

Vrednotenje ranljivosti sprejemnikov GNSS za napade z motenjem signala

Aljaž Blatnik

Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška cesta 25, 1000 Ljubljana, Slovenija
E-pošta: aljaz.blatnik@fe.uni-lj.si

Povzetek. Satelitska navigacija je temelj sodobnih tehnologij, vse od naprednih avtonomnih vozil do telekomunikacijskih omrežij naslednje generacije. Čedalje večje zanašanje gospodarstva na zanesljivo delovanje globalnih navigacijskih satelitskih sistemov (GNSS) ustvarja ranljivo točko za izvedbo zlonamernega napada z željo po prekinitvi delovanja njihovih sprejemnikov. Napad sam po sebi ni kritičen, če je uporabnik o tem ustrezno obveščen; težava nastane, ko namerna motnja povzroči poslabšanje zanesljivosti ustvarjenih informacij (položaja in časa), ne pa tudi popolne odpovedi navigacijskega sistema. Temu se kljub uporabi najsodobnejših sprejemnikov GNSS ni mogoče povsem izogniti. To delo obravnava kar 400-odstotno letno rast števila namernih napadov GNSS z motnjami, predstavi tehnološke protiukrepe za zmanjševanje njihovih posledic in poda priporočila končnim uporabnikom za gradnjo odpornejših sprejemnikov. Rezultati meritev treh sprejemnikov GNSS v nadzorovanih laboratorijskih pogojih potrjujejo nedeterminističen odziv na motnje, ki ga je mogoče ovrednotiti zgolj z uporabo več merilnih vzorcev v daljšem časovnem obdobju. Prispevek vzpostavlja novo metodologijo za ustrezno sistematično vrednotenje odziva s pomočjo simulacijskega okolja ali dolgotrajnega opazovanja resničnih signalov.

Ključne besede: satelitska navigacija, prenos časa, motenje, sprejemnik GNSS.

Assessing GNSS Receiver Vulnerability to Jamming Attacks

Modern technologies, spanning from sophisticated autonomous vehicles to next-generation telecommunication networks, deeply rely on satellite navigation. Precise positioning and accurate time transfer are not only vital for generating reliable navigation data but also serve as a crucial mechanism for synchronizing decentralized systems.

Our increasing economic reliance on dependable Global Navigation Satellite Systems (GNSS) creates a considerable weakness, making us susceptible to malicious attacks aimed at disrupting receiver operations. While a successful attack might not be inherently dangerous if users are aware of it, the true problem arises when intentional interference subtly alters navigation data. This leads to a gradual decline in the reliability of the provided position and time information, rather than an outright system failure. Even sophisticated GNSS receivers can't fully prevent this manipulation, and such compromised data can result in significant economic losses and, in critical situations, even put lives at risk.

This paper tackles a concerning fourfold (400%) surge in reported GNSS jamming incidents during the second quarter of 2024. It outlines technological countermeasures integrated into modern receivers to lessen the impact and consequences of such attacks. Furthermore, it provides recommendations for end users to enhance the resilience of GNSS-dependent systems. The article details comprehensive measurements conducted under controlled conditions to assess the behavior of three widely used, low-cost GNSS receivers when subjected to

jamming signals. Their response to single-frequency, multi-frequency, and broadband FM-modulated interference was examined and analyzed across six distinct jamming power levels. The findings are visually presented through the temporal evolution of the average code-to-noise ratio, the number of satellites utilized for positioning, and the effect of jamming on location accuracy, observed as the deviation from a known reference point.

The results reveal unpredictable behavior in GNSS receivers, highlighting the need for rigorous statistical analysis. Consequently, the paper proposes a suitable methodological framework for evaluating receiver vulnerability, applicable to measurements obtained in simulated environments or using extended sequences of real-world signals.

Keywords: Satellite navigation, Time synchronization, Jamming, GNSS receiver.

1 UVOD

V osnovi so vsi navigacijski satelitski sistemi delno odporni proti motnjam. Te se navadno pojavijo kot nenamerni signali popačenega delovanja zemeljskih sistemov, najizraziteje pri krmiljenju baznih postaj mobilnih omrežij v nasičenju, kar ustvari vrsto mešalnih produktov, signalov, ki lahko zaidejo v frekvenčni pas, namenjen navigaciji GNSS [1]. Če so signali ozkopasovni, kot rezultat mešanja dveh nosilcev, ali v primeru analognih govornih zvez se motnja pri kodni demodulaciji razširi v naključni šum, s čimer se njen

Prejet: 8. maj, 2025

Odobren: 8. september, 2025



Avtorske pravice: © 2025
Creative Commons Attribution 4.0
International License

vpliv na sprejem navigacijskih signalov močno zmanjša [2]. Domala vsi navigacijski sprejemniki so takšne motnje v svoji arhitekturni zasnovi sposobni v celoti odstraniti. Še več: če signale sprejemajo na več frekvenčnih območjih, je njihova pojavnost za končnega uporabnika tako rekoč nezaznavna [3], [4], [5].

Težava nastane, ko je sprejem podatkov GNSS moten namerno. Izjemno močni motilni signali ali signali, podobni izvorni obliki spektra satelitskih sistemov, niso odpravljeni v celoti in močno poslabšajo razmerje med signalom in šumom v sprejemniku [6], [7]. Učinkovitih protiukrepov z vidika zasnove strojne opreme ni, saj jih je nemogoče ločiti od koristnih signalov, zato so bili napor v zadnjih dveh desetletjih vloženi v izvedbo številnih rešitev digitalnih tehnik. Te se problema lotevajo na različne načine, vse od integracije adaptivnih sit in avtentikacije navigacijskih sporočil do poskusov rekonstrukcije degradiranega spektra z uporabo metod globokega učenja z vprašljivo ponovljivostjo rešitev [6], [8], [9], [10], [11].

Pogosto zmotno prepričanje je, da popoln izpad navigacijskih podatkov in sinhronizacije časa prinese nepopravljive posledice v delovanju krovne sistema, kot sta avtopilot avtonomnega plovila in sinhronizacijski modul decentraliziranega mobilnega omrežja [12]. Navadno, če je uporabnik o motnji ustrezno obveščen, večina sistemov preklopi na nadomestne pomožne storitve, ki manjkajoče podatke zagotavljajo v okrnjenem načinu, s tem pa preprečijo popolno odpoved sistema [13].

Zahrbtnejši primer motenja je nezaznavna degradacija natančnosti lociranja in točnosti sinhronizacije časa, ko programska oprema sprejemnika spremenjenih razmer ne opredeli kot motnjo, ne izvede načrtovanih protiukrepov in o tem ne obvesti končnega uporabnika [11], [14]. Napadalec z namernim prilagajanjem moči in načina motenja učinkovito povzroči povsem nezanesljivo delovanje končnega sistema, kar lahko privede do izpada celotnega omrežja in letališke infrastrukture ter celo do izgube življenj [5], [12], [15].

Skoraj vedno se omenjene razmere pojavijo na obrobju večjih območij namernih motenj, trenutno vojaških konfliktov v vzhodni Evropi in Sredozemlju. Poročilo združenja letalskih prevoznikov in upravljavcev letališke infrastrukture navaja kar 400-odstotno povečanje zaznave namernih motenj na krovih letal v bližini konfliktnih regij v drugi polovici leta 2024, kar v večini primerov povzroči odpoved navigacijskih sistemov plovil [16].

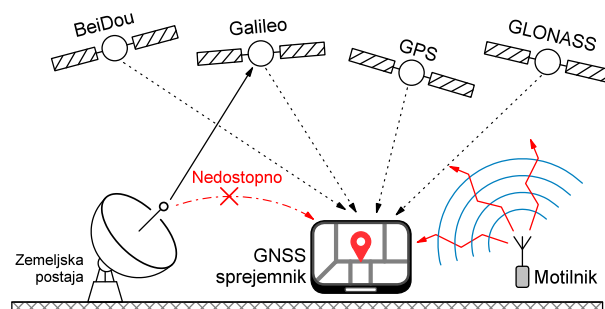
Nenadno zvečanje pogostnosti motenj je zopet spodbudilo številne raziskovalce in njihove skupine k proučevanju vpliva na zanesljivost sprejema in delovanja naprav GNSS v takšnem okolju ter razvoju ustreznih mehanizmov za odpravo posledic. Avtorji tako navajajo razvoj številnih protiukrepov, med katerimi so najpogostejši izvedba adaptivnih sit, rekonstrukcija degradiranega spektra s pomočjo časovnih vrst ter dinamično izločanje značilk z uporabo globokega učenja [17], [18], [19], [20], [21]. Skupna vsem raziskavam je

končna validacija odziva izbranega sprejemnika GNSS z opazovanjem poslabšanja razmerja koda/šum, deviacijo položaja ali številom uporabljenih satelitov za določanje 3D-položaja.

Pri tem raziskovalci pogosto zanemarijo dejstvo, da je določanje položaja s sprejemom navigacijskih signalov v osnovi precej nedeterminističen proces. Tudi v primeru izločanja vseh zunanjih spremenljivk, kot so vplivi ionosfere, razširjanje po večpotju in premikajoča konstelacija satelitov, se sprejemnik na motnjo odzove vsakič drugače [6], [22], [23], [24], [25]. Če želimo torej resnično ovrednotiti vpliv motnje, moramo vzpostaviti metodološko zanesljiv postopek zbiranja podatkov, njihovo statistično obdelavo in ustrezen prikaz. Šele izvajanje dolgotrajnih meritev in naknadna analiza vzorcev lahko vodi do ustvarjanja pravih zaključkov pri navajanju odziva sprejemnikov GNSS na motnje [4], [26].

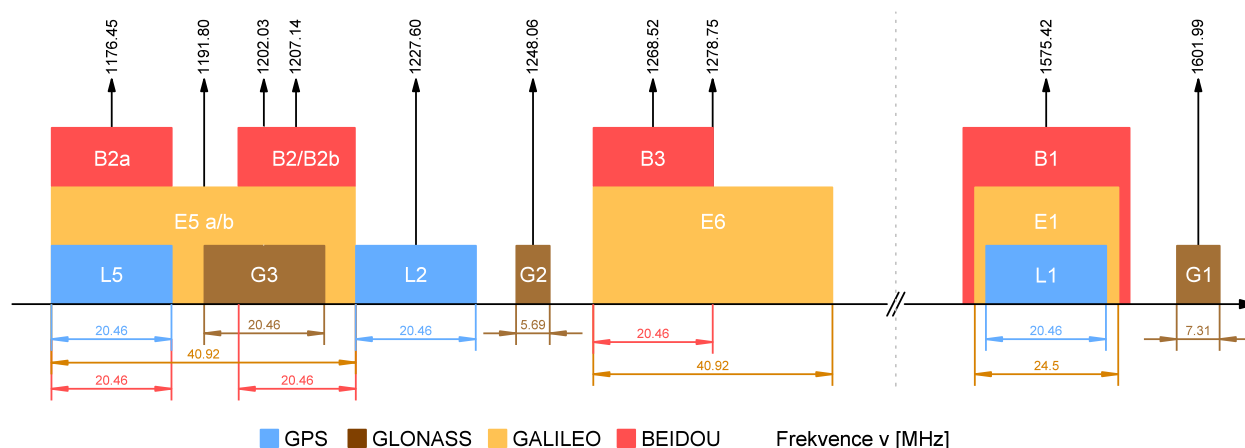
To delo obravnava probleme obstoječih analiz odziva sprejemnikov, predlaga namenski metodološki pristop in demonstrira predlagano rešitev na primeru odziva treh nizkocenovnih sprejemnikov GNSS v prisotnosti motenj. Za analizo je uporabljen večsistemski dvofrekvenčni simulator GNSS z namensko programsko opremo za izvajanje samodejnih meritev odziva, ugotovitve pa se lahko ustrezno prenesejo tudi v resnično okolje. Rezultati kažejo na nujno potrebo po večkratnem ponavljanju meritev v laboratorijskem okolju ali izvajanju dolgotrajnih meritev v resničnih razmerah z uporabo referenčnih sprejemnikov.

2 GNSS-SIGNALI IN MOTNJE



Slika 1: Prikaz avtonomnega sprejemnika GNSS v okolju z motnjami.

Večina sodobnih sprejemnikov GNSS lahko sočasno obdeluje podatke vseh štirih globalnih konstelacij, pri čemer največjo vlogo igrata ameriški GPS in kitajski BeiDou [27]. Drugačen z vidika obdelave signalov je zgolj ruski GLONASS, katerega modernizacija je trenutno nekoliko zastala, zato v tem delu ni posebej obravnavan [28]. Slika 1 prikazuje avtonomni navigacijski sprejemnik brez dostopa do zalednih korekcijskih sistemov, kot sta RTK in A-GNSS. Srednje močan motilec še ne preglasi vseh signalov iz satelitskih



Slika 2: Razdelitev frekvenčnega spektra štirih globalnih navigacijskih satelitskih sistemov s poimenovanjem pasov, kot jih navajajo upravljalci sistemov. Črna puščica označuje nosilno frekvenco signalov, širina stolpca pa uporabljeno pasovno širino.

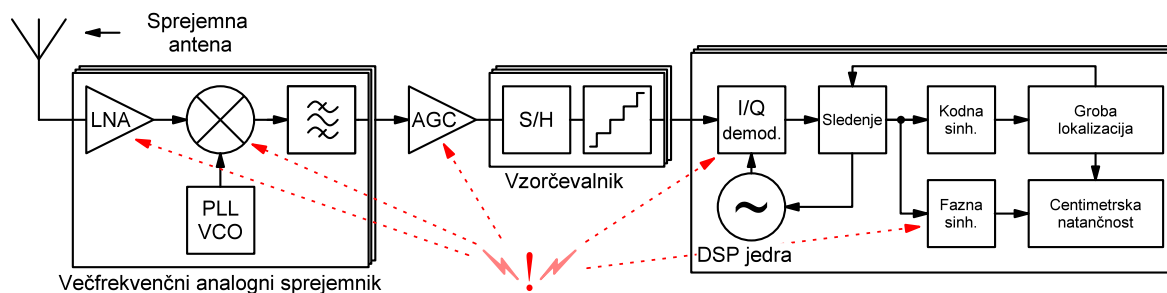
sistemov, zato ne pride do popolnega izpada navigacijskih podatkov oziroma onemogočanja prenosa točnega časa. Če je motnja ozkopasovna, se njena moč pri razširitvi z vnaprej znanim psevdonaključnim razpršilnim zaporedjem (kodni multipleks) razširi na precej večjo pasovno širino, s tem pa se pri sprejemu učinkovito zviša zgolj nivo šuma. Sprejemnik lahko preklopi tudi na uporabo pomožnih frekvenčnih pasov, na primer L2 in L5 v primeru GPS, ki morda niso moteni. Tako že s samo zasnovo arhitekture skoraj v celoti izničimo vpliv motnje [29].

Razmere pa so drugačne, kadar sprejemnik podvržemo širokopasovni motnji, zlasti če pri tem pride do večje korelacije med resničnimi in motilnimi signali [25]. Takrat razširjanje s psevdonaključnim zaporedjem prinese ožjenje motilnega signala, s tem pa izrazito oteževanje pravilnosti sprejema podatkov. Še večjo vlogo ima tu dolžina zaporedja, kjer novejši sistemi z daljšim zaporedjem in večjo pasovno širino navadno izkazujejo boljše lastnosti z vidika imunosti proti motnjam kot njihovi predhodniki [4]. Slika 2 prikazuje frekvenčni načrt sodobnih sistemov GNSS [30]. Označene so nosilne frekvence signalov in zahtevana pasovna širina v MHz (višina stolpcev zgolj omogoča lažji prikaz in ne odraža jakosti signalov). Iz prikaza je razvidno, da evropski sistem Galileo (oranžna barva) uporablja skoraj dvakrat širše frekvenčno področje kot

BeiDou ali GPS. S tem sicer povečuje odpornost proti motnjam, a njegova konstelacija (trenutno) še vedno ni popolna, zato ga večina sprejemnikov obravnava zgolj kot pomožni, in ne primarni sistem.

Opisano rušenje delovanja kodnega multipleksa pa ni edini način motenja sprejemnikov. Slika 3 prikazuje poenostavljeno blokovno shemo sodobnega večsistemskega modula GNSS. Motilni signal pri tem vpliva na delovanje različnih gradnikov sprejemnika, ne zgolj na I/Q-demodulacijsko stopnjo. Precej pogost način motenja je krmiljenje občutljivega ojačevalnika (LNA), ki je tik za sprejemno anteno, v zasičenje [31]. Intermodulacijski produkti popačenja se v mešalniku skupaj z lokalnim oscilatorjem množijo na številne frekvenčne slike, ki kljub samodejnemu zmanjševanju ojačenja s strani sistema AGC (angl. Automatic Gain Control) povsem prekrmlijo vzorčevalnik in s tem zakrijejo koristni signal [2]. Naključna motnja (skakanje po frekvencah) ruši fazno vklepanje sinhronizacijskega vezja in s tem slabšanje točnosti določanja položaja. In nazadnje, hipno spreminjanje načina motenja narekuje preklapljanje med različnimi načini protiukrepov, ki jih izvaja programska oprema sprejemnikov [24].

Navedenih ranljivosti navigacijskih sprejemnikov se njihovi načrtovalci dobro zavedajo, zato v programsko kodo sprejemnika vgrajujejo ustrezne mehanizme, ki s spreminjanjem načina delovanja posameznih segmentov



Slika 3: Poenostavljena blokovna shema sodobnega večfrekvenčnega večsistemskega sprejemnika GNSS. Rdeče puščice označujejo kritične točke napada z motenjem, ki jih kot ključne opredeljuje nedavna literatura.

blokovne verige poskušajo zmanjšati vpliv motnje. Do programske opreme navadno nimamo dostopa, zato natančno ne poznamo vnaprej določenih postopkov odziva. Ravno tako je nemogoče napovedati, kdaj ob pojavu motnje bo protiukrep sprožen, kateri bo izbran in kako močno bo izveden popravek končnega rezultata. To dejstvo številni raziskovalci zanemarijo in ob opisovanju odziva sprejemnikov na motnje navajajo zgolj enkratne, pogosto kratkotrajne meritve, večinoma v naravnem okolju [5], [14], [24], [32], [33]. To delo predstavi drugačen pristop k analizi odziva sprejemnikov pri namernem motenju in z izvedenimi meritvami treh nizkocenovnih sprejemnikov GNSS pokaže smiselnost v takšnem načinu opravljanja raziskav.

3 MERILNI SISTEM IN VREDNOTENJE ODZIVA

3.1 Testna postavitve v naravnem okolju

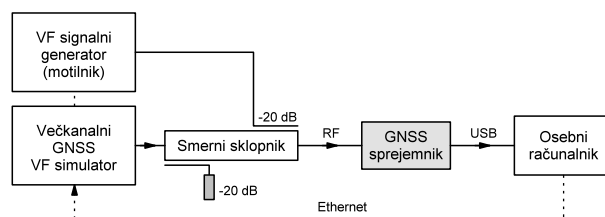
Oceno odziva na motenje sprejemnika GNSS navadno opravimo z analizo informacij, ki jih med delovanjem zagotavlja testna naprava. Najbolj smiselno je, da motilni signal ustvarimo sami, saj imamo tako na voljo vse podatke o njegovi moči, frekvenci in načinu motenja. Skoraj nujno je signal v sprejemno verigo uvesti s smernim sklopnikom, na katerega predhodno povežemo sprejemno anteno. S tem bo sprejemnik prejel združena signala za ojačevalnikom antene, ki ni vgrajena v sam sprejemnik. Preprost uporovni delilnik moči povzroča težave, saj motnjo vrne tudi v napačno smer, torej proti anteni, njeno izsevanje v zrak in sprejem z anteno GNSS pa izraža vprašljivost ponovitve meritev zaradi spreminjajočih se razmer v okolici. Sprejemnik nato poženemo z ugasnjenim motilcem in počakamo vsaj pet minut, da določimo zanesljiv tridimenzijski položaj. Sledi periodično prižiganje in ugašanje motilca ter beleženje sprejetih podatkov, torej odziva.

3.2 Laboratorijsko simulacijsko okolje

Meritve z resničnimi signali v naravnem okolju morajo biti dolgotrajne (večdnevne), če želimo resnično izluščiti zgolj odziv sprejemnika in se izogniti spremembam v konstelaciji satelitov, dinamičnim vplivom ionosfere ter razširjanju signala po večpotju [2]. Delo si precej olajšamo z uporabo namenskega simulatorja GNSS. Ta s pomočjo matematičnega izračuna proizvede zaporedje I/Q-vzorcev, ki jih nato predvaja vektorski signalni generator. Ker lahko iste vzorce predvajamo večkrat, se nam potreben čas za izvedbo ocene odziva sprejemnika drastično zmanjša in za 50 ponovitev traja približno pet ur. Slika 4 prikazuje izvedeno laboratorijsko postavitve, kjer se motilni signal proizvaja z ločenim vektorskim izvorom in je v merilno postavitve povezan s smernim sklopnikom, Slika 5 pa fotografijo fizične postavitve.

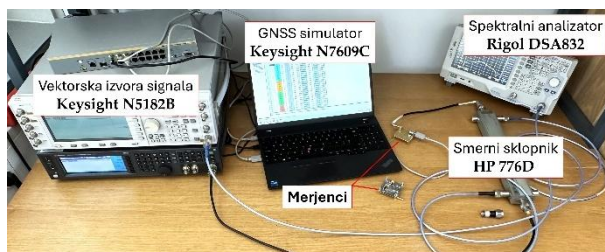
Simulacijska postavitve z vidika sprejemnika ne obstaja. Ta sprejema resnične signale, verodostojno obliko spektra in, če ni priključen na zaledno omrežje za pridobivanje podpornih informacij, lokalni čas, ki ga diktira vnaprej pripravljena simulacija. Pri tem pa sicer

naletimo na težavo ponavljanja meritev. Iste razmere moramo ponovno predvajati, saj želimo izolirati zgolj nepredvidljiv odziv sprejemnika, ne pa tudi spreminjanja preostalih parametrov pri resnični oddaji GNSS. Ob ponovitvi predvajanja konstelacije tako navidezno proizvedemo nedovoljen časovni premik referenčne ure. Tega večina sprejemnikov ne pričakuje, ne znajo se vrniti v preteklost, zato je treba poskrbeti za ustrezno ponastavljanje vseh notranjih pomnilnikov sprejemnega modula in s tem popolnoma izbrisati njegove dosedanje ugotovitve. Navadno zadostujeta že odstranjevanje baterije in proženje ponastavitve sistema z ustreznim ukazom prek komunikacijskega vodila.



Slika 4: Predlagana merilna postavitve laboratorijske izvedbe ocene ranljivosti sprejemnikov GNSS z namensko programsko opremo za samodejen zajem vzorcev.

Za vrednotenje odziva sprejemnikov GNSS na motnje so bili v tem delu izbrani trije testni moduli. Starejši U-blox NEO-6M (6. generacija), najnovejši U-blox MAX-M10 (10. generacija) ter kitajski Ai-Thinker GP-01. Simulirana je bila ena ura statične lokacije na Ljubljanskem gradu 10. junija 2024 ob 12. uri. Vsi trije sprejemniki so bili preizkušeni ločeno. Njihova programska koda je bila najprej ponastavljena, notranji pomnilniki pa izpraznjeni. Simulacija se je začela s tremi minutami predvajanja konstelacije vseh štirih sistemov na frekvenčnem območju L1 (1575,42 MHz) pri zmerni sončevi aktivnosti (zmeren vpliv ionosfere). V tem času so vsi sprejemniki uspešno določili lokacijo in točen čas. Nato se je sprožil zajem podatkov z modula s periodo 1 Hz. Prvih 100 s smo vzorčili referenčno začetno vrednost, sledilo je 100 s motenja z izbrano močjo in načinom motenja, zadnjih 80 s pa se je spremljalo odziv sprejemnika po končanju motilnih razmer. Meritve se za vsak tip motnje ponovijo 50-krat z možnostjo naknadne obdelave podatkov.



Slika 5: Fotografija laboratorijske merilne postavitve.

Preizkušeni so bili trije tipi motenj, ozkopasovna CW-motnja na frekvenci 1575,42 MHz, trifrekvenčna $3 \times$ CW-motnja na $1575,42 \text{ MHz} \pm 735 \text{ kHz}$ ter FM-motnja na isti osrednji frekvenci z 8 MHz globine modulacije in

1 kHz modulačijskim signalom. Podatki so se shranjevali v ločene datoteke, obdelava rezultatov pa je sledila po zaključku vseh meritev.

3.3 Metodologija vrednotenja odziva

Pričakovali bi, da bo vsakokratna meritev razmer med motenjem v laboratorijskih razmerah dala povsem enoznačen rezultat, saj uporabljamo popolnoma enake zunanje signale z vidika sistemov GNSS in motilca. Poskusi pa so pokazali, da ni tako, zato je meritve treba ponavljati, rezultate pa povprečiti.

V dosegljivi literaturi raziskovalci kot oceno motenja sprejemnikov GNSS največkrat navajajo razmerje C/N_0 v decibelih in število uporabljenih satelitov za določanje položaja [27]. Število uporabljenih satelitov za izračun položaja se ves čas spreminja, saj se programska oprema odloča za izbiro najboljših z vidika lokacije opazovalca, moči sprejema in doprinosa k variabilnosti končnega rezultata. Zmanjševanje števila uporabljenih satelitov kaže na zahtevnejše razmere, delno zasenčenje antene, urbane kanjone oziroma zunanje motnje. Še boljši pokazatelj je spreminjanje razmerja C/N_0 , ki opisuje moč signala po oženju s psevdonaključnim zaporedjem in šumnim nivojem. Ker motnja navadno vpliva na nivo šuma, ki ga zazna sprejemnik, podatek pa prejmemo za vsak sprejet satelit posebej, je to eden izmed prvih pokazateljev prisotnosti motnje.

Oceno obnašanja sprejemnika je najbolje izvesti z grafičnim prikazom v obliki časovne vrste. Ker gre za veliko količino podatkov (veliko število satelitov) in več ponovitev je smiselno podatke povprečiti in jih opisati s srednjo vrednostjo. Dober vpogled v dogajanje nudi tudi izračun standardnega odklona, ki opisuje variabilnost vzorcev. Večji standardni odklon nakazuje manj deterministične razmere, kar je ključen podatek pri napovedovanju vpliva motnje ali razvoju ustreznih protiučrepov za zmanjševanje njihovih vplivov.

Na primeru izračuna povprečne vrednosti in standardnega odklona vrednosti C/N_0 , lahko problem ustrezno matematično formuliramo:

3.3.1 Surovi vzorci SNR

Predpostavimo, da imamo za vsako ponovitev meritev GNSS N časovnih vzorcev. V vsaki točki časa t_i ($i = 1, 2, \dots, N$) opazujemo vrednosti C/N_0 vidnih satelitov različnih konstelacij GNSS (GPS, Galileo, BeiDou, GLONASS, QZSS). Naj bo $C/N_{0,j,k}(t_i)$ vrednost razmerja koda/šum k -tega satelita, j -te konstelacije v času t_i . Število vidnih satelitov in konstelacij se lahko seveda ves čas spreminja.

3.3.2 Povprečna vrednost C/N_0 v času t_i

Za vsak časovni vzorec t_i unikatne ponovitve meritev, je treba najprej izračunati povprečno vrednost razmerja C/N_0 vseh satelitov in konstelacij. Če je $M(t_i)$ število vseh poznanih vrednosti C/N_0 v času t_i , lahko zapišemo

$$\overline{C/N_0}(t_i) = \frac{\sum_{j \in \{GPS, Galileo, \dots\}} \sum_{k=1}^{K_j(t_i)} C/N_{0,j,k}(t_i)}{M(t_i)}, \quad (1)$$

kjer $K_j(t_i)$ predstavlja število vidnih satelitov v j -ti konstelaciji v času t_i in

$$M(t_i) = \sum_j K_j(t_i). \quad (2)$$

Če v konstelaciji ne vidimo nobenega satelita, privzamemo, da $C/N_0(t_i)$ zanj ne obstaja.

3.3.3 Srednja vrednost in standardni odklon C/N_0

Za niz N vzorcev ene meritve dobimo časovno vrsto sredinskih vrednosti $\overline{C/N_0}$ kot

$$\{\overline{C/N_0}(t_1), \overline{C/N_0}(t_2), \dots, \overline{C/N_0}(t_N)\}. \quad (3)$$

Za prikaz na grafu moramo v povprečje zajeti še vse ponovitve meritev L . Sredinsko vrednost časovne točke (v primeru simulacije, ko predvajamo enake vzorce spektra) izračunamo z

$$\mu_{i,l} = \frac{1}{L} \sum_{l=1}^L \overline{C/N_0}(t_i)_l, \quad (4)$$

kjer l označuje posamezno ponovitev meritve, i pa časovno točko vzorca. Opletanje vzorcev na grafu časovne vrste prikažemo kot osenčeno področje širine standardne deviacije

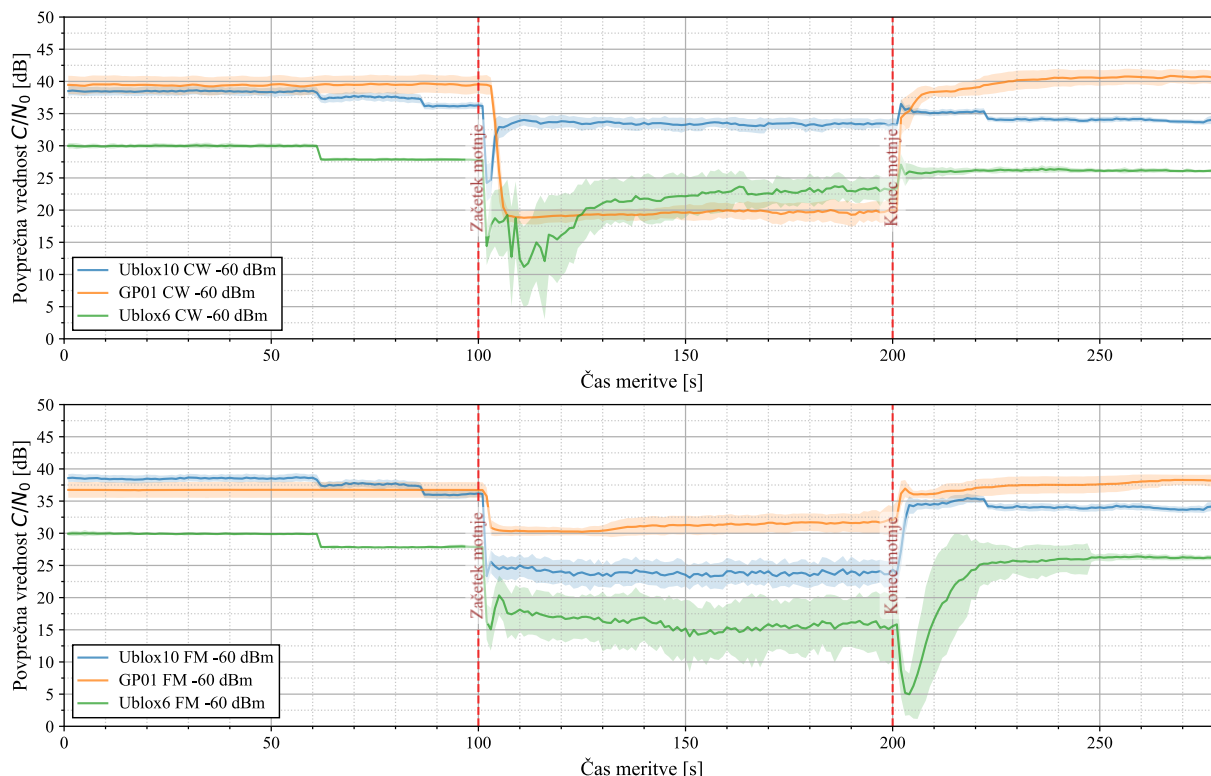
$$\sigma_{i,l} = \sqrt{\frac{1}{L-1} \sum_{l=1}^L (\overline{C/N_0}(t_i) - \mu_{i,l})^2}, \quad (5)$$

pri čemer je i časovna točka vzorcev in l posamezna ponovitev meritve. V našem primeru je $L = 50$.

Formulacija velja podobno za izračune pri vrednotenju števila uporabljenih satelitov, le da nam tokrat ni treba povprečiti vrednosti posamezne točke v ponovitvah meritev. Metodo lahko prenesemo tudi na opazovanja zunaj laboratorijske izvedbe. Pri tem si vzorci sledijo zaporedoma, izmenično z intervali motenj in brez njih. Preliminarni poskusi med pripravo tega dela kažejo, da je treba z vpeljavo vsake nove spremenljivke (ionosfera, spreminjanje konstelacije, urbani kanjoni) čas meritve povečati za 50-krat, kar hitro prinese večtedenska opazovanja.

4 REZULTATI

Med izvajanjem laboratorijskih meritev je bil izdelan obsežen nabor podatkov, sledeči rezultati pa prikazujejo zanimivejše pojave, ki jih je mogoče s predlagano metodologijo opaziti pri izrisu časovnega poteka parametrov. Postopek izvajanja meritev striktno sledi načrtu, opisanem v poglavju 3.2. GNSS-moduli podatke sporočajo v obliki nabora NMEA-stavkov, iz katerih



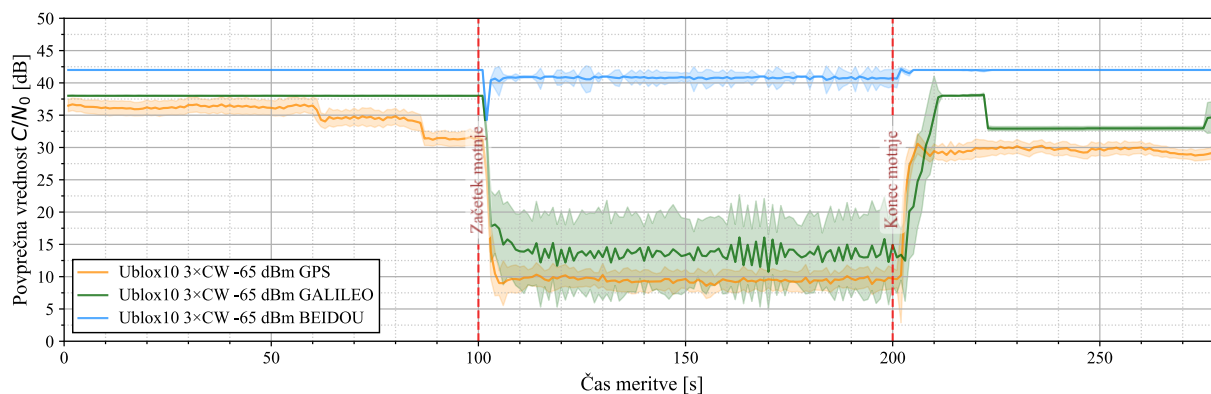
Slika 6: Primerjava odziva treh testnih sprejemnikov po pojavu ozkopasovne (CW) frekvenčne motnje z močjo -60 dBm (zgoraj) in širokopasovne (FM) motnje z enako močjo (spodaj). Začetek in konec motnje je označen z navpično črtkano črto. Debela črta označuje srednjo vrednost, širina osenčenega dela pa standardni odklon.

naknadno izluščimo informacijo o položaju, času, razmerju C/N_0 in številu uporabljenih satelitov ter vrsto drugih informacij, ki v tem delu niso prikazane. Skladno z enačbama (4) in (5) so bile posamezne časovne točke ponovljenih vzorcev matematično obdelane in prikazane v odvisnosti od časa meritve na graf. Polna črta pri vseh grafih predstavlja srednjo vrednost rezultatov, osenčeno področje okoli nje pa standardni odklon vzorcev.

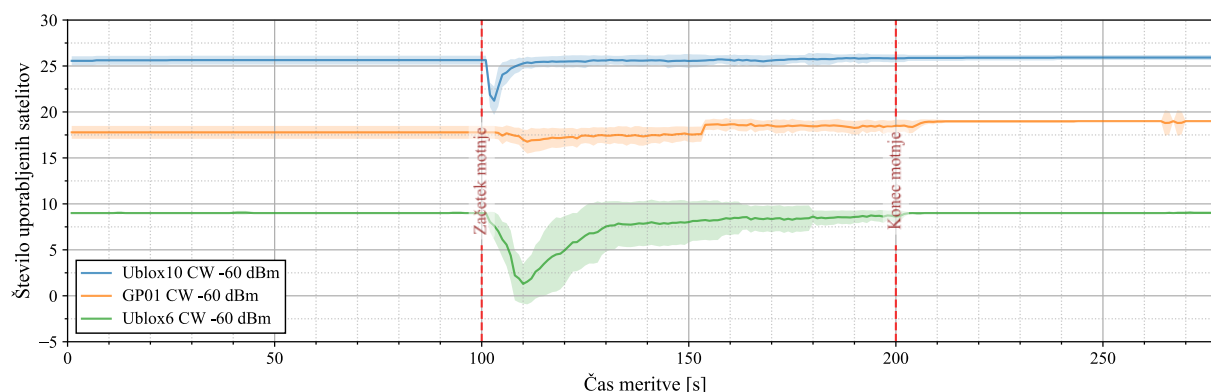
Slika 6 prikazuje odziv testnih modulov na isti tip in moč motnje, s čimer lahko neposredno primerjamo njihovo obnašanje v enakih razmerah. Povsem jasno se vidi, da ozkopasovna motnja (zgornji graf) ne pomeni večje težave za najnovejša sprejemnika, kot je Ublox10, medtem ko starejši sprejemniki (Ublox6) le s težavo

odpravljajo posledice motenj, precej večja je tudi variabilnost razmerja C/N_0 , saj programska koda poskuša najti neustreznejši protiukrep za izničenje vpliva. Drugačen vzorec vidimo pri širokopasovni motnji (spodnji graf). Vsem sprejemnikom razmerje degradira, pričakovano ponovno najstarejšim generacijam. Pri teh se razmere po koncu motenja za kratek čas celo poslabšajo, in to precej bolj drastično kot med samo motnjo. To kaže na počasen odziv mehanizmov odpravljanja motnje, ki se novim razmeram ne znajo dovolj hitro prilagoditi, s tem pa si celo škodujejo.

Slika 7 prikazuje dovzetnost različnih navigacijskih sistemov za enak tip motnje znotraj istega sprejemnika, v tem primeru novejšega Ublox10. Za tri-frekvenčno



Slika 7: Primerjava vpliva tri frekvenčne motnje na U-blox MAX-M10 sprejemnik glede na izbran sistem (GPS, Galileo, BeiDou) z vidika opazovanja povprečne vrednosti C/N_0 .



Slika 8: Primerjava odziva treh testnih sprejemnikov ob pojavu ozkopasovne motnje z opazovanjem spremembe števila uporabljenih satelitov za določanje položaja.

motnjo (skakanje ozkopasovnega motilca med tremi frekvencami) najbolj drastičen vpliv izmerimo pri sprejemu signalov GPS. Kitajski BeiDou zaradi drugačne oblike spektra moduliranega signala (spektralna gostota moči je na drugih frekvencah kot v primeru GPS in Galileo) motnje pravzaprav sploh ne občuti. Sprejemnik je tako sposoben preklopiti s sistema GPS ali Galileo na uporabo konstelacije BeiDou ter nemoteno zagotavljati lokacijske in časovne informacije uporabniku. Večsistemski sprejemniki (Ublox10, GP-01) so tako pri delovanju v okolju z motnjami precej zanesljivejši kot njihovi enosistemski predhodniki (Ublox6).

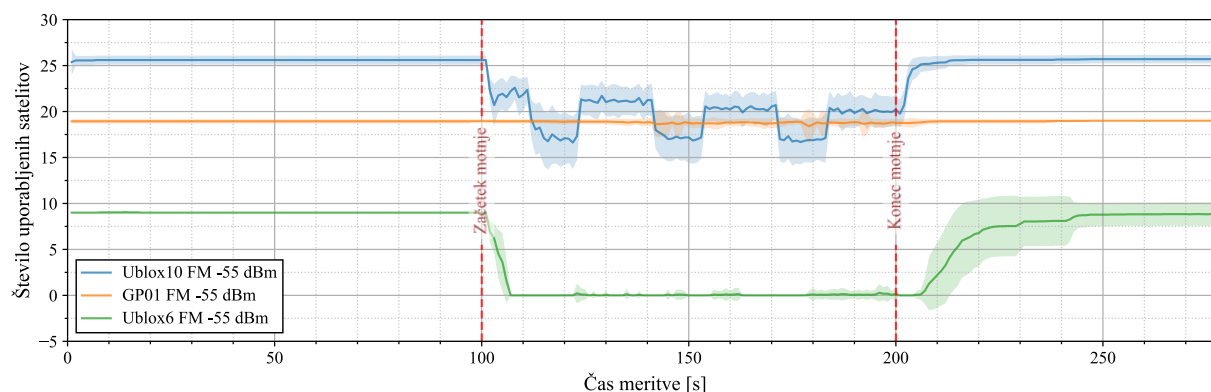
Slika 8 prikaže pogled na problem z drugega zornega kota, s številom satelitov, ki jih sprejemnik uporablja za izračun položaja. Ta se lahko odloči, kateri izmed njih so najzanesljivejši za izračun, torej kateri signali niso toliko popačeni, da uporaba njihovih informacij ni več smiselna. Nad tem bdi programska oprema, odziv pa je jasno viden pri sprejemniku Ublox6, kjer se ob pojavu motnje sprejemnik najprej odloči za odstranitev večine satelitov, ki jih nato počasi nadomesti z novimi, ali pa v izračun celo vrne prvotne. Po dobrih 80 sekundah se vrnemo v razmere, podobne tistim pred začetkom motenja, modul se je torej spremenjenim razmeram uspešno prilagodil.

Nazadnje Slika 9 prikazuje zanimiv pojav s širokopasovnim motenjem vseh treh modulov. Za Ublox6 so razmere pretežke, pride do popolne odpovedi sprejema. GP-01 motnje zares sploh ne občuti, struktura sprejemnika jo že predhodno uspešno izlušči. Ublox10 se znajde v dilemi, kaj zares storiti. Preklaplja med različnimi možnostmi protiukrepov (ali zgolj dvema) in zaradi precejšnje variabilnosti razmer (osenčeno področje odklona) mu ne uspe izbrati končne odločitve.

5 DISKUSIJA

Zgolj z opazovanjem ene same izvedbe meritev vzorcev, prikazanih v poglavju 4, ni mogoče prepoznati. Obstoječe raziskave [4], [14], [24], [25] rezultate vpliva bodisi skrijejo v grafih, polnih krivulj, ali pa prikažejo razmere za eno samo ponovitev, iz katere ni mogoče razbrati nepredvidljivega značaja sprejemnika, kar jasno ilustrira Slika 7. Po drugi strani takšna izvedba zahteva uporabo namenskega simulacijskega orodja in kljub laboratorijskemu okolju traja več ur, da pridobimo zadostno količino podatkov (za samo en tip motnje in eno moč). Če želimo oceno ranljivosti izvesti pri različnem naboru motilcev in razdaljah do sprejemnika (sprememba moči), se meritve hitro zavlečejo v več mesecev.

Izzivi postanejo še večji, ko želimo takšna opazovanja prenesti v resnično okolje oziroma nimamo dostopa do



Slika 9: Vpliv širokopasovne (FM) motnje na testne sprejemnike. Na sliki je viden pulzirajoči pojav spreminjanja števila uporabljenih satelitov U-blox MAX-M10-modula, kar kaže na preklapljanje programske opreme med različnimi mehanizmi odziva na spremenjene razmere (naključna modulacija motnje se občasno korelira z resničnimi signali).

simulatorja. Takrat je treba zaradi dodajanja novega nabora spremenljivk (konstelacije ne moremo preprosto ponovno predvajati) ustrezno povečati čas meritve, kar še podaljša trajanje raziskave. V tem primeru je k problemu smiselno pristopiti na drugačen način. Sprva zgolj grobo ocenimo odziv sprejemnika na motnjo in določimo tiste razmere, kjer že v krajšem času meritve pridobimo skrajno vrednost rezultatov, torej primer, ki ga z zeleno krivuljo prikazuje Slika 9. Nato z dolgotrajno meritvijo opazujemo zgolj slučaje, kjer prihaja do največjih dinamičnih razmer opazovanih parametrov (največjega standardnega odklona pri ponovitvi meritev). Pri tem moramo še vedno uporabljati zunanji vir motnje, nad katerim imamo popoln nadzor, in seveda zagotoviti, da v bližini merilnega območja ni preostalih namernih ali nenamernih motilnih izvorov. S tem čas zbiranja podatkov skrajšamo na nekaj tednov, naknadna matematična analiza pa nas pripelje do podobnih zaključkov kot pri laboratorijski izvedbi.

6 ZAKLJUČEK

Predstavljena metodologija je korak k bolj sistematičnemu pristopu ocenjevanja vpliva motnje na zanesljivost sprejema GNSS. Tega ni mogoče izvesti zgolj z enkratnim opazovanjem pojava, saj s tem zanemarimo dinamično območje opazovanih parametrov, ki kljub enakim razmeram zaradi odziva programske opreme sprejemnika ne bo povsem predvidljivo. Postopek je deloma zahteven (potrebuje namensko merilno postavitve, vsaj smerni sklopnik), predvsem pa dolgotrajen. Vendar s tem zagotovimo resnično ponovljivost rezultatov. S predstavljenimi metodo pridemo do enakih zaključkov, enakih časovnih odzivov opazovanih parametrov.

Druga ključna ugotovitev tega dela je način izogibanja izpadom delovanja sprejemnikov GNSS v razmerah z namernim motenjem. Temu se najuspešneje zoperstavimo z uporabo sodobnih modulov GNSS, ki naj obvezno podpirajo večsistemski sprejem, še bolj pa večfrekvenčni, saj je širokopasovno motnjo v celotnem spektru, dodeljenem signalom GNSS, tehnično precej težje oziroma dražje izvesti. Rezultati raziskave v okviru nastajanja tega dela so pokazali, da se povsem zanesljivo obnašajo tudi nekoliko nepoznani oziroma nepriznani sprejemniki, kot je AiThinker GP-01. Seveda je treba poudariti, da visokonamenski sprejemniki GNSS, namenjeni kritičnim aplikacijam, kot sta geodezija in avtonomna vožnja, uporabljajo vrsto drugih protiukrepov za zmanjševanje vpliva motenj, od posebnih antenskih struktur do naprednejše digitalne obdelave signalov ter več vzporednih sprejemnih verig z možnostjo adaptivnega prilagajanja razmeram. Takšni sprejemniki so navadno nekoliko zahtevnejši za prenos v laboratorijske razmere, saj so hermetično zaprti in nimajo fizičnega dostopa do antenskega priključka, kar narekuje delno poškodbo končne naprave. Delo se namenoma posveča nizkocenovnim izvedbam, saj večina današnjih

aplikacij, ki se zanaša na informacije sistemov GNSS, uporablja takšne (zgoraj predstavljene) module.

Nadaljnje raziskovalno delo poteka v smeri izdelave avtonomnega sistema za dolgotrajno zbiranje podatkov, z možnostjo zlivanja v osrednji informacijski sistem, ter sprotno obdelavo in opozarjanje na namerne motnje širšega področja države.

ZAHVALA

Raziskava je bila sofinancirana iz sredstev Javne agencije za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije v okviru projektov V2-2342 in L7-60164.

LITERATURA

- [1] A. Al-Jumaily *idr.*, „Evaluation of 5G Coexistence and Interference Signals in the C-Band Satellite Earth Station“, *IEEE Trans. Veh. Technol.*, let. 71, št. 6, str. 6189–6200, jun. 2022, doi: 10.1109/TVT.2022.3158344.
- [2] T. Pany, *Navigation signal processing for GNSS software receivers*. v Artech House GNSS technology and applications series. Boston London: Artech House, 2010.
- [3] F. Dimc, M. Bažec, D. Borio, C. Gioia, G. Baldini, in M. Basso, „An Experimental Evaluation of Low-Cost GNSS Jamming Sensors: Evaluation of Low-Cost GNSS Jamming Sensors“, *Navigation*, let. 64, št. 1, str. 93–109, mar. 2017, doi: 10.1002/navi.184.
- [4] M. Ding, W. Chen, in W. Ding, „Performance analysis of a normal GNSS receiver model under different types of jamming signals“, *Measurement*, let. 214, str. 112786, jun. 2023, doi: 10.1016/j.measurement.2023.112786.
- [5] R. Ziebold, D. Medina, M. Romanovas, C. Lass, in S. Gewies, „Performance Characterization of GNSS/IMU/DVL Integration under Real Maritime Jamming Conditions“, *Sensors*, let. 18, št. 9, str. 2954, sep. 2018, doi: 10.3390/s18092954.
- [6] D. Borio, C. O'Driscoll, in J. Fortuny, „GNSS Jammers: Effects and countermeasures“, v *2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing*, Noordwijk, Netherlands: IEEE, dec. 2012, str. 1–7. doi: 10.1109/NAVITEC.2012.6423048.
- [7] P. Craven, R. Wong, N. Fedora, in P. Crampton, „Studying the Effects of Interference on GNSS Signals“, v *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation*, San Diego, California, jan. 2013.
- [8] X. Chen, R. Luo, T. Liu, H. Yuan, in H. Wu, „Satellite Navigation Signal Authentication in GNSS: A Survey on Technology Evolution, Status, and Perspective for BDS“, *Remote Sens.*, let. 15, št. 5, str. 1462, mar. 2023, doi: 10.3390/rs15051462.
- [9] A. Ghanbarzade in H. Soleimani, „GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning“, 4. januar 2025, *arXiv*: arXiv:2501.02352. doi: 10.48550/arXiv.2501.02352.
- [10] H. Elghamrawy, M. Karaim, M. Korenberg, in A. Noureldin, „High-Resolution Spectral Estimation for Continuous Wave Jamming Mitigation of GNSS Signals in Autonomous Vehicles“, *IEEE Trans. Intell. Transp. Syst.*, let. 23, št. 7, str. 7881–7895, jul. 2022, doi: 10.1109/TITS.2021.3074102.
- [11] V. Tripathi in S. Caizzzone, „Virtual Validation of In-Flight GNSS Signal Reception during Jamming for Aeronautics Applications“, *Aerospace*, let. 11, št. 3, str. 204, mar. 2024, doi: 10.3390/aerospace11030204.
- [12] Andrej Novak, Alena Novak Sedlackova, Anna Stelmach, in Doris Novak, „Safety Implications of GNSS Signal Interference at Zilina Airport“, *Commun. - Sci. Lett. Univ.*

- Zilina, let. 22, št. 3, str. 40–48, jul. 2020, doi: 10.26552/com.C.2020.2.40-48.
- [13] O. Sharifi-Tehrani in M. H. Ghasemi, „A Review on GNSS-Threat Detection and Mitigation Techniques“, *Cloud Comput. Data Sci.*, str. 1–25, okt. 2022, doi: 10.37256/ccds.4320231678.
- [14] H. Elghamrawy, M. Karaim, M. Tamazin, in A. Nouredin, „Experimental Evaluation of the Impact of Different Types of Jamming Signals on Commercial GNSS Receivers“, *Appl. Sci.*, let. 10, št. 12, str. 4240, jun. 2020, doi: 10.3390/app10124240.
- [15] B. Figueet, M. Waltert, M. Felux, in X. Olive, „GNSS Jamming and Its Effect on Air Traffic in Eastern Europe“, v *The 10th OpenSky Symposium*, MDPI, dec. 2022, str. 12. doi: 10.3390/engproc2022028012.
- [16] GPS Spoofing WorkGroup, „GNSS Spoofing - Final Report of the GPS Spoofing Workgroup“. OPS Group, 6. september 2024. [Na spletu]. Dostopno na: <https://ops.group/dashboard/wp-content/uploads/2024/09/GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24.pdf>
- [17] Y. Hao, C. Shi, A. Xu, X. Sui, in M. Xia, „Revealing Methods of GNSS Spoofing Mitigation Through Analyzing the Spoofing Impacts on Adaptively Robust Estimation-Based RTK/INS Tightly Coupled Integration“, *IEEE Sens. J.*, let. 23, št. 20, str. 25165–25178, okt. 2023, doi: 10.1109/JSEN.2023.3303199.
- [18] X. Shang, F. Sun, B. Liu, L. Zhang, in J. Cui, „GNSS Spoofing Mitigation with a Multicorrelator Estimator in the Tightly Coupled INS/GNSS Integration“, *IEEE Trans. Instrum. Meas.*, str. 1–1, 2022, doi: 10.1109/TIM.2022.3232668.
- [19] J. Zhou, W. Wang, X. Hong, in C. Zhang, „Multi-UAV Cooperative Anti-Jamming for GNSS Signals Based on Frequency-Domain Power Inversion“, *IEEE Sens. J.*, let. 24, št. 19, str. 30778–30791, okt. 2024, doi: 10.1109/JSEN.2024.3437643.
- [20] D. Zmysłowski, M. Kryk, in J. Kelner, „Testing GNSS Receiver Robustness for Jamming“, *Aviat. Secur. Issues*, let. 4, št. 2, str. 139–155, dec. 2023, doi: 10.55676/asi.v4i2.64.
- [21] I. Iudice, D. Pascarella, G. Corrado, in G. Cuciniello, „A real/fast-time simulator for impact assessment of spoofing & jamming attacks on GNSS receivers“, v *2024 11th International Workshop on Metrology for AeroSpace (MetroAeroSpace)*, jun. 2024, str. 309–314. doi: 10.1109/MetroAeroSpace61015.2024.10591529.
- [22] Y.-W. Lee, Y.-C. Suh, in R. Shibasaki, „A simulation system for GNSS multipath mitigation using spatial statistical methods“, *Comput. Geosci.*, let. 34, št. 11, str. 1597–1609, nov. 2008, doi: 10.1016/j.cageo.2008.01.004.
- [23] J. Jakobsen, A. B. O. Jensen, in A. A. Nielsen, „Simulation of GNSS reflected signals and estimation of position accuracy in GNSS-challenged environment“, *J. Geod. Sci.*, let. 5, št. 1, maj 2015, doi: 10.1515/jogs-2015-0006.
- [24] D. Borio, F. Dovis, H. Kuusniemi, in L. Lo Presti, „Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers“, *Proc. IEEE*, let. 104, št. 6, str. 1233–1245, jun. 2016, doi: 10.1109/JPROC.2016.2543266.
- [25] T. Morong, P. Puričar, in P. Kovář, „Study of the GNSS Jamming in Real Environment“, *Int. J. Electron. Telecommun.*, str. 65–70, jan. 2019, doi: 10.24425/ijet.2019.126284.
- [26] K. Radoš, M. Brkić, in D. Begušić, „Recent Advances on Jamming and Spoofing Detection in GNSS“, *Sensors*, let. 24, št. 13, str. 4210, jun. 2024, doi: 10.3390/s24134210.
- [27] S. Gunawardena in Y. T. J. Morton, „Fundamentals and Overview of GNSS Receivers“, v *Position, Navigation, and Timing Technologies in the 21st Century*, 1. izd., Y. T. J. Morton, F. Diggelen, J. J. Spilker, B. W. Parkinson, S. Lo, in G. Gao, Ur., Wiley, 2020, str. 307–338. doi: 10.1002/9781119458449.ch14.
- [28] S. Thøelert, P. Steigenberger, in O. Montenbruck, „GLONASS-K2 signal analysis“, *GPS Solut.*, let. 28, št. 3, str. 141, jul. 2024, doi: 10.1007/s10291-024-01681-z.
- [29] Senhaji. M. Issam, A. Adnane, in A. Madiabdessalam, „Anti-Jamming techniques for aviation GNSS-based navigation systems: Survey“, v *2020 IEEE 2nd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS)*, Kenitra, Morocco: IEEE, dec. 2020, str. 1–4. doi: 10.1109/ICECOCS50124.2020.9314449.
- [30] C. J. Hegarty, „GNSS signals — An overview“, v *2012 IEEE International Frequency Control Symposium Proceedings*, Baltimore, MD, USA: IEEE, maj 2012, str. 1–7. doi: 10.1109/FCS.2012.6243707.
- [31] J. J. H. Wang, „Antennas for Global Navigation Satellite System (GNSS)“, *Proc. IEEE*, let. 100, št. 7, str. 2349–2355, jul. 2012, doi: 10.1109/JPROC.2011.2179630.
- [32] A. Minetto, B. D. Polidori, M. Pini, in F. Dovis, „Investigation on the Actual Robustness of GNSS-based Timing Distribution Under Meaconing and Spoofing Interferences“, predstavljeno na 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022), Denver, Colorado, okt. 2022, str. 3848–3862. doi: 10.33012/2022.18569.
- [33] V. Hamza, B. Stopar, O. Sterle, in P. Pavlovčič-Prešeren, „Recent advances and applications of low-cost GNSS receivers: a review“, *GPS Solut.*, let. 29, št. 1, str. 56, jan. 2025, doi: 10.1007/s10291-025-01815-x.

Aljaž Blatnik je leta 2023 doktoriral na Fakulteti za elektrotehniko Univerze v Ljubljani na temo zasnove in izvedbe visokofrekvenčnih merilnih instrumentov. Od leta 2017 je zaposlen na Fakulteti za elektrotehniko, kjer izvaja pedagoško delo s področja sevanja, razširjanja valov, visokofrekvenčne tehnike in satelitskih komunikacij. Raziskovalno je aktiven na področju vrednotenja delovanja visokofrekvenčnih gradnikov, navigacijskih sistemov in radarske tehnike.