SVEUČILIŠTE U SPLITU
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

DOKTORSKI STUDIJ ELEKTROTEHNIKE I INFORMACIJSKE TEHNOLOGIJE

KVALIFIKACIJSKI DOKTORSKI ISPIT

KLASIFIKACIJA INTERFERENCIJA U SUSTAVU GNSS PRIMJENOM METODA STROJNOG UČENJA

Marta Balić

Split, rujan 2026.

SADRŽAJ

1 UVOD

U današnje vrijeme korisnici mobilnih i sličnih uređaja svakodnevno se oslanjaju na aplikacije za navigaciju i pozicioniranje. Iako vrlo pouzdane i gotovo nepogrešive, takve aplikacije za rad koriste globalne navigacijske satelitske sustave (GNSS, *Global Navigation Satellite System*) što ih čini vrlo osjetljivima na prijetnje.

Globalni navigacijski satelitski sustav opći je naziv za svaku satelitsku konstelaciju koja omogućuje autonomno geoprostorno pozicioniranje, navigaciju i precizno mjerenje vremena na globalnoj razini. Uz globalni pozicijski sustav (GPS, *Global Positioning System*) kao najpoznatiji i najrasprostranjeniji navigacijski satelitski sustav, postoje i drugi navigacijski sustavi, a to su: europski Galileo (*European Global Navigation Satellite System*), ruski GLONASS (*Navigazionnaya Sputnikovaya Sistema*), kineski BeiDou (*Chinese Global Navigation Satellite System*), japanski QZSS (*Quasi-Zenith Satellite System*) i indijski IRNSS/NavIC (*The Indian Regional Navigation Satellite System/Navigation with Indian Constellation*). S vremenom su ovi sustavi značajno napredovali što je pridonijelo poboljšanju preciznosti. Samim time korisnici se sve više oslanjaju na ove sustave što dovodi do veće ranjivosti tih sustava na različite prijetnje.

Namjerne smetnje poput GNSS ometanja (*jamming*) i lažiranja (*spoofing*) predstavljaju aktivne prijetnje globalnim navigacijskim satelitskim sustavima. Ovi napadi predstavljaju sigurnosne rizike i mogu prouzročiti ozbiljne posljedice za korisnike. Mogu ugroziti funkcionalnost GNSS-a i dovesti do kritičnih kvarova ili smanjene sigurnosti u brojnim aplikacijama temeljenim na pružanju lokacijskih usluga. Stoga ih je potrebno pravovremeno detektirati i učinkovito suzbiti.

Ometanje GNSS signala tehnika je kojom se namjerno ometaju signali. Ova vrsta interferencije ima za cilj krivotvoriti signal ili učiniti signal ili jedan njegov dio nerazumljivim na način da se prijamnik spriječi u prikupljanju autentičnih GNSS signala. Lažiranje GNSS signala definira se kao namjerno odašiljanje lažnih GNSS signala kako bi se prijamnik naveo na pogrešno tumačenje tih signala kao autentičnih te kako bi se krivotvorila lokacija prijamnika.

U literaturi se može pronaći značajan broj radova koji predstavljaju različite metode koje detektiraju interferencije u GNSS sustavu s vrlo visokom točnošću. Autori primjenjuju različite metode obrade signala, metode podatkovnih bitova, metode pozicioniranja te metode strojnog učenja (ML, *Machine Learning*) i dubokog učenja (DL, *Deep Learning*). No osim detekcije, interferencije je potrebno i razlikovati kada stignu na prijamnik kako bi se pravovremeno primijenila odgovarajuća metoda suzbijanja dolazne interferencije. Rješenja za klasifikaciju GNSS interferencija u literaturi nema mnogo, stoga je potrebno raditi na razvoju novih sustava i unaprjeđenju postojećih.

Ovaj rad sastoji se od pet poglavlja. Prvo poglavlje donosi uvod i motivaciju rada. Drugo poglavlje opisuje rad GNSS sustava te ukratko opisuje različite sustave za pozicioniranje i navigaciju. Uz to, ukratko su opisane značajke signala u sustavu GNSS. U trećem poglavlju detaljnije su opisani napadi ometanjem i lažiranjem te različite vrste ovih napada. Dan je kratak pregled nekoliko radova u kojima je pokazano kako se ovi napadi mogu izvesti na jednostavan način uz malo jeftine i lako dostupne opreme. Četvrto poglavlje daje kratak pregled stanja u literaturi na temu metoda za detekciju napada ometanjem i lažiranjem. Također je dan i detaljniji pregled stanja u literaturi na temu klasifikacije različitih vrsta GNSS signala.

2 GLOBALNI SATELITSKI NAVIGACIJSKI SUSTAV GNSS

Globalni navigacijski satelitski sustav ili GNSS sustav opisuje bilo koju satelitsku konstelaciju koja pruža usluge pozicioniranja, navigacije i mjerenja vremena (PNT, *Positioning, Navigation, and Timing*) na globalnoj ili regionalnoj osnovi. Konstelacije satelita daju signale iz svemira, a ti signali prenose podatke o položaju i vremenu do GNSS prijamnika. Signali iz svemira sadrže podatke o efemeridama svakog satelita. Efemeride su tablice koje sadrže podatke o gibanju i položaju satelita. Prijamnici zatim koriste podatke o efemeridama kako bi odredili položaj, tj. lokaciju.

GNSS prijamnici sastoje se od antene pomoću koje se prikupljaju signali sa satelita i od prijamnika na čijoj se strani odvija obrada primljenih signala te se daje smisao prikupljenim signalima na način da ih se pretvara u zemljopisne koordinate. Iako prijamnici vrše obradu primljenih signala, antena je komponenta na temelju čijeg se položaja računaju položaj, brzina i nadmorska visina.

Osnovne zadaće GNSS prijamnika uključuju: primanje i razdvajanje signala sa satelita, izračun pseudoudaljenosti do svakog satelita na temelju vremena primitka signala, demodulaciju navigacijske poruke u svrhu dobivanja podataka sa efemerida te procjenu rješenja koje obuhvaća položaj, brzinu i vrijeme (PVT, *Position, Velocity, and Time*).

Rad prijamnika temelji se na principu trilateracije. Prijamnik prvo računa koliko je vremena potrebno signalu da stigne sa svakog prijamniku vidljivog satelita. Zatim izračunato vrijeme množi s brzinom svjetlosti te na taj način dobije udaljenost od svakog satelita, a ta udaljenost naziva se pseudoudaljenost (ρ) jer sadrži pogrešku zbog nesinkroniziranosti sata prijamnika i drugih efekata. Koristeći poznate koordinate satelita i izmjerene pseudoudaljenosti, prijamnik rješava sustav jednadžbi te određuje svoj položaj u tri dimenzije (X, Y, Z) i korekciju sata prijamnika. Za jedinstveno rješenje s nesinkroniziranim satom prijamnika potrebna su minimalno četiri satelita, jer je potrebno izračunati četiri nepoznanice – X, Y i Z koordinate te korekciju sata prijamnika.

Za svaki satelit i vrijedi:

$$P_i = \sqrt{(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2} + c * \Delta t \quad (2.1)$$

gdje su (x_i, y_i, z_i) koordinate satelita i, (x, y, z) su koordinate prijamnika, c je brzina svjetlosti, a Δt je nepoznata razlika vremena sata prijamnika. S obzirom na to da su x, y, z i Δt nepoznanice, potrebno je postaviti sustav 4 jednadžbe (4 satelita):

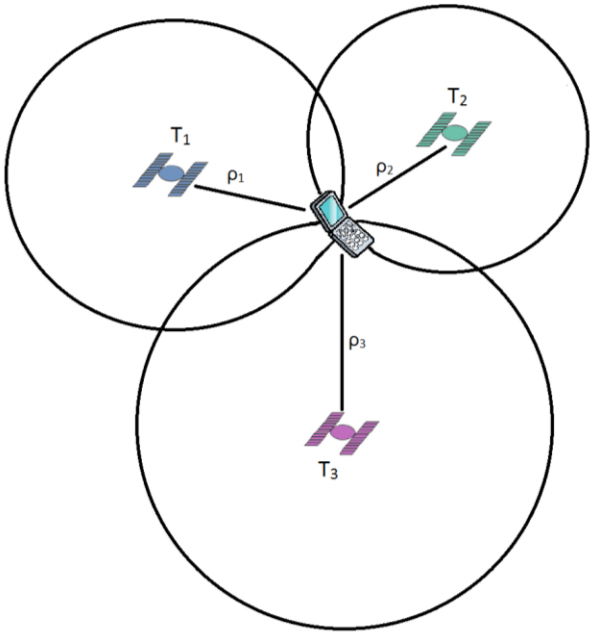
$$P_1 = \sqrt{(x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2} + c * \Delta t$$

$$P_2 = \sqrt{(x - x_2)^2 + (y - y_2)^2 + (z - z_2)^2} + c * \Delta t$$

$$P_3 = \sqrt{(x - x_3)^2 + (y - y_3)^2 + (z - z_3)^2} + c * \Delta t$$

$$P_4 = \sqrt{(x - x_4)^2 + (y - y_4)^2 + (z - z_4)^2} + c * \Delta t$$

Rješavanjem ovog sustava dobiju se koordinate prijamnika. Korištenjem više od četiri satelita dobit će se veća preciznost. Slikom u nastavku jednostavno je ilustriran pojednostavljeni 2D prikaz trilateracije.



Slika 2-1 Trilateracija. [1]

Izvedba GNSS-a ocjenjuje se na temelju četiri kriterija:

1. Točnost – razlika između izmjerenog i stvarnog položaja prijamnika, brzine ili vremena.
2. Integritet – sposobnost sustava da osigura prag pouzdanosti te alarm u slučaju anomalije u podacima o pozicioniranju.
3. Kontinuitet – sposobnost sustava da funkcionira bez prekida.
4. Dostupnost – postotak vremena u kojem signal ispunjava prethodno navedene kriterije točnosti, integriteta i kontinuiteta. [1] [2] [3]

2.1 Sustavi za pozicijske, navigacijske i vremenske signale (PNT)

Iako je GPS najrasprostranjeniji satelitski radionavigacijski sustav, i druge države razvile su vlastite sustave kako bi osigurale neovisne PNT mogućnosti. To su europski Galileo, ruski GLONASS, kineski BeiDou, japanski QZSS i indijski IRNSS/NavIC. U nastavku su opisani navedeni satelitski sustavi.

2.1.1 Globalni pozicijski sustav (GPS)

Globalni pozicijski sustav svemirski je radionavigacijski sustav koji se sastoji od konstelacije satelita koji emitiraju navigacijske signale i mreže zemaljskih postaja i satelitskih kontrolnih stanica koje se koriste za kontrolu i nadzor.

Ovaj radionavigacijski sustav razvile su Sjedinjene Američke Države 1973. godine, a prvi satelit lansiran je 1978. godine. GPS sustav u početku se sastojao od 24 satelita, a danas 31 satelit aktivno kruži oko Zemlje u 6 orbitalnih ravnina. Ti sateliti korisnicima pružaju točne informacije o položaju, brzini i vremenu bilo gdje u svijetu te u svim vremenskim uvjetima.

GPS sustav radi tako da GPS prijamnik izračunava vlastiti četverodimenzionalni položaj u prostoru i vremenu na temelju podataka koje prima od više GPS satelita. Svaki satelit sadrži točan zapis o svojoj poziciji i vremenu pa te podatke šalje prijamniku. Na svakom satelitu nalazi se stabilan atomski sat. Satovi sa satelita sinkronizirani su jedan s

drugim te sa zemaljskim satovima. Svakodnevno se ispravlja svako odstupanje od vremena koje se održava na terenu. Na isti način poznate su i satelitske lokacije i to s velikom preciznošću. Kao i sateliti, i GPS prijamnici imaju satove, no oni su manje precizni i manje stabilni od satova satelita.

Brzina radiovalova je konstantna i neovisna o brzini satelita, pa je vremensko kašnjenje između trenutka kada satelit odašilje signal i prijamnik ga prima proporcionalno udaljenosti od satelita do prijamnika. Potrebno je da najmanje četiri satelita budu u vidokrugu prijamnika kako bi izračunao četiri nepoznate veličine - tri koordinate položaja i odstupanje vlastitog sata od vremena satelita.

Svaki GPS satelit kontinuirano emitira signal koji sadrži pseudoslučajni kod (*pseudorandom code*) i poruku koja sadrži informaciju o vremenu slanja. Pseudoslučajni kod je kod koji se sastoji od niza jedinica i nula i on je poznat prijamniku, tj. primatelju. Verzija koda koju je generirao prijamnik vremenski se usklađuje s verzijom koda koju je izmjerio prijamnik. Tako se u vremenskoj skali sata prijamnika može pronaći vrijeme dolaska (TOA, *Time of Arrival*) određene točke u kodnom nizu. To vrijeme naziva se epoha. Poruka koju sadrži signal sastoji se od vremena prijenosa (TOT, *Time of Transmission*) epohe koda i položaja satelita u tom trenutku.

Detaljnije, prijamnik za četiri satelitska signala mjeri vrijeme dolaska. Iz vremena dolaska i vremena prijenosa, prijamnik kreira četiri vrijednosti vremena leta (TOF, *Time of Flight*). Te vrijednosti približno su ekvivalentne udaljenosti puta signala između satelita i prijamnika, što se naziva pseudoudaljenost. Nakon toga, prijamnik računa svoj trodimenzionalni položaj i odstupanje sata od vrijednosti četiriju vremena leta. Izračunate vrijednosti pretvaraju se u zemljopisnu visinu, širinu i dužinu u odnosu na model Zemlje.

GPS sateliti konstantno odašilju dva vala nosioca u L pojasu koji se označavaju kao L1 i L2. Ti valovi nosioci putuju natrag na Zemlju brzinom svjetlosti. L1 je na frekvenciji 1575.42 MHz, a L2 je na frekvenciji 1227.6 MHz. Valovi nosioci na Zemlju donose informacije sa satelita. Te informacije omogućuju prijamniku tj. korisniku da utvrdi gdje se nalazi.

S obzirom na to da GPS sateliti odašilju signale prijamnoj jedinici, važno je spomenuti kod pseudoslučajnog šuma (PRN, *Pseudo-Random Noise*). Svaki satelit ima jedinstveni PRN kod, pa prijamnik uz pomoć njih može identificirati koji satelit prima. PRN kodovi generirani su algoritmom koji koristi posmačne (*shift*) registre.

Kod GPS-a postoje dva PRN koda – C/A-kod i P-kod koji se koriste za očitavanja sata satelita:

- C/A-kod (*Coarse/Acquisition* = grubo označavanje) je niz od 1023 binarne znamenke i ponavlja se svake milisekunde. Jednostavniji je od P-koda te je dostupan za civilnu upotrebu, no moduliran je samo na L1 frekvenciju kako bi se spriječila potpuna točnost za civilne korisnike. Potpuna točnost dostupna je samo za vojne korisnike.
- P-kod (*Precision code*) je precizniji, detaljniji i brži od C/A-koda. Koristi se isključivo za potrebe američke vojske. Moduliran je i na frekvenciju L1 i na frekvenciju L2 kako bi se dobili što precizniji rezultati pri lociranju.

Tri su glavna segmenta sustava GPS:

- Svemirski segment odnosi se na satelite u orbiti. Postoji 24 do 31 aktivni satelit, a dodatni sateliti poboljšavaju preciznost proračuna lokacije. Dizajn GPS-a čini šest jednako razmaknutih orbitalnih ravnina, a svaka ravnina sadrži barem četiri satelita. Orbite su raspoređene tako da je najmanje šest satelita uvijek unutar linije vidljivosti sa svih strana Zemljine površine. Svaki satelit svemirskog segmenta kruži jednom, otprilike svakih 12 sati, na visini od oko 20200 km te obiđe dvije pune orbite svakog sideričkog dana, ponavljajući istu putanju svakog dana. Siderički dan je period rotacije planeta u odnosu na udaljene zvijezde.
- 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. Kontrolni segment sastoji se od: glavne kontrolne stanice (MCS, *Master Control Station*), alternativne glavne kontrolne stanice (AMCS, *Alternate Master Control Station*), četiri zemaljske antene i šest nadzornih stanica.

- Korisnički segment uključuje bilo koga ili bilo što što koristi ili ima GPS prijamnik, a uključuje vojne korisnike usluge preciznog pozicioniranja te civilne korisnike usluge standardnog pozicioniranja. [4] [5] [6]

2.1.2 Globalni navigacijski satelitski sustav Galileo

Galileo je europski navigacijski satelitski sustav koji pruža informacije o položaju i vremenu. Razvojem sustava Galileo, korisnici su dobili pouzdanu alternativu koja, za razliku od GPS-a i GLONASS-a, ostaje pod civilnom kontrolom. Sustav Galileo dizajniran je da bude kompatibilan sa svim postojećim i planiranim GNSS sustavima te da bude interoperabilan s GPS-om i GLONASS-om.

Galileo testni satelit lansiran je 2005. godine, a danas se u orbiti nalazi 27 potpuno operabilnih satelita i 5-7 satelita koji kruže u orbiti te su izvan glavne funkcije, a neki od njih služe kao pričuva. Za potpunu pokrivenost Zemlje dovoljno je imati 24 satelita, a s obzirom na to da se u orbiti trenutno nalazi njih 27, može se zaključiti da je Galileo sustav iznimno precizan.

Sustav Galileo sastoji se od svemirskog, zemaljskog i korisničkog segmenta.

• Svemirski segment sustava Galileo definiran je kao 27/3/1 Walker konstelacija. To označava da 27 satelita kruži na nominalnoj visini srednje Zemljine orbite (MEO, *Medium Earth Orbit*) od 23222 km. Raspoređeni su u 3 orbitalne ravnine s nagibom od 56 stupnjeva, sa svojim uzlaznim čvorovima ravnomjerno raspoređenim u intervalima od 120 stupnjeva.

• Zemaljski Galileo segment sastoji se od dva Galileo kontrolna centra (GCC, *Galileo Control Center*) smještena u Njemačkoj i u Italiji. Svaki Galileo kontrolni centar upravlja kontrolnim funkcijama koje podržava Segment zemaljske kontrole (GCS, *Ground Control Segment*) i funkcijama misije koje podržava Segment zemaljske misije (GMS, *Ground Mission Segment*).

• Galileo korisnički segment sastoji se od svih kompatibilnih prijamnika i uređaja koji prikupljaju Galileo signal i izračunavaju svoju lokaciju. Postoji širok raspon različitih korisničkih aplikacija – od prijevoza do aplikacija za mjerenje vremena. [9] [10]

2.1.3 Globalni navigacijski satelitski sustav GLONASS

Sustav GLONASS razvio je Sovjetski Savez 1970-ih godina kao eksperimentalni vojni komunikacijski sustav, a vrlo brzo prepoznat je njegov puni potencijal i komercijalna primjena te je prvi GLONASS satelit odaslan 1982. godine.

Sastoji se od 24 satelita raspoređena po 8 jednako udaljenih satelita u 3 orbitalne ravnine. GLONASS sustav može funkcionirati i s manje od 24 satelita – 18 je minimalan broj satelita potreban da se pokrije samo teritorij Rusije. Kao i kod GPS sustava, i kod GLONASS sustava 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. GLONASS sateliti postavljeni su oko 1060 km niže od GPS satelita i odašilju svoje signale u L1, L2 i L3 pojasevima.

GLONASS sustav koristi višestruki pristup s frekvencijskom raspodjelom (FDMA, *Frequency-Division Multiple Access*) za odašiljanje signala sa satelita. To znači da svaki satelit odašilje signal na vlastitoj, jedinstvenoj frekvenciji unutar zadanog pojasa kako bi se izbjegle međusobne smetnje. Najnoviji GLONASS-K2 sateliti koriste višestruki pristup s kodnom raspodjelom (CDMA, *Code-Division Multiple Access)* umjesto FDMA tehnologije. Iako FDMA tehnologija pruža dobru otpornost na smetnje s vremenom je postala tehnološko ograničenje, dok je s druge strane CMDA tehnologija pokazala veću preciznost, otpornost na refleksije te smanjenje pogrešaka. Osim toga, CDMA sustavi su ekonomski isplativiji i kompatibilni s ostalim navigacijskim sustavima. [7] [8]

2.1.4 Globalni navigacijski satelitski sustav BeiDou

Satelitski sustav BeiDou kineski je navigacijski satelitski sustav. Iako je svoj razvoj započeo kao lokalni i regionalni sustav za Kinu i dio Azije, dovršetkom razvoja treće generacije satelita 2020. godine postao je potpuno operativan na globalnoj razini.

Prva generacija BeiDou sustava, poznata i kao BeiDou-1, sastojala se od tri satelita koji su nudili ograničenu pokrivenost i navigacijske usluge, uglavnom za korisnike u Kini. Druga generacija sustava BeiDou-2, u potpunosti je zamijenila prvu generaciju sustava nakon što je postala potpuno operativna. Imala je djelomičnu konstelaciju od 10 satelita u orbiti i prešla je s usko ograničenog domaćeg prostora na znatno širi, regionalni azijsko-pacifički prostor sa znatno većom točnošću. Treća generacija BeiDou-3 navigacijskog satelitskog sustava ima nominalni dizajn od 30 operativnih satelita, od toga 24 MEO satelita, osigurava globalnu pokrivenost za mjerenje vremena i navigaciju te može poslužiti kao alternativa GPS-u, GLONASS-u i Galileu. Planira se i četvrta faza razvoja Beidou sustava, a s njenim razvojem planira se započeti do 2029. godine. [11] [12] [13]

2.1.5 Satelitski sustav QZSS

QZSS japanski je regionalni satelitski sustav za pozicioniranje. Ovaj satelitski sustav dizajniran je s orbitalnom konfiguracijom koja osigurava da su sateliti uvijek vidljivi blizu zenita s bilo kojeg mjesta u Japanu. Upravo to omogućuje postizanje preciznog i stabilnog pozicioniranja diljem Japana. Prvi satelit QZSS satelitskog sustava lansiran je 2010. godine. Prvotni plan bio je uspostaviti konstelaciju od 4 satelita i težiti konstelaciji od 7 satelita. Konstelacija od 4 satelita postignuta je 2017. godine kada su lansirana tri dodatna satelita. Očekuje se da bi rad na konstelaciji od 7 satelita trebao početi ubrzo. Kao neki od budućih planova ističu se razvoj konstelacije od 11 satelita i rad na kompatibilnosti s GPS sustavom. [14] [15]

2.1.6 Satelitski sustav IRNSS/NavIC

IRNSS/NavIC je Indijski regionalni navigacijski satelitski sustav. Osmišljen je za pružanje informacija o položaju korisnicima u Indiji i u regiji koja se proteže do 1500 km od njezine granice, ima konstelaciju od 7 aktivnih satelita te vrlo visoku točnost pozicioniranja. IRSS pruža dvije vrste usluga – standardnu uslugu pozicioniranja (SPS, *Standard Positioning Service*) i ograničenu uslugu (RS, *Restricted Services*) koja je šifrirana i dostupna samo ovlaštenim korisnicima. [16]

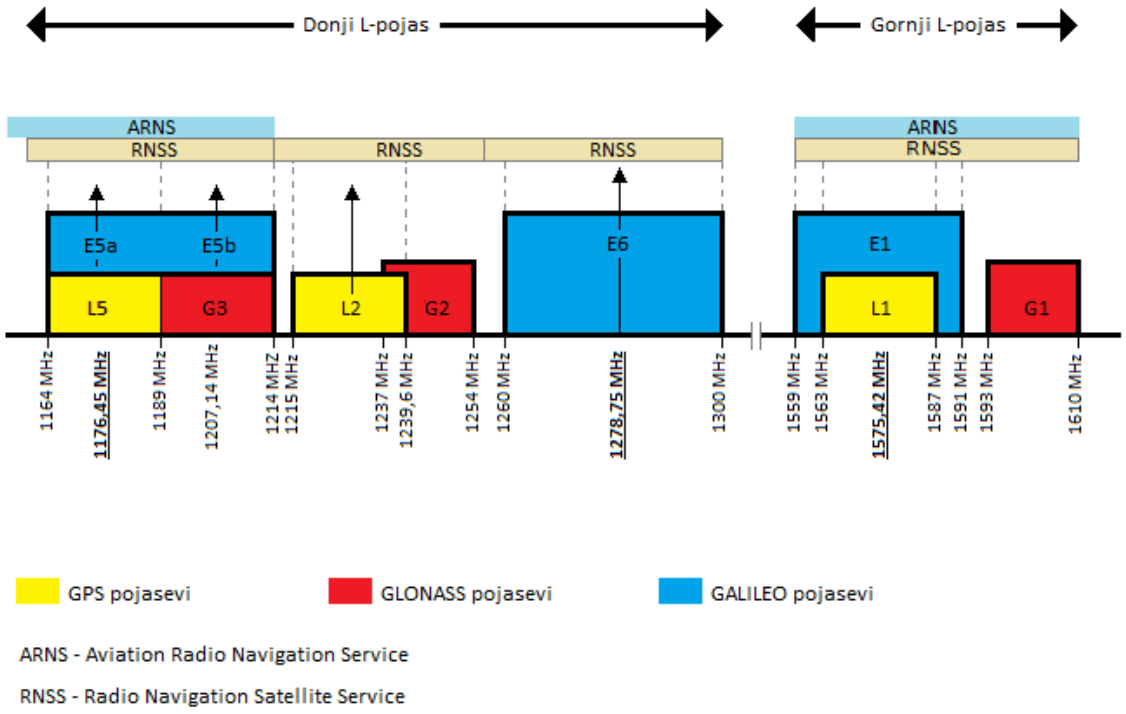
2.2 Značajke signala u sustavu GNSS

GNSS sateliti kontinuirano emitiraju navigacijske signale na dvije ili više frekvencija u L pojasu. Signali svakog satelitskog sustava imaju specifične karakteristike, ali ipak svaki sustav nastoji biti kompatibilan s drugima kako bi se spriječile interferencije i slabljenje signala.

Dodjela frekvencijskih pojaseva složen je proces zbog toga što više korisnika može koegzistirati u istom rasponu. Međunarodna telekomunikacijska unija (ITU, *International Telecommunications Union*) koordinira zajedničko globalno korištenje radijskog spektra. ITU je radio na dodjeli radio frekvencijskih pojaseva koje koriste radionavigacijske satelitske usluge (RNSS, *Radio Navigation Satellite Services*) u koje se ubraja i GNSS. Dostupni spektar koji se može koristiti za razvoj radionavigacijskih satelitskih sustava prikazan je na slici 2-2.

Kao što se vidi na slici, postoje dva pojasa dodijeljena zrakoplovnoj radionavigacijskoj službi (ARNS, *Aeronautical Radio Navigation Service*) na primarnoj osnovi u cijelom svijetu. ARNS je po ITU-u definiran kao „Radionavigacijska usluga namijenjena za dobrobit i siguran rad zrakoplova“. Dva spomenuta pojasa posebno su prikladna za aplikacije za „sigurnost života“ zbog toga što nitko ne smije ometati signale u ovim pojasevima. Odgovaraju dnu donjeg L-pojasa i gornjem L-pojasu. Dno donjeg L-pojasa čine frekvencije od 1164 do 1214 MHz i tu se ubrajaju GPS L5, GLONASS G3 te Galileo E5a i E5b pojasevi. Gornji L-pojas čine frekvencije od 1559 do 1610 MHz i tu se ubrajaju GPS L1 pojas, GLONASS G1 pojas te Galileo E1 pojas.

Vidljivo je kako su preostali neki pojasevi. To su GPS L2 pojas, GLONASS G2 pojas i Galileo E6 pojas. Njihov frekvencijski opseg je od 1215 do 1350 MHz. Ovi pojasevi dodijeljeni su radiolokacijskim uslugama kao što su zemaljski radari i RNSS na primarnoj osnovi. Zbog toga su signali u tim pojasevima više osjetljivi na smetnje od signala u ostalim pojasevima.



Slika 2-2 Podjela radiofrekvencijskih pojaseva za GNSS sustave. [1]

Signal koji se emitira sa svakog satelita sadrži kodove za domet i navigacijske podatke. Ovi podaci potrebni su kako bi se korisnicima omogućilo izračunavanje vremena putovanja signala od satelita do prijamnika.

Signal se sastoji od nekoliko komponenti:

1. Kod dometa – nizovi nula i jedinica koji prijamniku omogućavaju da odredi vrijeme putovanja signala od satelita do prijamnika. Ovi kodovi nazivaju se PRN kodovima.

2. Podaci navigacije (navigacijska poruka) – binarno kodirana poruka koja sadrži informacije o satelitskim efemeridama, satu satelita, orbitama satelita, GPS vremenu, zdravstvenom stanju satelita, porukama o statusu sustava i drugim dodatnim informacijama. Ova navigacijska poruka sadrži mnogo vitalnih informacija i poprilično je duga. Kontrolni segment povremeno ažurira informacije koje prenosi navigacijska poruka. Mana je što je, zbog male brzine slanja, potrebno 12.5 minuta da se pošalje jedna kompletna poruka.

3. Nosilac – sinusoidni radiofrekvencijski signal na nekoj frekvenciji. Koriste se dva vala nosioca na frekvencijama L1 = 1575.42 MHz i L2 = 1227.6 MHz. [45]

3 OMETANJE I LAŽIRANJE SIGNALA U SUSTAVU GNSS

Međunarodna organizacija za standardizaciju (*International Organization for Standardization*, ISO) ometanje GNSS signala definira kao prijenos visokofrekvencijskog radijskog signala koji je jednak ili blizak frekvencijama na kojima rade GNSS prijemnici. [17]

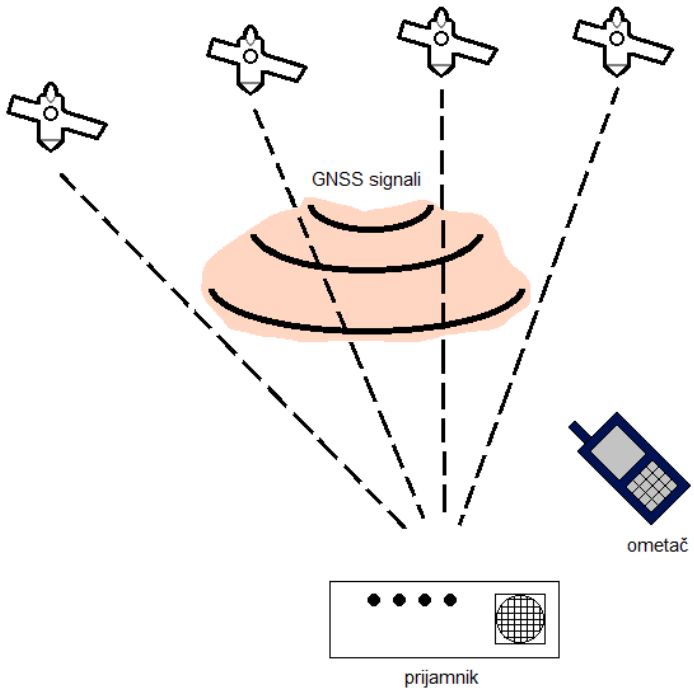
Europski Institut za telekomunikacijske standarde (*European Telecommunications Standards Institute*, ETSI) napad lažiranjem u GNSS sustavu definira kao prijenos signala namijenjenih obmanjivanju lokacije ili vremena kako bi se dobili lažni podaci o lokaciji i vremenu žrtve napada. [18]

3.1 Ometanje GNSS signala (*jamming*)

Ometanje GNSS signala (*jamming*) tehnika je kojom se namjerno ometaju signali. Ova vrsta interferencije ima za cilj krivotvoriti signal ili učiniti signal ili jedan njegov dio nerazumljivim na način da se prijamnik spriječi u prikupljanju autentičnih GNSS signala. Izvodi se na način da napadač namjerno odašilje radiofrekvencijski signal visoke snage na frekvenciji koja je jednaka ili vrlo bliska frekvenciji uređaja čiji se rad želi omesti. Radiofrekvencijiski signali visoke snage, kojima se prijamnik želi omesti, odašilju se u blizini frekvencijskih pojaseva na kojima rade GNSS prijamnici - L1, L2 i L5. Frekvencije za ometanje namijenjene su preopterećenju prijamnika do te mjere da izgube vezu sa satelitima, a njihov je glavni učinak onemogućavanje ili smanjenje učinkovitosti GNSS sustava za korisnike na području zahvaćenom ometanjem [19]. Na taj način prijamnik se preoptereti do te mjere da izgubi povezanost sa satelitima.

Važno je pravovremeno reagirati i detektirati ovakve signale. Uređaji koji se koriste za ometanje signala (*jammers*) vrlo su jednostavni i lako ih je izraditi. Sposobni su blokirati svu radiokomunikaciju na bilo kojem uređaju koji radi na radiofrekvencijama unutar njegovog dometa te emitirati radiofrekvencijske valove koji onemogućuju uspostavu ili održavanje veze. Oprema za izradu ovakvih uređaja, kao i sami uređaji, lako su dostupni te čak i najmanji uređaji za ometanje imaju domet od nekoliko metara te mogu izazvati

značajnu štetu. Slika 3-1 prikazuje način izvođenja napada ometanjem, a slika 3-2 prikazuje ilegalni prijenosni ometač koji se koristi za ometanje u automobilima.



Slika 3-1 Način izvođenja napada ometanjem.

Slika 3-2 Ilegalni automobilski ometač. [31]

Li i suradnici [20] podijelili su GNSS ometanje u dvije kategorije:

1. Ometanje potiskivanjem (*supression jamming*) opisuje ometanje gdje se satelitski signal potiskuje odašiljanjem ometajućeg signala velike snage u frekvencijskom pojasu satelitskog signala. Pritom se smanjuje omjer signala i šuma prijamnika, a signal satelitske navigacije potiskuje se signalom za ometanje. Kao posljedica ovog napada dobije se smanjena točnost pozicioniranja prijamnika ili nemogućnost njegova pravilnog rada. Glavne karakteristike ove metode su jednostavna izvedba i velik domet.

   Ometanje potiskivanjem dalje se dijeli na tri potkategorije:

   - Jednofrekvencijsko ometanje (*single-frequency jamming*) najjednostavnija je vrsta GNSS ometanja u kategoriji ometanja potiskivanjem. Glavna značajka ove vrste ometanja je relativno koncentrirana energija, pa ovakvo ometanje ima dobar učinak ometanja signala u blizini frekvencijske točke. Signali različitih navigacijskih sustava različito se ponašaju pod utjecajem jednofrekvencijskog ometanja. Jednofrekvencijsko ometanje opisuje se formulom:

     $$J(t) = Acos(2\pi f_c t) \tag{3.1}$$

     gdje je $J(t)$ ometajući signal, A je amplituda jednofrekvencijskog ometajućeg signala, a f_c je frekvencija nosioca ometajućeg signala.

   - Impulsno ometanje (*pulse jamming*) je vrsta GNSS ometanja u kojoj se ometajući signal sastoji od kontinuiranih idealnih pravokutnih impulsa. Ova vrsta ometanja ima malu propusnost ometanja i visoku učinkovitost ometanja. To znači da zrači smetnju samo u kratkim impulsima, ali u tom kratkom periodu daje jak ometajući signal. Impulsno ometanje opisuje se formulom:

     $$J(t) = Acos(2\pi f_c t)s(t) \tag{3.2}$$

     gdje je A amplituda impulsno ometajućeg signala, f_c je frekvencija nosioca satelitskog signala, a $s(t)$ je idealni pravokutni valni signal.

- Ometanje pomicanjem (*sweep jamming*) slično je jednofrekvencijskom ometanju. Razlika je u tome što se frekvencija nosioca kod ometanja pomicanjem mijenja s vremenom, a frekvencija nosioca jednofrekventnog ometanja je fiksna. Ometanje pomicanjem opisuje se formulom:

$$J(t) = Acos\big(2\pi(f_c + f_{sweep}t)t\big) \tag{3.3}$$

  gdje je A amplituda signala ometanja pomicanjem, f_c je frekvencija nosioca satelitskog signala, a f_{sweep} je frekvencija pomicanja.

- Ometanje usklađenim spektrom (*matched spectrum jamming*) kombinira karakteristike satelitskog navigacijskog signala te usmjerava ometajući signal na silazni satelitski signal (*downlink signal*) uvođenjem koda širenja (*spread code*) satelitskog signala. Ova vrsta ometanja je zapravo ometanje u kojem se interferencijski signal oblikom ili spektrom usklađuje sa silaznim signalom, tako da ga je teže prepoznati i potisnuti. Ometanje usklađenim spektrom opisuje se formulom:

$$J(t) = Acos(2\pi f_c t)p(t) \tag{3.4}$$

  gdje je A amplituda ometajućeg signala, f_c je frekvencija nosioca ometajućeg signala, a $p(t)$ je pseudokodna sekvenca satelitskog signala.

2. Ometanje obmanjivanjem (*deception jamming*) radi na način da izvor, tj. napadač generira signal za obmanjivanje koji je strukturom sličan stvarnom satelitskom signalu, no ima nešto veću snagu od stvarnog signala. Ovaj napad može se izvoditi i na način da napadač ponavlja stvarni satelitski signal u prostoru. Ometanjem obmanjivanjem napadač postiže da prijamnik „uhvati" pogrešne informacije o vremenu i lokaciji te ih takve i prenosi na prijamnik. Ovom vrstom napada postiže se dobra pokrivenost i teško otkrivanje napada od strane prijamnika. No ova metoda ima i nedostatke a to su složenost izvođenja napada i uzak raspon ometanja (samo za određene korisnike).

   Postoje dvije vrste ometanja obmanjivanjem:

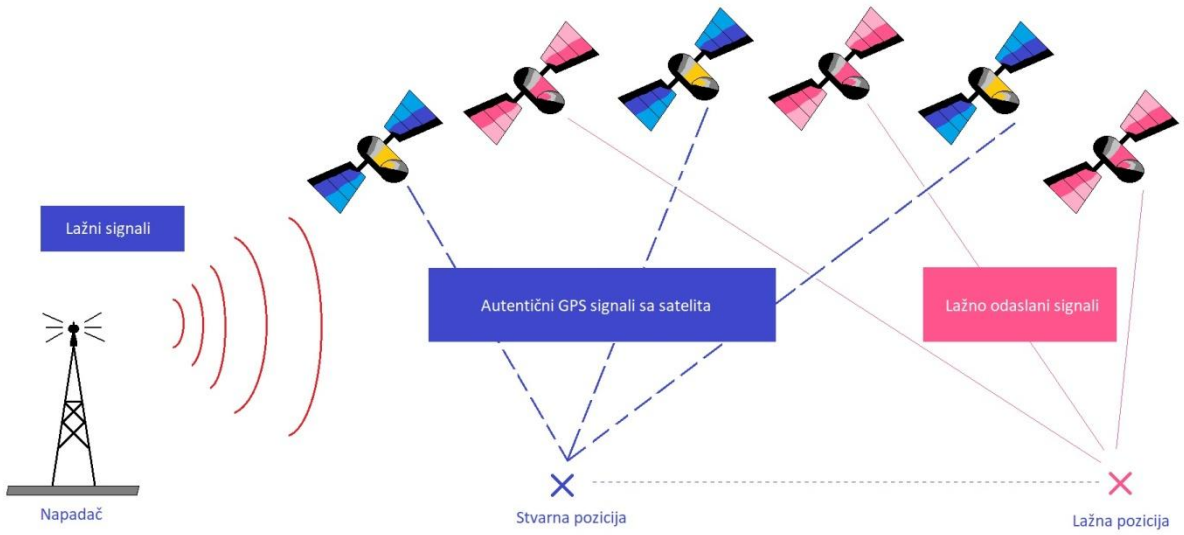
   - Generirano ometanje obmanjivanjem (*generated deception jamming*) je metoda ometanja u kojoj napadač generira i prenosi signal obmane.

Generirani signal ima istu strukturu kao i stvarni navigacijski signal. Postupno zamjenjuje stvarni signal u petlji praćenja prema strategiji kontrole signala i prednosti snage. Nakon toga, kontrolira petlju praćenja kako bi se postigao cilj obmane. [21]

- Ometanje repetitorom dodaje određeno vremensko kašnjenje na temelju prijema stvarnog satelitskog signala. Nakon toga, ponavlja se signal podešavanjem snage kako bi satelitski navigacijski prijamnik primio signal repetitora te na taj način prenio ometajući signal. [22]

3.2 Lažiranje GNSS signala (*spoofing*)

Lažiranje GNSS signala (*spoofing*) definira se kao namjerno odašiljanje lažnih GNSS signala kako bi se prijamnik naveo na pogrešno tumačenje tih signala kao autentičnih te kako bi se krivotvorila lokacija prijamnika. Lažiranje GNSS signala nešto je složenije od ometanja GNSS signala. Slika 3-3 prikazuje način izvođenja napada lažiranjem.



Slika 3-3 Način izvođenja napada lažiranjem. [1]

Primljeni matematički signali mogu se matematički opisati kao kombinacija nekoliko signala [26]:

$$y(t) = Re\left\{\sum_{i=1}^{N} A_i D_i[t - \tau_i(t)] C_i[t - \tau_i(t)] e^{j[\omega_c t - \phi_i(t)]}\right\}, i = 1, \dots, N \qquad (3.5)$$

gdje je N broj signala koji čine kod širenja (*spreading code*), A_i je amplituda i-tog signala, D_i je tok podatkovnih bitova (bitovi podataka svakog GNSS signala) i-tog signala, C_i je kod širenja i-tog signala, tj. niz impulsa koje GNSS koristi za širenje spektra odaslanog signala (uglavnom binarana fazna modulacija kodirana pseudoslučajnim šumom (BPSK PRN kod)), $\tau_i(t)$ je faza koda i-tog signala, ω_c nominalna frekvencija nosioca, ϕ_i je faza nosioca impulsa i-tog signala. Kod širenja C_i prenosi se kao dio navigacijske poruke i omogućuje prijamniku da identificira satelit s kojeg je primio signal.

Napadač šalje lažne signale slične autentičnim signalima sa satelita i replicira nosioca, PRN kod i bitove podataka svakog GNSS signala, a lažni signal matematički se opisuje kao:

$$y_s(t) = Re\left\{\sum_{i=1}^{N_s} A_{si} \widehat{D}_i[t - \tau_{si}(t)] C_i[t - \tau_{si}(t)] e^{j[\omega_c t - \phi_{si}(t)]}\right\}, i = 1, \dots, N_s \qquad (3.6)$$

gdje je τ_{si} faza koda (uspoređuje PRN kodove kako bi se otkrila udaljenost između satelita i prijamnika), ϕ_{si} je faza nosioca na prijamniku, a A_{si} je amplituda lažnih signala. Ove tri vrijednosti ovise o vrsti napada i razlikuju se od vrijednosti autentičnih signala. $N_s = N$ je broj lažnih signala koji je jednak broju autentičnih signala. Svaki lažni signal treba imati isti kod širenja/PRN kod kao i odgovarajući autentični signal kako bi prevario prijamnik i izveo uspješan napad lažiranjem. Najčešća praksa je da emitira svoju najbolju procjenu istih podataka $\widehat{D}_i$.

Ukupni primljeni signal tijekom napada lažiranjem jednak je:

$$y_{tot(t)} = y(t) + y_s(t)v(t) \tag{3.7}$$

gdje je $v(t)$ primljeni šum koji se može klasificirati kao unutarnji i vanjski u odnosu na prijamnik. Antena prima vanjske izvore šuma, a uključuje atmosferski šum, šum iz svemira, šum uzrokovan ljudskim djelovanjem i šum interferencije koji stvaraju drugi korisnici u susjednom ili istom kanalu. Unutarnji šum generiraju komponente unutar prijamnika. Ovaj šum rezultat je slučajnih procesa poput protoka naboja u uređaju ili toplinskih vibracija u bilo kojoj komponenti. Izvori bijelog šuma u GNSS prijamnicima obično su karakterizirani temperaturnim šumom prijamnika i antene.

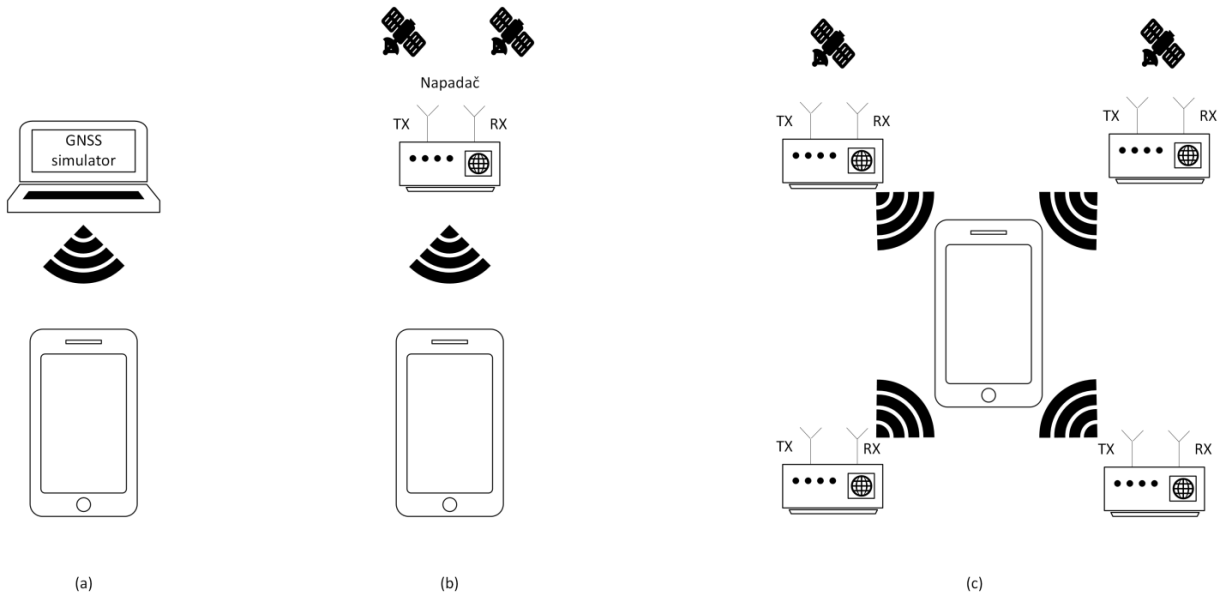
Napad lažiranjem moguće je izvesti na više načina, a po složenosti autori u [24], [25] i [27] podijelili su ga na:

1. Napad lažiranjem jednostavne razine složenosti (*simplistic spoofing attack*) – kod ove vrste lažiranja koristi se simulator signala za generiranje krivotvorenih GNSS signala koji se zatim odašilju putem radiofrekvencijskog sučelja. Prednost korištenja ove vrste lažiranja je u tome što je potreban samo jeftini hardver za odašiljanje krivotvorenih signala i za samo izvođenje ovakvog napada nije potrebno poznavati složene tehnike. No, ova vrsta lažiranja ima i nedostatke. Lažne signale odašiljane ovom metodom lako je detektirati zato što takvi GNSS signali imaju snagu znatno veću od snage autentičnih GNSS signala te takvi GNSS signali nisu sinkronizirani sa signalima sa satelita.
2. Napad lažiranjem srednje razine složenosti (*intermediate spoofing attack*) – ova vrsta napada složenija je od napada lažiranjem jednostavne razine složenosti zato što je za izvođenje ovog napada potrebna skuplja oprema – potreban je uređaj koji istovremeno prima autentične i odašilje krivotvorene GNSS signale. Ova vrsta napada, osim zbog složenije i skuplje opreme, zahtjevnija je za izvođenje i zbog toga što napadač mora paziti da krivotvoreni signali budu sinkronizirani s autentičnim signalima sa satelita. Ovu vrstu napada nije lako detektirati, jer napadač prati signale sa satelita i na temelju njihovih

karakteristika kreira lažne signale. Zbog tako precizne izvedbe nema diskontinuiteta u računanju PVT rješenja.

3. Napad lažiranjem visoke razine složenosti (*sophisticated spoofing attack*) – ova vrsta napada najsloženija je iz razloga što je za izvođenje ovakvog napada potrebno puno opreme čiji rad mora biti sinkroniziran. Preciznije, koristi se nekoliko uređaja koji se koriste za izvođenje napada srednje razine složenosti i svi ti uređaji sinkronizirani su putem jedinstvene komunikacijske veze te na taj način generiraju i odašilju lažne signale. Sama sinkronizacija uređaja za izvođenje napada vrlo je složena, a hardverska oprema vrlo je skupa. Sve to ovakve napade ne čini praktičnima i povoljnima za izvođenje u realnim scenarijima.

Na slici 3-4 prikazane su vrste napada lažiranjem po složenosti.



Slika 3-4 Vrste napada lažiranjem po složenosti: (a) napad jednostavne razine, (b) napad srednje razine, (c) napad visoke razine.

3.3 Izvođenje napada lažiranjem i ometanjem

Već su 2008. godine Humphreys i njegov tim osvijestili problem koji nosi napad lažiranjem te su razvili prijenosni uređaj za odašiljanje lažnih GPS signala [23]. Napad su uspješno izveli i testirali na standardnom komercijalnom prijamniku. Posljednjih godina izvesti ovakav napad postaje sve jednostavnije.

Autori [24] i [25] u svojim radovima pokazuju da je lokaciju pametnog telefona lako krivotvoriti izvođenjem jednostavnog napada lažiranjem. Predlažu jednostavan i ekonomičan pristup u kojem napad lažiranjem izvode pomoću simulatora otvorenog koda GPS-SDR-SIM i jeftinog softverski-definiranog radija (SDR, *Software Defined Radio*), u ovom slučaju HackRF One-a.

Autori u [24] ispitivali su domet HackRF One-a, uređaja kojim su odašiljali lažne signale. Eksperiment je pokazao da već na 6 metara udaljenosti prijamnik više ne može primati signale odaslane s HackRF One-a. U ovom slučaju, domet SDR-a je samo 5 metara.

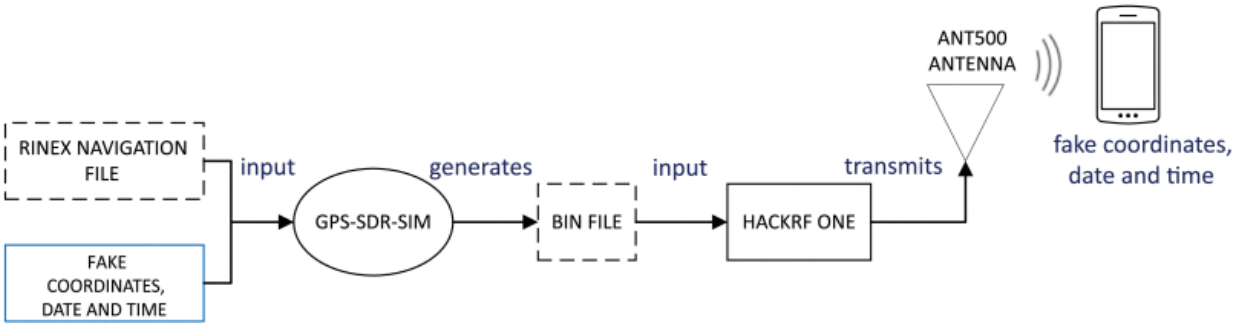
Autori u [25] izvode jednostavan napad lažiranjem na različitim pametnim telefonima te ispituju domet uređaja za izvođenje napada lažiranjem u zatvorenom prostoru. Osim ispitivanja dometa ovisno o udaljenosti od prijamnika u njihov eksperiment uključuju i ispitivanje dometa ovisno o različitim razinama snage kojom se odašilju lažni signali. Uz lažiranje lokacije prijamnika, autori su lažirali i njegov datum i vrijeme. Na slici 3-5 vidi se da je napad uspješan – napad je izvršen 4.5. u 14:40 u Splitu, a vidi se i da datum i vrijeme ne odgovaraju tome, kao ni lokacija koja pokazuje Maldive.

Slika 3-5 Prikaz lažirane lokacije, datuma i vremena u GPS Test aplikaciji. [25]

Rezultati eksperimenta pokazali su da je domet uređaja za lažiranje 25 metara i što je veća snaga odašiljanja, to će napad biti uspješniji. Autori su isti eksperiment izveli i na otvorenom, pod otvorenim nebom, no u tom slučaju rezultati nisu bili posebno uspješni – samo dva pametna telefona uspješno su „napadnuta" i to na udaljenosti od samo jednog metra. Iz toga se može zaključiti da sateliti u otvorenom vanjskom okruženju imaju puno bolju vidljivost i razinu snage u odnosu na snagu lažiranja. Stoga su u ovom slučaju sateliti dominantniji od lažiranja i gotovo je nemoguće napasti pametne telefone u takvim uvjetima.

Na slici 3-6 prikazan je blok dijagram izvođenja napada lažiranjem koji su izveli autori u [25]. Simulator otvorenog koda GPS-SDR-SIM koristi se za stvaranje i odašiljanje lažnih GPS signala. Za stvaranje lažnih signala potrebni su podaci o satelitima, stoga je korištena navigacijska datoteka u formatu RINEX (*Receiver Independent Exchange Format*) s NASA-ine (*National Aeronautics and Space*

Administration) mrežne stranice CDDIS (*Crustal Dynamics Data Information System*). Navigacijska datoteka RINEX, zajedno s lažnim koordinatama, datumom i vremenom, učitava se u GPS-SDR-SIM koji generira binarnu datoteku. Generirana binarna datoteka učitava se kao ulazni podatak u softverski-definirani radio HackRF One, koji putem antene odašilje lažne GPS signale pametnim telefonima.



Slika 3-6 Blok dijagram izvođenja napada lažiranjem. [25]

Što se tiče izvođenja napada ometanjem, u literaturi se uglavnom mogu naći radovi u kojima su autori provodili eksperimente uz pomoć simulatora.

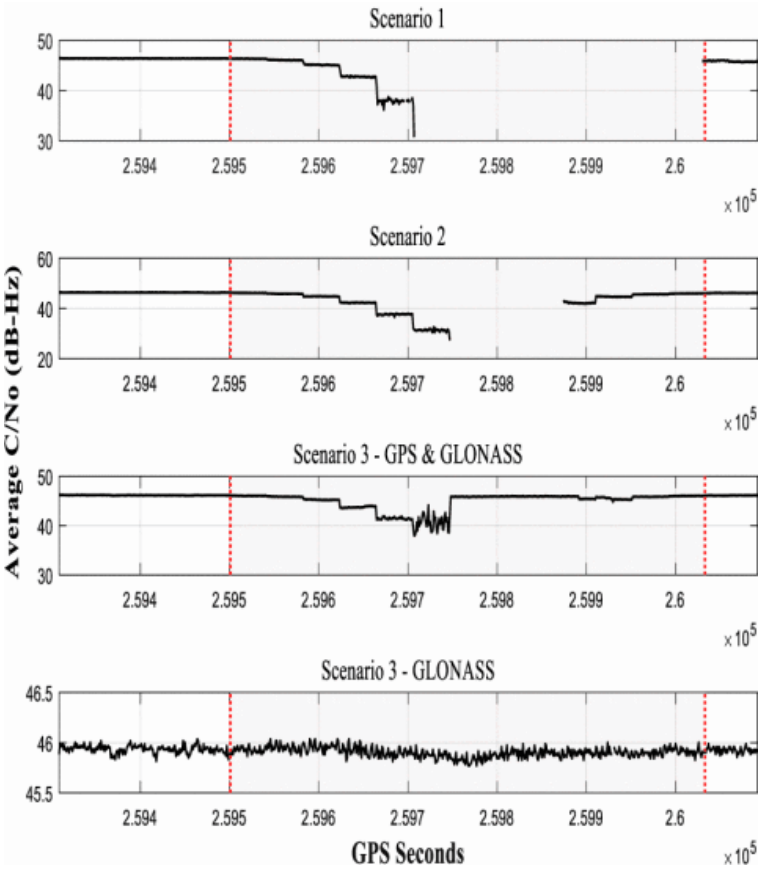
Autori u [28] izvode eksperimente u laboratorijskim uvjetima koristeći simulator. Testiraju napad ometanjem koristeći uskopojasni ometač koji odašilje trokutasto modulirani Gaussov šum u dinamičkom scenariju, tj. pretpostavljaju da se položaj prijamnika mijenja tijekom vremena. Postupno povećavaju snagu ometača tijekom promatranog vremenskog intervala, od -119 dBW do -112 dBW primljene snage. Prijamnik je ušao u status ometanja kada je snaga signala ometanja premašila -118 dBW što znači da je napad uspješno izveden. Osim napada ometanjem, autori su izveli i napad lažiranjem. Izveli su dva scenarija, statički i dinamički, kako bi usporedili u kojem je scenariju lakše izvesti napad. Napade su izvodili postupno povećavajući razinu snage signala lažiranja sve dok prijamnik nije ušao u status lažiranja, što se dogodilo nakon što je snaga signala lažiranja značajno povećana. Uz to, zaključili su da je napad lažiranjem lakše izvesti u statičkom scenariju. Na kraju, autori su izveli i napad u kojem kombiniraju i ometanje i lažiranje. Prvo su pokrenuli napad ometanjem te odmah nakon njega i napad

lažiranjem. Zaključili su da zajedničko djelovanje ometanja i lažiranja omogućuje uspjeh napada lažiranjem s nižim pojačanjem snage za razliku od slučaja kada se primjenjuje samo lažiranje. Eksperiment je pokazao da je napad lažiranjem sam po sebi uspješan ako je pojačanje snage napadačkog signala u odnosu na autentični signal veće od 14 dB, dok je u slučaju kada ometač djeluje prije uređaja za lažiranje, potonji uspješan uz pojačanje snage veće od 10 dB u odnosu na autentični signal.

Autori u [29] proveli su eksperiment u kojem su procijenili osjetljivost pet komercijalnih GNSS prijamnika na napade ometanjem i lažiranjem. Fokusiraju se na ponašanje prijamnika u fazi akvizicije analizirajući utjecaj smetnji na vrijeme do prvog izračuna pozicije i vrijeme ponovne akvizicije nakon napada. Za generiranje signala koristili su sustav temeljen na SDR-u koji je sposoban generirati GPS L1 i Galileo E1 signale. Rezultati eksperimenta pokazali su da ometanje i lažiranje signala utječu na GNSS prijamnike na različite načine – ometanje prvenstveno smanjuje dostupnost signala i često rezultira potpunim gubitkom navigacije značajno povećavajući vrijeme ponovnog pronalaženja, dok lažiranje radi tako da naizgled održava ispravan rad prijamnika a zapravo potpuno i trajno izmijeni navigacijsko rješenje. Uz to, autori su provedenim eksperimentom pokazali da je korištenje više konstelacija učinkovitije od korištenja samo jedne konstelacije. Kad je u pitanju napad ometanjem, dodavanje dodatne konstelacije može podržati ponovnu akviziciju izvan intervala napada. Kad je u pitanju napad lažiranjem, potpunija krivotvorena konstelacija može povećati stabilnost i kontinuitet rješenja lažne navigacije.

Autori u [30] istražuju utjecaj ometanja linearnim „cvrkutavim" (*chirp*) signalom na komercijalne prijamnike u visoko dinamičnim scenarijima. Osim GPS prijamnika, u eksperimente s napadima ometanjem uključili su i GLONASS prijamnike te su pokazali da korištenje prijamnika s dvostrukom konstelacijom daje veću otpornost na napade ometanjem u odnosu na prijamnike koji koriste samo GPS konstelaciju. Slika 3-7 prikazuje prosječni omjer nosioca i šuma $C/N0$ (*Carrier-to-Noise Density* Ratio) svih vidljivih GPS i GLONASS satelita. Sivi dio između dvije okomite crvene crte predstavlja period u kojem je ometač uključen. Na početku eksperimenta, prosječni $C/N0$ bio je oko 47 dB-Hz. Nakon što je ometač uključen, prosječni $C/N0$ značajno se smanjio sve dok oba prijamnika u

scenariju 1 i 2 nisu izgubila sve GPS satelite. No, u scenariju 3 prisutnost GLONASS konstelacije značajno je poboljšala performanse prijemnika i pomogla u održavanju dobrog prosječnog $C/N0$ tijekom cijele putanje.



Slika 3-7 Prosječni omjer C/N0 GPS i GLONASS satelita. [30]

4 STROJNO I DUBOKO UČENJE KAO TEHNIKA ZA KLASIFIKACIJU INTERFERENCIJA U SUSTAVU GNSS

Sustavi za navigaciju i pozicioniranje uglavnom se oslanjaju na GNSS sustave, što ih čini još ranjivijima na prijetnje [46]. Takvi sustavi izloženi su velikim sigurnosnim rizicima što može donijeti velike negativne posljedice korisnicima tih sustava. GNSS zajednica nije bila svjesna mogućih rizika sve dok Humphreys i suradnici nisu razvili sustav za izvođenje napada lažiranjem [23].

Kako bi se ovakvi napadi pravovremeno detektirali i suzbili, potrebno je provesti pravovremenu detekciju signala ometanja i lažiranja. U dostupnoj literaturi mogu se pronaći različite metode koje uključuju metode obrade signala, metode podatkovnih bitova, metode pozicioniranja te metode strojnog i dubokog učenja [85].

Metode obrade signala uključuju praćenje vrhova korelacije [47], [48], metode temeljene na snazi [49], [50], [70], [71], [72], [78], [79], [87] te metode koje koriste antenske nizove za detekciju interferencija [51], [52], [73]. Metode podatkovnih bitova uključuju praćenje vremena [53], [54], [74] i smjera dolaska signala [55], [56], [80] te analizu NMEA (*National Marine Electronics Association*) poruka [57], [58]. Pod metode pozicioniranja svrstavaju se mjerenja pseudoudaljenosti [59].

Što se tiče metoda strojnog i dubokog učenja, te su metode posljednjih godina najčešće zastupljene u literaturi. Tradicionalne metode strojnog učenja kao što su metoda potpornih vektora (SVM, *Support Vector Machine*) [60], [83], [84], k najbližih susjeda (KNN, *k-Nearest Neighbors*) [61] i neuronske mreže (NN, *Neural Network*) [62], [63], [64], [81], [82] daju obećavajuće rezultate prilikom detekcije interferencija.

Metode radiofrekvencijskog otiska dosad su bile korištene pretežno u kontekstu interneta stvari, Wi-Fi i mobilnih mreža, no sve se više počinju koristiti i u kontekstu GNSS-a te daju obećavajuće rezultate [65], [66], [67], [68], [69].

GNSS zajednica suočava se s manjkom gotovih skupova podataka čije bi postojanje olakšalo provođenje novih eksperimenata, a samim tim donijelo i nove metode detekcije i klasifikacije različitih vrsta interferencija. Korisno je spomenuti skupove podataka *Texas Spoofing Test Battery* (TEXBAT) [75] i *Oak Ridge Spoofing and Interference Test Battery*

(OAKBAT) [76]. To su javno dostupni skupovi podataka koji sadrže različite scenarije lažiranja, a na kojima su mnogi autori proveli vlastite eksperimente treniranja i testiranja modela. Postoji i javno dostupan skup podataka SatGrid [77] koji je nešto rjeđe korišten u literaturi, a koristili su ga autori u [86].

4.1 Klasifikacija GNSS signala primjenom strojnog i dubokog učenja

Strojno i duboko učenje u posljednje su vrijeme najčešće korištene metode za detekciju interferencija u sustavu GNSS, pa su te metode u ovom radu detaljnije obrađene. Fokus je na klasifikaciji različitih vrsta signala korištenjem metoda strojnog i dubokog učenja. Korištenje ovih metoda daje vrlo visoku točnost što su pokazali autori u radovima koji su opisani u nastavku.

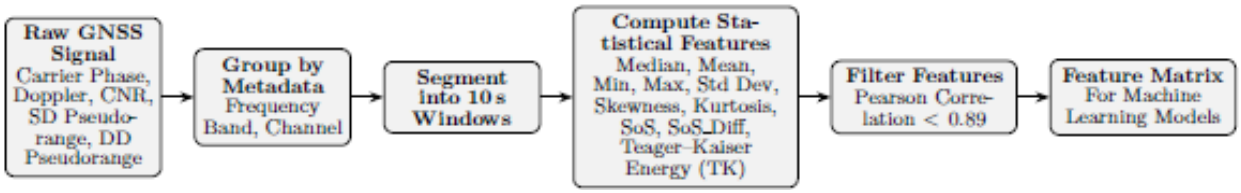
Trenutno u literaturi nema mnogo radova koji se bave višeklasnim klasificiranjem različitih vrsta interferencija što daje prostora za daljnja istraživanja u tom smjeru. U literaturi se može pronaći značajno više radova na temu klasifikacije različitih vrsta ometača, a setovi podataka sastoje se od slika, tj. spektrograma. U ovom radu fokus je na najčešće korištenim metodama strojnog i dubokog učenja koje se koriste u svrhu klasifikacije u posljednje vrijeme. U nastavku se nalazi pregled takvih radova.

4.1.1 Klasifikacija signala korištenjem modela neuronskih mreža (NN)

Pronalaženje učinkovitih rješenja za suočavanje sa smetnjama obično zahtijeva pristup realnim podacima o smetnjama, no prijenos bežičnih signala lažiranja i ometanja zabranjen je u većini zemalja. *Jammertest* je događaj koji je rijetka zakonski odobrena iznimka za prikupljanje podataka o smetnjama, a provodi se jednom godišnje u Norveškoj. Javni pristup *Jammertest* skupovima podataka još je uvijek ograničen zbog ograničenja intelektualnog vlasništva, pa se i u literaturi može naći skroman broj radova koji su proveli detekciju interferencija na temelju *Jammertest* skupova podataka. Autori u [37] predlažu algoritme temeljene na neuronskim mrežama za otkrivanje smetnji i klasifikaciju ometanja, lažiranja i autentičnih signala iz podataka *Jammertest* 2024. Analizirali su i usporedili 7

algoritama neuronskih mreža u jednom i više GNSS pojaseva te su postigli točnost klasifikacije u tri klase do 84,6%.

Autori su prvo izdvojili relevantne značajke iz dostupnih podataka, a nakon toga proveli su klasifikaciju temeljenu na strojnom učenju. Podaci koje su obradili izvukli su iz RINEX datoteka, a fokusirali su se na sirove parametre: fazu nosioca (*Carrier Phase*), Doppler, omjer nosioca i šuma (CNR, *Carrier-to-Noise Ratio*) i dvije derivacije podataka o pseudoudaljenosti – jednostruka derivacija pseudoudaljenosti (*Single Derivation* (SD) *Pseudorange)* i dvostruka derivacija pseudoudaljenosti (*Double Derivation* (DD) *Pseudorange)*, jer sirove vrijednosti pseudoudaljenosti nisu korištene kao ulazi. Na svaki od ovih parametara primijenjeno je deset transformacija za izdvajanje statističkih značajki, čime je dobiveno ukupno 55 početnih značajki – 5 sirovih + 5x10 transformiranih. Od ovih 55 značajki, zadržali su samo najrelevantnije, jer su mnoge od njih bile korelirane. Primijenili su tehniku redukcije značajki temeljenu na Pearsonovom pragu korelacije. Statističke značajke koje su autori odabrali pomno su odabrane nakon pažljivog razmatranja i pretraživanja dostupne literature kako bi klasifikacija bila što uspješnija. Na slici 4-1 nalazi se grafički prikaz ekstrakcije značajki iz sirovih GNSS signala koju su proveli autori.



Slika 4-1 Ekstrakcija značajki iz neobrađenih GNSS signala. [37]

Nakon što su sve pripremili, autori su krenuli u klasifikaciju. Odabrali su metode temeljene na neuronskim mrežama, prvenstveno zbog toga što rade s velikim skupom podataka. Za analizu i klasifikaciju autori su se odlučili za sedam modela neuronskih mreža.

Autori su izveli klasifikaciju u 3 klase:

- čisti signal
- lažni signal
- signal s ometanjem.

Izveli su i detekciju u 2 klase:

- čisti signal
- signal izobličen smetnjama.

Izveli su testiranja za scenarije s jednim pojasom (L1-GPS), jednim pojasom i više sustava (L1/E1/B1 sva četiri GNSS-a) i više pojasa i više sustava (svi pojasevi, svi GNSS). Najbolji rezultati klasifikacije dobiveni su korištenjem konvolucijske rekurentne neuronske mreže (CRNN, *Convolutional Recurrent Neural Network*), nakon čega slijede algoritmi dvosmjerni LSTM (BiLSTM, *Bidirectional Long Short-Term Memory)* i upravljana povratna jedinica (GRU, *Gated Recurrent Unit*) i bili su dosljedni u višepojasnoj i višesustavskoj analizi. Najbolja točnost postignuta je za slučaj jednog sustava s jednim pojasom što je i očekivano zbog najmanje varijabilnosti u skupovima podataka za treniranje i testiranje u odnosu na ostale razmatrane scenarije. Utjecaj na točnost prelaskom s jednog na više pojaseva i s jednog na više GNSS sustava bio je umjeren, do 10%. U tablici u nastavku prikazane su postignute točnosti za algoritam CRNN.

Tablica 4-1 Točnosti CRNN algoritma za binarnu i višeklasnu klasifikaciju. [37]

Klasifikacija u 3 klase	Detekcija u 2 klase	Broj sustava/pojaseva
84,7%	81,2%	1/1
73,5%	75,0%	1/više
74,2%	73,5%	više/više

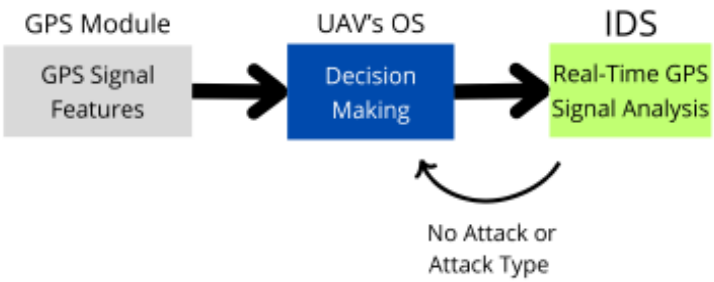
Jednodimenzionalna konvolucijska neuronska mreža (CNN1D, *1D Convolutional Neural Network*) ne postiže dobre rezultate ni u jednom od razmatranih scenarija. Autori smatraju da je razlog to što taj algoritam pretpostavlja da su ulazni podaci jednodimenzionalni.

Što se tiče složenosti korištenih algoritama, od onih koji su postigli najbolje točnosti klasifikacije i detekcije, tri najbolja algoritma redom su: GRU, BiLSTM i CRNN. GRU je atraktivna opcija za jeftinija rješenja i prijamnike s ograničenim resursima jer pruža najnižu složenost, dok je CRNN najbolji u scenarijima unakrsnog testiranja.

4.1.2 IDS sustavi za detekciju upada

I rad [38] fokusira se na višeklasnu klasifikaciju koristeći strojno učenje kako bi se bespilotne letjelice (UAVs, *Unmanned Aerial Vehicles*) zaštitile od napada ometanjem i lažiranjem. Sigurnost mreže bespilotnih letjelica postala je hitna potreba kako bi se izbjegle katastrofalne posljedice. Autori predlažu sustav za otkrivanje upada (IDS, *Intrusion Detection System*) koji koristi tehnike strojnog učenja kako bi klasificirali normalan rad, ometanje i više različitih tipova lažiranja u GPS sustavu. Ovakvi napadi mogu poremetiti let bespilotne letjelice i potencijalno uzrokovati sudare s preprekama ili je usmjeriti na nepristupačno područje, što rezultira gubitkom letjelice. Uz to, napad lažiranjem nosi dodatni rizik pada pod kontrolu napadača i curenje osjetljivih podataka.

Autori predlažu IDS, koji bi bio unaprijed instaliran na disk bespilotne letjelice, kako bi se otkrili napadi te kako bi se upozorio operativni sustav bespilotne letjelice. Pretpostavljaju da će dron sam pokrenuti IDS softver za identifikaciju potencijalnih napada te će on analizirati podatke iz primljenih GPS signala te odrediti događa li se napad i koji je napad u pitanju. Slika 4-2 ilustrira rad predloženog IDS-a u stvarnom okruženju i podatkovni cjevovod između njega i operativnog sustava bespilotne letjelice.



Slika 4-2 Način djelovanja IDS sustava. [38]

Podaci korišteni za treniranje i naknadne testove izvedeni su iz skupa podataka iz rada [39]. S obzirom na to da skup podataka iz rada [39] sadrži autentične signale te tri vrste lažiranih signala, autori ovog rada proširili su njihov skup podataka dodavanjem signala ometanja. Skup podataka iz spomenutog rada temelji se na stvarnim mjerenjima za bespilotnu letjelicu. Pretražujući dostupnu literaturu, autori su zaključili da će povećanjem razine buke smanjiti vrijednost parametra $C/N0$ što će poremetiti lokalizaciju bespilotne letjelice. Stoga su simulirali napad ometanjem unošenjem vrijednosti $C/N0$ u rasponu od 21 do 24 dB-Hz. Konačan skup podataka sadrži 73,46% uzoraka koji predstavljaju normalan rad, 6,73% uzoraka jednostavnog napada lažiranjem, 8,17% uzoraka napada lažiranjem srednje razine, 5,91% uzoraka sofisticiranog napada lažiranjem te 5,73% uzoraka ometanja. Autori su proveli pred obradu podataka kako bi uklonili redundantne značajke te kako bi smanjili skup podataka i poboljšali performanse klasifikatora. Spearmanovom korelacijom otkrivena su dva para visoko koreliranih značajki. Na kraju su autori izbalansirali skup podataka što znači da su postavili da svaka klasa ima jednaki broj uzoraka kako bi spriječili pristranost klasifikatora. Koristili su različite modele strojnog učenja za klasifikaciju.

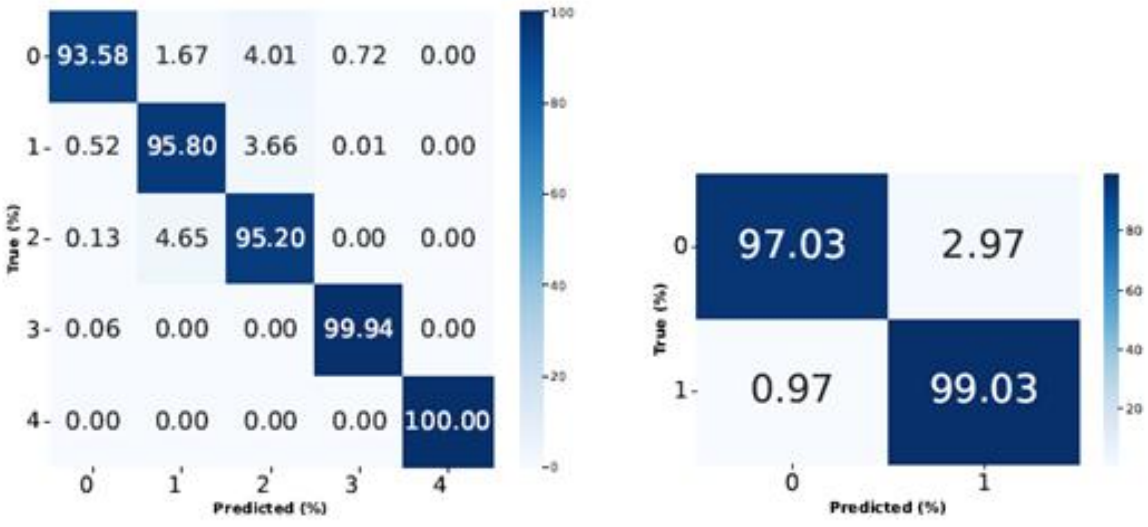
Tablica u nastavku prikazuje rezultate točnosti dobivene od osnovnih klasifikatora u njihovim binarnim i višeklasnim verzijama. Vidi se da najbolje vrijednosti daju klasifikatori KNN, stablo odlučivanja (DT, *Decision Tree*), NN, slučajna šuma (RF, *Random Forest*) i gradijentno pojačavanje (GB, *Gradient Boosting*).

Tablica 4-2 Točnosti različitih klasifikatora za binarnu i višeklasnu klasifikaciju. [38]

Klasifikator	Točnost binarne klasifikacije (%)	Točnost višeklasne klasifikacije (%)
Gaussov naivni Bayes (GNB, *Gaussian Naive Bayes*)	62,99	53,80
KNN	90,18	87,56
DT	96,62	95,33
NN	95,36	94,08
Linearna diskriminantna analiza (LDA, *Linear Discriminant Analysis*)	62,95	56,10
Logistička regresija (LR, *Logistic Regression*)	62,93	55,23
Prilagodljivo pojačavanje (AB, *Adaptive Boosting*)	90,23	78,90
RF	95,57	93,89
GB	96,70	95,50

Autori su pokušali poboljšati rezultate korištenjem metoda ansambla (*Ensemble methods*). Metode ansambla spajaju predviđanja različitih modela strojnog učenja kako bi se dobila veća točnost, stabilnost i pouzdanost konačnog rezultata u odnosu na rezultat koji bi se dobio korištenjem samo jednog modela. Prvo se trenira više različitih modela na istom skupu podataka, a nakon toga se predviđanja prethodno treniranih modela poslužuju kao nove značajke, meta-značajke, za treniranje meta-klasifikatora. Meta-klasifikator uči kako najbolje kombinirati te izlaze te donosi konačnu odluku. Ansambl metodom *Stacking* postigli su najveće poboljšanje točnosti od 96,91% za verziju s višeklasnom klasifikacijom i 98,03% za verziju s binarnom klasifikacijom za klasifikatore KNN, DT, NN, RF i GB. Očekivano je da će binarna klasifikacija dati veću točnost, jer se dodavanjem klasa povećava složenost.

Slika 4-3 prikazuje konfuzijske matrice za višeklasnu i binarnu klasifikaciju za *Stacking* klasifikator. Lijeva konfuzijska matrica odnosi se na višeklasnu klasifikaciju. Oznaka 0 označava normalan rad, a oznake 1, 2 i 3 predstavljaju jednostavne, srednje i sofisticirane napade lažiranjem. Oznaka 4 označava napad ometanja. Jasno je vidljivo da je svaki napad ometanjem ispravno klasificiran kao takav, dok su se u ostalim kategorijama dogodile pogreške u klasifikaciji. 100%-tna uspješnost klasifikacije signala ometanja proizlazi iz toga što klasifikator lako može naučiti da se vrijednosti $C/N0$ u slučaju ometanja kreću ispod 25 dB-Hz. Kad se ova konfuzijska matrica uspoređuje s konfuzijskom matricom binarne klasifikacije, vidi se da konfuzijska matrica binarne klasifikacije ima nešto višu točnost. Međutim, detaljnim pregledom njihovih konfuzijskih matrica može se otkriti da višeklasna verzija proizvodi manje lažno negativnih rezultata, koji predstavljaju najkritičnije pogreške u IDS-u jer ukazuju na neotkrivene napade. Binarna verzija imala je 0,97% slučajeva lažno negativnih rezultata, dok je višeklasna verzija imala 0,71%, što implicira da bi u stvarnom scenariju binarna IDS verzija previdjela više napada od višeklasne verzije. Smanjena točnost višeklasne verzije prvenstveno proizlazi iz izazova u razlikovanju vrsta napada, što je, unutar konteksta IDS-a, mnogo manje ozbiljno od lažno negativnog rezultata.



Slika 4-3 Konfuzijske matrice višeklasne (lijevo) i binarne (desno) klasifikacije za Stacking klasifikator. [38]

I autori u [41] predlažu IDS sustav za detekciju upada. U predloženom IDS-u koristi se samoučeno učenje (STL, *Self-Taught Learning*) s višeklasnim SVM-om za prepoznavanje GPS napada ometanjem i lažiranjem. Preciznije, duboka neuronska mreža koristi STL algoritam za identifikaciju jakih značajki i višeklasni SVM za klasifikaciju. STL je DL algoritam nenadziranog učenja koji se koristi kako bi se pronašle jake značajke za skup podataka za obuku. Autori ovoga rada odlučili su se za korištenje STL-a zato što je problem taj što nemaju dovoljno pouzdano označenih podataka za sve moguće vrste napada. Stoga se u takvim situacijama koristi STL koji je prikladniji od nadziranog učenja, jer STL prvo uči reprezentacije iz neoznačenih podataka a tek onda te reprezentacije koristi za klasifikaciju. S druge strane, nadzirano učenje zahtijeva veliki skup označenih primjera – za svaki uzorak potrebno je unaprijed znati je li normalan ili je pogođen napadima ometanja ili lažiranja. Napadi u UAV okruženju su rijetki, a često i novi, pa je prikupljanje kvalitetno označenih podataka gotovo nemoguće. Autori ne koriste STL samostalno, već ga koriste prije primjene višeklasnog SVM-a. Klasifikator radi bolje kad dobije kvalitetniji ulaz, pa autori koriste STL da pomoću njega dobiju čišće i informativnije značajke, a SVM-om onda dodijele klase napadima.

Podaci o napadima prikupljaju se iz različitih hardverskih komponenti drona, a prikupljaju se u trenutku kada dron skrene s planirane putanje kretanja. Klasificiraju napade u četiri klase: bez napada, lažiranje, ometanje i kombinirano ometanje + lažiranje. Višeklasni SVM koristi se u ovom radu kao nadzirani algoritam klasifikacije, a temelji se na arhitekturi binarnog stabla. SVM je odabran jer dobro radi i na linearnim i na nelinearnim podacima. Taj je algoritam modificirani SVM algoritam koji koristi metodu jedan-na-jedan za rješavanje problema višeklasne klasifikacije. Izvorni SVM prirodno dijeli podatke samo u dvije klase, tj. traži jednu hiperravninu za razdvajanje dvije klase. Višeklasni SVM koristi kombiniranje više binarnih modela za rad s K različitih klasa. Gradi se $\frac{K(K-1)}{2}$ modela za svaku moguću kombinaciju parova klasa, a konačna odluka donosi se glasanjem. Izlaz STL algoritma koristi se kao ulaz, tj. uzorci za obuku za višeklasni SVM.

Autori su implementirali predloženi IDS na dva načina: višeklasnim SVM-om i STL-om u kombinaciji s višeklasnim SVM-om, a rezultati su pokazali da je IDS temeljen na

dubokom učenju učinkovitiji od IDS-a temeljenog na strojnom učenju po pitanju detekcije GPS interferencija. U tablici 4-3 vidi se usporedba rezultata klasifikacije za implementirane verzije IDS-a.

Tablica 4-3 Točnost klasifikacije za predložene verzije IDS-a. [41]

Vrsta interferencije	Točnost za višeklasni SVM	Točnost za STL + višeklasni SVM
Lažiranje	78%	94%
Ometanje	82%	93%
Lažiranje + ometanje	72%	92%

4.1.3 Klasifikacija interferencija korištenjem transfernog učenja

Autori u [42] predstavljaju robusnu tehniku temeljenu na dubokom učenju koja koristi transferno učenje za karakterizaciju vrste poremećaja GNSS signala na temelju vremensko-frekvencijske analize (skalograma). Prethodno obučena konvolucijska neuronska mreža (CNN, *Convolutional Neural Network*) koristi se za izdvajanje informativnih značajki iz skalograma primljenih signala. Radi se na klasifikaciji 4 vrste interferencija – ometanje, lažiranje, višestazno prostiranje i aditivni bijeli Gaussov šum (AWGN, *Additive White Gaussian Noise*).

Skup podataka korišten u ovom radu čine sintetički GNSS IQ (*In-phase / Quadrature*) zapisi generirani Orolia GNSS simulatorom. Za kreiranje signala ometanja zadržana je referentna razina snage od -130 dBm, a zatim je primljena razina snage pretvorena u odgovarajuće vrijednosti omjera snage ometajućeg signala i snage korisnog signala (JSR, *Jamming-to-Signal Ratio*) dodavanjem snaga različitih vrsta ometanja za stvaranje signala ometanja snimljenih pri JSR-u u rasponu od 1 do 23 dB. Napad lažiranjem simuliran je posebnom konfiguracijom SDR kanala gdje izvor lažiranja odašilje signal snagom većom od snage autentičnog signala. Višestazno prostiranje simulirano je s do tri reflektirajuća puta po satelitu s variranjem kašnjenja, amplitude i faze. Nadalje, za fazu

klasifikacije potrebno je izdvojiti značajke signala. Sirovi signali su signali vremenske domene, pa se broj značajki izdvaja pretvaranjem u vremensko-frekvencijski prikaz - skalograme. Skalogram je kvadratna magnituda kontinuirane valićne transformacije (CWT, *Continuous Wavelet Transform*) te je pogodna reprezentacija jer hvata nestacionarne i tranzijentne osobine signala.

Korišten je Morseov valić za izračunavanje skalograma korisnog signala (SoI, *Signal of Interest*) i njegove kombinacije s:

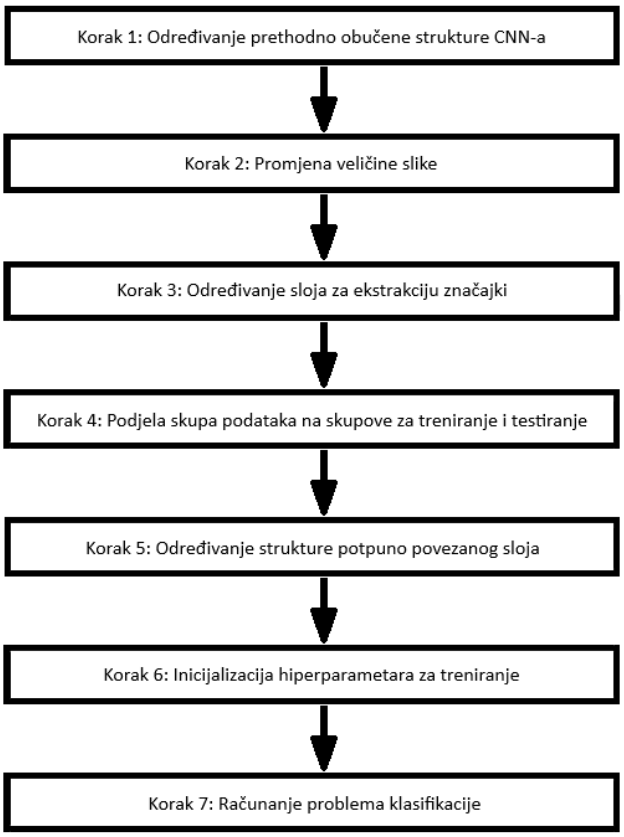
- uskopojasnim ometanjem kontinuiranim valom (CWI, *Continuous Wave Interference*)
- ometanjem „cvrkutavim“ ometačem (CI, *Chirp Interference*)
- višetonskim ometanjem kontinuiranim valom (MCWI, *Multi-Continuous Wave Interference*)
- impulsnim ometanjem (PI, *Pulse Interference*) te
- AWGN-om.

Dobiveni skalogram pretvara se u RGB (*Red, Green, Blue*) sliku koja će se poslati pretreniranim CNN-ovima za daljnju obradu. Skalogrami signala snimljeni su pri tri razine snage – niska (1-4 dB), srednja (9-13 dB) i jaka (19-23 dB).

Transferno učenje znači uzimanje samo nekih slojeva prethodno obučenog modela strojnog učenja i njegovo samo djelomično obučavanje za dotični zadatak. Transferno učenje može se koristiti primjerice u klasifikaciji slika za izdvajanje značajki pomoću prethodno obučene CNN mreže. Ulazni vektor značajki za fazu klasifikacije izdvaja se iz jednog ili više slojeva prethodno obučene mreže. S obzirom na to da dublji slojevi sadrže detaljnije značajke, sloj neposredno prije faze klasifikacije može se smatrati prikladnim izborom za izdvajanje značajki. U ovom radu zamrznut je konvolucijski dio. To znači da je konvolucijski dio ostao nepromijenjen, a njegov izlaz proslijeđen je novom klasifikatoru. Pojednostavljeno, prethodno obučeni modeli smatraju se fiksnom bazom za ekstrakciju značajki, što je korisno u slučaju malog skupa podataka i nedostatka računalne snage. Analizirana je učinkovitost pet poznatih CNN arhitektura u pogledu preciznosti klasifikacije i vremena učenja: AlexNet, GoogleNet, ResNet18, VGG16 (*Visual Geometry Group*) i MobileNet-V2.

Za primjenu transfernog učenja korišten je MATLAB *Deep Learning* alat. Veličine ulaznih slika prilagođene su zahtjevima svakog modela. Skup podataka podijeljen je na 70/30 za treniranje/testiranje.

Rezultati su pokazali da je najveća točnost klasifikacije postignuta korištenjem MobileNet-V2 s točnošću od 99,80%. Najkraće i najdulje ukupno proteklo vrijeme, uključujući korak ekstrakcije značajki i fazu treniranja, pripada AlexNet-u i VGG16. S obzirom na to da je MobileNet-V2 pružio vrlo dobru točnost klasifikacije, autori su odabrali ovaj model za treniranje i testiranje neviđenog tipa podataka pri jakoj razini JSR s točnošću od 98,86%. Uočeno je da se SoI često pogrešno klasificira kao višestazno prostiranje i obrnuto. Slika u nastavku prikazuje blok-dijagram implementiranog procesa klasifikacije korištenjem transfernog učenja.



Slika 4-4 Blok-dijagram implementiranog procesa klasifikacije korištenjem transfernog učenja. [42]

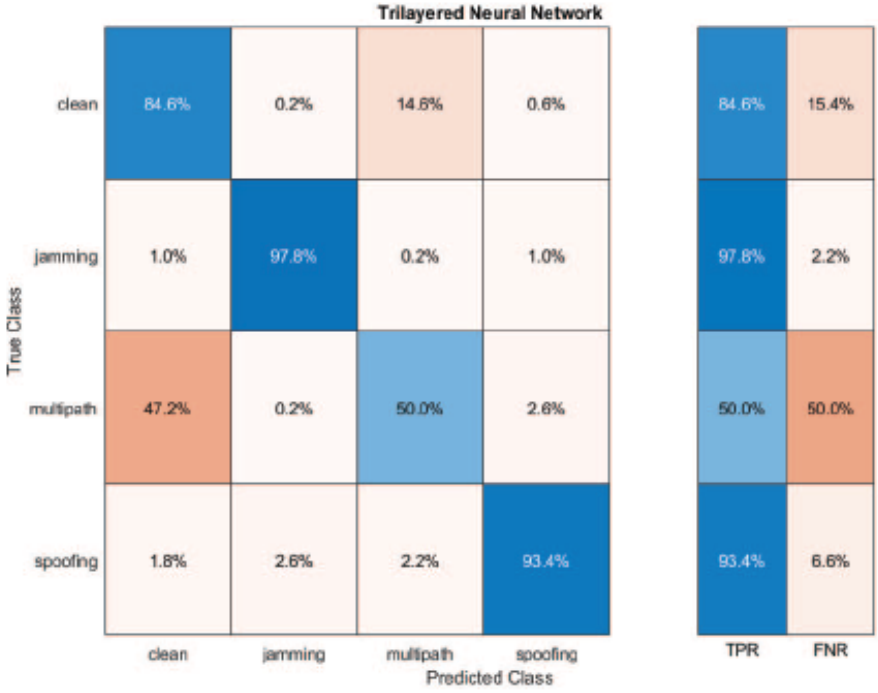
4.1.4 Klasifikacijski modeli temeljeni na izlazima multikorelacijskih prijamnika

Autori u [43] provode studiju u kojoj se fokusiraju na klasifikaciju primljenih GNSS signala u multikorelacijskom GNSS prijamniku. Provode klasifikaciju primljenih signala na temelju dvije značajke koje su dostupne u standardnom multikorelacijskom prijamniku – prosječne snage i distorzije korelacije. Prosječna snaga odnosi se na prosječnu snagu signala u određenom opsegu, a distorzija korelacije odnosi se na to koliko je korelacijski oblik signala izobličen u odnosu na idealni oblik. Korelacijski izlaz GNSS prijamnika je signal koji nastaje kada prijamnik usporedi primljeni satelitski signal sa svojom lokalno generiranom replikom koda i nosioca, pa dobije vrijednost koja pokazuje koliko se ta dva signala podudaraju. Množi se primljeni satelitski signal s lokalno generiranom kopijom pseudoslučajnog koda. Taj izlaz mjeri sličnost između signala i kopije. Prijamnik stvara identičan kodni niz kao i satelit. Jednostavno rečeno, prijamnik „pomiče“ svoju lokalnu verziju GNSS koda i traži trenutak kad se ona najbolje poklopi s primljenim signalom. Tada korelacija postaje najveća, pa prijamnik može procijeniti vrijeme dolaska signala, Dopplerov pomak i fazni pomak. Pomaže u pronalasku točnog vremena dolaska signala, praćenju satelita i skidanju navigacijske poruke.

Primljeni signali klasificiraju se u četiri klase: čisti signal, višestazno prostiranje, ometanje i lažiranje. Autori koriste klasifikatore neuronskih mreža, potpornih vektora, najbližih susjeda, aproksimacije jezgre, stabala odlučivanja, diskriminantne analize, naivni Bayes i klasifikatore ansambla. Skup podataka koji autori koriste sastoji se od 10 000 uzoraka. Performanse korištenih modela procijenjene su korištenjem metrike točnosti. Razmatraju se uzorci u rasponu od 1 000 do 10 000, tj. rade se testovi za 1 000, 5 000 i 10 000 uzoraka. Najveća točnost od 81,45% zabilježena je za model troslojne neuronske mreže na 5 000 uzoraka.

Konfuzijska matrica za troslojnu neuronsku mrežu prikazana je na slici 4-5. Može se iščitati da klase čisti signal, ometanje, višestazno prostiranje i lažiranje pokazuju stope stvarno pozitivnih rezultata (TPR, *True Positive Rate*) 84,6%, 97,8%, 50,0% i 93,4%. Ometanje ima visok TPR zbog svog disruptivnog ponašanja u snazi – prosječna snaga se proteže od 2 dB do 10 dB. I lažiranje također ima visok TPR zbog ponašanja izobličenja korelacijske funkcije – 2 do 40. Višestazno prostiranje ima TPR 50% što

ukazuje na preklapanje s autentičnim signalima. Može se uočiti da je stopa TPR visoka za ometanje i lažiranje što znači da klasifikator uspješno klasificira, s rijetkim pogreškama. Može se zaključiti da se signali ometanja i lažiranja lako razlikuju od autentičnih signala zbog njihove visoko izobličene korelacijske funkcije i veće prosječne snage u usporedbi s autentičnim signalima.



Slika 4-5 Konfuzijska matrica troslojne neuronske mreže. [43]

I u radu [44] koriste se izobličenje korelacijske funkcije i snaga signala za detekciju interferencija. Snaga primljenog signala i izobličenje korelacijske funkcije koriste se kao vektor značajki te se primljeni signali klasificiraju na signale s ometanjem, lažiranjem, na one s višestaznim prostiranjem i signale bez smetnji. Detekcija i klasifikacija anomalija provodi se korištenjem višeslojne perceptronske neuronske mreže (MLP, *Multi-Layer Perceptron*) čije se težine optimiraju algoritmom naziva optimizacija rojem čestica (PSO, *Particle Swarm Optimization*). Umjesto klasičnog treniranja neuronske mreže gradijentnim spustom, autori koriste PSO. U PSO-u svaka čestica predstavlja jedan mogući skup težina neuronske mreže. Za svaki skup težina izračunava se pogreška klasifikacije, odnosno

srednja kvadratna pogreška (MSE, *Mean Squared Error*). Čestice se zatim pomiču prema vlastitom najboljem pronađenom rješenju i najboljem rješenju cijelog roja. Cilj je pronaći težine koje minimiziraju MSE. Nakon konvergencije PSO-a dobivene težine koriste se u MLP klasifikatoru. Jednostavno rečeno, PSO pokušava pronaći najbolju konfiguraciju težina bez oslanjanja isključivo na lokalni gradijent.

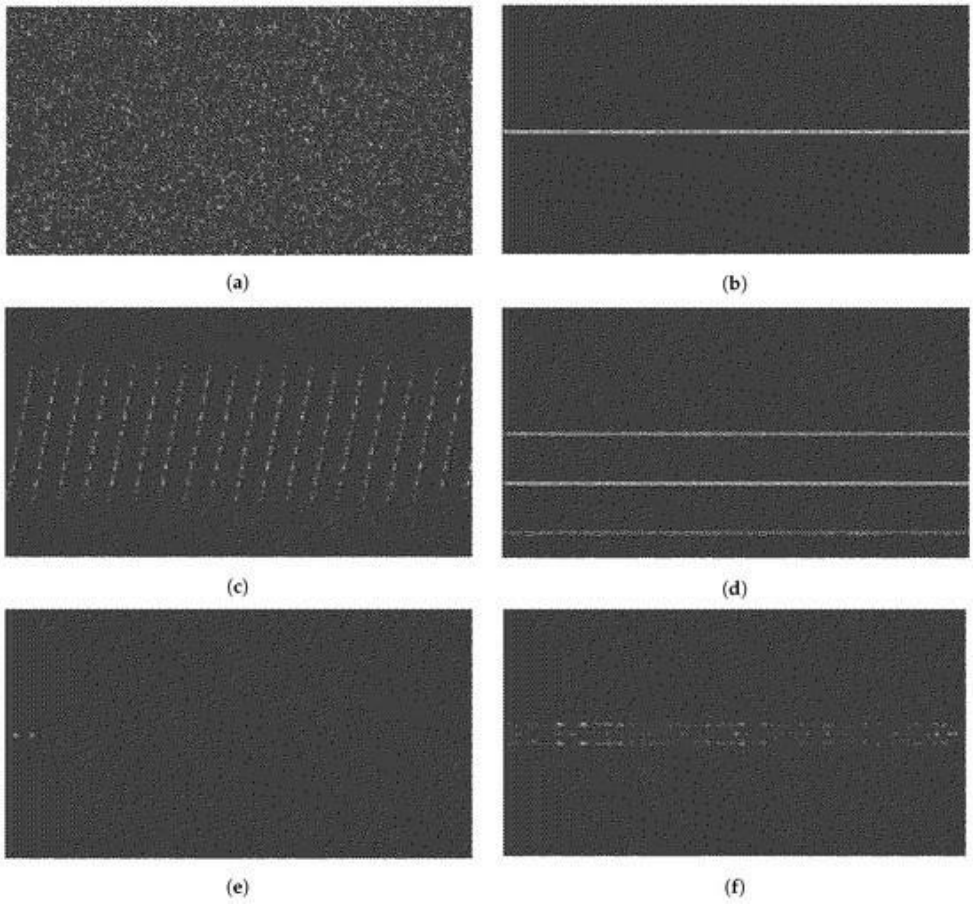
Kako bi se validirala učinkovitost predloženog, rezultati su uspoređeni s rezultatima postignutim klasifikacijom temeljenom na Bayesovom pravilu. Rezultati simulacije pokazuju da se otkrivanje napada lažiranjem poboljšalo za otprilike 4% i 2% u usporedbi s rezultatima postignutim klasifikacijom temeljenom na Bayesovom optimalnom pravilu i višehipoteznom Bayesovom klasifikatoru koji su se do tada često koristili u literaturi.

4.2 Primjena konvolucijskih neuralnih mreža na spektrograme kao tehnika za klasifikaciju različitih vrsta ometača

U radu [32] autori predlažu metodu klasifikacije ometača korištenjem spektrograma i metoda strojnog učenja. Generirali su skup podataka koji se sastoji od 61 800 različitih slika (spektrograma) generiranih od različitih vrsta ometača. Predlažu pristup u kojem primljeni signal klasificiraju u 6 klasa. Skup generiranih slika koriste za treniranje različitih algoritama strojnog učenja. Koriste SVM metodu koja primljene signale klasificira s vrlo visokom točnošću od 94,40% te CNN metodu koja daje nešto nižu točnost klasifikacije od 91,36%. Na temelju dobivenih rezultata autori su zaključili da se korištenjem malog skupa podataka slika i prilično jednostavnim parametrima i arhitekturama mrežnog sloja može postići visoka točnost klasifikacije.

Na slici 4-6 prikazana je po jedna slika od svake vrste ometača. Najveća točnost klasifikacije postignuta je kod primjene impulsnog ometača. To je rezultat činjenice da su spektrogrami impulsnih ometača znatno drugačiji od onih u ostalim scenarijima što se vidi i sa slike. S druge strane, iako i dalje preko 90%, najniža točnost klasifikacije postignuta je u slučaju amplitudno moduliranog (AM, *Amplitude Modulated*) i frekvencijski moduliranog (FM, *Frequency Modulated*) ometača. Razlog je u tome što spektrogrami tih dvaju ometača imaju isto obilježje – jednu ili više vodoravnih linija koje odgovaraju

specifičnim tonovima frekvencije kontinuiranog vala (CW, *Continuous Wave*), pa ih je teže klasificirati.



Slika 4-6 Spektrogrami različitih vrsta ometača u binarnom obliku: (a) Bez ometača, (b) AM ometač, (c) „Cvrkutavi"ometač, (d) FM ometač, (e) Impulsni ili DME (Distance Measurement Euipment) ometač, (f) Uskopojasni (NB, Narrow Band) ometač. [32]

Pretvorba signala ometanja u slike radi se kako je opisano u nastavku. Sirovi IQ podaci transformiraju se u vizualne prikaze, tj. spektrograme. Ovaj proces pretvorbe započinje prikupljanjem IQ uzoraka koji bilježe podatke o amplitudi i fazi primljenih signala tijekom vremena. Sljedeći korak uključuje primjenu vremensko-frekvencijske transformacije, poput kratkotrajne Fourierove transformacije (STFT, *Short-Time Fourier Transform*), za pretvaranje 1D signala vremenske domene u 2D prikaz vremensko-frekvencijske domene. Ova transformacija stvara spektrogram koji vizualno ilustrira kako

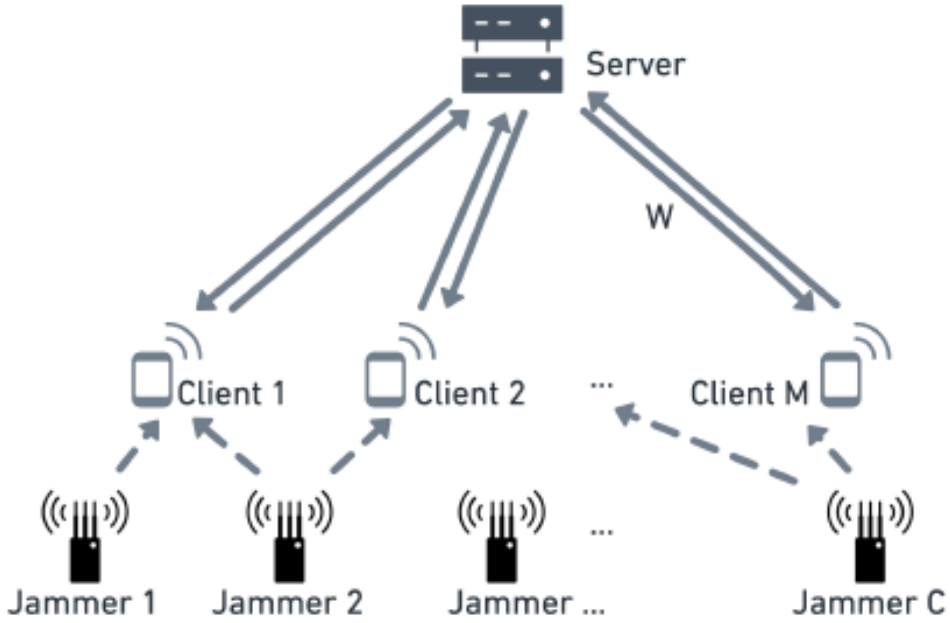
se frekvencijski sadržaj signala mijenja tijekom vremena, omogućujući lakšu identifikaciju i klasifikaciju različitih vrsta ometanja. Dobivene slike služe kao ulaz za modele strojnog i dubokog učenja, omogućujući klasifikaciju signala ometanja na temelju njegovih jedinstvenih spektralnih značajki. [34]

U radu [33] također je pokazano da kombinacija strojnog učenja i spektrograma daje izvrsne rezultate za otkrivanje ometanja signala. Autori istražuju korištenje federiranog učenja (FL, *Federated Learning*) za treniranje klasifikatora signala ometanja lokalno na svakom uređaju s ažuriranjima modela na centralnom poslužitelju. Ističu federirano učenje kao obećavajuće rješenje koje omogućuje zajedničko obučavanje modela strojnog učenja uz održavanje lokalne decentralizacije podataka. Korištenjem federiranog učenja za lokalno treniranje klasifikatora signala ometanja na svakom uređaju postiže se treniranje podataka uz očuvanje privatnosti, a istovremeno se prikuplja ogromna količina korisničkih podataka. Skup podataka na kojem se provodi treniranje sastoji se od spektrogramskih slika simuliranog interferiranog GNSS signala.

Autori predstavljaju rezultate za klasifikaciju spektrograma simuliranog GNSS signala pod prijetnjom šest različitih vrsta ometača. Rezultati su pokazali da DME ometač daje najbolju točnost klasifikacije od 99%. Kao i u prethodno analizanom radu, i u ovom su radu autori pokazali da je klasifikatoru teško razlikovati AM i FM ometač, kao i NB i „cvrkutavi” ometač.

FL je tehnika učenja koja omogućuje korisnicima da zajednički koriste prednosti dijeljenih modela obučenih na podacima prikupljenim od mnoštva korisnika bez potrebe za centralnim pohranjivanjem podataka. U ovom pristupu, svaki klijent zadržava lokalni skup podataka za obuku koji se nikada ne prenosi na središnji poslužitelj. Umjesto toga, klijenti primaju trenutni globalni model, izračunavaju ažuriranja na temelju svojih lokalnih podataka i šalju samo ta ažuriranja poslužitelju. Središnji poslužitelj zatim agregira ta ažuriranja kako bi poboljšao globalni model i proces se ponavlja. Korištenjem rubnih uređaja za izvođenje lokalne obuke, federirano učenje učinkovito smanjuje latenciju, povećava skalabilnost i optimizira korištenje resursa, uz poboljšanje privatnosti i sigurnosti podataka. [35]

Slika 4-7 prikazuje okvir federiranog učenja za obuku klasifikatora signala ometanja. Pretpostavlja se da postoji C različitih vrsta ometanja. M suradničkih klijenata prima parametre klasifikatora s poslužitelja. Ovi klijenti ponovno obučavaju model na temelju lokalnih podataka i prenose svoj ažurirani klasifikator na poslužitelj zadužen za spajanje rezultata. Ovaj proces ne zahtijeva razmjenu stvarnih podataka ili pozicija od klijenata, čime se čuva njihova privatnost.



Slika 4-7 Okvir federiranog učenja za obuku klasifikatora signala ometanja. [33]

Autori u [34] istražuju učinkovitost različitih algoritama strojnog i dubokog učenja za klasifikaciju različitih oblika lažiranja. Skup podataka korišten za detekciju signala ometanja je skup slika dobivenih iz sirovih IQ podataka. Sastoji se od šest različitih klasa od kojih svaka predstavlja različitu vrstu signala ometanja i formatiran je kao spektrogramske slike koje omogućuju učinkovitu analizu i klasifikaciju korištenjem tehnika strojnog i dubokog učenja.

Što se tiče klasifikacije signala ometanja, autori kombiniraju duboku ekstrakciju značajki s klasičnim tehnikama strojnog učenja kako bi postigli točnije i učinkovitije

rješenje za otkrivanje ometanja. Za klasifikaciju signala ometanja korišteni su modeli slučajna šuma, stablo odlučivanja i logistička regresija. Ovi modeli su odabrani zbog svoje učinkovitosti u zadacima klasifikacije. Kako bi dodatno poboljšali performanse njihovog modela, implementirali su funkciju ekstrakcije značajki koristeći model ResNet18. Ova arhitektura dubokog učenja poznata je po svojoj sposobnosti hvatanja složenih uzoraka u podacima slike putem svog okvira za učenje reziduala. Nakon što su izdvojili značajke iz slika pomoću ResNet18 modela, te su značajke koristili za obuku spomenutih modela strojnog učenja. Ovaj pristup im je omogućio da iskoriste snažne mogućnosti reprezentacije CNN-ova, a istovremeno koriste tradicionalne algoritme strojnog učenja za klasifikaciju. Ovim pristupom postigli su točnost od gotovo 99%.

Autori u [36] za klasifikaciju ometanja predlažu korištenje konvolucijskih neuronskih mreža sa šiljastim učinkom (CSNN *, Convolutional Spiking Neural Network*). Neuronske mreže sa šiljcima (SNN, *Spiking Neural Network*) su vrsta umjetnih neuronskih mreža koje oponašaju ponašanje bioloških neurona obradom i prijenosom informacija putem diskretnih, asinkronih šiljaka ili događaja. Za razliku od tradicionalnih umjetnih neuronskih mreža koje obrađuju signale kontinuirane vrijednosti, SNN-ovi komuniciraju putem signala kratkog trajanja (šiljaka), što im omogućuje učinkovito hvatanje složenih prostornih i vremenskih obrazaca u podacima.

Autori u ovom radu smatraju da se postojeće metode detekcije ometanja oslanjaju na DL modele koji zahtijevaju mnogo energije što ih čini neprikladnima za rubne uređaje s ograničenom snagom i resursima koji se koriste u GNSS sustavima, te su skloni pogreškama u bučnim okruženjima. Smatraju da će pristupom u kojem se koristi CSNN iskoristiti energetsku učinkovitost, asinkronu i rijetku prirodu SNN-ova.

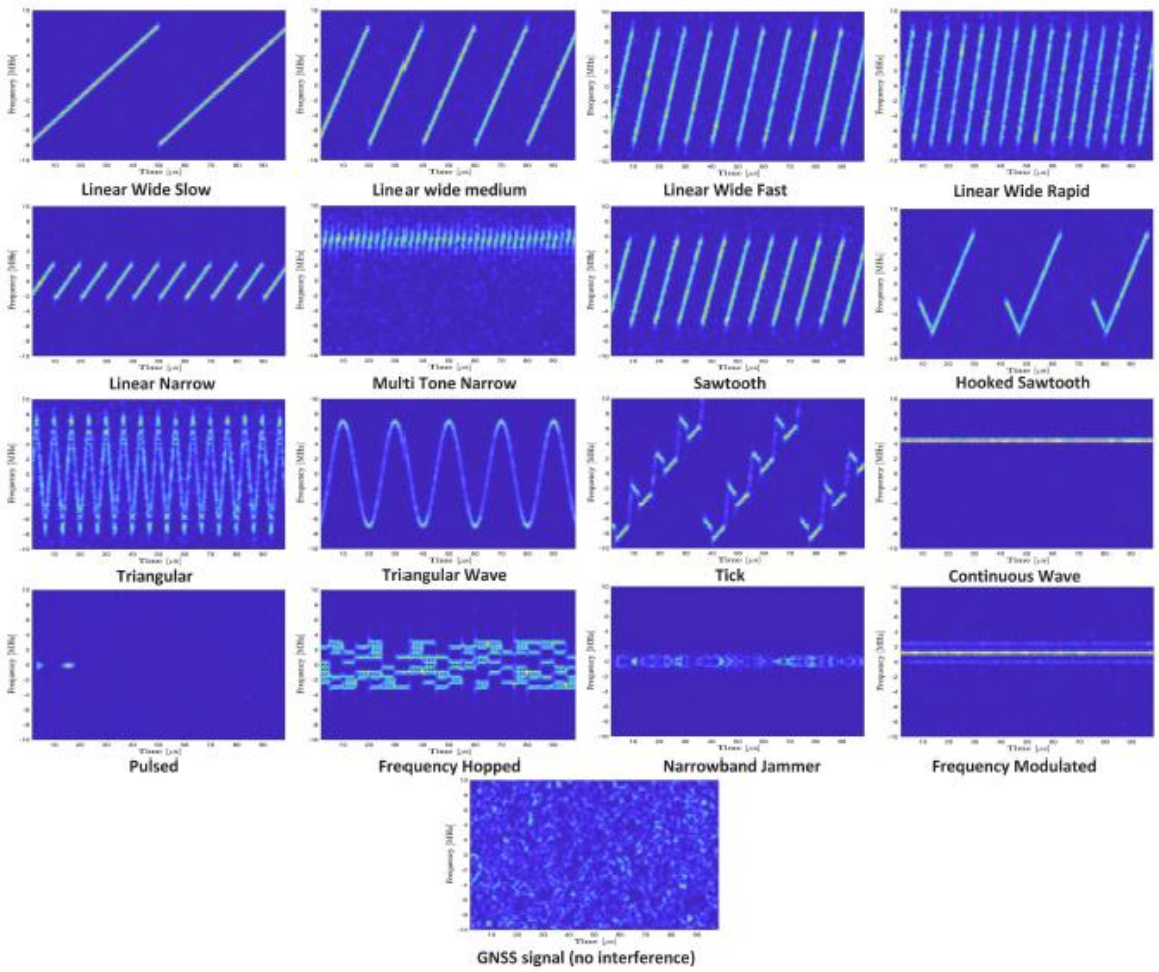
Kao i u prethodno opisanim radovima, i u ovom je radu korišten skup podataka koji se sastoji od slika, tj. spektrograma, normaliziranih u sive tonove u svrhu računalne jednostavnosti. Autori su postigli vrhunsku točnost klasifikacije ometanja. Dodali su čak i šum kako bi procijenili performanse modela u uvjetima pojačane buke.

Eksperimentalni rezultati pokazuju da modeli temeljeni na CSNN-ovima postižu konkurentnu točnost do 98%, usporedivu s konvolucijskom neuronskom mrežom s modulom pažnje za konvolucijske blokove (CNN-CBAM, *Convolutional Neural Network -*

Convolutional Block Attention Module) i ResNet18, a istovremeno održavaju točnost do 97% s vrhunskom računalnom učinkovitošću, gdje tradicionalni modeli degradiraju na samo 33%. Iako su VGG i ResNet18 postigli veću točnost klasifikacije na čistim testnim podacima, eksperimentalni rezultati pokazali su koliko je CSNN energetski učinkovitiji u odnosu na te modele – 1,6 puta u odnosu na CNN, 17 puta u odnosu na ResNEt18 te 148 puta u odnosu na VGG16. Za usporedbu, model CSNN postigao je 97% točnosti u 56 epoha, dok je model CNN postigao 95% točnosti u 74 epohe.

I autori u [40] postigli su impresivnu točnost od 99,69% korištenjem CNN modela i spektrograma za klasifikaciju različitih vrsta ometanja. Koristili su CNN model ResNet i pokazali da bi mogao biti moćan alat za klasifikaciju smetnji. Kao bitnu stvar napominju da se kod detekcije GNSS smetnji, gdje se izlaz *front-enda* koristi kao ulazni podatak za ML pristup, bez obzira na dosljednost faktora kao što su propusnost, frekvencija uzorkovanja i kvantizacija bitova, mogu pojaviti varijacije u izlazima različitih *front-end* arhitektura. Stoga bi za implementaciju predložene metode u uređaje u realnom svijetu trebalo uzeti u obzir specifični hardver *front-enda* koristeći instance signala koje potječu upravo s tog *front-enda*. Izračun STFT-a i pretvaranje u slike, kao i u radovima [32] i [34], čini najveći dio predobrade podataka. Slika 4-8 prikazuje primjere spektrograma za svaku vrstu interferencije.

Iako se CNN metoda u mnogim radovima pokazala kao izvrsna za klasifikaciju signala ometanja kada su ulazni podaci slike, proces treniranja CNN arhitekture zahtijeva značajne računalne resurse, pa je nije uvijek moguće ni isplativo koristiti. Stoga, ovisno o resursima kojima se raspolaže, treba odvagati isplati li se koristiti ovu metodu klasifikacije.



Slika 4-8 Primjeri spektrograma za svaku vrstu interferencije. [40]

5 ZAKLJUČAK

Aplikacije za navigaciju i pozicioniranje u današnje se vrijeme koriste u svakodnevnom životu. Pametni telefoni, kao najkorišteniji uređaji u svakodnevnom životu, oslanjaju se na aplikacije za navigaciju i pozicioniranje. Takve aplikacije za rad koriste GNSS sustave što ih čini vrlo osjetljivima na prijetnje. Od svih razvijenih satelitskih sustava najpoznatiji i najrasprostranjeniji je GPS a s njegovim većim razvojem i unaprjeđivanjem, kao i s unaprjeđivanjem ostalih navigacijskih sustava, dolazi do češće korištenosti a samim tim i ranjivosti tih sustava na različite prijetnje.

Najčešće namjerne interferencije koje se javljaju u GNSS sustavu su ometanje i lažiranje, pa je i u ovom radu stavljen naglasak na njih. Ove interferencije predstavljaju aktivne prijetnje i sigurnosne rizike u GNSS sustavima te mogu prouzročiti ozbiljne posljedice za korisnike. Prisutnost signala ometanja i lažiranja dovodi do smanjene sigurnosti u brojnim aplikacijama koje pružaju lokacijske usluge.

Ovaj rad daje pregled postojećih rješenja za klasifikaciju različitih vrsta interferencija u sustavu GNSS. Postojeća rješenja, opisana u četvrtom poglavlju rada, temelje se na metodama strojnog i dubokog učenja. Tradicionalne metode klasifikacije smetnji oslanjaju se na unaprijed definirana pravila i pragove. S druge strane, pristupi temeljeni na strojnom učenju nude model koji treba obučiti za točnu i automatsku klasifikaciju interferencija. Prednost je i u tome što se u slučaju novih scenarija ili novih vrsta interferencija isti model ponovnim obučavanjem može prilagoditi tim promjenama. Nedostatak strojnog učenja je to što njegova implementacija u uređaje masovnog tržišta može biti izazovna, često zahtijevajući veću računalnu snagu ili čak promjene u dizajnu hardvera.

Gledajući postojeća rješenja, može se zaključiti da su metode temeljene na dubokom učenju superiornije nad tradicionalnim metodama strojnog učenja, pa su i češće korištene u svrhu klasifikacije interferencija. Razlog je u tome što imaju mogućnost automatskog izdvajanja značajki i mogu izravno učiti apstraktne značajke visoke razine u podacima iz izvornog ulaza. S obzirom na to da su interferencije sve češća pojava u sustavu GNSS, potrebno je poraditi na razvoju novih i unaprjeđenju postojećih sustava za klasifikaciju interferencija. Federirano učenje perspektivan je smjer u kojem bi se mogla provoditi daljnja istraživanja, jer takvih radova u literaturi nema puno a njegova primjena ima brojne

prednosti za korisnike i očuvanje privatnosti. Na temelju postojećih rješenja može se zaključiti da je duboko učenje smjer kojim treba ići kada se radi o klasifikaciji interferencija u sustavu GNSS što pokazuje i visoka klasifikacijska točnost radova analiziranih u ovom radu.

LITERATURA

[1] Marta Brkić, Detekcija lažnog signala u sustavu GNSS, Fakultet elektrotehnike, strojarstva i brodogradnje Split, diplomski rad, 2024.

[2] „What is GNSS“, https://www.gps.gov/systems/gnss/, s Interneta, 20.7.2026.

[3] „An Introduction to GNSS“,, s Interneta, 20.7.2026.

[4] „Satellite Navigation – Global Positioning System (GPS)“, https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/gps, s Interneta, 20.7.2026.

[5] „Global Positioning System“, https://en.wikipedia.org/wiki/Global_Positioning_System, s Interneta, 20.7.2026.

[6] „Satellite Navigation – GPS – Control Segment“, https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/gps/controlsegments, s Interneta, 20.7.2026.

[7] „FDMA vs. CDMA“, https://gssc.esa.int/navipedia/index.php/FDMA_vs._CDMA, s Interneta, 20..2026.

[8] „Directions 2019: High-orbit GLONASS and CDMA“, https://www.gpsworld.com/directions-2019-high-orbit-glonass-and-cdma-signal/, s Interneta, 20..2026.

[9] „Galileo System“, https://www.gsc-europa.eu/galileo/system, s Interneta, 20.7.2026.

[10] „Galileo Satellites“, https://www.esa.int/Applications/Satellite_navigation/Galileo/Galileo_satellites, s Interneta, 20.7.2026.

[11] „BeiDou“, https://en.wikipedia.org/wiki/BeiDou, s Interneta, 20.7.2026.

[12] „China Launches Second Compass (BeiDou-2) Satellite in $1.46 Billion First Phase“, https://insidegnss.com/china-launches-second-compass-beidou-2-satellite-in-1-46-billion-first-phase/, s Interneta, 20.7.2026.

[13] „BeiDou Future and Evolutions“, https://gssc.esa.int/navipedia/index.php/BeiDou_Future_and_Evolutions, s Interneta, 20.7.2026.

[14] „QZSS Michibiki: Quasi-Zenith Satellite System of Japan“, https://jgtimes.org/articles/8_QZSS, s Interneta, 20.7.2026.

[15] „Quasi-Zenith Satellite System“, https://en.wikipedia.org/wiki/Quasi-Zenith_Satellite_System, s Interneta, 20.7.2026.

[16] „IRNSS Programme“, https://www.isro.gov.in/IRNSS_Programme.html, s Interneta, 20.7.2026.

[17] ISO 24246:2022(en). Space systems — Requirements for global navigation satellite system (GNSS) positioning augmentation centers. Dostupno online: https://www.iso.org/obp/ui#home (pregledano 15.7.2026.)

[18] ETSI TS 103 246-5 V1.1.1 (2016-01) and V1.3.1 (2020-10). Satellite Earth Stations and Systems (SES). GNSS-based location systems, Part 5: Performance Test Specification. Available online: https://portal.etsi.org/Services/editHelp/Search/FAQs/TEDDI (pregledano 15.7.2026.

[19] Mukherji, V.; AKS Chandele, Lt. Gen. GNSS Jamming: An Omnipresent Threat. Geospatial World. Available online: https://www.geospatialworld.net/prime/special-features/gnss-jamming-an-omnipresent-threat/ (pregledano 18.7.2026).

[20] Li, X.; Chen, L.; Lu, Z.; Wang, F.; Liu, W.; Xiao, W.; Liu, P. Overview of Jamming Technology for Satellite Navigation. Machines 2023, 11, 768. https://doi.org/10.3390/machines11070768

[21] Todd, E.; Brent, M.; Mark, L.; Brady, W.; Paul, M. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008), Savannah, GA, USA, 16–19 September 2008.

[22] He, X.; Liao, K.; Peng, S.; Tian, Z.; Huang, J. Interrupted-Sampling Repeater Jamming-Suppression Method Based on a MultiStages Multi-Domains Joint Anti-Jamming Depth Network. Remote Sens. 2022.

[23] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O´Hanlon and P. M. Kintner, "Assesing the spoofing threat: Development of a portable GPS civilian spoofer," in Proc. Radionavigation Lab. Conf., 2008, pp. 2314-2325.

[24] Songala, K. K.; Ammana, S. R.; Ramachandruni, H. C.; Achanta, D. S. "Simplistic Spoofing of GPS Enabled Smartphone". In Proceedings of the 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-ECE52138.2020.939798.

[25] K. Radoš, M. Brkić and D. Begušić, "Vulnerability of Smartphones on GNSS Simplistic Spoofing Attack," 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2024, pp. 812-817, doi: 10.1109/MIPRO60963.2024.10569351.

[26] Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. Proc. IEEE 2016, 104, 1258–1270.

[27] Garbin Manfredini, E. Signal Processing Techniques for GNSS Anti-Spoofing Algorithms. Ph.D. Thesis, Polytechnic University of Turin, Torino, Italy, 2017.

[28] Miljanovic, S.; Ardizzon, F.; Crosara, L.; Laurenti, N.; Canzian, L.; Lovisotto, E.; Montini, N.; Pozzobon, O.; Ioannides, R.T. Experimental Testing and Impact Analysis of Jamming and Spoofing Attacks on Professional GNSS Receivers. In Proceedings of the ICL-GNSS 2022, Tampere, Finland, 7–9 June 2022; CEUR Workshop Proceedings, Volume 3183.

[29] Dułowicz, J.; Skokowski, P.; Kelner, J.M. Experimental Evaluation of GNSS Receiver Vulnerability to Spoofing and Jamming Using SDR-Based Testbed. Sensors 2026, 26, 4551. https://doi.org/10.3390/s26144551.

[30] M. Tamazin, M. Karaim, H. Elghamrawy and A. Noureldin, "A Comprehensive Study of the Effects of Linear Chirp Jamming on GNSS Receivers under High-Dynamic Scenarios," 2018 13th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 2018, pp. 9-14, doi: 10.1109/ICCES.2018.8639399.

[31] Lemieszewski, Ł.; Radomska-Zalas, A.; Perec, A.; Dobryakova, L.; Ochin, E. GNSS and LNSS Positioning of Unmanned Transport Systems: The Brief Classification of Terrorist Attacks on USVs and UUVs. Electronics 2021, 10, 401. https://doi.org/10.3390/electronics10040401.

[32] Morales Ferre, R.; de la Fuente, A.; Lohan, E.S. Jammer Classification in GNSS Bands Via Machine Learning Algorithms. Sensors 2019, 19, 4841. https://doi.org/10.3390/s19224841

[33] P. Wu, H. Calatrava, T. Imbiriba and P. Closas, "Jammer classification with Federated Learning," 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 2023, pp. 228-234, doi: 10.1109/PLANS53410.2023.10140124.

[34] Ghanbarzade, A., & Soleimani, H. (2025). GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. https://doi.org/10.48550/arXiv.2501.02352

[35] M. Jaramillo-Civill, P. Wu, A. Nardin, T. Imbiriba and P. Closas, "Jammer Source Localization with Federated Learning," 2025 IEEE/ION Position, Location and Navigation Symposium (PLANS), Salt Lake City, UT, USA, 2025, pp. 362-371, doi: 10.1109/PLANS61210.2025.11028278.

[36] G. Velusamy and R. Lent, "A Study of Attention-Driven Spiking Neural Networks in Enhancing GNSS Jamming Classification," ICC 2025 - IEEE International Conference on Communications, Montreal, QC, Canada, 2025, pp. 6741-6746, doi: 10.1109/ICC52391.2025.11161893.

[37] Pervysheva, Yelyzaveta & Käppi, Jani & Nurmi, Jari & Lohan, Elena Simona. (2025). GNSS interference detection and classification with real-field Jammertest 2024 data and neural networks. 10.21203/rs.3.rs-7864272/v1.

[38] de Lemos, G. G. R., & da Silva, R. A. C. (2026). Multiclass Classification for Detection of GPS Spoofing and Jamming Attacks on UAVs. Journal of the Brazilian Computer Society, 32(1), 374–386. https://doi.org/10.5753/jbcs.2026.5309.

[39] Aissou, G., Slimane, H. O., Benouadah, S., and Kaabouch, N. (2021). Tree-based supervised machine learning models for detecting GPS spoofing attacks on UAS. In 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pages 0649–0653. DOI: 10.1109/UEMCON53757.2021.9666744.

[40] I. E. Mehr and F. Dovis, "A Deep Neural Network Approach for Classification of GNSS Interference and Jamming," in IEEE Transactions on Aerospace and Electronic Systems, vol. 61, no. 2, pp. 1660-1676, April 2025, doi: 10.1109/TAES.2024.3462662.

[41] M. P. Arthur, "Detecting Signal Spoofing and Jamming Attacks in UAV Networks using a Lightweight IDS," *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Beijing, China, 2019, pp. 1-5, doi: 10.1109/CITS.2019.8862148.

[42] 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.

[43] 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.

[44] S. Tohidi and M. R. Mosavi, "Effective Detection of GNSS Spoofing Attack Using A Multi-Layer Perceptron Neural Network Classifier Trained by PSO," 2020 25th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Iran, 2020, pp. 1-5, doi: 10.1109/CSICC49403.2020.9050078.

[45] „GNSS signal“, https://gssc.esa.int/navipedia/index.php/GNSS_signal, s Interneta, 21.7.2026.

[46] Psiaki, M.L.; Humphreys, T.E.; Stauffer, B. Attackers can spoof navigation signals without our knowledge. Here is how to fight back GPS lies. IEEE Spectr. 2016, 53, 26–53.

[47] Yang, B.; Tian, M.; Ji, Y.; Cheng, J.; Xie, Z.; Shao, S. Research on GNSS Spoofing Mitigation Technology Based on Spoofing Correlation Peak Cancellation. IEEE Commun. Lett. 2022, 26, 3024–3028.

[48] Zhou, W.; Lv, Z.; Li, G.; Jiao, B.; Wu, W. Detection of Spoofing Attacks on Global Navigation Satellite Systems Using Kolmogorov–Smirnov Test-Based Signal Quality Monitoring Method. IEEE Sens. J. 2024, 24, 10474–10490.

[49] Zhu, X.; Lu, Z.; Hua, T.; Yang, F.; Tu, G.; Chen, X. A Novel GPS Meaconing Spoofing Detection Technique Based on Improved Ratio Combined with Carrier-to-Noise Moving Variance. Electronics 2022, 11, 738.

[50] Pardhasaradhi, B.; Yakkati, R.R.; Cenkeramaddi, L.R. Machine Learning-Based Screening and Measurement to Measurement Association for Navigation in GNSS Spoofing Environment. IEEE Sens. J. 2022, 22, 23423–23435.

[51] Lee, Y.-S.; Yeom, J.S.; Jung, B.C. A Novel Array Antenna-Based GNSS Spoofing Detection and Mitigation Technique. In Proceedings of the 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2023; pp. 489–492.

[52] Chen, J.; Wang, X.; Fang, Z.; Jiang, C.; Gao, M.; Xu, Y. A Real-Time Spoofing Detection Method Using Three Low-Cost Antennas in Satellite Navigation. Electronics 2024, 13, 1134.

[53] Truong, V.; Vervisch-Picois, A.; Rubio Hernan, J.; Samama, N. Characterization of the Ability of Low-Cost GNSS Receiver to Detect Spoofing Using Clock Bias. Sensors 2023, 23, 2735.

[54] Zhang, Z.; Zhan, X. Statistical analysis of spoofing detection based on TDOA. IEEJ Trans. Electr. Electron. Eng. 2018, 13, 840–850.

[55] Chen, S.; Ni, S.; Lei, T.; Cheng, L.; Song, X. GNSS Spoofing Detection via the Intersection Angle between Two Directions of Arrival in a Single Rotating Antenna. Sensors 2024, 24, 1116.

[56] Chang, H.; Pang, C.; Zhang, L.; Guo, Z. Rotating Single-Antenna Spoofing Signal Detection Method Based on IPNN. Sensors 2022, 22, 7141.

[57] Lee, D.-K.; Miralles, D.; Akos, D.; Konovaltsev, A.; Kurz, L.; Lo, S.; Nedelkov, F. Detection of GNSS Spoofing using NMEA Messages. In Proceedings of the European Navigation Conference (ENC), Dresden, Germany, 23–24 November 2020; pp. 1–10.

[58] Spravil, J.; Hemminghaus, C.; von Rechenberg, M.; Padilla, E.; Bauer, J. Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring. J. Mar. Sci. Eng. 2023, 11, 928.

[59] Xiao, L.; Li, X.; Wang, G. GNSS Spoofing Detection Using Pseudo-range Double Differences between Two Receivers. In Proceedings of the 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 19–20 October 2019; pp. 498–502.

[60] Shafique, A.; Mehmood, A.; Elhadef, M. Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models. IEEE Access 2021, 9, 93803–93815.

[61] Gallardo, F.; Yuste, A.P. SCER Spoofing Attacks on the Galileo Open Service and Machine Learning Techniques for End-User Protection. IEEE Access 2020, 8, 85515–85532.

[62] Elango, A.; Ujan, S.; Ruotsalainen, L. Disruptive GNSS Signal detection and classification at different Power levels Using Advanced Deep-Learning Approach. In Proceedings of the 2022 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 7–9 June 2022; pp. 1–7.

[63] Borhani-Darian, P.; Li, H.; Wu, P.; Closas, P. Detecting GNSS spoofing using deep learning. EURASIP J. Adv. Signal Process. 2024, 2024, 14.

[64] Marchand, M.; Toumi, A.; Seco-Granados, G.; López-Salcedo, J.A. Machine Learning Assessment of Anti-Spoofing Techniques for GNSS Receivers. In Proceedings of the WIPHAL 2023: Work-in-Progress in Hardware and Software for Location Computation, CEUR Workshop Proceedings, Castellon, Spain, 6–8 June 2023.

[65] Babić, Katarina; Balić, Marta; Begušić, Dinko. GNSS Spoofing Detection Based on Wavelets and Machine Learning // Electronics (Basel), 14 (2025), 12; 1-27. doi: 10.3390/electronics14122391

[66] Wang, W.; Aguilar Sanchez, I.; Caparra, G.; McKeown, A.; Whitworth, T.; Lohan, E.S. A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting with Focus on the GNSS Pre-Correlation Sampled Data. Sensors 2021, 21, 3012.

[67] Morales-Ferre, R.; Wang, W.; Sanz-Abia, A.; Lohan, E.-S. Identifying GNSS Signals Based on Their Radio Frequency (RF) Features—A Dataset with GNSS Raw Signals Based on Roof Antennas and Spectracom Generator. Data 2020, 5, 18.

[68] Wang, W.; Lohan, E.S.; Sanchez, I.A.; Caparra, G. Pre-correlation and post-correlation RF fingerprinting methods for GNSS spoofer identification with real-field measurement data. In Proceedings of the 10th Workshop on Satellite Navigation Technology (NAVITEC), Noordwijk, The Netherlands, 5–7 April 2022; pp. 1–10.

[69] Zhang, X.; Huang, Y.; Tian, Y.; Lin, M.; An, J. Noise-Like Features-Assisted GNSS Spoofing Detection Based on Convolutional Autoencoder. IEEE Sens. J. 2023, 23, 25473–25486.

[70] Manfredini, E.G.; Akos, D.M.; Chen, Y.-H.; Lo, S.; Walter, T.; Enge, P. Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers. In Proceedings of the 2018 International Technical Meeting of The Institute of Navigation, Reston, VA, USA, 29 January–1 February 2018; pp. 672–689.

[71] Spens, N.; Lee, D.-K.; Nedelkov, F.; Akos, D. Detecting GNSS Jamming and Spoofing on Android Devices. NAVIGATION J. Inst. Navig. Sept. 2022, 69, navi.537.

[72] Spens, N.; Lee, D.-K.; Akos, D. An application for detecting GNSS jamming and spoofing. In Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+), St. Louis, MO, USA, 20–24 September 2021; pp. 1981–1988.

[73] Zhang, J.; Cui, X.; Xu, H.; Lu, M. A Two-Stage Interference Suppression Scheme Based on Antenna Array for GNSS Jamming and Spoofing. Sensors 2019, 19, 3870.

[74] Hu, Y.; Bian, S.; Li, B.; Zhou, L. A Novel Array-Based Spoofing and Jamming Suppression Method for GNSS Receiver. IEEE Sens. J. 2018, 18, 2952–2958.

[75] Humphreys, T.E.; Bhatti, J.A.; Shepard, D.P.; Wesson, K.D. The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal

Authentication Techniques. In Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 17–21 September 2012.

[76] Albright, A.; Powers, S.; Bonior, J.; Combs, F. Oak Ridge Spoofing and Interference Test Battery (OAKBAT)—GPS; Oak Ridge National Laboratory (ORNL): Oak Ridge, TN, USA, 2020.

[77] Foruhandeh, M.; Mohammed, A.Z.; Kildow, G.; Gerdes, R.; Berges, R. SatGrid Dataset, Realtime Genuine and Spoofing Traces of GPS Signals Collected at Different Geographical Locations, Times and Environmental Conditions; Dataset; University Libraries, Virginia Tech: Blacksburg, VA, USA, 2020.

[78] Axell, E.; Eklöf, F.M.; Johansson, P.; Alexandersson, M.; Akos, D.M. Jamming Detection in GNSS Receivers: Performance Evaluation of Field Trials. J. Inst. Navig. 2015, 62, 73–82.

[79] Strizic, L.; Akos, D.M.; Lo, S. Crowdsourcing GNSS Jammer Detection and Localization. In Proceedings of the 2018 International Technical Meeting of the Institute of Navigation, Reston, VA, USA, 29 January–1 February 2018; pp. 626–641.

[80] Osman, A.; Moussa, M.M.E.; Tamazin, M.; Korenberg, M.J.; Noureldin, A. DOA Elevation and Azimuth Angles Estimation of GPS Jamming Signals Using Fast Orthogonal Search. IEEE Trans. Aerosp. Electron. Syst. 2020, 56, 3812–3821.

[81] Wu, Z.; Zhao, Y.; Yin, Z.; Luo, H. Jamming signals classification using convolutional neural network. In Proceedings of the 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Bilbao, Spain, 18–20 December 2017; pp. 62–67.

[82] Swinney, C.J.; Woods, J.C. GNSS Jamming Classification via CNN, Transfer Learning & the Novel Concatenation of Signal Representations. In Proceedings of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 14–18 June 2021; pp. 1–9.

[83] Panice, G.; Luongo, S.; Gigante, G.; Pascarella, D.; Di Benedetto, C.; Vozella, A.; Pescape, A. A SVM-based detection approach for GPS spoofing attacks to UAV. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–11.

[84] Li, W.; Huang, Z.; Lang, R.; Qin, H.; Zhou, K.; Cao, Y. A Real-Time Interference Monitoring Technique for GNSS Based on a Twin Support Vector Machine Method. Sensors 2016, 16, 329.

[85] Radoš, K.; Brkić, M.; Begušić, D. Recent Advances on Jamming and Spoofing Detection in GNSS. Sensors 2024, 24, 4210. https://doi.org/10.3390/s24134210.

[86] K. Radoš, M. Brkić and D. Begušić, "GNSS Signal Classification based on Machine Learning Methods," 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2024, pp. 806-811, doi: 10.1109/MIPRO60963.2024.10569174.

[87] M. Balić, K. Radoš and Z. Blažević, "GNSS Spoofing Attack in Real-time Static and Dynamic Scenarios," 2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2024, pp. 1-6, doi: 10.23919/SoftCOM62040.2024.10721889.

POPIS SKRAĆENICA

AB Adaptive Boosting

AM Amplitude Modulated

AMCS Alternate Master Control Station

ARNS Aeronautical Radio Navigation Service

AWGN Additive White Gaussian Noise

BiLSTM Bidirectional Long Short-Term Memory

BPSK Binary Phase-Shift Keying

C/N0 Carrier-to-Noise-Density Ratio

CDDIS Crustal Dynamics Data Information System

CDMA Code-Division Multiple Access

CI Chirp Interference

CNN Convolutional Neural Network

CNN-CBAM Convolutional Neural Network - Convolutional Block Attention Module

CNN1D 1D Convolutional Neural Network

CNR Carrier-to-Noise Ratio

CRNN Convolutional Recurrent Neural Network

CSNN Convolutional Spiking Neural Network

CW Continuous Wave

CWI Continuous Wave Interference

CWT Continuous Wavelet Transform

DD Double Derivation

DL Deep Learning

DME Distance Measurement Euipment

DT Decision Tree

ETSI European Telecommunications Standards Institute

FDMA Frequency Division Multiple Access

FL Federated Learning

FM Frequency Modulated

GB Gradient Boosting

GCC Galileo Control Center

GCS Ground Control Segment

GLONASS Navigazionnaya Sputnikovaya Sistema

GMS Ground Mission Segment

GNB Gaussian Naive Bayes

GNSS Global Navigation Satellite System

GPS Global Positioning System

GRU Gated Recurrent Unit

IDS Intrusion Detection System

IQ In-phase / Quadrature

IRNSS/NavIC The Indian Regional Navigation Satellite System/Navigation with Indian Constellation

ISO International Organization for Standardization

ITU International Telecommunications Union

JSR Jamming-to-Signal Ratio

KNN k-Nearest Neighbors

LDA Linear Discriminant Analysis

LR Logistic Regression

LSTM Long Short-Term Memory

MCS Master Control Station

MCWI Multi-Continuous Wave Interference

MEO Medium Earth Orbit

MLP Multi-Layer Perceptron

MSE Mean Squared Error

NASA National Aeronautics and Space Administration

NB Narrow Band

NMEA National Marine Electronics Association

NN Neural Network

OAKBAT Oak Ridge Spoofing and Interference Test Battery

PI Pulse Interference

PNT Positioning, Navigation, and Timing

PRN Pseudo-Random Noise

PSO Particle Swarm Optimization

PVT Position, Velocity, and Time

QZSS Quasi-Zenith Satellite System

RF Random Forest

RGB Red, Green, Blue

RINEX Receiver Independent Exchange Format

RNSS The Indian Regional Navigation Satellite System/Navigation with Indian Constellation

RS Restricted Services

SD Single Derivation

SDR Software Defined Radio

SNN Spiking Neural Network

SoI Signal of Interest

SPS Standard Positioning Service

STFT Short-Time Fourier Transform

STL Self-Taught Learning

SVM Support Vector Machine

TEXBAT Texas Spoofing Test Battery

TOA Time of Arrival

TOF Time of Flight

TOT Time of Transmission

TPR True Positive Rate

UAV Unmanned Aerial Vehicle

VGG Visual Geometry Group

POPIS SLIKA

POPIS TABLICA

SAŽETAK

Korištenje sustava za navigaciju i pozicioniranje postalo je svakodnevica u životima ljudi. Zahvaljujući GNSS sustavima i njihovom sve većem razvoju, aplikacije koje nude usluge navigacije i pozicioniranja dovedene su do zavidne razine što se tiče preciznosti. Međutim, sa sve većom dostupnosti i učestalijim korištenjem usluga koje nude GNSS sustavi, dolazi i do nekih negativnih pojava kao što su namjerne interferencije. Napadi ometanjem i lažiranjem najčešće su namjerne interferencije čija pojava može prouzročiti opasne posljedice za korisnike. Stoga je, osim pravovremene detekcije, potrebno klasificirati dolazne interferencije kako bi se iste moglo pravovremeno i učinkovito suzbiti. Ovaj rad donosi detaljan opis napada ometanjem i lažiranjem i različite vrste ovih napada. Dan je pregled dosad razvijenih metoda za klasifikaciju različitih interferencija. Metode strojnog, a posebice metode dubokog učenja, visokim klasifikacijskim rezultatima pokazale su se kao vrlo pouzdan način za klasifikaciju interferencija u GNSS sustavu.

Ključne riječi:

GNSS, napad ometanjem, napad lažiranjem, strojno učenje, duboko učenje, klasifikacija

SUMMARY

The use of navigation and positioning systems has become an everyday part of people's lives. Thanks to the ongoing development of GNSS systems, applications offering navigation and positioning services have achieved impressive levels of precision. However, the increasing availability and frequent use of GNSS-based services have also led to negative phenomena, such as intentional interference. Jamming and spoofing attacks are the most common types of intentional interference, and their occurrence can have dangerous consequences for users. Therefore, in addition to timely detection, it is necessary to classify incoming interference so that it can be mitigated promptly and effectively. This paper provides a detailed description of jamming and spoofing attacks, as well as the various types of such attacks. It presents an overview of existing methods for classifying different types of interference. Machine learning methods, and especially deep learning methods have proven to be highly reliable for classifying interference in GNSS systems, yielding excellent classification results.

Keywords:

GNSS, jamming attack, spoofing attack, machine learning, deep learning, classification