kaabouch, “Tree-based Supervised Machine Learning Models For Detecting GPS Spoofing Attacks on UAS,“ 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2021, pp. 0649-0653, doi: 10.1109/UEMCON53757.2021.9666744.

[27] Z. Wu, Y. Zhang, Y. Yang, C. Liang and R. Liu, “Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey,“ IEEE Access, vol. 8, pp. 165444-165496, 2020, doi: 10.1109/ACCESS.2020.3022294.

[28] B. Pardhasaradhi, R. R. Yakkati and L. R. Cenkeramaddi, “Machine Learning-Based Screening and Measurement to Measurement Association for Navigation in GNSS Spoofing Environment,“ in IEEE Sensors Journal, vol. 22, no. 23, pp. 23423-23435, 1 Dec.1, 2022, doi: 10.1109/JSEN.2022.3214349.

[29] R. R. Yakkati, B. Pardhasaradhi, J. Zhou and L. R. Cenkeramaddi, “A Machine Learning based GNSS Signal Classification,“ 2022 IEEE International Symposium on Smart Electronic Systems (iSES), Warangal, India, 2022, pp. 532-535, doi: 10.1109/iSES54909.2022.00116.

[30] A. Broumandan, S. Kennedy, J. Schleppe: “Demonstration of a Multi-Layer Spoofing Detection Implemented in a High Precision GNSS Receiver”, 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), 2020.

[31] D. -K. Lee et al., “Detection of GNSS Spoofing using NMEA Messages,“ 2020 European Navigation Conference (ENC), Dresden, Germany, 2020, pp. 1-10, doi: 10.23919/ENC48637.2020.9317470.

[32] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter, and P. Enge, "Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers," Proceedings of the 2018 International Technical Meeting of The Institute of Navigation, Reston, Virginia, January 2018, pp. 672-689.

[33] N. Spens, D.-K. Lee, F. Nedelkov, and D. Akos, "Detecting GNSS Jamming and Spoofing on Android Devices", NAVIGATION: Journal of the Institute of Navigation September 2022, 69 (3) navi.537; doi: 10.33012/navi.537.

[34] Z. Chen, J. Li, J. Li, X. Zhu and C. Li, “GNSS Multiparameter Spoofing Detection Method Based on Support Vector Machine,“ in IEEE Sensors Journal, vol. 22, no. 18, pp. 17864-17874, 15 Sept.15, 2022, doi: 10.1109/JSEN.2022.3193388.

[35] M. Turner, S. Wimbush, C. Enneking and A. Konovaltsev, “Spoofing Detection by Distortion of the Correlation Function,“ 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 2020, pp. 566-574, doi: 10.1109/PLANS46316.2020.9110173.

[36] B. Yang, M. Tian, Y. Ji, J. Cheng, Z. Xie and S. Shao, “Research on GNSS Spoofing Mitigation Technology Based on Spoofing Correlation Peak Cancellation,“ in IEEE Communications Letters, vol. 26, no. 12, pp. 3024-3028, Dec. 2022, doi: 10.1109/LCOMM.2022.3204944.

[37] G. Aissou, S. Benouadah, H. El Alami and N. Kaabouch, “Instance-based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS,“ 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0208-0214, doi: 10.1109/CCWC54503.2022.9720888.

[38] S. Semanjski, I. Semanjski, W. De Wilde, and A. Muls, “Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-World Meaconing and Spoofing Data—Part I,” Sensors, vol. 20, no. 4, p. 1171, Feb. 2020, doi: 10.3390/s20041171.

[39] S. Semanjski, I. Semanjski, W. De Wilde, and S. Gautama, “Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-World Meaconing and Spoofing Data—Part II,” Sensors, vol. 20, no. 7, p. 1806, Mar. 2020, doi: 10.3390/s20071806.

[40] L. Meng, L. Yang, W. Yang, and L. Zhang, “A Survey of GNSS Spoofing and Anti-Spoofing Technology,” Remote Sensing, vol. 14, no. 19, p. 4826, Sep. 2022, doi: 10.3390/rs14194826.

[41] A. Elango, S. Ujan and L. Ruotsalainen, “Disruptive GNSS Signal detection and classification at different Power levels Using Advanced Deep-Learning Approach,“ 2022 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 2022, pp. 1-7, doi: 10.1109/ICL-GNSS54081.2022.9797026.

[42] R. Morales-Ferre, W. Wang, A. Sanz-Abia, and E.-S. Lohan, “Identifying GNSS Signals Based on Their Radio Frequency (RF) Features—A Dataset with GNSS Raw Signals Based on Roof Antennas and Spectracom Generator,” Data, vol. 5, no. 1, p. 18, Feb. 2020, doi: 10.3390/data5010018.

[43] J. Magiera, “A Multi-Antenna Scheme for Early Detection and Mitigation of Intermediate GNSS Spoofing,” Sensors, vol. 19, no. 10, p. 2411, May 2019, doi: 10.3390/s19102411.

[44] T. Bašić, “Globalni navigacijski satelitski sustavi, Systems - GNSS, Praktični primjeri naknadne obrade multi-GNSS mjerenja otvorenim i komercijalnim programima”, Stručno usavršavanje HKOIG 2020 – GF (11).

[45] T. T. Khoei, A. Gasimova, M. A. Ahajjam, K. A. Shamaileh, V. Devabhaktuni and N. Kaabouch, “A Comparative Analysis of Supervised and Unsupervised Models for Detecting GPS Spoofing Attack on UAVs,“ 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 2022, pp. 279-284, doi: 10.1109/eIT53891.2022.9813826.

[46] A. Rustamov, A. Minetto and F. Dovis, "Improving GNSS Spoofing Awareness in Smartphones via Statistical Processing of Raw Measurements," in IEEE Open Journal of the Communications Society, vol. 4, pp. 873-891, 2023, doi: 10.1109/OJCOMS.2023.3260905.

[47] L. Huang and Q. Yang, “Low-cost GPS simulator GPS spoofing by SDR,” in Proceedings of DEFCON, 2015.

[48] M. Brkić, “Detekcija lažnog signala u sustavu GNSS“, Diplomski rad, Fakultet elektrotehnike, strojarstva i brodogradnje (FESB), Split, 2022.

[49] "Software-Defined GPS Signal Simulator," Accessed: March 20, 2023. [Online]. Available: https://github.com/osqzss/gps-sdr-sim.

[50] "MIT Licence." Accessed: March 20, 2023. [Online]. Available: https://opensource.org/licenses/mit-license.php.

[51] Great Scott Gadgets, "HackRF One", accessed: April 15, 2023. [Online]. Available: https://greatscottgadgets.com/hackrf/.

[52] L. Huang and Q. Yang, "Low-cost GPS simulator GPS spoofing by SDR," in Proceedings of DEFCON, 2015.

[53] S. Ceccato, F. Formaggio, G. Caparra, N. Laurenti and S. Tomasin, "Exploiting side-information for resilient GNSS positioning in mobile phones," 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 2018, pp. 1515-1524, doi: 10.1109/PLANS.2018.8373546.

[54] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," Int. J. Navig. Observ., vol. 2012, Jul. 2012, Art. no. 127072, doi: 10.1155/2012/127072.

[55] T. E. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," in IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 2, pp. 1073-1090, APRIL 2013, doi: 10.1109/TAES.2013.6494400.

[56] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on using signal strength noise powerand C/No observables," Int. J. Satellite Commun. Netw., vol. 30, pp. 181–191, Jul. 2012, doi: 10.1002/sat.1012.

[57] N. Spens, D.-K. Lee, and D. Akos, "An application for detecting GNSS jamming and spoofing," in Proc. 33rd Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+), Sep. 2021, pp. 1981–1988, doi: 10.33012/2021.18027.

[58] J. Van Sickle, "GEOG 862: GPS and GNSS for Geospatial Professionals - Multipath", John A. Dutton e-Education Institute, College of Earth and Mineral Sciences, The Pennsylvania State University; V3 Consultants, Lakewood, CO.

[59] L. Massarweh, M. Fortunato and C. Gioia, "Assessment of Real-time Multipath Detection with Android Raw GNSS Measurements by Using a Xiaomi Mi 8 Smartphone," 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 2020, pp. 1111-1122, doi: 10.1109/PLANS46316.2020.9110169.

[60] G. A. McGraw, P. D. Groves, and B. W. Ashman, "Robust Positioning in the Presence of Multipath and NLOS GNSS Signals," book chapter in *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, IEEE, 2021, pp.551-589, doi: 10.1002/9781119458449.ch22.

[61] V. Mukherji, and Lt. Gen. (Dr.) AKS Chandele, "GNSS Jamming: An Omnipresent Threat", Geospatial World, accessed on June 25, 2023, https://www.geospatialworld.net/prime/special-features/gnss-jamming-an-omnipresent-threat/

[62] R. Yozevitch, R. Marbel, N. Flysher, and B. Ben-Moshe, “Save Our Roads from GNSS Jamming: A Crowdsource Framework for Threat Evaluation,” Sensors, vol. 21, no. 14, p. 4840, Jul. 2021, doi: 10.3390/s21144840.

[63] S. Kim, H. Lee and K. Park, "GPS Multipath Detection Based on Carrier-to-Noise-Density Ratio Measurements from a Dual-Polarized Antenna," 2021 21st International Conference on Control, Automation and Systems (ICCAS), Jeju, Korea, Republic of, 2021, pp. 1099-1103, doi: 10.23919/ICCAS52745.2021.9648845.

[64] G. MacGougan, G. Lachapelle, R. Klukas, K. Siu, L. Garin, J. Shewfelt, and G. Cox, “Performance analysis of a stand-alone high-sensitivity receiver,” GPS Solut., vol. 6, no. 3, pp. 179–195, 2002.

[65] P. Groves, Z. Jiang, B. Skelton, P. Cross, L. Lau, Y. Adane, and I. Kale, “Novel multipath mitigation methods using a dual-polarization antenna,” in Proc. ION GNSS, Sep. 2010, pp. 140–151.

[66] N. Kubo, K. Kobayashi, and R. Furukawa, “GNSS Multipath Detection Using Continuous Time-Series C/N0,” Sensors, vol. 20, no. 14, p. 4059, Jul. 2020, doi: 10.3390/s20144059.

[67] P. Špánik, J. Hefty, “Multipath detection with the combination of SNR measurements – Example from urban environment”, Geodesy and Cartography Vol. 66, No 2, 2017, pp. 305-315.

[68] P. Closas and C. Fernandez-Prades, "A Statistical Multipath Detector for Antenna Array Based GNSS Receivers," in IEEE Transactions on Wireless Communications, vol. 10, no. 3, pp. 916-929, March 2011, doi: 10.1109/TWC.2011.011111.100412.

[69] X. Bai, W. Wen, and L. T. Hsu, “Using sky-pointing fish-eye camera and LiDAR to aid GNSS single-point positioning in urban canyons,” IET Intel. Transport Syst., vol. 14, no. 8, pp. 908–918, 2020.

[70] J. Marais, S. A. Kazim, Y. Cocheril and C. Meurie, "Multipath and NLOS detection based on the combination of CN0 values and a fish-eye camera," 2020 European Navigation Conference (ENC), Dresden, Germany, 2020, pp. 1-13, doi: 10.23919/ENC48637.2020.9317408.

[71] R. Kumar and M. G. Petovello, “A novel GNSS positioning technique for improved accuracy in urban canyon scenarios using 3D city model,” in Proc. ION GNSS+, Sep. 2014, pp. 2139–2148.

[72] Li-Ta Hsu, Y. Gu and S. Kamijo, “NLOS Correction/Exclusion for GNSS Measurement Using RAIM and City Building Models”, Sensors 2015, 15, 17329-17349.

[73] P. Pisova, and J. Chod, “Detection of GNSS Signals Propagation in Urban Canyons Using 3D City Models”, Information and Communication Technologies and Services, Volume: 13, No 1, March, 2015.

[74] S. Zhang, S. Lo, Y.-H. Chen, T. Walter, and P. Enge, ”GNSS Multipath Detection in Urban Environment Using 3D Building Model”, IEEE/ION Position, Location and Navigation Symposium (PLANS), IEEE, 2018.

[75] G. Zhang, H.-F. Ng, W. Wen, and Li-Ta Hsu, “3D Mapping Database Aided GNSS Based Collaborative Positioning Using Factor Graph Optimization”, IEEE Transactions on Intelligent Transportation Systems, Vol. 22, No. 10, October 2021.

[76] Li-Ta Hsu, ”GNSS Multipath Detection Using a Machine Learning Approach”, IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2017.

[77] L. Wang, P. Groves, and M. Ziebart, ”GNSS Shadow Matching: Improving Urban Positioning Accuracy Using a 3D City Model with Optimized Visibility Scoring Scheme”, Navigation - Journal of The Institute of Navigation 60(3), September 2013.

[78] Z. Jiang, and P. D. Groves, “NLOS GPS signal detection using a dual-polarisation antenna”, GPS Solutions, 18:15–26., Springer, 2014. , doi: 10.1007/s10291-012-0305-5.

[79] B. Guermah, H. El Ghazi, and T. Sadiki, “Support Vector Machines for Improving Vehicle Localization in Urban Canyons”, MATEC Web of Conferences, Volume 200, 2018.

[80] B. Guermah, H. El Ghazi, T. Sadiki, and H. Guermah, “A Robust GNSS LOS/Multipath Signal Classifier based on the Fusion of Information and Machine Learning for Intelligent Transportation Systems”, IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD), IEEE, 2018.

[81] R. Yozevitch, B. Ben Moshe, and A. Weissman, “A Robust GNSS LOS/NLOS Signal Classifier”, NAVIGATION: Journal of The Institute of Navigation, Vol. 63, No. 4, 2016.

[82] H. Xu, A. Angrisano, S. Gaglione, and Li Ta Hsu, ”GNSS Shadow Matching based on Intelligent LOS/NLOS Classifier”, The 16th world congress of the international association of institutes of navigation (IAIN), Chiba, Japan, 2018.

[83] H. Xu, A. Angrisano, S. Gaglione, and Li Ta Hsu, ”Machine learning based LOS/NLOS classifier and robust estimator for GNSS shadow matching”, Satellite Navigation, Springer, 2020.

[84] L. Wang, P. Groves, and M. Ziebart, ”GNSS Shadow Matching: Improving Urban Positioning Accuracy Using a 3D City Model with Optimized Visibility Scoring Scheme”, Navigation - Journal of The Institute of Navigation 60(3), September 2013.

[85] T. Suzuki, Y. Nakano, and Y. Amano, ”NLOS Multipath Detection by Using Machine Learning in Urban Environments”, 30th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2017), Portland, Oregon , 2017.

[86] T. Suzuki, and Y. Amano, “NLOS Multipath Classification of GNSS Signal Correlation Output Using Machine Learning”, MDPI, Sensors 2021, 21, 2503.

[87] Y. Quan, L. Lau, G. W. Roberts, X. Meng, and C. Zhang, “Convolutional Neural Network Based Multipath Detection Method for Static and Kinematic GPS High Precision Positioning,” Remote Sensing, vol. 10, no. 12, p. 2052, Dec. 2018, doi: 10.3390/rs10122052.

[88] Y. Lee, and B. Park, “Nonlinear Regression-Based GNSS Multipath Modelling in Deep Urban Area”, Mathematics, 10(3), 412, 2022, doi: 10.3390/math10030412.

[89] A. Siemuri, H. Kuusniemi, M. S. Elmusrati, P. Välisuo and A. Shamsuzzoha, "Machine Learning Utilization in GNSS—Use Cases, Challenges and Future Applications," 2021 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 2021, pp. 1-6, doi: 10.1109/ICL-GNSS51451.2021.9452295.

[90] S. Kim, J. Byun, and K. Park, "Machine Learning-Based GPS Multipath Detection Method Using Dual Antennas", The 13th Asian Control Conference (ASCC 2022), Jeju Island, Korea, May 4-7, 2022.

[91] S. Kim, and J. Seo, "Machine-Learning-Based Classification of GPS Signal Reception Conditions Using a Dual-Polarized Antenna in Urban Areas," 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, April 2023, pp. 113-118.

Obrada signala u svrhu otklanjanja interferencije u prijamnicima sustava GNSS

Sažetak:

Aplikacije za navigaciju i pozicioniranje su postale svakodnevnica bilo da negdje putujemo ili radimo svoj posao. Sve te usluge navigacije i pozicioniranja nam pružaju GNSS sustavi koji su i jedan od značajnijih izvora referentnog signala za sinkronizaciju. Zbog sve veće upotrebe satelitskih navigacijskih sustava, javlja se sve više rizika i opasnosti kao što je korištenje ovih sustava u zlonamjerne svrhe. Ključne interferencije u prijamnicima sustava GNSS koje utječu na sinkronizaciju, navigaciju i pozicioniranje su napad lažiranjem GNSS signala, višestazno prostiranje GNSS signala i ometanja GNSS signala. Napad lažiranjem je danas vrlo lako izvesti zbog lake dostupnosti jeftinih softverski definiranih radija. Višestazno prostiranje GNSS signala se najčešće javlja u urbanim sredinama tj. urbanim kanjonima u kojima ne postoji izravna vidljivost u prijamu između satelita i antene prijamnika. Kako bi se ove smetnje na vrijeme detektirale i izbjegle, potrebno je raditi na poboljšavanju sustava i metoda za njihovu detekciju. U ovom radu detaljno su opisane interferencije koje se javljaju u prijamnicima sustava GNSS: napad lažiranjem, višestazno prostiranje i ometanje signala. Također, dan je pregled postojećih rješenja vezanih uz izvođenje napada lažiranjem korištenjem softverski definiranog radija te ranjivost pametnih telefona na ove napade uz promatranje određenih značajnih parametara. U radu je dan i pregled različitih metoda za detekciju ovih interferencija uz naglasak na detekciju pomoću metoda strojnog učenja. Prikazana je točnost i učinkovitost pojedinih metoda i korištenih parametara. Visoka točnost istreniranih modela pokazuje da su metode strojnog učenja pouzdan i prikladan pristup za detekciju navedenih smetnji u prijamnicima sustava GNSS.

Ključne riječi:

GNSS, napad lažiranjem, višestazno prostiranje, detekcija, klasifikacija, softverski definirani radio, strojno učenje.

Signal processing for the purpose of eliminating interference in the receivers of the GNSS system

Abstract:

Navigation and positioning applications have become a part of our daily life whether we are traveling somewhere or just doing our work. All these navigation and positioning services are provided by GNSS systems, which are also one of the most important sources of the reference signal for synchronization. Due to the increasing use of satellite navigation systems, there are more and more risks and dangers, such as use of these systems for malicious purposes. The key interferences occuring in GNSS receivers that have an impact on synchronization, navigation and positioning are: GNSS spoofing attacks, multipath propagation of GNSS signals and signal jamming. GNSS spoofing attack is very easy to carry out today due to easy accessible and low-cost software defined radios. Multipath propagation of GNSS signals mostly occurs in urban areas, i.e. urban canyons where there is no direct visibility in the reception between the satellites and receiver antennas. In order to detect and avoid these interferences in time, it is necessary to improve the systems and methods for their detection. In this paper, interferences that occur in GNSS receivers: GNSS spoofing attack, multipath propagation of GNSS signals and signal jamming, are described in details. Also, an overview of the existing solutions related to the performance of spoofing attacks using software defined radio and smartphones' vulnerability on these attacks with the observation of certain important parameters, is given. This paper also provides an overview of methods for detecting these interferences with an emphasis on detection using machine learning methods. The accuracy and efficiency of certain methods and used parameters are used. The high accuracy of the trained models shows that machine learning methods are a reliable and suitable approach for detecting the listed interferences in GNSS receivers.

Keywords:

GNSS, spoofing attack, multipath, detection, classification, software defined radio, machine learning.