https://doi.org/10.26552/aer.C.2023.1.2

UNIVERSITY OF ŽILINA

DETEKCIA RUŠENIA SIGNÁLU GNSS NA LETISKÁCH

DETECTION OF GNSS SIGNAL INTERFERENCE IN AIRDROME PROXIMITY

Ján Velčický
Katedra leteckej dopravy
Žilinská univerzita v Žiline
Univerzitná 8215/1
010 26, Žilina
john.velcicky@gmail.com

Andrej Novák
Katedra leteckej dopravy
Žilinská univerzita v Žilina
Univerzitná 8215/1
010 26, Žilina
andrej.novak@uniza.sk

Abstract

Although the Global Navigation Satellite System provides an increased precision in instrument approaches, it is vulnerable to various signal interferences causing either decreased position accuracy or a complete loss of GNSS signal reception. One of the major threats to a GNSS receiver is the intentional interference known as jamming. Incoming airplanes can be seriously endangered by such signal loss. This bachelor's thesis addresses the detection and classification of possible unintentional and intentional interference and spoofing attacks on airplanes in proximity to the airdrome Žilina. Besides that, other systems which show sufficient reliability are compared. Additionally, critical parts of RNP approach chart map are evaluated. Finally, a device called HackRF ONE is selected to be put in aerodrome proximity for detection of possible GNSS interference. Using this software defined radio as unmanned aerial vehicle alarm and protection system is another suggested possibility.

Keywords

GNSS, aerodrome, jamming, interference detection, SDR, UAV

1. Úvod

Globálne navigačné satelitné systémy (GNSS), sú systémy satelitnej navigácie, ktoré poskytujú globálne pokrytie, pre určovanie polohy a času, ktorý zahŕňa konšteláciu jedného alebo viacerých systémov (Khan, 2023). Tvoria ho v súčasnosti systémy GPS, GLONASS, Galileo, Beidu ako aj rozšírené satelitné systémy WAAS, EGNOS, MSAS, GAGAN, SDCM, BDSBAS, KASS, ANGA (Sekera & Novák, 2021). Signál môže byť rušený úmyselne alebo neúmyselne. Našou úlohou je navrhnúť systém, ktorý by detegoval toto rušenie.

1.1. Časti GNSS

Vesmírna časť pozostáva z satelitov strednej veľkosti o hmotnosti niekoľko stoviek až tisíc kilogramov, ktoré využívajú časti frekvenčného pásma označované ako L-band na vysielanie navigačných signálov pre rôzny rozsah poskytovaných služieb. Tieto satelity majú zvyčajne kruhovú obežnú dráhu s polomerom 25 až 30 tis. kilometrov.

Rozšírené systémy GNSS používajú geostacionárnu obežnú dráh (Khan, 2023). Navigačné signály sú vysielané a generované zariadením družice, ktoré obsahuje jedno alebo viac atómových hodín, ktoré poskytujú presný časový a frekvenčný referenčný bod. Na šetrenie energie sú vysokovýkonné zosilňovače (HPA) navrhnuté tak, aby pracovali v bode saturácie. Avšak, keďže viaceré služby sú vysielané ako jeden signál v jednom frekvenčnom pásme, malé variácie vstupných signálov na HPA môžu spôsobiť nelineárne efekty na zosilňovaných signáloch. Na riešenie tohto problému sa používajú techniky multiplexovania signálov, pričom kombinovanie rôznych signálov do konštantnej obálky, ktorú následne zosilňujeme v koncovom stupni satelitu (Ioannides et al., 2016)

Kontrolný segment GNSS využíva niekoľko prijímačov GNSS umiestnených v tzv. monitorovacích (alebo senzorových) staniciach rozmiestnených po celom svete, aby získal pseudovzdialenosti od všetkých satelitov pre všetky senzorové stanice. Keďže polohy senzorových staníc sú presne známe a pohyb družíc podlieha Keplerovým zákonom, tieto údaje možno použiť na určenie a predpovedanie polohy satelitov, na odhad drobných odchýlok atómových hodín na palube satelitov a na odhad oneskorení, ktoré navigačné signály zaznamenajú pri prechode cez atmosféru. Tieto údaje sú zakódované do formátu navigačnej správy a nahrávané na satelity. Nahrávanie na satelit sa uskutočňuje v inom frekvenčnom pásme (C-pásmo), pomocou techník šírenia spektra alebo signálového modulovania fázy. Nahrávanie sa zvyčajne uskutočňuje každé niekoľko hodín (Ioannides et al., 2016).

Signály vysielané satelitmi majú oneskorenie pri príchode k prijímaču, čo môže spôsobiť rozdiel v čase medzi satelitom a prijímačom. Toto oneskorenie, označované ako Taum pre m-ty satelit, spôsobuje aj zmenu frekvencie signálu, známu ako Dopplerov posun. Prijímanie signálov od štyroch alebo viac satelitov umožňuje používateľovi určiť svoju polohu, rýchlosť a čas. Treba si uvedomiť, že prijatý signál r(t), ktorý sa spracúva v DSP časti prijímača, je filtrovaný v prednej časti prijímača. V DSP častiach prijímača vytvára prijímač kópiu vysielaného signálu s odhadmi oneskorenia δ a Dopplerovského posunu fD. Použitím prístupu s vyrovnávacím filtrom získava prijímač odhadované hodnoty oneskorenia satelitu a dopplerovského posunu. Multikanálové prijímače majú niekoľko paralelných kanálov, takže môžu sledovať niekoľko satelitov naraz. Toto riešenie je

drahšie a hlavne sa používa tam kde sú vysoké nároky na dynamiku (navádzané rakety) (Ioannides et al., 2016). Sekvenčné prijímače menia sledovanie satelitov približne každú sekundu. Z toho vyplýva, že potrebný čas k získaní pozícii je 4-5s. Nie je taký dobrý ako multikanálový prijímač, ale v statickom prípade je rozdiel minimálny. Pri počiatočnom získaní polohy musí prijímač sledovať každý satelit 6s. Multiplexné prijímače prejdú celým cyklom 4-och až 5 satelitov v priebehu jednej dátovej správy (20ms). Vzorkujú signály len raz za cyklus a používajú tie hodnoty na aktualizovanie sledovacieho softvéru. Dokážu čítať dáta a aj vyhľadávať nové satelity popri tom ako podávajú ďalej navigačné dáta (Mitola, 1993).

1.2. Útoky na prijímače GNSS

Ak je prítomný interferenčný signál I(t), môže sa stať, že prijímač GNSS prestane fungovať, vygeneruje nesprávne pozíciu alebo umelo nastavený nesprávny odhad polohy alebo času. To závisí od prijímaného signálu I(t) (Coudé, 2020).

Existujú dva hlavné druhy zámerného rušenia, ktoré môžu ovplyvniť systémy GNSS a ich používateľov: rušenie (jamming) a falšovanie (spoofing). Útočník môže použiť rôzne modulácie signálu pre I(t) s vysokou silou, aby ovplyvnil dostupnosť signálov zo satelitov GNSS a súvisiace služby. Na rozdiel od toho sa falšovanie snaží oklamať používateľa GNSS tým, že vysiela signály I(t) s rovnakými charakteristikami ako legitímne signály satelitov GNSS s(t). Ak je GNSS prijímač falšovaný, bude hlásiť nesprávnu polohu a/alebo časovú informáciu, v závislosti od druhu útoku, dokonca aj s potvrdeným kontrolou integrity (Coudé, 2020).

Rušenie a jamming (úmyselné vysielanie rušivých signálov) boli dlhodobo v centre pozornosti GNSS komunity kvôli ich negatívnemu vplyvu na GNSS signály. V literatúre sa rozlišuje medzi neúmyselným rušením z iných komunikačných systémov ovplyvňujúcich nízko výkonné GNSS signály a jammingom, ktorý sa snaží úmyselne ovplyvniť prevádzku GNSS prijímača. Medzi neúmyselné rušenie patrí:

- Rušenie mimo pásma spôsobené harmonickými a intermodulačnými produktmi, ako napríklad signály digitálneho terestriálneho vysielania (DVB-T), signály VHF omnidirectional range (VOR) a prístrojového pristávacieho systému (ILS), multikariérovo modulované satelitné komunikačné systémy a amatérske rádiové služby.
- Rušenie v pásme, vrátane civilných a vojenských terestriálnych navigačných systémov, ako sú systémy merania vzdialenosti (DME) a taktická letecká navigácia (TACAN), vojenské rozšírené spektrumové komunikačné systémy ako spoločný taktický informačný distribučný systém (JTIDS) a multifunkčný distribučný systém informácií (MIDS), ako aj radary na zisťovanie vetra a civilné radary (1215-1400 MHz) (Novák et al. 2019).

Zámerné rušenie alebo rušenie je dosiahnuté pomocou zariadení, ktoré môžu vysielať silné signály v pásme GNSS, spôsobujúc rôzne účinky. Veľká časť z nich patrí do kategórie osobných zariadení na ochranu súkromia (PPD), ktoré sa používajú ako rušiče v automobiloch na zabránenie sledovania vozidla napríklad pri cestnej mýte, a ktoré majú účinné dosahy v rozsahu od niekoľkých desiatok metrov do kilometrov. Účinky rušenia môžeme zhrnúť takto: strata sledovania, zvýšené pseudovzdialenostné chyby, vysoké chyby demodulácie, odmietnutie získania signálu a falošné detekcie signálu a neustále cyklické posuvy. Účinok rušenia je opísaný účinným pomerom nosnej frekvencie k hustote šumu.

Spoofing nastáva vtedy, keď interferenčný signál I(t) má rovnakú štruktúru ako signál s(t), čo vedie k identickým tvarom pre Gs(f) a GI(f) a umožňuje maximálne prekrytie signálov. Signály vytvorené na účely spoofingu nemožno traktovať ako náhodné signály a teória C/N0 redukcie vyjadrená vzťahom sa na ne nevzťahuje. Namiesto toho sa v cielovom prijímači objavujú deterministické efekty.

Hoci nie sú preukázané záznamy o zámerných útokoch typu spoofing, niekoľko demonstrácií ukázalo, že je to realizovateľné s dnešnými softvérovo definovanými rádiami (SDR) a GNSS simulátormi. Tým sa význam spoofingu zvýšil ako závažné nebezpečenstvo pre GNSS systémy. Môže existovať mnoho rôznych variantov útokov typu spoofing, ktoré závisia od konkrétnej formy aplikovanej oneskorenia tau I(t) a výkonu spoofera CI(t) (Coudé, 2020).

Spoofing je zamierený na zavádzanie GNSS prijímačov do poskytovania nepresných informácií o polohe a čase. Proces navigácie v GNSS prijímači sa spolieha na predvídateľný modulovaný rozsah kódov (c (t)) a informácie o navigačných dátach (d (t)), ktoré sú prítomné v signáli Open Service (OS) GNSS, čo ho robí zraniteľným voči dvom typom útokov: útokom na úrovni navigačnej správy a útokom na úrovni kódu. Okrem toho by jeho výkon CI nemal byť významne vyšší ako výkon autentického signálu C, aby sa vyhol detekcii.

Spoofer musí zahrnúť kompenzáciu rôznych faktorov, vrátane vnútorných oneskorení hardvéru, posunov hodín, relatívnych Poyntingových vektorov a ziskov antén na oboch koncoch. Aj keď takýto útok predstavuje výzvu, nemožno ho považovať za nemožný, najmä v prípadoch, keď používateľ jazdí autom s COTS (commercial-of-the-shelf) anténou a protivník je odborný inžinier alebo používa zariadenie na samospoofovania (Coudé, 2020).

2. Metodika a metodológia

Známe metódy získavania údajov sú: pozorovanie, experiment, rozhovor, dotazník. Každá z týchto metód má výhody aj nevýhody. Výskum si obvykle vyžaduje použitie viacero metód. V článku používame výskumné metódy analýzy, evaluácie, komparácie a testovania.

Kvalitatívna evaluácia znamená proces posudzovania a hodnotenia podstaty, hodnoty a ceny skúmaného objektu a procesu s cieľom urobiť určité rozhodnutia o prijatí, odmietnutí alebo formulácii prijatej stratégie na určitej úrovni rozhodovania.

Princíp metódy porovnávania (komparácie) spočíva v tom, že skutočný jav porovnávame vždy s určitou porovnávacou základňou. Túto základňu považujeme za normu pre hodnotenie. Pre porovnávanie je nutné, aby porovnávané javy mali rovnaký obsah alebo rovnaké položky (Mašková, 2016).

3. Analýza systémov pre detekciu rušenia signálu na letiskách

Proti rušeniu poznáme opatrenia na úrovni detekcie a zmierňovania daného rušenia.

3.1. Detekcia rušenia

V každom modernom prijímači sa pred analógovo-digitálnou konverziou (ADC) používa automatická regulácia zosilnenia (AGC). Schémy detekcie rušenia satelitného navigačného signálu zahŕňajúce AGC, spočívajú v skutočnosti, že AGC je viac riadený okolitým šumom alebo interferenciou než silou signálu GNSS a teda zmena zosilnenia AGC môže byť použitá na detekciu prítomnosti interferencie (California Institute of Technology, 2022).

3.2. Zmierňovanie dôsledkov rušenia

Existuje niekoľko metód na redukciu rušenia satelitného navigačného signálu, ktoré sa dajú rozdeliť do štyroch oblastí: časová, frekvenčná, časovo-frekvenčná a priestorovo-časová. Medzi nimi je najpoužívanejšou metódou v časovej oblasti technika pulzného vypínania (blanking), ktorá sa snaží odstrániť impulzné rušenie, ako napr. DME/TACAN. Táto technika spočíva v tom, že sa výstup vzoriek z ADC vypne, ak prekročia definovaný amplitúdový prah na základe očakávaného šumu. Aby sa zabránilo silným potlačujúcim AGC pulzami, AGC zisk sa nastavuje pomocou iba 2-3 bitov z multirezolučného ADC. Hoci sa technika pulzného vypínania často používa v GNSS prijímačoch, uvádza sa, že nie je tak efektívna ako techniky založené na TFR, hlavne kvôli odstráneniu významných časových intervalov užitočného signálu v prítomnosti silného a dlhodobého rušenia (Ioannides et al., 2016).

3.3. Detekcia a zmierňovanie spoofingu

Mnoho prijímačových protiopatrení proti útokom typu spoofing zdieľa rovnaké princípy s technikami detekcie a zmierňovania rušenia. Hlavným rozlišovacím znakom je, že opatrenia proti spoofingu môžu byť zahrnuté aj na úrovni GNSS systému zlepšením dizajnu signálu (Ioannides et al., 2016).

4. Vyhodnotenie a návrh systému identifikujúceho riešenia na letiskách

Pre návrh systému identifikujúceho rušenia na letiskách je dôležité najprv vyhodnotiť a porovnať iné systémy u ktorých bola preukázaná dostatočná spoľahlivosť pri odhaľovaní rušenia.

4.1. Vyhodnotenie systémov

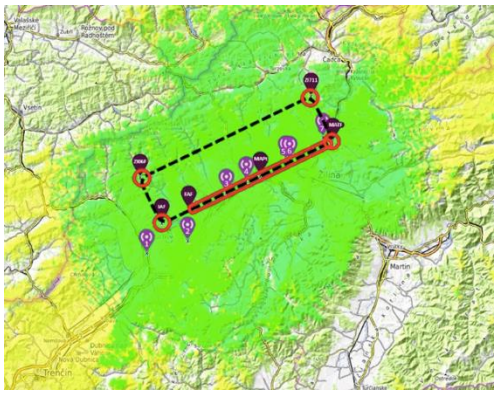
Mapovaniu rušenia sa venuje viacero služieb, pričom sa vyhodnocuje aj prostredníctvom satelitov. SMAP (Soil Moisture Active Passive) je projekt NASA a má jeden z najpokročilejších detektorov rušenia rádiových frekvencií (RFI), ktorý je momentálne na obežnej dráhe. Aj keď misia SMAP meria jasovú teplotu Zeme v chránenom spektre 1400-1427 MHz, merania SMAP sú stále rušené rádio-frekvenčnou interferenciou (RFI) (California Institute of Technology, 2022).

V Measurement Of Gnss Interference At Airport Zilina (Kováčik et al., 2019) autori so svojím výskumom potvrdzujú, že na meranie interferencií GNSS na Žilinskom letisku by bola vhodná sieť pozostávajúca z viacerých antén a prijímačov. Štúdia Jamming of GNSS Receiver on B737 MAX Aircraft and Its Impact on ADS-B Technology (Kraus et al. 2020) prináša hlbšie vedomosti správania sa GPS prijímača na lietadle v prítomnosti rušiča. Ako príkladné lietadlo si vybrali aerolinkové lietadlo B737 MAX 8. Počas testovania prvého scenáru zistili, že na vyradenie oboch polôh GNSS je potreba rušič s výkonom 0,79mW (-1dBm). Ak to napríklad porovnáme s modernými mobilnými telefónmi, takáto úroveň rušenia by im nerobila žiadne problémy s určovaním polohy podľa GPS. Zistili aj, že počas takto silného rušenia lietadlový prijímač nedodáva žiadne dáta. Zistili aj, že počas takto silného rušenia lietadlový prijímač nedodáva žiadne dáta. Z testovania druhého scenáru zistili, že na vyradenie jedného zdroja GNSS polohy je potreba rušič s výkonom 2mW (3dBm) a na vyradenie oboch 2,51mW (4dBm). V treťom scenári vypadla GNSS poloha v kokpite vo výške 4,4m a obe polohy vo výške 6,5m nad zemou. Výsledky týchto meraní ukázali, že dopad rušenia na avioniku je pozorovateľný napríklad zvýšenou variabilitou informácii o polohe vysielanou správami ADS-B (Novák et al., 2019).

4.2. Vyhodnotenie kritických častí príletu

Na základe analýzy existujúcich systémov sme v tejto časti navrhli nový systém detekcie rušenia signálov GNSS na letisku Žilina. Podľa Bc. Mariána Buľáka (Marián Buľák, 2019) je najkritickejšou fázou letu priblíženie a pristátie. Rozhodli sme sa sústrediť na túto časť letu pretože v tejto časti môže mať výpadok navigačného signálu katastrofálne následky. Pri analýze a následnom rozbore problému sme sa rozhodli použiť existujúce mapové podklady z OpenTopoMap do ktorých sme implementovali a označili tmavofialovou značkou letecké informácie z AIP príletovej mapy. Následne sme identifikovali kritické miesta z pohľadu možného rušenia GNSS signálu ktorými môže byť priemyselná infraštruktúra, logistická infraštruktúra, výroba elektrickej energie a jej rozvodná sústava, cesty prvej triedy, rýchlostné cesty a diaľnice. Fialovou značkou a príslušným číslom sme zahrnuli tieto konkrétne možné zdroje rušenia: Gumárne Púchov, Považské Strojárne, Úsek diaľnice D1 Považská Bystrica - Dolný Hričov, Priemyselný park Bytča, Priemyselný park Horný Hričov, Vodná elektráreň Hričov – rozvodňa a Schaeffler Kysuce. Z pohľadu vplyvu na priblíženie sme rozčlenili jednotlivé fázy letu nasledovne: od IAF po FAF, od FAF po MAPt, od MAPt po MATF a v otočných bodoch (ZI711, ZI712, MATF).

Strata signálu GNSS/GPS počas prístrojového priblíženia RNP RWY 06 v časti od fixu počiatočného priblíženia po fix konečného priblíženia nie je kritická. Pri strate signálu od bodu konečného priblíženia (FAF) po bod začatia postupu nevydareného priblíženia (MAPt) kde lietadlo za normálnych okolností klesá, je šanca že lietadlo podklesá pod bezpečnú výšku a môže dôjsť k nebezpečnému priblíženiu s terénom. Ak dôjde k state signálu v tejto časti trate priblíženia, pilot musí prerušiť priblíženie a zahájiť procedúru pre opakované priblíženie s použitím záložného systému a príslušného postupu. Kritickou časťou trate je aj úsek od MAPt po fix začatia zatáčky pri postupe nevydareného priblíženia (MATF). Pri strate signálu v tejto časti trate pilot nevie kedy má začať zatáčať a tak ako aj v predošlej časti trate, môže dôjsť k nebezpečnému priblíženiu s terénom. Pretože je lietadlo pri zatáčaní citlivé na rušenie zo zeme [10], označili sme za kritické časti aj otočné body ZI711, ZI712 a MATF. Na nasledujúcej mape (Obrázok 1) sú červenou znázornené kritické časti.



Obrázok 1: Mapa možného rušenia lietadla z pozemných zdrojov pri priblížení. Zdroj: autor, podľa (Coudé, 2020)

4.3. Návrh systému pre detekciu rušenia

Pre laboratórne merania a prácu v RF spektre boli vyvinuté zariadenia Softvérovo navrhnuté rádiá (SDR). SDR je termín definovaný v 90. rokoch jeho tvorcom Josephom Mitolom ako identifikátor triedy rádií, ktoré by bolo možné preprogramovať a prekonfigurovať pomocou softvéru namiesto hardvéru (Del Barrio et al., 2023). Koncept softvérovo definovaného rádia sa v priebehu desaťročí vyvíjal. SDR sa skladá z troch základných častí: RF/IF modul, Digitálny Front End modul a Base Band Processing. Moduly RF/IF a Digitálny Front End sú realizované hardwarovým riešením na základe rôznorodých koncepcii výrobcov príslušných modulov.

Pre náš výskum rušenia a detekcie rušenia signálu GNSS bolo vybraných päť základných SDR zariadení, ktoré sa využívajú pre vzdelávacie účely. Prvým je HackRF One od Great Scott Gadgets, druhým je bladeFR, tretím je ADALM-PLUTO, štvrtým je LimeSDR od Lime microsystems a piatym je USRP N200 od Ettus Research. Pre všetky nami vybrané zariadenia sú zakladené technické parametre uvedené v tabuľke 4, pričom ich použitie ako aj rozsah použitia vyhovuje nášmu výskumu.

5. Diskusia

Na základe faktu, že sa v civilnom letectve stále zväčšuje použitie signálov GNSS autori analyzovali možné typy rušenia na prijímače a ich zmierňovanie. Schopnosti popísaných metód je potrebné ešte podrobnejšie preskúmať v rôznych prostrediach a použitiach, pretože väčšina poznatkov pochádza z dedinských alebo zastrešených prostredí. Okrem toho je potrebné hodnotiť výkon týchto techník v závislosti na sofistikácii podvodov a aj pre rôzne architektúry prijímačov. Boli pritom použité vedecké metódy.

Ďalej autori analyzovali kritické miesta AIP príletovej mapy z pohľadu možného rušenia signálu GNSS. Do týchto miest sme v rámci simulácie pomocou internetového nástroja Radio Mobile umiestnili zdroje rušenia. Túto príletovú mapu rozdelili aj z pohľadu závažnosti prípadného rušenia. Pre umiestnenie vo vyznačených oblastiach sme bolo rozhodnuté použiť zariadenie SDR HackRF One. Toto softvérovo definované rádio bolo vybrané spomedzi iných nielen vďaka svojej dostupnosti v laboratóriu na Žilinskej Univerzite ale hlavne vďaka ponúkanému výkonu za prijateľnú cenu. Je predpoklad, že práve toto zaujme prípadných investorov. Bola otestovaná funkcia vysielania a signál bol prijatý ako rušenie laboratórnym prijímačom TOPGNSS GN702UB. Autori tento jav vysvetľujú veľkým výkonom vysielača a tým, že prijímač rozpoznal, že ide o útok a rozhodol neuviesť polohu.

Použitie daného zariadenia na rušenie signálov UAV by efektívne vyradilo jeho schopnosť komunikovať s ovládačom. Využitie HackRF ONE je však viacnásobné, dokáže aj prijímať signál. Okrem umiestnenia v kritických častiach príletovej mapy, autori navrhujú multispektrálne využitie zariadení HackRF na zabezpečenie perimetra letiska, a to tak, že by detegovali najčastejšie používané frekvencie na ovládanie UAV a v prípade detekcie takéhoto signálu by prerušili spojenie UAV s ovládačom.

6. Záver

článok analyzuje základné princípy fungovania globálnych satelitných navigačných systémov. Článok ďalej popisuje ako aj samotné falšované signály, tak aj metódy zmierňovania ich dopadov na prijímače, ale schopnosti popísaných metód je ešte potrebné podrobnejšie preskúmať v rôznych prostrediach a použitiach, pretože väčšina poznatkov pochádza z dedinských alebo zastrešených prostredí. Okrem toho je potrebné hodnotiť výkon týchto techník v závislosti na sofistikácii podvodov a aj pre rôzne architektúry prijímačov.

Prínosom článku je návrh nového detekčného systému pre letisko Žilina. Na základe simulácie pomocou internetového nástroja Radio Mobile, a následného zhodnotenia kritických častí prístrojovej príletovej mapy RNP autori, na základe vyhodnotenia dostupných SDR prijímačov, navrhli použitie SDR HackRF ONE na detekciu rušenia signálu GNSS. Autori nainštalovali externý TCXO a overili ich vzájomnú spoluprácu. Autori pomocou denne aktualizovaných efemeridov vytvorili a odvysielali falošný signál GPS. Laboratórny prijímač TOPGNSS GN702UB síce prijal vysielaný signál, ale odmietol uviesť polohu. Autori tento jav vysvetľujú veľkým výkonom vysielača a tým, že prijímač rozpoznal, že ide o útok a rozhodol neuviesť polohu vôbec. Okrem umiestnenia v kritických častiach príletovej mapy, článok navrhuje multispektrálne využitie zariadení HackRF na zabezpečenie perimetra letiska, a to tak, že by detegovali najčastejšie používané frekvencie na ovládanie UAV a v prípade detekcie takéhoto signálu by prerušili spojenie UAV s ovládačom. Od toho bodu systém detekcie a ochrany splnil svoju úlohu a situáciu môžu prevziať letiskové orgány.

Poďakovanie

Článok je publikovaný ako jeden z výstupov projektu Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky **KEGA 040ŽU-4/2022** *Transfer progresívnych metód vzdelávania do študijného programu "Technológia údržby lietadiel" a "Letecká doprava"*.

Referencie

California Institute of Technology; 2022. Global Radio Frequency Interference, SMAP, <https://smap.jpl.nasa.gov/rfi>.

Coudé, R.; 2020. Radio Mobile WEB Site, <https://www.ve2dbe.com/english1.html>.

Del Barrio A. A. et al.; 2023. HackRF + GNU Radio: A software-defined radio to teach communication theory,

International Journal of Electrical Engineering & Education, 60, 1, pp. 23–40, <10.1177/0020720919868144>.

Ioannides, R. T.; Pany, T.; Gibbons, G.; 2016. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques, Proceedings of the IEEE, 104, 6, pp. 1174–1194, <10.1109/JPROC.2016.2535898>.

Khan, A. K.; 2023. Uncovering Unauthorized Flights: Utilizing the HackRF One for Drone Detection and Identification, <://khandronesorigin.com/2023/01/23/uncovering-unauthorized-flights-utilizing-the-hackrf-one-fordrone-detection-and-identification>.

Kováčik, Ľ.; Novák, A.; Lusiak, T.; 2019. MEASUREMENT OF GNSS INTERFERENCE AT AIRPORT ZILINA, AER, 13/2, pp. 6, <10.26552/aer.C.2019.2.1>.

Kraus, J. et al.; 2020. Jamming of GNSS Receiver on B737 MAX Aircraft and Its Impact on ADS-B Technology, New Trends in Civil Aviation (NTCA), pp. 123–128. <10.23919/NTCA50409.2020.9290995>.

Mašková, K.; 2016. Metody vědecké práce; Výběr metod vědecké práce pro zpracování ZP; Stylizace textu, <https://docplayer.cz/845346-Tematicky-blok-4metody-vedecke-prace-vyber-metod-vedecke-prace-pro-zpracovani-zp-stylizace-textu.html>.

Mitola, J.; 1993. Software radios: Survey, critical evaluation and future directions, IEEE Aerospace and Electronic Systems Magazine, 8/ 4, pp. 25–36, <10.1109/62.210638>.

Novák, A.; Jůn, F.; Škultéty, F.; Sedlačková, A. N.; 2019. Experiment Demonstrating the Possible Impact of GNSS Interference on Instrument Approach on RWY 06 LZZI, Transportation Research Procedia, 43, pp. 74–83, <10.1016/j.trpro.2019.12.021>.

Sekera, J.; Novák, A.; 2021. The future of data communication in Aviation 4.0 environment. In: Incas Bulletin, vol. 13, no. 3, doi:10.13111/2066-8201.2021.13.3.14.