Vidulin, M., Polovina, M., Grgić, M. (2013): Razvoj i primjena uređaja za ometanje signala GNSS satelita
Ekscentar, br. 16, pp. 76-80

Mauricio Vidulin ‣ preddiplomski studij, Geodetski fakultet Zagreb, Kačićeva 26, 10000 Zagreb, e-mail: mauricio.vidulin@geof.hr
Marko Polovina ‣ preddiplomski studij, Geodetski fakultet Zagreb, Kačićeva 26, 10000 Zagreb, e-mail: marko.polovina@geof.hr
Marijan Grgić, mag. ing. geod. et geoinf. ‣ Zavod za geomatiku, Geodetski fakultet Zagreb, Kačićeva 26, 10000 Zagreb, e-mail: mgrgic@geof.hr

Razvoj i primjena uređaja za ometanje signala GNSS satelita

SAŽETAK: *Uz razvoj tehnologija pozicioniranja putem globalnih navigacijskih satelitskih sustava (GNSS), razvijale su se i tehnologije ometanja prijema signala odaslanih sa satelita. Tako su nastali ometači (eng. jammer) GNSS signala – radio-frekvencijski odašiljači dizajnirani tako da blokiranjem, prigušivanjem ili drugim načinima ometanja signala djelomično ili u potpunosti onemogućavaju određivanje položaja u prostoru. Iako je u velikom dijelu svijeta ometanje radijskih signala ilegalno, korištenje ometača sve je češće u civilnim i vojnim djelatnostima. U ovom radu prikazana je teorijska osnova tehnologija za ometanje signala te primjena jednostavnog uređaja kratkog dometa za ometanje signala GPS (Global Positioning System) satelita na više različitih GPS prijamnika. Dobiveni rezultati međusobno su uspoređeni te analizirani.*

KLJUČNE RIJEČI: *ometanje GNSS signala, GPS ometač, pozicioniranje, zaštita od ometanja signala, sustavi za detekciju ometanja*

Development and application of devices for GNSS signal jamming

SUMMARY: *Besides the development of the positioning technologies that use the Global Navigation Satellite Systems (GNSS), the GNSS jamming technologies were developed. Thus, the GNSS signal jammers were invented - RF transmitters designed to block, reduce or otherwise interfere signals and partially or completely disable GNSS positioning. Although, in many countries around the world RF jamming is illegal, the use of the jamming devices is not very rare in the civilian and military activities. This paper presents the theoretical basis of the signal jamming technology and the application of the simple short range GPS (Global Positioning System) jammer on several different GPS receivers. The results were compared and analyzed.*

KEYWORDS: *GNSS jamming, GPS jammer, Positioning, Anti-jam technologies, Jamming detection systems*

1. UVOD

Globalni navigacijski satelitski sustavi (*Global Navigation Satellite System* - GNSS) nalaze primjenu u vojnim i civilnim djelatnostima za precizno pozicioniranje, navigaciju, određivanje oblika Zemlje, ali i praćenje, kontrolu, nadzor i zaštitu objekata, pojedinaca i dr. (Zhao i dr., 2012). Uz dobronamjerne ciljeve korištenja tih sustava, vrlo je često njihovom upotrebom ugrožena privatnost pojedinca, a sve češći su i slučajevi pokušaja preuzimanja kontrole nad prijamnicima GNSS signala. Tako se može ustvrditi da razvoj GNSS-a prati i razvoj tehnologija za njegovo ometanje. Praktični rezultat tog razvoja su ometači (*eng. jammer*) i drugi uređaji koji su sposobni emitirati sustavima slične signale koje GNSS prijamnici interpretiraju i obrađuju na sličan način kao i izvorne signale. GNSS ometači signala su radio-frekvencijski odašiljači koji blokiraju, prigušuju ili na drugi način ometaju GNSS signale, najčešće odašiljanjem radiofrekvencijskih valova koji ometaju stvarne signale te sprječavaju uspostavljanje ili kontinuirano opažanje signala u prijamnicima GNSS uređaja (URL-1).

Ometanje prijamnika globalnih sustava za pozicioniranje danas je moguće čak i na udaljenostima do 100 kilometara od izvora ometanja pri izlaznoj snazi od samo 1 W (Mukhopadhyay i dr., 2007). Sateliti sustava emitiraju signale izlaznom snagom od otprilike 30 W, 20200 kilometara iznad površine Zemlje (Thiel i Ammann, 2009), a kako je udaljenost koju signal mora prijeći razmjerno velika ti signali značajno oslabe i nije ih teško nadjačati (Hendricks, 2011). Svi uređaji koji rade na istim ili sličnim frekvencijama kao i GNSS odašiljači mogu biti prigušivači signala. Tako se ometanje prijema signala događa i zbog polja zračenja visokog intenziteta radara, povezanih radijskih odašiljača, izvora zračenja ultra-širokih pojasa (*eng. ultra-wide band*), odaslanih mikrovalova visoke snage i dr. (Hendricks, 2011).

Kako bi se zaštitio GNSS signal, razvijene su metode detekcije ometača GNSS-a (najčešće Globalnog pozicijskog sustava - *eng. Global Positioning System* - GPS) u obliku regionalnih mreža kao što su Gaardian u Velikoj Britaniji i JLOC u SAD-u (Kuusniemi, 2012, URL-2). Osim uređaja i sustava za detektiranje GPS ometača, razvija se i tehnika zaštite od ometanja signala (*eng. anti-jam*) koja za cilj ima poboljšanja robusnosti prijamnika, uglavnom u vojne svrhe (Landry, 2005) te razvoj softverskih algoritama koji anuliraju učinak ometajućeg signala.

U ovom radu bit će prikazana teorijska osnova tehnologija za ometanje signala i postupaka zaštite od ometanja. Na terenu je ispitan način rada ometača signala, njegova uspješnost u ometanju te su istražene posljedice ometanja. Posebna pozornost posvećena je ispitivanju ometača u različitim uvjetima i na različitim udaljenostima od prijamnika.

2. OMETANJE GNSS SIGNALA

Uređaji za ometanje signala globalnih sustava za pozicioniranje generiraju i odašilju signale radijskih frekvencija sličnih stvarnim frekvencijama uz pojačani šum što uzrokuje gubitak signala sa satelita, težu interpretaciju signala ili nemogućnost kontinuiranog opažanja u prijamniku. Izravna posljedica je nemogućnost pozici-

oniranja i navigacije. Većina tehnika ometanja GNSS signala svrstava se u tri kategorije na temelju širine raspona frekvencija koje ometač koristi (*eng. bandwidth*) - ometanje kontinuiranim valom (*eng. Continuous Wave jamming* - CW ometanje), uskopojasno ometanje (*eng. Narrowband jamming* - NB ometanje) i širokopojasno ometanje (*eng. Wideband jamming* - WB ometanje) (Mukhopadhyay i dr., 2007).

Prema frekvencijskom rasponu GPS signala, signali L-pojasa (*eng. L-band*) se emitiraju unutar dva pojasa od po 20,46 Mhz centriranih oko L1 i L2 frekvencija. L1 frekvencija iznosi 1575,42 Mhz, a L2 1227,60 Mhz (Bačić i Bašić, 1999). Ometanje kontinuiranim valom je definirano kao ometanje pri kojem signal zauzima manje od 100 kHz frekvencijskog raspona. Uskopojasno ometanje je definirano kao ometanje bilo kojeg neželjenog signala koji zauzima više od 1 Mhz frekvencijskog raspona i manje ili jednako cjelokupnom +/-1,023 Mhz frekvencijskom rasponu C/A koda GPS sustava za pozicioniranje te njemu ekvivalentnih kodova, a širokopojasno ometanje je definirano kao ometanje signalima koji u potpunosti zauzimaju frekvencijski raspon od +/-10,23 Mhz oko L1 ili L2 (Rash, 1997).

Učinkovitost tehnika ometanja kontinuiranim valom i uskopojasnog ometanja je potencijalno veća nego učinkovitost tehnika širokopojasnog ometanja zbog veće spektralne gustoće snage – signali su koncentrirani u rasponu frekvencija. S druge strane, za razliku od širokopojasnog šuma, signali kontinuiranog vala i uskopojasni signali se lakše detektiraju i filtriraju iz GPS signala s ugrađenim tehnikama obrade signala što rezultira samo manjim degradacijama u odnosu signal/šum (SNR – *Signal to noise ratio*) i navigacijskim funkcijama. Iako širokopojasno ometanje karakterizira mala spektralna gustoća snage, donedavno ga je bilo nemoguće filtrirati (Mukhopadhyay i dr., 2007), a danas se ublažava specifičnim algoritmima koji se temelje na interpretaciji podataka omjera nosač-šum satelita (eng. *carrier-to-noise-ratio*, C/No) (Thompson i dr., 2010).

Slika 2.1. Vojni GPS Jammer (URL-3)

Slika 2.2. GJ6 GPS Jammer (URL-4)
GJ6 *Portable All Civil Bands GPS Jammer, Anti Tracking Device* (URL-3)
- raspon frekvencija rada: L1, L2, L5
- radijus djelovanja: 15 metara
- 3 antene sa SMA (*SubMiniature version A*) konektorima
- napajanje: baterija 8,4V 2600mAh Li-ion, trajanje 2-3 sata

Slika 2.3. GP5000 GPS *Jammer* (URL-4)
GP5000 *Car Anti-Tracking GPS Blocker, Navigation Jammer* (URL-3)
- raspon frekvencija rada: L1
- radijus djelovanja: 5 metara
- jedna eksterna antena
- napajanje: auto upaljač 12V/ 24V

2.1. UREĐAJI ZA OMETANJE SIGNALA

Osim prema frekvencijskom rasponu ometanja, uređaje za ometanje GPS signala možemo podijeliti prema primjeni na ometače signala za civilnu primjenu te ometače signala za vojnu primjenu.

Jeftiniji civilni uređaji mogu ometati L1 frekvencije signala, a skuplji mogu ometati L1, L2 i druge frekvencije signala. Iako konkretne specifikacije nisu dostupne javnosti, ometači signala za vojnu primjenu su kompleksniji, imaju veću snagu i značajno su veći što se može utvrditi usporedbom vojnog GPS ometača na slici 2.1 s civilnim ometačima GJ6 GPS Jammer (slika 2.2) i GP5000 GPS Jammer (slika 2.3) koji su prikazani sa specifikacijama.

2.2. PRIMJERI OMETANJA SIGNALA

Ometanje GNSS signala događa se namjerno ili nenamjerno. Poznat je slučaj nenamjernog ometanja signala na Newark aerodromu u New Jersey-u 2009. godine kada su u svrhu poboljšanja navigacije, na aerodrom ugrađeni novi GPS prijamnici koji su imali kratke svakodnevne prekide u prijemu signala. Nakon dva mjeseca ispitivanja FAA (*Federal Aviation Administration*) utvrdila je kako je kratkotrajne prekide primanja signala sa satelita izazivao GPS ometač vozača kamiona koji je svakodnevno prolazio pored aerodroma. Moguće je nabrojati i brojne primjere namjernog ometanja signala - od krađa letjelica i automobila (poznat primjer krađe automobila u Velikoj Britaniji), pa sve do vojnih vježbi u Sjevernoj Koreji čijim je ometanjem zahvaćeno više od 300 civilnih zrakoplova i 250 brodova (URL-4).

2.2.1. Spoofing tehnika

Spoofing tehnika napredna je tehnika ometanja GNSS signala koja se temelji na emitiranju signala strukturom identičnih GNSS signalima koji nadjačavaju izvorne signale te kontinuiranim, unaprijed isplaniranim, malim pomacima GNSS prijamnike navode na željene koordinate. *Spoofing* tehnika ometanja signala vrlo je zahtjevna jer je za ometanje potrebno znati točne satelite s kojih konkretni prijamnik prima signal što uglavnom pretpostavlja da je ometač pokretan i na maloj udaljenosti od prijamnika (Ledvina i dr., 2008). Za sada nije potvrđen nijedan napad *spoofingom*, ali postoje pretpostavke da su se takvi napadi događali. Jedan primjer mogućeg *spoofing* napada je preuzimanje bespilotne letjelice RQ-170 Sentinel koje se dogodilo 2011. godine u sjeveroistočnom Iranu (URL-5).

3. ZAŠTITA OD OMETANJA SIGNALA

Postupci zaštite signala sustava za navigaciju mogu se objediniti engleskim nazivom *anti-jam*. Oni uključuju razvoj mreža za detekciju ometača signala, softverske i hardverske nadogradnje prijamnika i antena sustava te zaštitu signala poslanog sa satelita.

3.1. RAZVOJ SUSTAVA ZA DETEKCIJU OMETAČA GNSS SIGNALA

Više projekata lociranja uređaja za ometanje provedeni su u Europi i SAD-u. Istraživački projekt Sentinel tvrtke Chronos Technology koji je proveden u Velikoj Britaniji utvrdio je značajnu raširenost korištenja malih uređaja za ometanje u automobilima. Koristeći više uređaja za detekciju postavljenih na jednom frekventnom prometnom križanju, u šest mjeseci detektirano je više od 60 upotreba malih GNSS ometača (URL-6).

Konzorcij Gaardian u SAD-u razvio je sustav koji pruža informacije o pouzdanosti GPS-a na aerodromima i drugim značajnim lokacijama koristeći mrežu senzora (URL-6) koji kontinuirano opažaju signale GPS i eLoran sustava koji je unapređenje Loran susta-

va, terestričkog radio-navigacijskog sustava prvi put korištenog za Američku i Britansku mornaricu tijekom Drugog svjetskog rata koji emitira signale na niskim frekvencijama od 90 do 110 kHz (Hofmann-Wellenhof i dr, 2001). Takvi senzori pomoću malih atomskih satova detektiraju smetnje i klasificiraju vrste smetnji ovisno o tome jesu li smetnje prirodne ili umjetno stvorene.

U SAD-u je razvijen vojni sustav guste mreže stanica za otkrivanje i lociranje GPS ometača signala JLOC (*GPS Jammer Detection and Location system*) vođen od strane Nacionalne geoprostorne obavještajne agencije (*National Geospatial Intelligence Agency*). Sustav se sastoji od mreže prijamnika koji mogu detektirati područja s većom jačinom signala i slabijim odnosima signal/šum (SNR) koji mogu upućivati na ometanje navigacijskih signala (URL 7).

3.2. MEHANIČKE TEHNIKE ELIMINACIJE OMETANJA GNSS SIGNALA

Mehaničke zaštite od ometanja signala navigacijskih sustava realizirane su upotrebom različitih vrsta antena od kojih su najčešće *Controlled Reception Pattern Antenna* (CRPA) i *Fixed Reception Pattern Antenna* (FRPA). Koristeći ovakve antene moguće je anulirati lažne signale usmjeravanjem antene prema izvoru ometanja ili isključiti ona ometanja koja dolaze pod niskim elevacijskim kutom (URL 8).

3.3. SOFTVERSKE TEHNIKE ELIMINACIJE OMETANJA GNSS SIGNALA

Prema vrijednostima iskazanima u tablici 1 koja prikazuje omjer ometanja i signala - J/S (eng. *jamming to signal ratio* – J/S) za pojedinu metodu zaštite signala iskazanog u decibelima (veći iznos odnosa ometanja prema signalu ukazuje na jače ometanje i jači šum signala u prijamniku), možemo utvrditi kako u odnosu na mehaničke zaštite signala, softverske zaštite signala mogu značajnije doprinijeti kvalitetnoj interpretaciji navigacijskih poruka sa satelita.

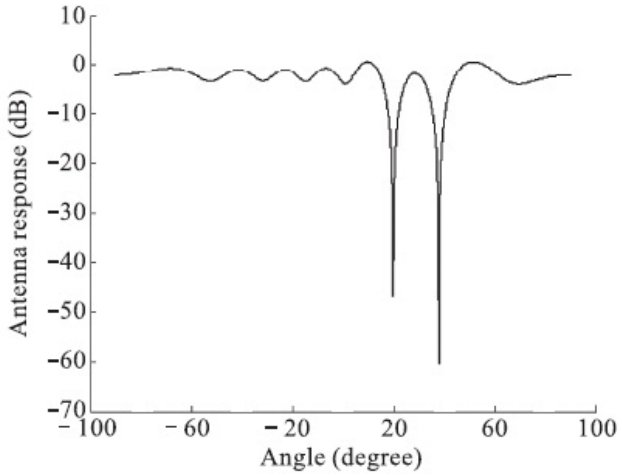
Tablica 1. *Anti-jam* metode (Pandžić i Kostić, 2005)

Anti-jam metode	J/S (db)
osnovna sposobnost GPS proširenog spektra - stacioniran GPS ili dodan INS (inercijalni navigacijski sustav) - P-kod (samo kod)	54
Antena (usmjerenje) - specijalno odvajanje ometača i GPS signala - CRPA antena	30-40
Filtriranje signala ometača - odrediti spektralne karakteristike ometača	0-20
Pomoć u podacima	5-6

Softverska zaštita signala dijeli se na *pre-correlation* tehnike, korištene prije faze korelacije, i *post-correlation* tehnike korištene za poboljšanje kvalitete signala nakon faze korelacije. Neke od *pre-correlation* tehnike su: *Adaptive radiation chart antenna*, *fixed bandpass filtering*, *Automatic Gain Control* (AGC), *Analog-to-Digital Converter* (ADC) i *Piranha* filter. Postoje brojne post-correlation tehnike koje mogu eliminirati širokopojasne interferencije. Tehnika amplitudnog procesiranja (eng. *Amplitude domain processing* - ADP) omogućava jednostavnu implementaciju i visoku učinkovitost kada su ometači unutar pojasa korisnog signala, a njen glavni nedostatak je nemogućnost uklanjanja ometanja u slučaju dvije ili više simultanih interferencija (Landry i dr., 2005).

3.3.1 Metode antenskih nizova

Zadnjih deset godina, sve veći broj istraživanja se fokusira na proučavanje metode antenskog niza (eng. *antenna array*). To su metode koje koriste grupu od nekoliko antena različitih amplituda i faza. Antenski nizovi koriste fenomen interferencije elektromagnetskih valova za pojačanje signala iz željenog smjera i za oslabljivanje signala iz neželjenog smjera (Swarte, 1993). Metode antenskih nizova uključuju programabilne nizove višestrukih



Slika 3.1. Uzorci zraka antena s dva ometača (Dawei i dr., 2008)

zraka (eng. *programmable multibeam arrays*) i upravljive nizove s najmanjom srednjom kvadratnom pogreškom (eng. *least mean square error adaptive arrays*). Antene s upravljivim antenskim nizom, koje se još nazivaju pametne antene (eng. *smart antennas*), sadrže algoritme za identificiranje smjera pristizanja signala (eng. *Direction of Arrival* – DOA). Algoritam najmanje srednje kvadratne pogreške (eng. *least mean square* – LMS) zahtijeva poznavanje karakteristika referentnog signala, detaljne informacije o strukturi željenog signala i kutu pristizanja željenog signala (Dawei i dr., 2008). LMS-u algoritam sličan PI algoritam (*Power inversion*) koji ne zahtijeva navedene ulazne parametre vrlo često se koristi za obradu signala u prijamniku.

Na slici 3.1 prikazan je efekt dva CW ometača smještenih u pravcu od 18 i 28 stupnjeva od smjera antenskog niza. Normalizirani PI algoritam anulira ometajuće signale iz dva smjera. Zbog tog svojstva algoritam eliminira utjecaj više ometača (Dawei i dr., 2008).

Problem metoda upravljivih antenskih nizova je da poništavanje ometajućih signala može oštetiti GPS signal ako je izvor ometanja blizu smjera pristizanja signala GPS satelita. Ovaj nedostatak može se riješiti prostorno-vremensko upravljivim procesiranjem (eng. *space-time adaptive processing* – STAP). Kod prostornog filtriranja, klasični upravljivi algoritmi uključuju LMS, *recursive least squares* (RLS), *direct matrix inversion* (DMI), *ortogonal projection* i dr. Ovi algoritmi zahtijevaju a priori poznate informacije kao što su referentni signal ili smjer pristizanja signala, stoga nisu prikladni za GPS prijamnike. „Slijepi" upravljivi algoritmi ne zahtijevaju a priori informacije te uključuju PI algoritam, potprostorni ortogonalni algoritam (eng. *subspace orthogonal algorithm*) i ostale (Zhao i dr., 2012).

3.4. TESTIRANJE PRIJAMNIKA NA OTPORNOST OD OMETANJA SIGNALA

GPS prijamnike je moguće testirati na otpornost od ometanja signala. Tim testom je moguće odrediti način na koji se zaštititi od uređaja za ometanje. Pri tom se ponajprije misli na kombinaciju opreme koja učinkovito ublažava ometanje signala. Testiranje se vrši u specijaliziranim laboratorijima u više Europskih država i SAD-u. U idealnom slučaju uređaj treba postaviti u rasponu testiranja s različitim konfiguracijama antene i prijamnika zajedno s *band-pass* filtrima i zaštitom od porasta napona (Hendricks, 2011). Time možemo uspostaviti najrobusniju kombinaciju opreme, instalacije i provesti potrebne protumjere na ometanje signala. Uzevši u obzir da je cijena laboratorijskih istraživanja od 5000 $ pa naviše, testiranja nisu uobičajena. U tom slučaju preporuča se instaliranje dodatnog hardvera koji uključuje visoke performanse *band-pass* filtera, RF limitator uređaja i izolirani kabelski vodič. Visoke performanse *band-pass* filtera instaliranih na antene sustava mogu značajno ublažiti ometajuće učinke. Ispravno projektirano

rješenje omogućilo bi samo preciznim GPS frekvencijama prolazak u pojačalo prijamnika, reducirajući područje ometanja ublažavanjem svih šumova van područja frekvencija koji inače prolaze kroz prijamnik antene. RF limitator uređaja unutar prijamnika može smanjiti vrhunac band energije koja prolazi. Ako se izvor ometanja nalazi dovoljno blizu da preopterećuje limitator dioda uređaja unutar prijamnika, dobro osmišljen filter može pružiti razumnu zaštitu od trajnog oštećenja. Bez obzira na zakonska ograničenja, uređaji za ometanje GPS signala su niskih cijena, lako nabavljivi te često u upotrebi. Samim tim GPS prijamnike je uputno na bilo koji način zaštiti od neželjenih posljedica (Hendricks, 2011).

4. TESTIRANJE GPS OMETAČA KRATKOG DOMETA

Iako su jednostavni uređaji za ometanje signala široko dostupni, ometanje radijskih frekvencija je u većem dijelu svijeta, pa tako i Hrvatskoj, ilegalno (NN, 2008) osim u slučajevima kada to zahtijevaju interesi obrane, nacionalne sigurnosti ili ako je to iznimno dopušteno.

Cilj praktičnog dijela ovog rada bio je ispitati te analizirati djelovanje GPS ometača signala na GPS prijamnike različite kvalitete. Prilikom testiranja korišteni su jednofrekventni prijamnici Garmin GPSmap 76CS (slika 4.3) i pametni telefon Samsung Galaxy S3 Mini te dvofrekventni prijamnik - Trimble 5700 Rover (slika 4.2). Korišteni ometač signala bio je Portable Mobile Signal Jammer (slika 4.1). Specifikacije korištenog instrumentarija dane su u nastavku.

Slika 4.1. GPS ometač Portable Mobile Signal Jammer
- jedna frekvencija (L1)
- *Omni – directional antenna* (CDMA/GSM, 3G, DCS/DHS)
- vrijeme rada: 3 – 4 sata
- masa: 180 g
- radijus ometanja: do 15 m

Slika 4.2. Trimble 5700 Rover
Trimble 5700 Rover
- dvofrekvencijski GPS prijamnik
- antena: Trimble Zephyr
- 24 kanala, L1 C/A kod i L1/L2 noseće faze
- masa: 1,4 kg

Slika 4.3. Garmin GPSmap 76CS
Garmin GPSmap 76CS
- jednofrekvencijski GPS prijamik
- antena: Quadrifilar
- masa: 218 g

Slika 4.4. Samsung Galaxy S3 mini
Samsung Galaxy S3 mini
- jedna frekvencija (L1 C/A kod) uz *Assisted* GPS
- GPS čip *broadcom* BCM47511 sa *skyworks* SKY65702-11 GaAs pHEMT modulom

4.1. TESTIRANJE OMETAČA

Ometanje prijamnika testirano je na različitim udaljenostima. Početno testiranje provedeno je na GPS uređaju Trimble 5700 Rover uz statička GPS mjerenja prilikom kojih je GPS ometač uključen po dvije minute na različitim udaljenostima (2 i 15 metara) uz vremenski odmak od desetak minuta za vrijeme mjerenja. Prikupljeni podaci naknadno su obrađeni. Osim prilikom provođenja statičkih GPS mjerenja, ometač je testiran i na različitim udaljenostima prilikom inicijalizacije i prikupljanja informacija sa satelita. Udaljenosti ometača od prijamnika mjerene su mjernom vrpcom. Tako su dobiveni podaci u tablici 2.

Tablica 2. Rezultati ometanja GPS prijamnika Trimble 5700 uređaja

Udaljenost (m)	Broj vidljivih satelita (ometač isključen)	Broj vidljivih satelita (ometač uključen)
0,5	8	0
10	8	0
20	8	0
30	9	3
40	8	3
50	8	4*
60	8	6

* broj satelita je varirao od 0 do 4

Iz rezultata ometanja GPS prijamnika je vidljivo da GPS ometač radi prema specifikacijama, a u uvjetima bez prepreka onemogućuje primanje signala i na većim udaljenostima. Utjecaj ometača primijećen je i na udaljenosti od 50 metara.

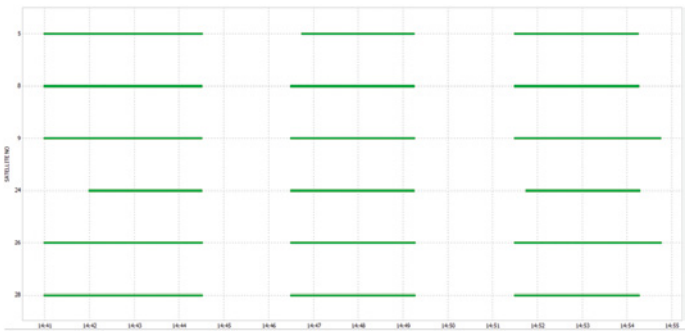
Druga testiranja provedena su na jednofrekvencijskim GPS prijamnicima Garmin GPSmap 76CS i mobilnom telefonu Samsung Galaxy S3 mini. Ometač je uključen na udaljenosti od 0,5 metara i 15 metara. Garmin prijamnik je primao signale s četiri satelita prije uključenja ometača, a nakon uključenja nije primao signal ni s jednog satelita. Ometanjem GPS signala na mobilnom uređaju primijećeno je da uređaj ne prima GPS signale, međutim pozicioniranje nije bilo potpuno onemogućeno zbog *Assisted* GPS tehnologije implementirane u uređaju.

4.2. OBRADA I ANALIZA PODATAKA

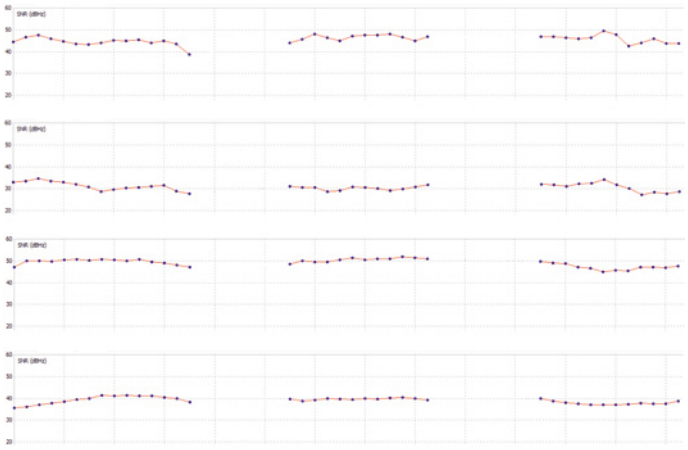
Prikupljeni podaci obrađeni su u programskom paketu RTKLIB_2.4.1 čiji je autor T. Takasu. RTKLIB je programski paket otvorenog koda za *post-processing* obradu GNSS mjerenja (URL 9).

Rezultati obrade prikazani su grafički te je potvrđen utjecaj ometača na dvofrekvencijski GPS prijamnik Trimble 5700 na kojem je onemogućen prijem signala sa svih satelita za vrijeme ometanja (slika 4.5). Usporedbom zapisnika i obrađenih podataka, može se utvrditi da je nakon isključivanja GPS ometača, GPS prijamnik nastavio opažati signale sa satelita nakon nekoliko sekundi.

Na grafu na slici 4.5. se na ordinatnoj osi nalaze identifikacijski brojevi GPS satelita, a na apscisnoj osi vremenska skala (UTC). Vidljivo je da je prijamnik Trimble 5700 Rover kontinuirano opažao šest satelita u vremenskom periodu od 4 minute od početka mjerenja. Nakon uključenja ometača prekida se prijem signala. Isključenjem ometača prijamnik ponovno prima signale satelita. Novi prekid prijema signala javlja se uključenjem ometača signala u vremenu od 14:44:30 UTC do 14:46:30 UTC. Utjecaj ometača na obje frekvencije vidljiv je na grafu odnosa signala i šuma (eng. *Signal to Noise Ratio* - SNR) (slika 4.6).



Slika 4.5. Grafički prikaz vidljivosti satelita



Slika 4.5. Grafički prikaz SNR-a satelita 8 i 28

Na slici 4.6. kao primjer su prikazani odnosi signala i šuma za osmi i dvadesetosmi satelit na L1 i L2 frekvencijama čime je pokazano da je djelovanje GPS ometača potpuno za prijem signala sa svih satelita i na obje frekvencije.

5. ZAKLJUČAK

Mnoge ljudske djelatnosti danas se teško mogu zamisliti bez informacija koje pružaju globalni navigacijski sustavi, a prostorna komponenta informacije ili usluge postaje jedan od presudnih kriterija tržišta i drugih sustava u koje je uključen pojedinac. Zato je prikupljanje kvalitetnih prostornih podataka i mogućnost njihovog nedvosmislenog interpretiranja od presudnog značaja. Uređaji za ometanje GNSS signala za cilj imaju upravo onesposobljavanje ili umanjivanje kvalitete prikupljanja prostornih podataka s raznim dobronamjernim (zaštita privatnosti pojedinca) ili zlonamjernim ciljevima.

Primjenom jednostavnog ometača signala kratkog dometa na različitim GPS prijamnicima utvrđena je učinkovitost takvih uređaja te je pokazano da se njihovim korištenjem može u potpunosti onemogućiti primanje signala satelita u prijamnicima na udaljenostima i većima od 15 metara.

Kako bi se sustavi pozicioniranja zaštitili od ometanja, provode se razne metode zaštite koje uključuju mehaničke nadogradnje na antene prijamnika, softverske nadogradnje u obliku algoritama za detekciju i anuliranje neželjenih signala te nadogradnje sustava za pozicioniranje modificiranjem načina slanja poruka za pozicioniranje sa satelita. Budući koraci zaštite od ometanja signala uključivat će sve mogućnosti poboljšavanja sustava za pozicioniranje, ali bez sumnje, isti razvoj pratit će i razvoj sustava za ometanje tog sustava (Zhao i dr., 2012).

LITERATURA

- Bačić, Ž., Bašić, T., (1999): Satelitska geodezija II, skripta, Sveučilište u Zagrebu, Geodetski fakultet.
- Dawei, M., Zhenming, F., Mingquan, L., (2008): Anti-Jamming with Adaptive Arrays Utilizing Power Inversion Algorithm, Tsinghua science and technology, vol. 13, no. 6
- Hendricks, M., (2011): GPS Jamming, Protection Technology Group, SAD.
- Hofmann-Wellenhof, B., Lichtenegger, H., Collins, J., (2001): Global Positioning System, Theory and Practice, Springer, Wien, New York.
- Kuusniemi, H., (2012), Effects of GNSS jammers and potential mitigation approaches, Finnish Geodetic Institute.
- Landry, R., Boutin, P., Constantinescu, A., (2005): New anti-jamming technique for GPS and GALILEO receivers using adaptive FADP filter, Digital Signal Processing, vol. 16, str. 255. - 274.
- Ledvina, B., Humphreys, T., Psiaki, M.L., O'Hanlon, B.W., Kintner, P.M., (2008):
- Mukhopadhyay, M., Sarkar, B. K., Chakraborty, A., (2007): Augmentation Of Anti-Jam Gps System Using Smart Antenna With A Simple Doa Estimation Algorithm, PIER 67, str. 231. – 249.
- Narodne Novine (2008): Zakon o elektroničkim komunikacijama, 73/08.
- Pandžić, L., Kostić, S., (2005), GPS signali, Ometanje i zaštita od ometanja, Univerzitet u Novom Sadu, Fakultet Tehničkih nauka, Novi Sad, Srbija.
- Rash, G. D., (1997), GPS Jamming in A Laboratory Environment, The Institute of Navigation, str. 389 – 398.
- Swarte, V. V, (2006): Electromagnetic Fields and Waves, New Age International Publishers, New Delhi, Indija.
- Thiel, A., Ammann, M., (2009): Anti-Jamming techniques in u-blox GPS receivers, u-blox, Švicarska.
- Thompson, R. J. R., Wu, J., Tabatabaei Balaei, A., Dempster, A. G. (2010): Detection of RF interference to GPS using day-to-day C/No differences, 2010 International Symposium on GPS/GNSS, Taipei, Tajvan.
- Zhao, H., Lian, B., Feng, J., (2012): Space-Time Adaptive Processing for GPS anti-jamming Receiver, Physics Procedia, vol. 33, str. 1060. - 1067.
- URL-1: Federal Communications Commission official website, [Internet],<raspoloživo na: http://transition.fcc.gov/, [pristupljeno 10.2.2013.]
- URL-2: Novatel official webpage, [Internet],<raspoloživo na: http://www.novatel.com/, [pristupljeno 15.2.2013.]
- URL-3: Blog Jammer Store, [Internet],<raspoloživo na: http://blog.jammer-store.com/2012/, [pristupljeno 15.2.2013.]
- URL-4: Research and Radionavigation General Lighthouse Authorities, [Internet],<raspoloživo na: , http://www.gla-rrnav.org/pdfs/interference_to_gps_v101_3_.pdf, [pristupljeno 20.2.2013.]
- URL-5: TechWorld, [Internet],<raspoloživo na: http://news.techworld.com/security/3325752/us-spy-drone-tricked-into-iran-landing-by-gps-spoofing/, [pristupljeno 11.3.2013.]
- URL-6: The E conomist, [Internet],<raspoloživo na: http://www.economist.com/node/18304246, [pristupljeno 11.3.2013.]
- URL-7: British Broadcasting Corporation, [Internet],<raspoloživo na: http://www.bbc.co.uk/news/technology-17119768, [pristupljeno 11.3.2013.]
- URL-8: Federation of American Scientists, [Internet],<raspoloživo na: http://www.fas.org/spp/military/program/nssrm/initiatives/frapa.htm, [pristupljeno 14.3.2013.]
- URL-9: RTKLIB: An Open Source Program Package for GNSS Positioning, [Internet],<raspoloživo na: http://www.rtklib.com/, [pristupljeno 7.4.2013.]