

Dejan V. Kožović*
Dragan Ž. Đurđević**

UDK 005.334:656.7
007.5:528.28]:004

DOI: 10.5937/MegRev2103281K
Pregledni naučni članak
Primljen 08.03.2021.
Odobren 24.03.2021.

SPUFING U CIVILNOJ AVIJACIJI: BEZBEDNOST I SIGURNOSNOST GPS/GNSS I ADS-B SISTEMA

Apstrakt: Avio sistemi koji se oslanjaju na tehnologiju satelitskog pozicioniranja poput GNSS i ADS-B, mogu biti meta spufing napada – sofisticiranog i veoma opasnog oblika radio-frekvencijskih interferencija u kome se u prijemnik “žrtve” ubacuju lažni signali u cilju pogrešnog pozicioniranja ili vremenskog određenja. Iako je spufing u civilnoj avijaciji potencijalna pretnja, njihova tehnička izvodljivost je realna, a primena spufinga postaje fleksibilnija usled veoma brzog napretka jeftinih SDR platformi. Naročito, realan rizik predstavljaju potencijalni napadi koji bi se mogli ostvariti iz vazduha, upotrebom bespilotnih letilica/dronova, u cilju otmice ili distrakcije bezbednosti u nadzoru vazdušnog prostora. Ipak, avijacija nije bezočno izložena spufing napadima bez ikakve odbrane; primenom određenih metoda/tehnika, spufing može biti ublažen u GNSS prijemniku. Takođe, i piloti su sposobljeni za detekciju i rešavanje problema u svakoj fazi leta. Svakako, zbog mogućih sofisticiranih oblika terorističkih napada, međunarodne organizacije, kao što su ICAO i EUROCA, proaktivno se bave povećanjem robustnosti GNSS i ADS-B sistema na spufing. S obzirom na značaj teme i činjenicu da testiranje spufinga/antispufinga ima izvesna ograničenja, razmatranje specifičnosti i različitih scenarija ovih napada, veoma su važni kod razvoja novih metoda za njihovo ublažavanje i detekciju. Ovaj rad fokusiran je na spufing/antispufing GNSS i ABS-B sistema u civilnoj avijaciji i daje pregled najnovijih istraživanja iz ovih oblasti.

Ključne reči: civilna avijacija, GPS/GNSS, ADS-B, radio-frekvencijske smetnje, bezbednost, spufing, antispufing metode

* Student doktorskih studija Megatrend univerziteta, Fakultet za kompjuterske nauke, Beograd; dejankozovic@gmail.com

** Vanredni profesor, Fakultet za civilno vazduhoplovstvo, Megatrend univerzitet, Beograd; djurdjevic.dragan@gmail.com

1. Uvod

Savremeni vazduhoplovni sistem, tj. civilna avijacija i kontrola letenja (*Air Trafic Control*, ATC), neraskidivo su povezani s različitim sistemima za komunikaciju, kontrolu i navigaciju, baziranih na upotrebi bežičnih tehnologija, a koje su veoma važni za bezbedno i sigurno funkcionisanje ovog, veoma kompleksnog sistema. Tako, upotreba ADS-B (*Automatic Dependent Surveillance – Broadcast*) bežičnog komunikacionog protokola, odnosno GNSS (*Global Navigation Satellite System*), kao sastavnog dela ADS-B, omogućava emitovanje statusnih podataka o vazduhoplovu, zatim, primarni (*Primary Surveillance Radar*, PSR) i sekundarni (*Secondary Surveillance Radar*, SSR) radari za nadzor omogućavaju lociranje vazduhoplova obezbeđujući relevantne informacije kontrolorima letenja, dok bežični sistem TCAS (*Traffic Alert and Collision Avoidance System*), nezavisno od ATC, detektuje i upozorava na potencijalne kolizije vazduhoplova s drugim vazduhoplovom u vazduhu. Zatim, avioni najčešće poseduju¹ ACARS (*Aircraft Communications, Addressing and Reporting System*), a to je sistem koji koristi radio-frekventne kanale za komunikaciju, omogućavajući slanje automatizovanih poruka u oba smera, avionima, avio-kompanijama i drugim entitetima avio sistema. I drugi radio navigacioni sistemi, kao što su VOR (*VHF Omnidirectional Radio Range*), DME (*Distance Measuring Equipment*) i ILS (*Instrument Landing System*), imaju ključne uloge u različitim fazama leta vazduhoplova.

Avio sistemi, koji su bazirani na satelitskim tehnikama navigacije, kao što je GPS (*Global Position System*), tj. GNSS ili ADS-B, s obzirom na to da imaju veoma jednostavan bezbednosni protokol, koji ne obezbeđuje autentifikaciju i enkripciju podataka, ranjivi su na različite vrste sajber napada, kao npr. radio-frekvencijske interferencije (*radio frequent interference*, RFI). Jedan od oblika namernih RFI, ali veoma opasan i štetan po sistem, jeste tzv. spufing (*spoofing*). U spufingu, predajnik u blizini, šalje lažni GPS signal ciljanom prijemniku, u cilju produkcije lažnih informacija (pogrešnog pozicioniranja ili vremenskog određenja). Pri tome, ukoliko prijemnik nema mogućnost razlikovanja autentičnih signala od lažnih, onda ne može ni upozoriti korisnika na nepouzdana navigaciona rešenja. Za implementaciju spufinga, može se npr. koristi jeftini i široko dostupni spufing uređaj –*Software Defined Radio*, SDR², koji upršćeno rečeno, „može naterati pametni telefon da misli da je na Mont Everestu”³.

¹ Manji avioni, koji se koriste u privatnoj avijaciji, nemaju ACARS, ali su oni opremljeni elektronskim uređajima – transponderima, koji omogućavaju prenošenje informacija i dobijanje odgovora na upite sa radara ATC-a; pri tome, veliki deo ove komunikacije je automatizovan.

² SDR je softverski definisani radio, tj. sistem za komunikaciju kod koga funkcije kao što su: podešavanje, filtriranje, modulacija/demodulacija, umesto hardvera, obavlja softver, a kao rezultat napretka digitalne elektronike. Dostupnost i kontinuirano smanjenje cena SDR, utiču na konstantni porast upotrebe ovih uređaja.

³ Simsky Maria: „What is spoofing and how can you ensure GPS security?”, Aerospace testing international, 30 October 2019 [online];

Dakle, u spufing napadu emituju se lažni signali, koji oponašaju originalne satelitske signale, ali su oni veće snage i različitog vremenskog kašnjenja u odnosu na autentične signale. Prenošenje lažnih GPS signala do prijemnika, može dovesti do toga da se prijemnik "zaključa" na ove lažne, umesto na autentične satelitske signale, a ukoliko se navigacioni sistem oslanja na GPS za pozicioniranje sistema, onda je GPS spufing veoma pogodan način za njegovo efikasno preuzimanje.

Do nedavno, stav civilne avijacije u vezi sa npr. GNSS spufingom bio je jednostavan⁴: "To nije naš problem", i smatralo se da je ovo pitanje u delokrugu vojnih struktura. Međutim, kako se sve više pažnje posvećuje uobičajenim RFI, tako se i pristup spufingu menja, što je i delimično inicirano incidentom,⁵ koji se dogodio 2010. godine na Hanoverskom aerodromu, a koji je bio uzrokovan radio-frekvencijskim interferencijama GPS repetitora i tako neadekvatnim pozicioniranjem ovog sistema. Danas je poznato da postoji čitav niz međufaza spufinga, od pogrešno podešenih repetitora, pa sve do onoga što bi mogla urediti neka vešta, ali nerazumna osoba korišćenjem jeftinih i široko dostupnih spufing uređaja (*spoofing devices*), kao što je SDR.

Postoje različite vrste spufing napada na GPS/GNSS i ABS-B, a njihova klasifikacija i specifičnosti pojedinačnih slučajeva, moraju se uzeti u obzir pri analizi i simulaciji spufinga, kao i testiranju performansi predloženih anti-spufing tehnika. Pri tome, efikasnost predložene anti-spufing metode dominantno zavisi od nivoa sofisticiranosti korišćenog spufing uređaja.

Kada se analiziraju različiti scenariji spufinga, osim onih koji se izvode sa zemlje, veoma su važni i potencijalni spufing napadi, koji bi se mogli ostvariti iz vazduha, upotrebom bespilotnih letilica (*Unmanned Aerial Vehicle*, UAV), odnosno dronova. Upotreba UAV eksponencijalno raste, a konstantni tehničko/tehnološki napredak autonomnih sistema za njihovu kontrolu, rezultirao je i u porastu broja akcidenata i opasnih situacija.⁶ Tako, korišćenje UAV/dronova i GPS-a za njihovu navigaciju, utiče na to da ovi sistemi budu zanimljive mete napada u cilju otmice ili distrakcije bezbednosti/sigurnosti u nadzoru vazdušnog prostora. Navigacione performanse bespilotnih letilica mogu biti ograničene, usled, između ostalog, spufinga, u kome napadač, proizvoljnom manipulacijom signala, može „naterati“ UAV da skrene sa postojeće putanje, i dovede je do ciljne tačke, a koju je on odredio. U hipotetičkoj borbenoj situaciji, manipulacija GPS prijemnikom

<https://www.aerospacetestinginternational.com/features/what-is-spoofing-and-how-can-you-ensure-gps-security.html>(20.12.2020.)

⁴ Berz Gerhard: „GNSS spoofing and aviation: An evolving relationship”, *Inside GNSS*, 25 September 2018 [online];<https://insidegnss.com/gnss-spoofing-and-aviation-an-evolving-relationship/> (20.12.2020.)

⁵ Steindl Eduard *et al.* (2013): „The impact of interference caused by GPS repeaters on GNSS receivers and services,” Proceedings of the European Navigation Conference (ENC),Vienna, 2013; GMCA 641613 White Paper (2015), DW/02/001/096/032/1.0

⁶ Gaspar João *et al.* (2020): „Capture of UAVs through GPS spoofng using low-cost SDR platforms,” *Wireless Personal Communications* 115/2020, 2729–2754.

protivnika, značilo bi preuzimanje kontrole nad UAV ili uređajima koji se oslanjaju na GPS pozicioniranje. Na primer, u oktobru 2018. Rusija je optužila SAD da su lažirale dron i preusmerile ga na napad na rusku vazduhoplovnu bazu u Siriji.³ Takođe, u poslednjih nekoliko godina, zabeleženi su brojni spufing incidenti u morima blizu ruske granice, a pretpostavlja se da su dronovi „transportovani“ do obližnjih aerodroma. Ova vrsta spufinga možda je bila odbrambeni mehanizam za prizemljenje špijunskih dronova. Naime, većina poluprofesionalnih bespilotnih letelica na tržištu, ima ugrađeni mehanizam „geo-grade“ (*built-in geo-fencing mechanism*), koji ih automatski spušta na zemlju ukoliko se približe aerodromima, ili drugim područjima sa restriktivnim prilazom.

Svakako, uloga koju GNSS tehnologija ima konstantno raste, usled porasta upotrebe UHV/dronova, zbog čega će novi koncepti navigacije i ATC-a biti neophodni u situaciji „prepunog neba“, gde će milioni dronova deliti vazdušni prostor sa vazduhoplovima sa posadom; u svetu ovoga, *Free Route Airspace* (FRA) jeste primer perspektivnog koncepta.⁷ Takođe, istraživački projekat *OpenSky Network* prikuplja izveštaje ADS-B i čini ih dostupnim za bezbednosno/sigurnosne analize, razvoj tehnika detekcije spufing napada, kao i lociranja spufing uređaja/izvora⁸.

Iako su različiti delovi avio sistema izloženi različitim napadima, a potencijalno i spufingu, postoje određena sigurnosna rešenja i protokoli, a različite radne grupe, konferencije i organizacije, kao što su ICAO (*International Civil Aviation Organization*), RTCA (*Radio Technical Commission for Aeronautics*) i EUROCAE (*European Organization for Civil Aviation Equipment*), kontinuirano analiziraju i prate razvoj efikasnih antispufling detekcionih metoda/tehnika i njihovu integraciju u sisteme kontrole letenja, komunikacije i navigacije. Na primer, RTCA je kao jedan od ciljeva u vezi sa vazduhoplovnom opremom sledeće generacije, postavila povećanje bezbednosne sigurnosti GNSS-a na rizike u prisustvu RFI, uključujući i spufing. Aktuelni pravci u rešavanju spufinga od strane RTCA i EUROCAE prvenstveno se odnose na uvođenje novih zahteva za detekciju spufinga GNSS-a, što omogućava korišćenje alternativne navigacione opreme, bez značajnijih bezbednosnih rizika⁹.

⁷ Nava-Gaxiola Cesar, Barrado Cristina, Royo Pablo (2018): „Study of a Full Implementation of Free Route in the European Airspace”, Proceedings of the 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), London, UK, 23–27, September, 2018.

⁸ Jansen Kai *et al.* (2017): „Localization of spoofing devices using a large-scale air traffic surveillance system”, ASIA CCS ’17, April 02–06, 2017, Abu Dhabi, United Arab Emirates.

⁹ Hegarty Christopher *et al.* (2018): „Spoofing detection for airborne GNSS equipment”, in Proceedings of 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, FL, 2018, 1350-1368;

2. Spufing u avijaciji – definicija i vrste

Global Positioning System (GPS) je satelitska navigacija, tj. konstelacija satelita koji emituju radio-frekventne talase u cilju preciznog određivanja pozicije na/u blizini površine Zemlje. Najpre je korišćen u vojne svrhe (od 50.-ih godina XX veka), a kasnije (80.-ih godina XX veka) GPS je stavljen na raspolaganje i za široku, civilnu upotrebu. Zajednički termin za različite tipove globalno korišćenih satelitskih navigacionih sistema je GNSS (*Global Navigation Satellite System*), kao što su GPS (SAD), GLONASS (Rusija), Galileo (Evropa), BEIDOU (Kina), itd. GPS/GNSS je sistem koji pilotima, kao i vazduhoplovnim sistemima, daje precizne informacije o poziciji vazduhoplova, kao i referentnom vremenu. Iako je GPS jedini potpuno operativan GNSS "prve generacije", dostupan je i ruski Globalni navigacioni satelitski sistem (GLONASS), koji obuhvata Rusiju, i susedne zemlje, dok Evropa razvija GNSS "druge generacije", pod nazivom Galileo program, a koji je 2003. godine potpisala i Kina. Danas, GNSS je dopunjena sa nekoliko dodatnih satelitskih sistema, generički nazvanih *Space Based Augmentation Systems* (SBAS)¹⁰, jer emituju dodatne signale koje određeni prijemnik može dekodirati i koristiti (zajedno sa globalnim GNSS signalima) u cilju unapređenja performansi pozicioniranja.

Iako GNSS tehnologija nije jedino sredstvo navigacije u civilnom vazduhoplovstvu i ATC, njena uloga konstantno raste, kako u generalnoj avijaciji, tako i kod upotrebe bespilotnih letelica (dronova), za čije upravljanje su neophodne informacije o položaju, brzini i vremenu, a koje se dobijaju od GNSS-a.

Međutim, sistemi koji se oslanjaju na tehnologiju satelitskog pozicioniranja poput GPS/GNSS mogu biti meta, tzv. spufing napada, u cilju generisanja pogrešnog pozicioniranja ili vremena, a koji se ostvaruje tako što se u prijemnik "žrtve" ubacuju lažni signali. To nas dovodi do napadača, koji pokušava da ubaci lažne informacije o pozicioniranju u sisteme koji na primer, omogućavaju navigaciju aviona.

Zbog svega toga, u vremenu koje dolazi, biće neophodni novi koncepti navigacije i ATC-a. Jedan od najznačajnijih koraka u modernizaciji kontrole letenja jeste prelazak na ADS-B bežični komunikacioni protokol. Funkcioniše samostalno, a s obzirom da je njegov sastavni deo GNSS, ADS-B sistem zavisi od preciznosti sistema za pozicioniranje. ADS-B standard reguliše razmenu emitovanih poruka između vazduhoplova i ATC zemaljskih stanica.¹¹ ADS-B sistem automatizovano dostavlja neophodne podatke korisnicima (i na zemlji, i u vazduhu). Može da radi kao predajnik (*ADS-B Out*) ili prijemnik (*ADS-B In*). Funkcija "*ADS-B In*" je opcionalna usluga, koja omogućava da vazduhoplov prima podatke,

¹⁰ Space Based Augmentation Systems (SBAS) [online]; https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/factsheets/media/SBAS_Worldwide_QFact.pdf (20.12.2020).

¹¹ Pavić Aleksandar, Lalić Batrić, Đurđević Miloš (2014): „Osnove ADS-B tehnologije i osmatranje područja Republike Srbije bez radarske pokrivenosti”, INFOTEH-JAHORINA 13/2014, 419-424.

koji se prikazuju na CDTI (*Cockpit Display of Traffic Information*) interfejsima (najčešće, MFD (*Multifunction Display*) i EFB (*Electronic Flight Bag*) uređaji), a koje emituju drugi vazduhoplovi iz relativno bliskog okruženju. Iste informacije koriste se i za TCAS (*Traffic Collision Avoidance System*) sisteme. U okviru "ADS-B Out" sistema, vrši se predaja statusnih informacija o vazduhoplovu.¹²

Pored prednosti, ADS-B sistem ima i određene nedostatake, kao što su zavisnost od sistema satelitske navigacije i veoma jednostavan bezbednosni protokol, koji ne obezbeđuje enkripciju i autentifikaciju podataka: ADS-B poruke se emituju na jednostavan način i u "otvorenom" formatu, bez potvrde identiteta, tj. bez dokaza da signal dolazi od pouzdanog (autorizovanog) entiteta, a ne od neovlašćenog. Sve ovo povećava ranjivost ADS-B sistema na različite vrste sajber napada, kao npr. radio-frekvencijske interferencije, uključujući i one koje mogu biti namerno izazvane, kao što je spufing.

Analiza ranjivosti i uticaja koji različiti sajber incidenti, kao i spufing, mogu imati na avio sistem nije jednostavna^{13,14}, iako su npr. predočene slabosti ATC sistema, uvođenjem "aviona-duha" u sistem kontrole letenja, imitiranjem ADS-B signala, korišćenjem jeftine tehnologije, uređaja i softvera¹⁵, zatim, pokazano je da su radio navigacioni sistemi, kao što su GPS¹⁶ i ILS¹⁷ podložni spufing napadima, kao i da se spufingom TCAS poruka, mogu kreirati lažne poruke *resolution advisories*, a što primorava pilota da pribegne manevrima izbegavanja sudara¹⁸. Uzimajući u obzir da verovatno postoje i incidenti koji nisu javno dostupni, sagleđivanje njihovog uticaja na avio sistem, donekle se dovodi u pitanje.

Svakako, RFI, mogu degradirati civilne GNSS signale i servise. Predstavljaju realnu opasnost, s obzirom na konstantni porast upotrebe IoT (*Internet of*

¹² ADS-B transpornder vrši predaju podataka o stanju vazduhoplova nezavisno i periodično, tj.u tačno definisanim periodima, za razliku od sekundarnog radara kod koga transponder odgovara samo po zahtevu sekundarnog radara.

¹³ Kožović Dejan (2019): „Uloga i značaj sajber bezbednosti u vazduhoplovstvu”, *Master rad*, Fakultet za civilno vazduhoplovstvo, Megatrend univerzitet, Beograd.

¹⁴ Kožović Dejan, Đurđević Dragan (2019): „Sajber bezbednost u avijaciji”, *Megatrend revija* 16(2)/2019, 39-56.

¹⁵ Costin Andrei, Francillon Aurélien (2012): „Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices”, *Black Hat USA* 2012, 1-12. https://www.researchgate.net/publication/267557712_Ghost_in_the_AirTraffic_On_insecurity_of_ADS-B_protocol_and_practical_attacks_on_ADS-B_devices (5.03.2021.)

¹⁶ GPS (1995): „Global positioning system standard positioning service signal specification”. (Technical Report.Global Positioning System); <http://www.gps.gov/technical/ps/1995-SPS-signal-specification.pdf>(15.12.2020.)

¹⁷ Sathaye Harshad *et al.*(2019): „Wireless attacks on aircraft instrument landing systems”, 28th USENIX Security Symposium, August 14–16, 2019, Santa Clara, CA, USA, 1-16.

¹⁸ Pierpaoli Pietro, Egerstedt Magnus, Rahmani Amir (2015): „Altering UAV flight path by threatening collision”, Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th (2015), IEEE, 4A4-1-4A4-10.

Things) uređaja¹⁹(internet stvari), GNSS repetitora, jeftinih SDR kartica, i očekivanu, širu upotrebu sofisticiranijih spufing uređaja u budućnosti.

Zbog svega toga, zaštita od RFI, predmet je konstantnog razmatranja regulatornih tela na nacionalnom, kao i međunarodnom nivou, koja se bave ispitivanjem RFI, postavljanjem smernica i definisanjem novih standarda za sledeću generaciju avionike.

2.1. Definicija spufinga

Međunarodna telekomunikaciona unija (*International Telecommunication Union*, ITU), definiše RFI kao „uticaj neželjene energije izazvane emisijom ili kombinacijom emisije, zračenja ili indukcije na prijemnik radiokomunikacionog sistema, manifestovan pogoršanjem performansi, pogrešnim tumačenjem ili gubitkom informacija²⁰. Ova definicija implicitno uključuje i najštetnije oblike RFI, a to su ometanje (*jammering*) i lažno predstavljanje (*spoofing*).

Ometanje označava emisije koje ne imitiraju GNSS signale, već ometaju prijemnik, tj. smanjuju sposobnost prijemnika da prima i prati GNSS signale, dok spufing označava emitovanje signala sličnih GNSS signalima, koji se mogu prikupljati i pratiti u kombinaciji sa legitimnim signalima, ili umesto njih. Prema tome, spufing je mnogo suptilniji i opasniji oblik pretnje na GNSS, jer se, u ovom slučaju, u prijemnik „žrtve“ ubacuju/podmeću lažni signali u cilju pogrešnog pozicioniranja ili vremenskog određenja.

Zavisno od definicije, spufing se može razmatrati ili kao poseban oblik ometanja radio frekvencije, ili kao potpuno zasebna kategorija. Međutim, danas je linija razdvajanja između spufinga i RF ometanja sve nejasnija, s obzirom na to da neki spufing napadi mogu dovesti do prestanka rada prijemnika, tj. „zaključavanja“ prijemnika usled anomalija u podacima, iako nema RF preopterećenja.

S obzirom na strukturu GPS signala (javan je i za razliku od vojnog GPS signala, nije šifrovan i entifikovan),^{21,22} spuferu ne bi bilo teško/skupo da izgradi sistem za kreiranje signala, koji se mogu primaocu podmenuti kao autentični satelitski signali. Kao što je pomenuto, prenošenjem ovih lažnih signala na prijemnik, može doći do zaključavanja prijemnika na lažne signale, umesto na autentične satelitske signale.

¹⁹ Stevanović Miroslav, Đurđević Dragan (2016): „Internet stvari, lična i materijalna bezbednost”, *Bezbednost* 3/2016, 113-128

²⁰ International Telecommunication Union, „Radio Regulations Articles – Volume 1,” ITU, 2016

²¹ Tippenhauer Nils Ole *at al.* (2011): „On the requirements for successful GPS spoofing attacks”, Proceedings of the ACM Conference on Computer and Communications Security, Chicago, IL. Association for Computing Machiner, 2011, 75-86.

²² Warner Jon, Johnston Roger (2002): „A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing”, *Journal of Security Administration* 25(2)/2002, 19-27.

Takođe, s obzirom na to da ADS-B poruke nisu enkriptovane, spufer može emitovanjem lažnih signala, koji oponašaju autentične satelitske signale, ali veće snage i različitog vremenskog kašnjenja u odnosu na autentične signale, značajno degradirati vazduhoplovni sistem. Kao rezultat ovog sufing napada, vazduhoplovi će biti izmešteni, tj. slaće putem ADS-B pogrešne informacije o svom položaju.²³

Radiofrekvencijske smetnje GPS/Galileo/GNSS-a, bile su predmet proučavanja od početka razvoja i primene GPS,²⁴ a 2001. godine, Ministarstvo za saobraćaj SAD izvršilo je opsežnu analizu i procenu uticaja poremećaja GPS-a u kritičnim primenama, uključujući i avijaciju, što je dovelo do porasta svesti o značaju i posledicama takvih poremećaja. U njihovom izveštaju, poznatom kao Volpeov izveštaj,²⁵ spufing je identifikovan kao mnogo opasniji oblik RFI od namernog ometanja, jer kod spufinga, ciljani prijemnik ne može otkriti napad, a tako ni upozoriti korisnike na nepouzdana navigaciona rešenja. Štaviše, i ako nije u potpunosti uspešan, spufing injektira štetne informacije i prouzrokuje značajne PVT (položaj, brzina, vreme) greške.

Zbog svega toga, spufing u avijaciji zaokuplja sve veću pažnju istraživača iz oblasti sajber bezbednosti, naročito zbog toga što primena spufinga postaje sve fleksibilnija i jeftinija²⁶ usled veoma brzog napretka SDR tehnologija. U poslednjoj deceniji, teorijsko i eksperimentalno ispitivanje spufinga, predmet je interesovanje brojnih istraživača i stručnjaka iz oblasti avijacije, koji se, između ostalog, bave i razvojem metoda/tehnika za detekciju i ublažavanje spufing napada, a sve u cilju povećanja sigurnosti/bezbednosti sistema vazdušnog saobraćaja.

2.2. Klasifikacija spufing napada u avijaciji

Iako se mora uzeti u obzir da postoje brojni, različiti oblici spufing napada, svršishodno je definisati tipične/reprezentativne oblike spufinga, a u cilju njihove analize, simulacije i testiranja. Na primer, spufing napadi mogu se klasifikovati na osnovu karakteristika spufinga, na sinhronizovane (napad u kome je lažni signal sinhronizovan sa autentičnim GNSS signalima) i nesinhronizovane,

²³ Wang Jing, Zou Yunkai, Ding Jianli (2020): „ADS-B spoofing attack detection method based on LSTM”, *EURASIP Journal on Wireless Communications and Networking* 160/2020, 1-12.

²⁴ Parkinson W. Bradford, Spilker J. James (1996): *Global positioning system: theory and Application*, Vol.I, American Institute of Aeronautics and Astronautics, Washington, DC.

²⁵ John A. Volpe National Transportation Systems Center (2001): „Vulnerability assessment of the transportation infrastructure relying on the global positioning system”. Final Report, 6-88, August 29, ES3; https://rntfnd.org/wp-content/uploads/Vople_vulnerability_assess_2001.pdf(20.12.2020.)

²⁶ Olson Parmy (2015): „Hacking a phone’s GPS may have just got easier,” *Forbes*, 7 AUG 2015. [Online]; <https://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/?sh=b1abbfb4efbf>(15.12.2020.)

zatim, prema nivou složenosti²⁷, na pojednostavljene, intermedijerne i sofistickane, kao i prema intenciji napada (spufing napadi S1–S7, Tabela 1).²⁸

Osobine različitih spufing napada, koji su klasifikovani prema nivou složenosti su sledeće:

Pojednostavljeni spufing napadi. Kod najjednostavnijeg oblika spufing napada, koristi se neka vrsta GNSS simulatora za dobijanje falsifikovanih GNSS signala. Prijemnik (u modu praćenja), može dobiti lažni signal kada izgubi prijem signala sa satelita, tako da se može "zaključati", odnosno preći na režim prijema spufing signala. Potencijalno, ometač bi mogao dovesti do toga da prijemnik izgubi "zaključani" signal sa satelita, i tako prouzrokuje ponovnu reaktivaciju satelita. Signali se najčešće ne sinhronizuju sa originalnim signalima, što omogućava upotrebu jednostavnih COTS²⁹ komponenata. Detekcija ove vrste spufinga je relativno jednostavna – zbog odsustva sinhronizacije signala, dolazi do naglog porasta izlaznih signala koji se odnose na položaj prijemnika i vreme. Pored toga, ukoliko su spufing signali velike jačine, prijemnik za monitoring, potencijalno može detektovati povećanu aktivnost u GNSS frekvencijskim opsezima.

Intermedijerni spufing napadi: Kod intermedijernog spufing napada, za razliku od pojednostavljenih, falsifikovani GNSS signali su sinhronizovani sa originalnim GNSS signalima koji dolaze sa satelita. Takav napad uključuje i poznatu lokaciju (i putanju) "napadnutog" prijemnika, relativno u odnosu na antenu prijemnika, kako bi se obezbedilo da se lažni, pseudo-opseg signala, "poravna" sa autentičnim kodovima na poziciji napadnutog prijemnika. Kada je prijemnik u režimu praćenja, a na početku napada, lažni signali su dovoljno dobro usklađeni sa autentičnim, tako da srufer može preuzeti kontrolu, postepenim povećanjem snage i sukcesivnim podešavanjem signala. Detekcija na ciljanom prijemniku je gotovo nemoguća, osim, kada se za procenu smera dolaska signala, koristi veći broj antena.

Sofisticirani spufing napadi: Sofisticirani spufing jeste kompleksnija verzija intermedijernog spufinga. Kod ovog napada, mogli bi se koristiti višestruko koordinisani „intermedijerni sruferi“ za repliciranje sadržaja i "poravnjanje" GNSS

²⁷ Humphreys E. Todd *et al.* (2008): „Assessing the spoofing threat: development of a portable GPS civilianspoofers”, Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savanna, GA, September 16-19, 2008, 2314-2325.

²⁸ Fernández-Hernández Ignacio *et al.* (2019): „Increasing international civil aviation resilience: a proposal for nomenclature, categorization and treatment of new interference threats,” in Proceedings of ITM 2019: International Technical Meeting of The Institute of Navigation, Reston, Virginia (USA), January 28-31, 2019, 389-407.

²⁹ COTS – softverski i hardverski proizvodi, napravljeni i dostupni za široku upotrebu/ prodaju; dizajnirani su tako da se jednostavno implementiraju u postojeće sisteme, bez potrebe za prilagođavanjima (na primer, Microsoft Office je COTS proizvod, tj. „upakovano“ softversko rešenje za kompanije).

signala, kao i njihovu prostornu raspodelu. Zbog toga, ovaj oblik spufinga je teže detektovati. Međutim, ovde, kao i kod intermedijernog spufing napada, prijemnik za nadzor na drugoj lokaciji (alociran) će verovatno imati nagli porast vrednosti izlaznih signala koji se odnose na položaj prijemnika i vreme, s obzirom na to da se njegov položaj razlikuje od položaja ciljanog prijemnika. Takođe, ukoliko su spufing signali velike jačine, onda alocirani nadzorni prijemnik potencijalno može detektovati povećanu aktivnost u GNSS frekvencijskim opsezima.

Kategorizacija spufing napada²⁸, a koja ne samo da uzima u obzir osobine spufinga, već razmatra i intenciju spufera, praveću razliku između kolateralna, ciljanog i sofisticiranog spufing napada, data je u Tabeli 1. Izraz kolateral koristi se kada vazduhoplov nije namerna meta ometanja, a lažni signali (njihov položaj, snaga, itd.), najverovatnije nisu usklađeni s originalnim signalima prijemnika (antena), zbog čega se očekuje nagli porast/smanjenje položaja, opsega i jačine signala. Izraz ciljani, koristi se kada su emisije namenjene da naročito utiču na jedan ili više vazduhoplova. U ovom slučaju, ometajući signali su usklađeni („poravnati”) sa autentičnim signalima, tako da greške na prijemniku nisu lako uočljive. Izraz sofisticirani koristi se kada se ometajući signali veoma teško detektuju, kao npr. u slučaju višestrukih signala koji dolaze iz različitih pravaca.

Klasifikacija spufinga data u Tabeli 1 (spufing napadi S1-S7), a s obzirom na deklarisanje mete spufing napada, veoma je značajna i ima za cilj podsticanje tehničke diskusije o načinima implementacije spufinga u postojeće avio standarde, i naročito u postupcima analize/provere GNSS prijemnika.

Tabela 1. Kategorizacija spufing napada

Vrste spufinga
S1 – Ponavljanja (<i>Repeaters</i>)
S2 – Pogrešni signali (<i>Errant Signals</i>)
S3 – Kolateralni spuferi –Simulatori (<i>Collateral Spoofer – Simulators</i>)
S4 – Kolateralni re-emitujući spuferi (<i>Collateral Re-radiating Spoofer</i>)
S5 – Ciljani spuferi – Simulatori (<i>Targeted Spoofer – Simulators</i>)
S6 – Ciljani re-emitujući spuferi (<i>Targeted Re-radiating Spoofer</i>)
S7 – Ciljani sofisticirani spuferi (<i>Target sophisticated spoofers</i>)

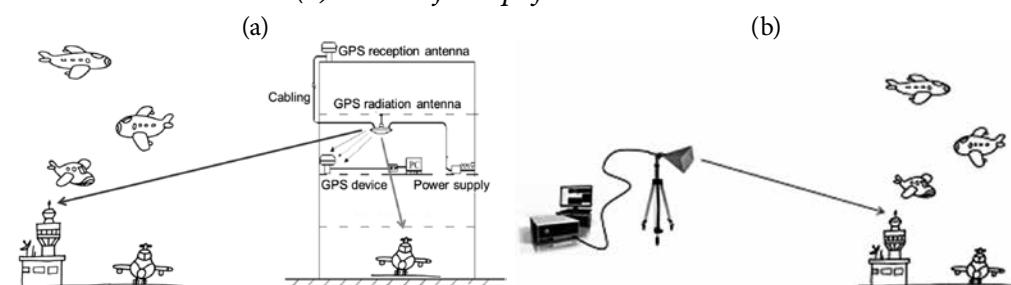
Izvor: Fernández-Hernández *et al.* (2019): “Increasing international civil aviation resilience: a proposal for nomenclature, categorization and treatment of new interference threats,” in Proceedings of ITM 2019: International Technical Meeting of The Institute of Navigation, Reston, Virginia (USA), January 28-31, 2019, p. 392

Tako^{28,30}, spufing napad S1 – Spufing ponavljanjem (*repeaters*) (slika 1a), odgovara pojednostavljenom spufing napadu. Na primer, pogrešno postavljeni ili pogrešno konfigurisani Galileo/GPS/GNSS repetitor koji se koristi za akviziciju signala prijemnika u aerodromskim hangarima, daju signale, koji mogu

³⁰ Turner Michael *et al.* (2020): „Spoofing detection by distortion of the correlation function”, Conference: 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), 566-574.

spufovat prijemnike aviona. Ili, S5 spufing napad (slika 1b), odgovara intermedijernom spufing napadu, čija je svrha spufing avionskih prijemnika, zbog čega emitovani signali moraju biti usaglašeni sa onim koje vazduhoplov prati. Inicialno, mogu imati usklađene greške u pozicioniranju, a prethodi im ometanje kako bi se prijemnik "prebacio" na spufovane signale. U ovu kategoriju spadaju sruferi koji unose netačne ili nevažeće digitalne podatke, što može rezultirati nizom efekata, od pogrešnih PNT (Position Navigation Time) do neadekvatnog rada prijemnika. Efekat napada može biti trenutan ili odložen, ali i dugotrajan. Ovaj spufing ograničen je na srufere koji koriste jedan predajnik, a koji je napravljen ili nabavljen sa ograničenim/jeftinim resursima i opremom.

Slika 1. Različite vrste spufing napada: (a) S1- Spufing ponavljanjem i (b) S5 – Ciljani sruferi – Simulatori



Izvor: Turner Michael *et al.* (2020): „Spoofing detection by distortion of the correlation function”, Conference: 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 568

Ovakva i slične klasifikacije spufinga i njihova analiza, predstavljaju okosnicu za razvoj efikasne analize/provere GNSS prijemnika, tj. postavljanje zahteva, koje mora ispuniti korisnički prijemnik. Potrebno je naglasiti da GNSS nije jedino sredstvo navigacije u civilnom vazduhoplovstvu i da piloti/avioni potrebne informacije dobijaju i od drugih sistema za navigaciju, kao i od vizuelnih referenci. Stoga, čak i u slučaju uspešnog sofisticiranog GNSS spufinga, koji nije ublažen u GNSS prijemniku, u većini situacija, pilot može ublažiti efekte spufinga, tj. značajno smanjiti njegovu efikasnost.

Kategorizacija i opisi mogućih spufing napada, koje su detaljno dati u rado-vima Humphreys i autora²⁷, kao i Fernández-Hernández i autora²⁸, omogućavaju definisanje različitih scenarija za testiranje performansi predloženih anti-spufing tehnika u avijaciji.³⁰ Klasifikacija potencijalnih spufing napada na ADS-B, čiji je GNSS esencijalni deo, data je u delu 3.2.

3. Spufing GPS/GNSS i ADS-B – bezbednosne pretnje

Unapređenje komunikacije korišćenjem vazduhoplovnih mreža, uvođenjem COTS softverskih i hardverskih rešenja u sisteme aviona, kao i enormni porast broja IoT (*Internet of Things*) uređaja¹⁹, je i bezbednosni rizik, s obzirom na to da se integritet avio sistema, između ostalog, može ugroziti aktivnom manipulacijom podataka, tj. njihovim prisluškivanjem, ponavljanjem, brisanjem, ometaњem i spufingom³¹. U ovom radu, razmatraćemo (ne)bezbedne aspekte spufinga u avijaciji, i to naročito GPS/GNSS i ADS-B sistema.

3.1. GPS/GNSS spufing

Zabrinutost i naročitu pažnju u oblasti avijacije izazivaju ranjivosti³² GNSS-a u vezi sa RFI, tj. incidentima nestanka GPS signala u civilnim avionima (naročito u oblastima s političkim tenzijama, kao što je npr. Jugoistočno Sredozemlje, pravci Bliski istok–Kanada i SAD preko Severnog pola kroz ruski vazdušni prostor) ili u blizini određenih aerodroma. Uzroci tome mogu biti različiti, kao npr. solarne oluje, vojne vežbe, itd., ali i namerno izazvani³³

Kao što je naglašeno, spufing je, u odnosu na druge oblike RFI, mnogo supertilniji i opasniji oblik pretnji na GNSS, jer se u prijemnik „žrtve“ ubacuju/podmeću lažni signali u cilju pogrešnog pozicioniranja ili vremenskog određenja. Iako je GNSS spufing potencijalna pretnja – još uvek su retki potvrđeni izveštaji o njihovoj eksplotaciji u civilnoj avijaciji, tehnička izvodljivost spufinga je realna, a potencijal veliki. Istraživanja iz ove oblasti³⁴ pokazuju da je skoro svaki uređaj, koji koristi civilni GPS signal, ranjiv na spufing, a primena spufinga postaje fleksibilnija i jeftinija usled veoma brzog napretka SDR tehnologija/platformi.

Spufing napadi su stvarna pretnja¹⁶, s obzirom na to da, u zavisnosti od položaja satelita i atmosferskih uslova, jačina GPS autentičnog signala može legitimno varirati od 160 dBW do 153 dBW, a već je odnos jačine lažnog (spufovanog) i autentičnog signala od 1.1, dovoljan da „otključa“ prijemnik na spufovane signale. Uočljiva razlika između legitimnih satelitskih signala i spufing signala može biti diskrepanca u vremenu, smeru signala, jačini, Doplerovom pomeraju

³¹ Sampigethaya Krishna *et al.* (2011): „Future e-enabled aircraft communications and security: The next 20 years and beyond”, Proceedings of the IEEE 99(11)/2011, 2040–2055.

³² Morales-Ferre Ruben *et al.* (2019): „A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft”, IEEE Communications Surveys&Tutorials, 22/2019, 249–291

³³ Eurocontrol. EUROCONTROL Voluntary ATM Incident Reporting (EVAIR) safety bulletin 20, 2013–2017; Safety Bulletin 20; EUROCONTROL: Brussels, Belgium; <https://www.eurocontrol.int/publication/eurocontrol-voluntary-atm-incident-reporting-evair-safety-bulletin-20>. (1.02.2021.)

³⁴ Horton Eric, Ranganathan Prakash (2018): „Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter, Journal of Global Positioning Systems 16(9)/2018, 1–11.

ili vrednosti odnosa, signal/šum. Međutim, većina prijemnika nije opremljena za otkrivanje ovih razlika.

Primena AGC³⁵ (*Automatic Gain Control*) za pojačavanje GNSS signala, čime se kompenzuje jačina fluktuirajućeg signala, dovodi i do ranjivosti prijemnika na spufing.³⁶ Takođe, mora se uzeti u obzir i da prijemnik nema mogućnost utvrđivanja odakle dolazi signal (iz lokalno generisanog lažnog ili legitimog izvora) s obzirom na to da se antena prijemnika najčešće nalazi u jednoj tački u prostoru: ako prijemnik nije zaštićen, spufing signal se može direktno ubaciti preko izvora spufinga. Ili, ukoliko spufer poznačuje tačno mesto ciljanog prijemnika, onda se mogu na autentične signale superponirati spufer signali. Alternativno, mogu se koristiti i jači nesinhronizovani signali, ali je ovaj način spufinga efikasan samo onda kada je prijemnik u inicijalnoj fazi rada (prijema) ili u slučaju da je "nasilno otključan" ometajućim signalom.

Slučaj ometanja na Hanoverskom aerodromu, koji se dogodio 2010. godine, jeste primer realnog „nenamernog“ spufinga⁵, a koji pokazuje da je detekcija/trenutno upozorenje na spufing GNSS neophodna protivmera u cilju obezbeđivanja sigurnosti i bezbednosti aerodroma. Naime, avion, koji se nalazio blizu praga piste Hanoverskog aerodroma, a čiji su avio sistemi funkcionali po signalima reperitora za testiranje avioničke poslovnih aviona u hangaru blizu praga piste, imao je prikaz pogrešne GPS pozicije tokom faze taksiranja i poletanja. Ovaj scenario, iako jednostavan, može se koristiti kao polazna tačka za testiranje GNSS prijemnika ili bilo kog hardvera koji zavisi od preciznog pozicioniranja ili podataka o vremenu koje daje prijemnik. Zatim, u toku FAA instaliranja novog sistema za sletanje aviona baziranog na GPS-u, na internacionalnom aerodromu Newark, 2010. godine, uočeno je da su zemaljski GPS prijemnici (korišćeni kao asistencija GPS prijemnicima u avionu, koji je u prilazu), imali i po nekoliko prekida, i to skoro svakoga dana. Višemesecnom FAA istragom utvrđeno je da su ove smetnje bile izazvane³⁷ od *personal protection devices* (PDD). Takođe, ranije je bilo prijavljeno FAA (jul, 2003. godine), da je uključeni mobilni telefon simultano uticao na rad tri različita avionska GPS prijemnika, prouzrokujući kompletan gubitak signala; sva tri GPS prijemnika koristila su tri različite antene,

³⁵ AGC je pojačivač s adaptivnim pojačanjem. Osnovna uloga je usklađivanje amplitute primljenog signala s ulaznim opsegom analogno-digitalnog pretvarača (ADC), kako bi se minimizirali gubici u jačini signala. Kod GNSS prijemnika, signal je veoma slab, i može biti prekriven signalom termalnog šuma. Kod jakih smetnji, amplituda signala se povećavaju, zbog čega AGC smanjuje pojačanje signala, u cilju sprečavanja zasićenja ADC-a. Tako, varijacije u pojačanju AGC-a su dragocen pokazatelj prisustva smetnji.

³⁶ Borowski Holly *et al.* (2012): „Detecting false signals with automatic gain control“. GPS World Staff, April 1, 2012; <https://www.gpsworld.com/detecting-false-signals-automatic-gain-control-12804/> (1.02.2021.)

³⁷ National PNT Advisory board comments on jamming the global positioning system – A National security threat: recent events and potential cures, November 4, 2010, 1-10.

instalirane na malom avionu, a mobilni telefon je bio uključen (bez ostarivanja poziva), tokom incidenata, kao i kasnijem testiranju.³⁸

Korišćenje GNSS u procedurama sletanja i poletanja vazduhoplova, prouzrokuje ranjivost avio sistema na spufing. Većina komercijalnih vazduhoplova prevashodno koristi ILS, ali je u porastu i upotreba sistema za potpuno automatsko sletanje, GBAS (*Ground Based Augmentation System*), naročito u Evropi i Rusiji. Međutim, uvođenje GBAS, kao međunarodnog standarda, usporeno je zbog činjenice da ovaj sistem nije autentifikovan i može biti spufovan. Kako je većina GNSS prijemnika koji se koriste za GBAS sistem pozicionirana na zemlji (aerodromima), određenu visinu aviona je moguće spufovati, što potencijalno može dovesti do udesa. Takođe, ometanje (slučajno ili namerno) GNSS prijemnika aviona u prilazu ili odlasku, bilo bi relativno jednostavno i moglo bi dovesti do značajnih gubitaka ljudskih života.

Zbog svega toga, analiza i razvoj efikasnih i robustnih anti-spufing metoda je od izuzetnog značaja. U tom kontekstu, predložene su brojne metode za detekciju i ublažavanje spufing napada na GNSS,^{39,40,41} kao što su AGC nadzor, SNR (*signal to noise ratio*) nadzor, provera konzistentnosti PVT (*Position/Velocity/Time*), kriptografske metode⁹, kao i monitoring korelace funkcije signala i multipletnih pikova.³⁰ Generalno, efikasnost predložene antispufing metode zavisi od nivoa sofisticiranosti uređaja za generisanje lažnih signala, odnosno scenarija spufing napada, a ispitivanja iz ove oblasti vrše se u cilju nalaženja osetljive, brze, pouzdane i robustne metode za detekciju spufinga. Kako se u većini spufing scenarija koristi jedna antena za prenos falsifikovanih signala, tako se prostorne karakteristike lažnih signala razlikuju od karakteristika autentičnih GPS signala. Prema tome, anti-spufing tehnike bazirane na prostornoj obradi signala, mogu se koristiti kao generičke, a simulacije i testiranja pokazuju da su veoma efikasne u detekciji spufinga.⁴⁰

Različite radne grupe, konferencije i organizacije, kao što su ICAO, RTCA i EU-ROCA, kontinuirano analiziraju i prate razvoj efikasnih antispufing detekcionih metoda/tehnika, kao i njihovu integraciju u sisteme kontrole letenja, komunikacije i navigacije. Pored toga, ove organizacije, razvijaju standarde za sledeću generaciju GNSS u civilnoj avijaciji i promovišu diskusiju o evoluciji uloge GNSS-a u vazduhoplovstvu, a paralelno s tim podstiču i neophodni tehničko-tehnološku razvoj.^{4,42}

³⁸ NASA/TM-2004-213001: Evaluation of a mobile phone for aircraft GPS interference, Truong X. Nguyen, Langley Research Center, Hampton, Virginia, march 2004.

³⁹ Schmidt Desmond *et al.* (2016): „A survey and analysis of the GNSS spoofing threat and countermeasures”, *ACM Computing Surveys* 48(4)/2016, A1-31.

⁴⁰ Jafarnia-Jahromi Ali *et al.* (2012): „GPS vulnerability to spoofing threats and a review of antispoofing techniques,” *International Journal of Navigation and Observation*, vol. 2012, 1-16.

⁴¹ Magiera Jaruslaw, Katulski Ryszard (2015): „Detection and mitigation of GPS spoofing based on antenna array processing”, *Journal of Applied Research and Technology* 13/2015, 45-57.

⁴² GSA (2018): Report on Aviation User Needs and Requirements; Technical Report; European GNSS Agency (GSA): Prague, Czechia, 2018; <https://www.gsa.europa.eu/system/files/2018-03/2018-03-01%20Report%20on%20Aviation%20User%20Needs%20and%20Requirements.pdf>

Tako, ICAO je objavila⁴³ verziju (za verifikaciju i validaciju) koncepta operacija za upotrebu *Dual-Frequency Multi-Constellation* (DFMC) GNSS u avijaciji, čija bi konačna verzija trebalo da bude završena do 2022 god., dok je *Minimum Operational Performance Standard* (MOPS) za GPS i Galileo na opsezima frekvencija L1/E1 i L5/E5a, u procesu definisanja. Očekuje se da će DFMC GNSS zameniti trenutni jednofrekventni GPS L1-C/A u budućim regulativama za civilno vazduhoplovstvo. Drugi evolutivni koncepti koji obuhvataju promininetnu upotrebu GNSS-a uključuju sledeće sisteme: *Advanced Receiver Autonomous Integrity Monitoring* (ARAIM),⁴⁴ *Airbone Separation Assurance System* (ASAS)⁴⁵ i *Multi-dimensional trajectory management*⁴⁶.

Svakako, u avijaciji, specifični zahtevi koji se odnose na snimanje svih GNSS podataka relevantnih za GNSS operacije, detaljno su date u ICAO smernicama.⁴⁷ Država je vodeći autoritet, koji odobrava operacije, koje se zasnivaju na GNSS i trebalo bi da obezbedi evidentiranje GNSS podataka relevantnih za te operacije, kao i podrži periodičnu potvrdu da se tačnost, integritet, kontinuitet i dostupnost ovih podataka, održava u granicama potrebnim za odobrene operacije. Aerodromski kontrolni tornji i jedinice, koje pružaju uslugu kontrole prilaza, moraju raspolažati podacima/informacijama o operativnom statusu aerodromskih radio-navigacionih sistema, koji su od suštinskog značaja za prilaz, sletanje i poletanje aviona. Performanse svih navigacionih sistema moraju biti u skladu sa zahtevima⁴⁷ *ICAO GNSS Signal in Space Performance Requirements*, a u kojoj meri navigacioni sistem zadovoljava unapred propisane vrednosti, određuje i koje se operacije mogu izvršiti.

3.2. Spufing ADS-B sistema

Automatic Dependent Surveillance – Broadcast (ADS-B) jeste savremeni tehnološki sistem, koji objedinjuje postojeća tehnička rešenja iz oblasti telekomuni-

tem/files/reports/gnss_user_tech_report_2018.pdf(1.03.2021.)

⁴³ ICAO (2018): Concept of Operations (CONOPS) for Dual-Frequency Multi-Constellation (DFMC) Global Navigation Satellite System (GNSS). 2018; <https://www.icao.int/Meetings/anconf13/> (15.01.2020.)

⁴⁴ Zhai Yawei et al. (2019): „Impact quantification of satellite outages on air navigation continuity”, *IET Radar Sonar Navigation* 13/2019, 376-383.

⁴⁵ SkyBrary (2020): Airborne Separation Assurance Systems (ASAS); [https://www.skybrary.aero/index.php/Airborne_Separation_Assurance_Systems_\(ASAS\)](https://www.skybrary.aero/index.php/Airborne_Separation_Assurance_Systems_(ASAS)) (10.01.2021.)

⁴⁶ Enea Gabriele, Porretta Marco (2012): „A comparison of 4D-trajectory operations envisioned for NextGen and SESAR, some preliminary findings”, Proceedings of the 28th International Congress of Aeronautical Sciences (ICAS), Brisbane, Australia, 23–28 September 2012.

⁴⁷ ICAO Annex 10 to the convention on international civil aviation: „Aeronautical Telecommunications, Volume1, Radion Navigation Aids”, Sixth Edition, July 2006.

kacija, navigacije i osmatranja vazdušnog prostora.⁴⁸ Esencijalna je komponenta FAA (*Federal Aviation Administration*) projekta *NextGen (Next Generation Air Transportation System)* i *Eurocontrol CASCADE* programa, koji bi trebalo da unaprede sistem vazdušnog saobraćaja, i to u pogledu bezbednosti, ekonomičnosti, automatizacije, ekologije i sl.

ADS-B sistem je tehnologija budućnosti, s brojnim benefitima, kao što su dostupnost i ušteda: automatizovana razmena informacija između vazduhoplova i kontole letenja bez uticaja pilota i kontrolora značajno utiče na autonomnost i efikasnost letenja, a samim tim i na uštedu resursa. Međutim, nedostatak ovog sistema u vezi je sa sigurnosno/bezbednosnim aspektom, tj. nedostatkom osnovnih sigurnosnih mehanizama,⁴⁹ tako da je ova infrastruktura nedovoljno zaštićena i otvorena je za sajber napade – komunikacija između aviona i kontrole letenja ostaje nedovoljno enkriptovana i nesigurna, tj. ranjiva je na ometanje i lažiranje informacija. Pomenute bezbednosne ranjivosti su u konstatnom porastu, naročito usled sve većeg razvoja/dostupnosti jeftinih SDR tehnologija^{15,50}

Dakle, bezbednosni rizici sa kojima se suočava ADS-B sistem, suštinski su u vezi s komunikacijom, koja se ostvaruje radio talasima, odnosno u vezi su sa činjenicom da se poruke prenose kao tekstualne, a koje nemaju enkripciju. Zbog značaja koje ove poruke sadrže, iste su glavne mete zlonamernih hakera.^{13,14}

Sajber napadi na ADS-B, obuhvataju prisluškivanje, ometanje, ubacivanje i brisanje poruka, kao i modifikaciju poruka.^{51,52} Ovi napadi imaju različite nivoje uticaja (štetnog) na avio sisteme. Tako, prisluškivanje prouzrokuje minimalnu štetu (ne oštećuje direktno ATC sistem), dok brisanje poruka utiče na sistem nadzora vazduhoplova (vaduhoplov privremeno nestaje sa ATC mape), ali se može identifikovati radarom ili multilateracionim sistemima. Modifikacija poruka jeste tipičan spufing napad i ima veliki uticaj na ATC sistem. Na primer, spufing napad, tzv. „kuvana žaba”,⁵³ odnosi se na situaciju u kojoj napa-

⁴⁸ Ali Busyairah Syd (2016): „System specifications for developing an Automatic Dependent Surveillance-Broadcast (ADS-B) monitoring system”, *International Journal of Critical Infrastructure Protection* 15/2016, 40-46.

⁴⁹ McCallie Donald, Butts Jonathan, Mills Robert (2011): „Security analysis of the ADS-B implementation in the next generation air transportation system,” *International Journal of Critical Infrastructure Protection* 4(2)/2011, 78-87.

⁵⁰ Schäfer Matthias., Lenders Vincent, Martimović Ivan (2013): „Experimental analysis of attacks on next generation air traffic communication,” in *International Conference on Applied Cryptography and Network Security*. Springer, 2013, 253-271.

⁵¹ Leonardi Mauro, Di Gregorio Luca, Di Fausto Davide (2017): „Air traffic security: aircraft classification using ADS-B messages phase-pattern”, *Aerospace* 4(4)/2017, 44-51

⁵² Ghose Nirnimesh, Lazos Loukas (2015): „Verifying ADS-B navigation information through Doppler shift measurements”, IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), 13-17 Sept. 2015.

⁵³ Chan-Tin Eric *et al.* (2011): „The frog-boiling attack: limitations of secure network coordinate systems”, *ACM Transactions on Information and System Security* (TISSEC) 14(3)/2011, 1-23.

dač u maloj meri, ali kontinuirano, menja informaciju o poziciji vazduhoplova u ADS-B porukama. U ovom slučaju, tehnologije nadzora (sistemi radarskog nadzora i pozicioniranja), teško detektuju male razlike, a koje su u okviru tačnosti podešavanja, što rezultuje u nepreciznom vođenju vazduhoplova od strane kontrole letenja, kao i zakasnelog (odloženog) odgovora sistema za sprečavanje kolizije u vazduhu.

Dakle, spufing napad modifikacijom ADS-B poruka, ostvaruje se ubacivanjem lažnih/falsifikovanih poruka. Može se razmatrati kao napad sa zemlje i napad iz vazduha.⁵⁴

Kod prve vrste napada (napad sa zemlje), napadač koristi jeftini SDR za: 1) reemitovanje prethodno snimljene poruke (tzv. napadi ponavljanjem, tj. napad reprodukcijom IQ podataka⁵⁵) ili 2) prenos novogenerisane i korektno modulisane lažne poruke (napad uvođenjem "aviona duha"). Konkretno, kod napada reprodukcijom IQ podataka, napadač sa zemlje snima sadržaj poruka ili IQ podatke primljenih autentičnih ADS-B poruka koristeći SDR uređaj, nakon čega ih emituje s kašnjenjem, ali bez promene njihovog sadržaja. Ovaj napad je veoma sofisticiran, jer snimljeni IQ podaci sadrže brojne informacije, kao što su one u vezi sa Doplerovim efektom, karakteristikama predajnika i karakteristikama kanala. U slučaju napada ubacivanjem "aviona-duha", napadač sa zemlje, koristeći SDR uređaj, prenosi lažne ADS-B poruke proizvoljnog sadržaje. Naročito, napadač može simulirati putanje nepostojećih vazduhoplova ("duhova") i generisati odgovarajuće ADS-B poruke pažljivim izborom Doplerovih pomeraja, i tako učiniti da ovi "avioni-duhovi" postanu vidljivi zemaljskim stanicama.

U drugoj vrsti napada, tj. napadu iz vazduha (spufing na avion), napadač modifikuje ICAO adresu u ADS-B porukama pomoću ADS-B transpondera u vazduhu, predstavljajući se kao poznati/pouzdani vazduhoplov, tako zaobilazeći nadzor. Konkorno, napadač sa vazduhoplovom (zlonamerni avion) pokušava da se maskira u poznati ili pouzdani avion, lažiranjem ICAO adrese i prikrivanjem svog stvarnog identiteta. Kako je avion fizički prisutan, ovaj napad neće biti otkriven, čak ni od strane sekundarnog radara za nadzor (SSR).

Kada se analiziraju različiti scenariji napada na ADS-B sistem, mora se naglasiti da su, za razliku od napada sa zemlje, potencijalni napadi koji bi se mogli ostvariti iz vazduha (napadač je u vazduhu), i dalje nedovoljno ispitani¹⁵, ali da predstavljaju realnu pretnju. Oni se mogu realizovati korišćenjem UAV/dronova, a s obzirom na konstantni tehničko/tehnološki napredak, na ovu vrste potencijalnih napada mora se obratiti naročita pažnja. Zbog svega toga, istraživački projekat *OpenSky Network* prikuplja izveštaje ADS-B i čini ih dostupnim

⁵⁴ Ying Xuhang *et al.* (2019): „Detecting ADS-B spoofing attacks using deep neural networks”; <https://arxiv.org/pdf/1904.09969v1.pdf> (15.12.2020.)

⁵⁵ IQ podaci (signali, uzorci ili kvadraturni signali), su periodični signali, koji se razlikuju u fazu za 90°; oznaka I, odnosi se na *in*-fazu (referentni signal), dok se Q odnosi na fazno pomereni signal.

za bezbednosno/sigurnosne analize, razvoj koncepcija detekcije spufing napada, kao i lociranja spufing uređaja/izvora.

Za detekciju spufinga, tj. zaštitu bežične ADS-B komunikacije, predložene su različite sigurnosne metode, koje se zasnivaju na postojećim kriptografskim tehnikama^{56,57}. Alternativa ovome, su nekriptografski pristupi, koji se zasnivaju na razdvajanju signala (*PHY-layer signal separation*)⁵⁸, verifikaciji vremena i položaja,⁵⁹ Doplerovom pomeraju,⁶⁰ mrežnoj analizi^{23,51,54}, itd.

Najskorije razvijene metode/tehnike za detekciju spufinga ADS-B sistema, zasnivaju se na predikcijama matematički postavljenih modela i mrežnoj analizi, kao što je npr. metoda koja se zasniva na SODA-DNN (*Deep Neural Network*) spufing detektoru.⁵⁴ Svakako, za karakterizaciju spufing detektorskog sistema, neophodno je analizirati veliki broj realnih podataka (spufing napada), tj. imati na raspolaganju/kontruisati adekvatnu opremu, kao npr. ADS-B resiver (laptop, RTL-SDR adapter, 1090 MHz filter i ADS antena) i ADS-B spufer (laptop, SDR i ADS-B antena), koji imitira ADS-B spufing napad.

Ovakva istraživanja su neophodna i veoma značajna, s obzirom na to da piloti i kontrolori letenja donose vrlo važne odluke na osnovu instrumenata, i da pogrešna odluka može imati nesagleđive posledice. Zato je vrlo važno analizirati uticaj potencijalnih sajber napada na ADS-B, koja je svakako tehnologija budućnosti, s brojnim benefitima, a čiji je poseban značaj naglašen dodelom posebne kategorije 21 ASTERIX protokola za razmenu informacija o vazduhoplovima.⁶¹ Standardizacija i unifikacija, kako hardvera tako i softvera, a posebno komunikacionih sistema omogući će upotrebu ADS-B tehnologije ravnopravno s postojećim avio sistemima.

⁵⁶ Finke Cindy *et al.* (2013): "Enhancing the security of aircraft surveillance in the next generation air traffic control system", *International Journal of Critical Infrastructure Protection*, 6(1)/2013, 3-11

⁵⁷ Alghamdi Fatimah, Alshhrani Amal, Hamza Nermin (2018): „Effective security techniques for automatic dependent surveillance-broadcast (ADS-B)”, *International Journal of Computer Applications* 180(2)/2018, 23-28.

⁵⁸ Leonardi Mauro, Piracci G. Emilio, Galati Gaspare (2017): „ADS-B jamming mitigation: a solution based on a multichannel receiver”, *IEEE Aerospace and Electronic Systems Magazine* 32 (11)/2017, 44-51.

⁵⁹ Schäfer Matthias, Lenders Vincent, Schmitt B. Jens (2015): "Secure track verification", Security and privacy (SP), 2015 IEEE Symposium on IEEE, 2015, 199-213.

⁶⁰ Schäfer Matthias, Lenders Vincent, Schmitt B. Jens (2016): „Secure motion verification using the Doppler effect”, Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016, 135-145.

⁶¹ EUROCONTROL (European Organisation for the Safety of Air Navigation) (may, 2011): „Coding rules for reserved expandione fileds”, ASTERIX part 12 Category 21, Appendix A.

4. Zaključak

Funkcionisanje sistema baziranih na satelitskim tehnikama pozicioniranja, kao što su GPS/GNSS i ADS-B, može biti ugroženo različitim vrstama ometanja, među kojima su i radio-frekvencijske interferencije, tj. spufing. Spufing napadi smatraju se veoma ozbilnjom pretnjom – njihova realizacija ne zahteva korišćenje skupe tehničke opreme, što je dovoljna motivacija za napadača, koji pokušava da ubaci lažne informacije o pozicioniranju u sisteme, kao što su na primer navigacioni sistemi aviona ili bespilotnih letilica (dronova).

Za detekciju spufinga predložene su i eveluirane brojne metode/tehnike, kao značajna etapa u razvijanju standarda za avio GNSS prijemnike. Primenom anti-spufing metoda, GNSS prijemnici mogu detektovati spufing tragajući za anomalijama u signalu ili koristeći signale koji su tako dizajnirani da spreče spufing, a napredne tehnologije za ublažavanje interferencija, koriste algoritme za obradu signala. Svakako, efikasnost predložene antispufing metode zavisi od nivoa sofisticiranosti uređaja za generisanje lažnih signala, odnosno scenarija spufing napada, a ispitivanja iz ove oblasti vrše se u cilju nalaženja osetljive, brze i pouzdane metode za detekciju i ublažavanje spufinga. Ipak, i u slučaju uspešnog sofisticiranog spufinga koji nije ublažen u GNSS prijemniku, a s obzirom na to da GNSS nije jedino sredstvo navigacije u civilnom vazduhoplovstvu i ATC, u većini slučajeva, piloti mogu ublažiti ove napade, smanjujući njihovu efikasnost.

Međutim, bezbednosne ranjivosti avio sistema i dalje rastu, usled veoma brzog napretka jeftinih SDR tehnologija, tako da je očekivano preduzimanje brojnih istraživačkih aktivnosti u vezi s povećanjem sigurnosti/bezbednosti GNSS prijemnika na spufing napade. Za rešavanje pitanja ranjivosti avio sistema na spufing i definisanje bezbednosnih zahteva, neophodan je sveobuhvatan pristup, koji, između ostalog, podrazumeva, kako razvoj savremene tehničke opreme za otkrivanje spufinga, tako i edukaciju pilota da prepoznaju spufing u njegovoj ranoj fazi i primene adekvatne protivmere, ali i obuku celokupnog vazduhoplovnog osoblja u cilju podizanja svesti o postojanju ovakve vrste potencijalne bezbednosne ugroženosti i implementiranju adekvatnih protokola u cilju zaštite avio sistema.

Literatura

- Alghamdi Fatimah, Alshhrani Amal, Hamza Nermin (2018): „Effective security techniques for automatic dependent surveillance-broadcast (ADS-B)”, *International Journal of Computer Applications* 180(2)/2018, 23-28.
- Ali Busyairah Syd (2016): “System specifications for developing an Automatic Dependent Surveillance-Broadcast (ADS-B) monitoring system”, *International Journal of Critical Infrastructure Protection* 15/2016, 40-46.
- Berz Gerhard: “GNSS spoofing and aviation: An evolving relationship”, *Inside GNSS*, 25 september 2018 [online];<https://insidegnss.com/gnss-spoofing-and-aviation-an-evolving-relationship/>(20.12.2020.)
- Borowski Holly *et al.* (2012): “Detecting false signals with automatic gain control”. GPS World staff, April 1, 2012; <https://www.gpsworld.com/detecting-false-signals-automatic-gain-control-12804/>(1.02.2021.)
- Chan-Tin Eric *et al.* (2011): “The frog-boiling attack: limitations of secure network coordinate systems”, *ACM Transactions on Information and System Security* (TISSEC) 14(3)/2011, 1-23.
- Costin Andrei, Francillon Aurélien (2012): “Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices”, *Black Hat USA* 2012, 1-12. https://www.researchgate.net/publication/267557712_Ghost_in_the_AirTraffic_On_insecurity_of_AMS-B_protocol_and_practical_attacks_on_AMS-B_devices(5.03.2021.)
- Enea Gabriele, Porretta Marco (2012): “A comparison of 4D-trajectory operations envisioned for NextGen and SESAR, some preliminary findings”, Proceedings of the 28th International Congress of Aeronautical Sciences (ICAS), Brisbane, Australia, 23–28 September 2012.
- Eurocontrol. EUROCONTROL Voluntary ATM Incident Reporting (EVAIR) safety bulletin 20, 2013–2017; Safety Bulletin 20; EUROCONTROL: Brussels, Belgium; <https://www.eurocontrol.int/publication/eurocontrol-voluntary-atm-incident-reporting-evar-safety-bulletin-20> (1.02.2021.)
- EUROCONTROL (may, 2011): “Coding rules for reserved expandione fileds”, ASTERIX part 12 Category 21, Appendix A.
- Fernández-Hernández Ignacio *et al.* (2019): “Increasing international civil aviation resilience: a proposal for nomenclature, categorization and treatment of new interference threats,” in Proceedings of ITM 2019: International Technical Meeting of The Institute of Navigation, Reston, Virginia (USA), January 28-31, 2019, 389-407.
- Finke Cindy *et al.* (2013): “Enhancing the security of aircraft surveillance in the next generation air traffic control system”, *International Journal of Critical Infrastructure Protection*, 6(1)/2013, 3-11
- Gaspar João *et al.* (2020): “Capture of UAVs through GPS spoofng using low-cost SDR platforms,” *Wireless Personal Communications* 115/2020, 2729–2754.

- Ghose Nirnimesh, Lazos Loukas (2015): “Verifying ADS-B navigation information through Doppler shift measurements”, IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), 13-17 Sept. 2015.
- GPS (1995): “Global positioning system standard positioning service signal specification”. (Technical Report. Global Positioning System); <http://www.gps.gov/technical/ps/1995-SPS-signal-specification.pdf>(15.12.2020.)
- GSA (2018): Report on Aviation User Needs and Requirements; Technical Report; European GNSS Agency (GSA): Prague, Czechia, 2018; https://www.gsa.europa.eu/system/files/reports/gnss_user_tech_report_2018.pdf(1.03.2021.)
- Hegarty Christopher *et al.*(2018): “Spoofing detection for airborne GNSS equipment”, in Proceedings of 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, FL, 2018, 1350-1368.
https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/factsheets/media/SBAS_Worldwide_QFact.pdf(20.12.2020)
- Horton Eric, Ranganathan Prakash (2018): „Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter”, *Journal of Global Positioning Systems* 16(9)/2018, 1-11.
- https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/factsheets/media/SBAS_Worldwide_QFact.pdf (20.12.2020.)
- Humphreys E. Todd *et al.* (2008): „Assessing the spoofing threat: development of a portable GPS civilian spoofe”, Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savanna, GA, September 16-19, 2008, 2314-2325.
- ICAO Annex 10 to the convention on international civil aviation: “Aeronautical Telecommunications”, Volume 1, Radion Navigation Aids”, Sixth Edition, July 2006.
- ICAO (2018): Concept of Operations (CONOPS) for Dual-Frequency Multi-Constellation (DFMC) Global Navigation Satellite System (GNSS). 2018; <https://www.icao.int/Meetings/anconf13/>(15.01.2020.)
- International Telecommunication Union, „Radio Regulations Articles – Volume 1,” ITU, 2016.
- Jafarnia-Jahromi Ali *et al.* (2012): “GPS vulnerability to spoofing threats and a review of antispoofing techniques,” *International Journal of Navigation and Observation*, vol. 2012, 1-16.
- Jansen Kai *et al.* (2017): “Localization of spoofing devices using a large-scale air traffic surveillance system”, ASIA CCS ’17, April 02-06, 2017, Abu Dhabi, United Arab Emirates

- John A. Volpe National Transportation Systems Center (2001): "Vulnerability assessment of the transportation infrastructure relying on the global positioning system". Final Report, 6-88, August 29, ES3; https://rntfnd.org/wp-content/uploads/Vople_vulnerability_assess_2001.pdf(20.12.2020.)
- Kožović Dejan (2019): "Uloga i značaj sajber bezbednosti u vazduhoplovstvu", *Master rad*, Fakultet za civilno vazduhoplovstvo, Megatrend univerzitet, Beograd.
- Kožović Dejan, Đurđević Dragan (2019): "Sajber bezbednost u avijaciji", *Megatrend revija* 16(2)/2019, 39-56.
- Leonardi Mauro, Di Gregorio Luca, Di Fausto Davide (2017): "Air traffic security: aircraft classification using ADS-B messages phase-pattern", *Aerospace* 4(4)/2017, 44-51.
- Leonardi Mauro, Piracci G. Emilio, Galati Gaspare (2017): "ADS-B jamming mitigation: a solution based on a multichannel receiver", *IEEE Aerospace and Electronic Systems Magazine* 32 (11)/2017, 44-51.
- Magiera Jaruslaw, Katulski Ryszard (2015): "Detection and mitigation of GPS spoofing based on antenna array processing", *Journal of Applied Research and Technology* 13/2015, 45-57.
- McCallie Donald, Butts Jonathan, Mills Robert (2011): "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection* 4(2)/2011, 78-87.
- Morales-Ferre Ruben *et al.* (2019): "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft", *IEEE Communications Surveys&Tutorials*, 22/2019, 249–291.
- NASA/TM-2004-213001: "Evaluation of a mobile phone for aircraft GPS interference truong X". Nguyen Langley Research Center, Hampton, Virginia, march 2004.
- National PNT Advisory board comments on jamming the global positioning system – A National security threat: recent events and potential cures, November 4, 2010, 1-10.
- Nava-Gaxiola Cesar, Barrado Cristina, Royo Pablo (2018): "Study of a full implementation of free route in the European airspace", Proceedings of the 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), London, UK, 23–27, September, 2018.
- Olson Parmy (2015): „Hacking a phone's GPS may have just got easier,” *Forbes*, 7 AUG 2015. [Online]; <https://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/?sh=b1abbfb4efbf>(15.12.2020.)
- Parkinson W. Bradford, Spilker J. James (1996): *Global positioning system: theory and Application*, Vol. I, American Institute of Aeronautics and Astronautics, Washington, DC.

- Pavić Aleksandar, Lalić Batrić, Đurđević Miloš (2014): „Osnove ADS-B tehnologije i osmatranje područja Republike Srbije bez radarske pokrivenosti”, *INFOTEH-JAHORINA* 13/2014, 419-424.
- Pierpaoli Pietro, Egerstedt Magnus, Rahmani Amir (2015): “Altering UAV flight path by threatening collision”, Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th (2015), IEEE, 4A4-1-4A4-10.
- Sampigethaya Krishna *et al.* (2011): “Future e-enabled aircraft communications and security: The next 20 years and beyond”, Proceedings of the IEEE 99(11)/2011, 2040–2055.
- Sathaye Harshad *et al.* (2019): “Wireless attacks on aircraft instrument landing systems”, 28th USENIX Security Symposium, August 14–16, 2019, Santa Clara, CA, USA, 1-16.
- Schäfer Matthias., Lenders Vincent, Martimović Ivan (2013): “Experimental analysis of attacks on next generation air traffic communication,” in International Conference on Applied Cryptography and Network Security. Springer, 2013, 253-271.
- Schäfer Matthias, Lenders Vincent, Schmitt B. Jens (2015): “Secure track verification”, Security and privacy (SP), 2015 IEEE Symposium on IEEE, 2015, 199-213.
- Schäfer Matthias, Lenders Vincent, Schmitt B. Jens (2016): “Secure motion verification using the Doppler effect”, Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2016, 135-145.
- Schmidt Desmond *et al.* (2016): “A survey and analysis of the GNSS spoofing threat and countermeasures”, *ACM Computing Surveys* 48(4)/2016, A1-31.
- Simsky Maria: “What is spoofing and how can you ensure GPS security?”, Aerospace testing international, 30 October 2019 [online]; <https://www.aerospacetestinginternational.com/features/what-is-spoofing-and-how-can-you-ensure-gps-security.html>(20.12.2020.)
- SkyBrary (2020): Airborne Separation Assurance Systems (ASAS); [https://www.skybrary.aero/index.php/Airborne_Separation_Assurance_Systems_\(ASAS\)](https://www.skybrary.aero/index.php/Airborne_Separation_Assurance_Systems_(ASAS)) (10.01.2021.)
- Steindl Eduard *et al.* (2013): “The impact of interference caused by GPS repeaters on GNSS receivers and services,” Proceedings of the European Navigation Conference (ENC),Vienna, 2013; GMCA 641613 White Paper (2015), DW/02/001/096/032/1.0
- Stevanović Miroslav, Đurđević Dragan (2016): “Internet stvari, lična i materijalna bezbednost”, *Bezbednost* 3/2016, 113-128.
- Tippenhauer Nils Ole *et al.* (2011): “On the requirements for successful GPS spoofing attacks”, Proceedings of the ACM Conference on Computer and Communications Security, Chicago, IL. Association for Computing Machiner, 2011, 75-86.

- Turner Michael *et al.* (2020): “Spoofing detection by distortion of the correlation function”, Conference: 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), 566-574.
- Wang Jing, Zou Yunkai, Ding Jianli (2020): “ADS-B spoofing attack detection method based on LSTM”, *EURASIP Journal on Wireless Communications and Networking* 160/2020, 1-12.
- Warner Jon, Johnston Roger (2002): “A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing”, *Journal of Security Administration* 25(2)/2002, 19-27.
- Ying Xuhang *et al.* (2019): “Detecting ADS-B spoofing attacks using deep neural networks”; <https://arxiv.org/pdf/1904.09969v1.pdf>(15.12.2020.)
- Zhai Yawei *et al.* (2019): “Impact quantification of satellite outages on air navigation continuity”, *IET Radar Sonar Navigation* 13/2019, 376-383.

Dejan V. Kožović
Dragan Ž. Đurđević

UDC 005.334:656.7
007.5:528.28]:004

DOI: 10.5937/MegRev2103281K
Review scientific paper
Received 08.03.2021.
Approved 24.03.2021.

SPOOFING IN CIVIL AVIATION: SECURITY AND SAFETY OF GPS/GNSS AND ADS-B SYSTEMS

Abstract: Aircraft systems that rely on satellite positioning technology, such as GNSS and ADS-B, can be the target of a spoofing attack – a sophisticated and very dangerous form of radio frequency interference in which false signals are inserted into the „victim’s” receiver for incorrect positioning or timing. Although spoofing in civil aviation is a potential threat, its technical feasibility is realistic, and the application of spoofing is becoming more flexible due to the very rapid progress of cheap SDR platforms. In particular, the potential risk is posed by potential air strikes, using unmanned aerial vehicles/drones, for the purpose of hijacking or distracting security in airspace surveillance. However, aviation is not ruthlessly exposed to spoofing attacks without any defense; by applying certain methods/techniques, spoofing can be mitigated in the GNSS receiver. Also, pilots are trained to detect and solve problems at every stage of the flight. Due to more sophisticated forms of terrorist attacks are possible, international organizations, such as ICAO and EUROCA, are proactively working to increase the robustness of the GNSS and ADS-B systems to spoofing. Given the importance of the topic and the fact that spoofing/antispuffing testing has certain limitations, consideration of the specifics and different scenarios of these attacks are very important in the development of new methods for their mitigation and detection. This paper focuses on spoofing/antispuffing of GNSS and ABS-B systems in civil aviation and provides an overview of the latest research in these areas.

Keywords: civil aviation, GPS/GNSS, ADS-B, radio-frequency interference, security, spoofing, antispoofting methods