

Spoofing in aviation: Security threats on GPS and ADS-B systems



Dejan V. Kožović¹ , Dragan Ž. Đurđević² 

¹BEN AIR, Beograd

²Megatrend Univerzitet, Fakultet civilne avijacije, Beograd

Received: 30/12/2020

Revised: 11/03/2021

Accepted: 12/03/2021

Published: 29/03/2021

Corresponding author:

Dejan V. Kožović

Correspondence email:

dejankozovic@gmail.com

DOI: 10.5937/vojtehg69-30119



Abstract:

Introduction/purpose: The paper provides a review of recent research in the field of GPS and ADS-B spoofing. Systems that rely on satellite positioning technology can be targeted by spoofing in order to generate incorrect positioning/timing, which is accomplished by inserting false signals into the "victim's" receiver. Attackers try to insert false positioning information into systems that, for example, provide navigation of airplanes or drones for the purpose of hijacking or distracting security/safety in airspace surveillance. New concepts of navigation and ATC will thus be necessary. **Methods:** Using a scientific approach, the paper gives an evaluation of GPS and ADS-B spoofing/antispoofing and how spoofing affects the cyber security of aviation systems. **Results:** Based on the methodological analysis used, the importance of studying spoofing/anti-spoofing in aviation is shown. **Conclusion:** Although spoofing in aviation is only a potential threat, its technical feasibility is realistic and its potential is considerable; it becomes more flexible and cheaper due to very rapid advancement of SDR technologies. The real risk, in the time to come, are potential spoofing attacks that could occur from the air, using drones. However, aircraft systems are not exposed to spoofing without any defense; receivers can detect it by applying various anti-spoofing techniques. Also, pilots are able to detect and solve problems at every stage of the flight. However, due to a possibility of more sophisticated spoofing attacks, international organizations such as ICAO are proactively working to increase GPS and ADS-B systems robustness on spoofing.

Keywords: ADS-B; aviation; GPS; radio-frequency interference; spoofing; antispoofing

INTRODUCTION

The modern aerospace system relies heavily on the use of a number of wireless technologies necessary for the safe and secure operation of this very complex system. Thus, communication between air traffic controllers (ATC) and pilots is realized via VHF (30-300 MHz) radio frequency (RF) channels. The use of the ADS-B (Automatic Dependent Surveillance-Broadcast) wireless communication protocol or the GNSS (Global Navigation Satellite System), as an integral part of the ADS-B, allows the broadcasting of status data (aircraft position, speed, call sign, etc.), while Primary Surveillance Radar and Secondary Surveillance Radar allow locating aircraft and provide relevant information to air traffic controllers. The TCAS (Traffic Alert and Collision Avoidance System), independent of the air traffic control system, enables the detection and warning of potential collisions of aircraft with other aircraft in the air. In addition to the possibility of verbal communication, aircraft usually have the ACARS system (Aircraft Communications, Addressing and Reporting System) which uses RF communication channels, enabling the sending of automated messages in both directions, by aircraft as well as aircraft and other aircraft entities. Also, many radio navigation systems, such as the GPS (Global Positioning System), the VOR (VHF Omnidirectional Radio Range), the DME (Distance Measuring Equipment) and the ILS (Instrument Landing System), play key roles in different phases of aircraft flight.

Systems based on satellite positioning techniques, such as the GPS and the ADS-B, can be the target of various attacks, including the so-called spoofing attacks – a sophisticated form of RF interference (RFI) which makes the receiver believe it is at a false location. During a spoofing attack, a radio transmitter, a SDR (Software Defined Radio) for example, located nearby, sends fake GPS signals (which mimic

authentic satellite signals, but with higher power and different time delay compared to authentic signals) into the target receiver. Thus, "a cheap SDR can make a smartphone believe it's on Mount Everest" (Simsky, 2019).

Regarded as a "hoax", "trick", or "deceive" in the IT world, the term, spoof/spoofing has also been used in the aviation field, in recent studies. Related to the structure of the GPS signal (it is public and unlike military GPS signal, this is not encrypted/authenticated), it would not be difficult/expensive for an adversary to build a system that creates signals that would appear to a receiver to be from GPS satellites. Transmitting these false signals to receivers may cause them to lock onto the false signals instead of the authentic satellite signals. Thus, in 2001, the U.S. Department of Transportation assessed the U.S. transportation infrastructure's vulnerability to civil GPS disruption (John A. Volpe National Transportation Systems Center, 2001). Their report known as the Volpe report, considers civil GPS spoofing, a dangerous type of intentional interference whereby a GPS receiver is fooled into tracking counterfeit GPS signals. Spoofing is more sinister than intentional jamming because the targeted receiver cannot detect a spoofing attack and therefore cannot warn users that its navigation solution is untrustworthy. Moreover, even if not fully successful, spoofing usually will inject hazardously misleading information and create significant PVT (Position, Velocity, Time) errors. Ever since, civil GPS receivers remain as vulnerable as ever to this threat.

Recent efforts to modernize ATC have mandated the gradual replacement of the existing analogue radar system with a nextgeneration (NextGen) digital one. Part of this NextGen system is the ADS-B standard. The ADS-B aims at improving aviation safety by enabling aircraft to broadcast navigation information. However, the current ADS-B standard does not provide mechanisms for verifying the integrity of navigation broadcasts. Consequently, the ADS-B system is extremely vulnerable to various spoofing attacks (Schäfer et al, 2013). Therefore, concerns about its safety will continue to increase with the development of ATC and the further popularization and application of the ADS-B.

It should be emphasized that, unlike spoofing attacks from the ground, potential attacks that could be carried out from the air (the attacker is in the air) are still insufficiently investigated (Costin & Francillon, 2012), but they represent a real threat. These attacks can be realized with the use of drones, i.e. UAV (Unmanned Aerial Vehicle), and special attention must be paid to this type of potential attacks. Because of all this, the OpenSky Network research project collects ADS-B reports and makes them available for security/safety analysis and development of spoofing attack detection concepts, as well as locating spoofing devices/sources.

Also, the increasing use of UAV/drones and the GPS for their navigation makes these systems interesting targets for the purpose of hijacking or distracting safety/security in airspace surveillance. Thus, the normal navigation performance of drones may be limited due to natural signal noise or intentional RFI, jamming and spoofing. In particular, as for the spoofing of GPS, military GPS signals are encrypted and thus cannot be changed (Spilker et al, 1996), but civilian GPS signals are unencrypted/unauthenticated, and thus a user can arbitrarily generate or change signals. Namely, by using arbitrarily manipulated signals, it is possible to make a UAV target deviate from the existing path and lead the UAV to a target point designated by the spoofer. In recent years, the Federal Aviation Administration (FAA) announced a plan that the entrance of civilian UAV into the airspace of the US would be permitted by September 2015, and Amazon has been trying to implement a delivery system using drones. In this situation, spoofing could be a serious problem for the operation of UAV. In a hypothetical combat situation, manipulating the enemy's GPS receiver would mean taking control of the drone or devices that rely on GPS positioning. For example, in 2018, Russia accused the US of spoofing a drone and redirecting it to attack a Russian air base in Syria (Simsky, 2019). Also, in the last few years, numerous spoofing incidents have been recorded in the seas near the Russian border, and it is assumed that the drones were "transported" to nearby airports. This type of spoofing may have been a defense mechanism for landing spy drones. Namely, most semiprofessional UAV on the market have a built-in geo-fencing mechanism, which automatically lowers them to the ground if they approach airports or other areas with restrictive access.

Modernization and strengthening of aircraft systems through improvements and innovations in design, technology and efficiency is opposed by fragility in the field of cyber security. Cyber security threats are not only an assumption, but some have been realized. An overview of published cyber incidents and potential vulnerabilities of aircraft systems observed by aviation organizations and researchers/hacker community (from 1997 to 2019) is given in the paper (Kořović & Đurđević, 2019). For example, the weaknesses of the ATC system, by introducing a "ghost-plane" into a flight control system, by mimicking the ADS-B signal, by using low-cost technology devices, and software, have been pointed out (Costin & Francillon, 2012). Then, it was shown that radio navigation systems such as the GPS and the ILS (Sathaye et al, 2019) are susceptible to spoofing attacks, and that by spoofing TCAS messages, false messages can create resolution advisories, which forces pilots to resort to collision avoidance maneuvers.

In addition, until recently, the attitude of civil aviation regarding GNSS spoofing was simple (Berz, 2018): "This is not our problem", and this issue was considered to be within the scope of military structures. However, as more attention is paid to common RFI, the approach to spoofing is changing, which was partly initiated by the incident at Hanover Airport in 2010 (Steindl et al, 2013), and which was caused by the interference of GPS repeaters and thus inadequate positioning of the GNSS system. Today, it is known that there is a whole range of intermediate stages of spoofing, from incorrectly tuned repeaters, all the way to what a skilled, but unreasonable person could do by using cheap and widely available spoofing devices.

Although different parts of the aircraft system are exposed to various attacks, and potentially to spoofing, there are certain security solutions and protocols while different working groups, conferences and organizations, such as ICAO (International Civil Aviation Organization), RTCA (Radio Technical Commission for Aeronautics) and EUROCAE (European Organization for Civil Aviation Equipment), continuously analyze and monitor the development of effective antispoofing detection methods, as well as their integration into flight control, communication and navigation systems. For example, RTCA has set as a goal for nextgeneration aeronautical equipment, increasing the security of GNSS to risks in the presence of threats, including spoofing. Current directions in solving spoofing by RTCA and EUROCAE primarily relate to the introduction of new requirements for the detection of spoofing GNSS systems, which allows the use of alternative navigation equipment, without significant safety risks (Hegarty et al, 2018).

GPS: BECKGROUND AND SPOOFING OVERVIEW

GPS: a fundamental concept

The Global Positioning System (GPS) is satellite navigation, i.e. constellation of satellites that emit RF waves in order to accurately determine the position on/near the Earth's surface. They were first used for military purposes (since 1950s), and later (in 1980s) they were made available for wide, civilian use. A common term for different types of globally used satellite navigation systems is GNSS, such as GPS (USA), GLONASS (Russia), BEIDOW (China), etc. GNSS is a system that gives pilots, as well as aircraft systems, precise information about the position of the aircraft, as well as the reference time.

Although the GPS is the only fully operational GNSS "first generation", GLONASS, which covers Russia and neighboring countries, is also available, while Europe is developing a "second generation" GNSS, called the Galileo program, which in 2003 was also signed by China. Today, in addition to GNSS, there are several additional satellite systems, generically called Space Based Augmentation Systems (SBAS) (Sabatini et al, 2017), because they emit additional signals that a particular receiver can decode and use (along with global GNSS signals) in order to improve positioning performance.

The GPS consists of three segments: space¹, control² and user.

The GPS uses satellite transmitters whose locations L_i^S (coordinates, are known (x_i^S, y_i^S and z_i^S) are known (Tippenhauer et al, 2011). Each transmitter is equipped with a very precise synchronized clock for measuring the exact system time, t^S and emits a navigation signal $S_i(t)$, (low auto-/cross-correlation) which contains timestamps and deviations of the satellite from the predicted trajectory. The signal is transmitted at speed c .

A receiver V , located at the coordinates L (to be determined) and using an omnidirectional antenna, will receive the combined signal of all satellites in the range:

$$(1) \quad g(L, t) = \sum_i A_i S_i \left(t - \frac{|L_i^S - L|}{c} \right) + n(L, t)$$

Where A_i is the attenuation that the signal is undergoing on its way from L_i^S to L , $|L_i^S - L|$ denotes the Euclidean distance between L_i^S and L , and $n(L, t)$ is background noise.

Due to the properties of the signals $S_i(t)$, the receiver can separate the individual terms of sum (equation (1)) and extract the relative spreading code phase, the satellite ID, and data content using a replica of the used spreading code. Given the data and relative phase offsets, the receiver can identify the time delay $\frac{|L_i^S - L|}{c}$ for each satellite, i.e. "ranges": $d_i = L_i^S - L$, from where, knowing the positions of the transmitter, L_i^S , one can find the 3-dimensional position, L of the receiver.

However, the receiver clock is delayed, i.e. has a time offset, δ relative to the exact system time, t^S , so that the receiver gives "pseudoranges":

$$(2) \quad R_i = d_i - c \times \delta = d_i - \Delta$$

By measuring the distance from each satellite (at least four) and solving the system of nonlinear equations (2) for both L and δ , precise data (position and time) are obtained and then used for navigation, positioning and accurate time distribution.

Today, GNSS receivers are very cheap and compact devices, and are widely used in various systems (e.g. SCADA), in mobile phones and in many widely used products. The GNSS design allows three basic messages to be broadcasted, namely:

- positioning, velocity and time signal,
- precise ephemeris data, which determine the exact location of an individual satellite,
- an almanac, which determines the locations and orbits of all satellites in the constellation, together with information on the status of the selected tracking satellite.

All types of GNSS satellites broadcast on at least 2 bands: on the frequency L1—encrypted military code, the so-called P(Y) and unencrypted civil code (C/A), as well as frequency L2 (repeat P(Y) code). So, all satellites broadcast on 2 frequencies: 1575.42 MHz and 1227.6 MHz. As the GPS uses a wide range of techniques, the so-called multiple code-sharing approach, low-pass message data is encoded by a high-level pseudo-random sequence which is different for each satellite. Thus, the receiver can distinguish signals (PRN codes) coming from different satellites and message data is transmitted at a speed of 50 bit/s.

Two different encodings are used (Figure 1) (Warner & Johnston, 2002), i.e. two PRN codes: Coarse/Acquisition (C/A) code (so-called gold code) on 1.023 MHz and precision (P(Y)) on 10.23 MHz. The signals are modulated to a carrier signal, L1 and L2, by the binary phase shift keying method which encodes 1 bit per phase shift (Betz, 2002). Carrier L1 is modulated with both C/A and P codes, while L2 is modulated only with P code; the C/A code is public and used by civilian GPS receivers, while the P code can be

encrypted, and is only available to military equipment with the appropriate description key. Each L1 signal is composed of a navigation message which provides detailed data on the ephemeris (orbit data) of the satellite.

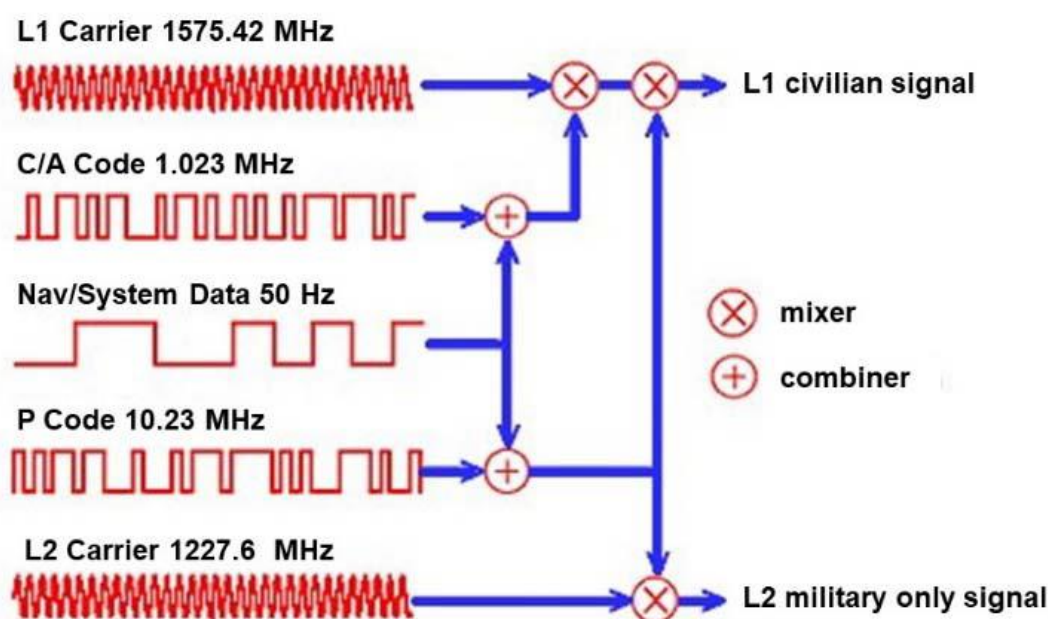


Figure 1.
Structure of a GPS signal (Warner & Johnston, 2002, p.20)

Рис. 1
Структура сигнала GPS (Warner & Johnston, 2002, p.20)
Слика 1
Структура ГПС сигнала (Warner & Johnston, 2002, p.20)

ICAO and EUROCAE are developing standards for the next generation of GNSS in civil aviation (Hegarty et al, 2015) and promoting a discussion on the evolution of the role of the GNSS in aviation, while encouraging the necessary technical and technological development (Berz, 2018). Thus, ICAO has published a version (for verification and validation) of the concept of operations for the use of the Dual-Frequency Multi-Constellation (DFMC) GNSS in aviation (ICAO, 2018), the final version of which should be completed by 2022, while the Minimum Operational Performance Standard (MOPS) for GPS and Galileo on the frequency bands L1/E1 and L5/E5a, is in the process of defining. The DFMC GNSS is expected to replace the current single-frequency GPS L1-C/A in future civil aviation regulations. Other evolutionary concepts involving the prominence use of the GNSS include the following systems: Advanced Receiver Autonomous Integrity Monitoring (ARAIM), Airborne Separation Assurance System (ASAS) (Skybrary, 2020) and Multidimensional trajectory management (Enea & Porretta, 2012).

GPS SPOOFING BASICS

GNSS vulnerabilities (Morales-Ferre et al, 2020) in connection with RFI cause concern and special attention in the field of aviation, i.e. incidents of disappearance of GPS signals in civilian aircraft (especially in areas with political tensions, e.g., Southeast Mediterranean, Black Sea–Caspian Sea axes and Mideast–Canada and the USA via North Pole through Russian airspace) or nearby airports. The reasons for this can be different, such as solar storms, military exercises, etc., but also intentionally provoked RFI, i.e. jamming (EUROCONTROL, 2019). Near airports, uninformed personal privacy devices could also be the cause of GPS jamming. Consequently, jamming can be considered as a realistic and threatening kind of interference. On the other hand, spoofing is a more subtle and potentially even more dangerous threat, where an ensemble of counterfeit GNSS-like signals are injected into a victim receiver with the purpose of inducing a wrong positioning or timing provision of measure (Nicola et al, 2020). Hence, a much more

subtle and dangerous form of a GNSS threat is spoofing, in which false signals are inserted/planted into the “victim’s” receiver for the purpose of mispositioning or timing.

Although GNSS spoofing is a potential threat (there are still a few confirmed reports of their exploitation in civil aviation), the technical feasibility of spoofing is realistic, and its potential is great. A noticeable difference between legitimate satellite signals and a spoofing signal can be a discrepancy in time, signal direction, intensity, Doppler shift, or the magnitude of the signal-to-noise ratio. However, most receivers are not equipped to detect these differences. Research in this area ([Horton & Ranganathan, 2018](#)) shows that almost every device that uses a civilian GPS signal is vulnerable to spoofing, and the application of spoofing becomes more flexible and cheaper due to the very rapid progress of SDR technologies.

The case of interference at Hanover Airport (in 2010), is an example of real “unintentional” spoofing ([Steindl et al, 2013](#)), which shows that the detection/immediate warning of GNSS spoofing is a necessary countermeasure to ensure airport safety and security. Namely, a plane which was located near the threshold of the runway of Hanover Airport, and whose aircraft systems functioned according to the repertoire signals for testing the avionics of business planes in the hangar near the threshold of the runway, had the wrong GPS position during the taxiing and takeoff phase. This scenario, although simple, can be used as a starting point for testing a GNSS receiver or any hardware that depends on precise positioning or time data provided by the receiver. Then, during the FAA's installation of a new GPS-based aircraft landing system at Newark International Airport in 2010, it was observed that ground-based GPS receivers (used to assist GPS receivers on the approaching aircraft) also had several interruptions, almost every day. Also, it was previously reported to the FAA (July, 2003) that the switched-on mobile phone simultaneously affected the operation of three different aircraft GPS receivers, causing a complete signal loss; all three GPS receivers used three different antennas, installed on a small plane, and a mobile phone was turned on (without making the call), during the incident, as well as subsequent testing ([Nguyen, 2004](#)).

The use of the GNSS in aircraft landing and take-off procedures causes the aircraft system to be vulnerable to spoofing. Most commercial aircraft still primarily use the ILS, but there is also a noticeable increase in interest in using the fully automatic landing system, the GBAS (Ground Based Augmentation System), especially in Europe and Russia. However, the introduction of this system, as an international standard, has been slowed down due to the fact that the GBAS system is not authenticated and can be spoofed. As most GNSS receivers used for the GBAS are positioned on the ground (airports), the height of each aircraft can be spoofed, which can potentially lead to an accident. Also, interfering (accidentally or intentionally) with the aircraft's GNSS receiver in approach or departure would be relatively simple and could lead to significant loss of life.

The use of AGC (Automatic Gain Control) to amplify the GNSS signal, which compensates for the strength of the fluctuating signal, also leads to the vulnerability of the receiver to spoofing ([Borowski et al, 2012](#)). It is also very important to consider that the receiver does not have the ability to determine where the signal is coming from (from a locally generated false or legitimate source) since the receiver antenna is usually located at one point in space: if the receiver is not protected, the spoofing signal can be inputted directly via the spoofing source. Or, if the spoofer knows the exact location of the target receiver, then the spoofer signals can be superimposed on the authentic signals. Alternatively, stronger asynchronous signals can be used, but this way of spoofing is effective only when the receiver is in the initial phase of operation (reception) or in case it is “forcibly unlocked” by an interfering signal.

There are different forms of GPS signal spoofing, and they can be classified in different ways, such as according to the level of complexation ([Humphreys et al, 2008](#)), to simplified, intermediate and sophisticated, or based on their characteristics, to synchronized (spoofing attack in which the false signal is synchronized with authentic GNSS signals) and unsynchronized.

Thus, in the simplest form of spoofing attacks, the receiver (in tracking mode) can receive a false signal when it loses the reception of the signal from the satellite, so that it can be "locked", i.e. switched to the mode of receiving the spoofing signal. The signals are usually not synchronized with the original signals, which allows the use of simple commercial (COTS) components. Detection of this type of spoofing is relatively simple – the lack of signal synchronization would cause a sudden jump in output signals related to the position of the receiver and time. Also, if the spoofing signals are high, then the monitoring receiver could potentially detect increased activity in the GNSS frequency bands. In a medium-strength (intermediate) spoofing attack, a kind of GNSS simulator is used to produce counterfeit GNSS signals, but they are synchronized with GNSS signals coming from the satellite. Such an attack includes the known location (and path) of the "attacked" receiver, relative to the receiver antenna, to ensure that the false, pseudo-signal band is "aligned" with the authentic codes at the position of the attacked receiver. When the receiver is in the tracking mode, and at the beginning of the attack, the false signals are well enough aligned with the authentic ones, so that the spoofer can take control by gradually increasing the power and successively adjusting the signal. Detection on the target receiver is almost impossible, except when a large number of antennas are used to estimate the signal arrival direction. A more complex version of intermediate spoofing is sophisticated spoofing in which multiple coordinated "intermediate spoofers" could be used to replicate the content and "align" GNSS signals, as well as their spatial distribution, making this form of attack more difficult to detect. However, in this type of attack, the receiver for monitoring at another location (allocated) is likely to have a sharp increase in the value of the output signals related to the position of the receiver and time, since its position differs from the position of the target receiver. Also, if the spoofing signals are high, then the allocated monitoring receiver could potentially detect increased activity in the GNSS frequency bands.

Numerous methods of spoofing detection and mitigation of spoofing attacks on GNSS ([Magiera & Katulski, 2015](#)) are proposed such as AGC surveillance, SNR (signal to noise ratio) monitoring, consistency checking of PVT, cryptographic methods ([Hegarty et al, 2018](#)), and monitoring of the correlation function of signals and multiple peaks ([Turner et al, 2020](#)). For example, one of the suggested methods is based on checking whether the received signals are modulated with the military P(Y) code, which is usually absent in spoofing signals ([Psiaki et al, 2011](#)). Despite being effective, this solution uses two receivers and requires that one of them be protected from spoofing, which is not always possible. In general, the effectiveness of the proposed antispoofing method depends on the level of sophistication of the device for generating false signals, i.e. scenarios of spoofing attacks, and tests in this area are performed to find sensitive, fast, robust, and reliable methods for detecting spoofing. As most spoofing scenarios use a single antenna to transmit counterfeit signals, the spatial characteristics of false signals differ from the characteristics of authentic GPS signals. Therefore, anti-spoofing techniques based on spatial signal processing can be used as generics, and simulations and tests show that they are very effective in detecting spoofing ([Jafarnia-Jahromi et al, 2012](#)).

In aviation, specific requirements for recording all GNSS data relevant to GNSS operations are detailed in the ICAO Guidelines ([ICAO, 2006](#)). The State is the lead authority for approving GNSS-based operations and should ensure that GNSS data relevant to those operations are recorded, as well as support periodic confirmation that accuracy, integrity, continuity, and availability are maintained within the limits required for approved operations. Airport control towers and units providing access control services must have data/information on the operational status of airport radio navigation systems, which is essential for the approach, landing and take-off of aircraft. The performance of all navigation systems must be in accordance with the requirements of the ICAO GNSS Signal in Space Performance Requirements ([ICAO, 2006](#)).

ADS-B: BACKGROUND AND VULNERABILITY AGAINST THE SPOOFING ATTACK

ADS-B: a fundamental concept

The Automatic Dependent Surveillance - Broadcast (ADS-B) is a modern technological system which combines the existing technical solutions in the field of telecommunications, navigation, and airspace

surveillance (Ali, 2016). It is an integral part of the FAA project NextGen and Eurocontrol CASCADE program which should improve the air traffic system in terms of safety, economy, automation, ecology, etc. The special importance of ADS-B technology is emphasized by the allocation of a special category 21 ASTERIX protocol for the exchange of information on aircraft (EUROCONTROL, 2011).

The ADS-B system automatically delivers the necessary data to users (both on the ground and in the air). Its integral part is the GNSS, so that the ADS-B system depends on the accuracy of the positioning system. The ADS-B standard regulates the exchange of broadcast messages between aircraft and ATC ground stations. It can work as a transmitter (ADS-B Out) or a receiver (ADS-B In). The ADS-B In allows the aircraft to receive data which is displayed on the CDTI (Cockpit Display of Traffic Information) interfaces (most often, MFD³ and EFB⁴ devices), and which are emitted by other aircraft positioned in a relatively close environment. The same information is used for TCAS systems. Within the ADS-B Out system, the status information of the aircraft is handed over.

The ADS-B system consists of three interdependent components:

- ground infrastructure (GBT stations⁵ and antenna system),
- aircraft equipment (ADS-B specialized transponder, GPS, receiver, altimeter, CDTI⁶, etc.),
- operational procedures (regulatory basis for the implementation and use of the ADS-B system).

Communication within the ADS-B is realized by using the radio system according to standardized communication protocols, such as 1090 MHz extended squitter (1090-ES), 987 MHz Universal Access Transceiver (UAT) and VHF Datalink Mode 4 (VDL-M4), which will be used depends on the type of aircraft (in accordance with the FAA guidelines). Each ADS-B message contains an 8 μ s preamble for synchronization and a 56-bit (short) or 112-bit (extended) data block. Thus, an extended ADS-B message has 112 bits which are transmitted using 1090 MHz (“extended squat”) data links (FAA, 2010). The ADS-B protocol format with a 112-bit message frames contain a preamble (8.0 μ s), which is used to synchronize transmitters and receivers and 112-bit payload which consists of five segments. The first, 5-bit segment contains telecommunication transmission data and refers to the downlink format used to encode broadcast messages, the second, 3-bit segment is the field of choice, while the third, 24-bit segment contains a unique aircraft address. The next 56 bits (ADS-B data) refer to sub-segment data such as flight identification (call sign), position (latitude/longitude), position accuracy, barometric and geometric height, vertical velocity, trajectory angle, and ground speed (Ghose & Lazos, 2015). ADS-B messages are not encrypted: the last 24 bits include a parity check that detects and corrects transmission errors in the messages. ADS-B frames are modulated by pulse modulation with a pulse length of 1 μ s. As the ADS-B protocol transmits data at a speed of 1 Mbit/s, the total duration of the ADS-B extended message is 120 μ s (including the preamble).

Cyber attacks on the ADS-B

The risks faced by the ADS-B system are essentially related to communications realized by RF waves, i.e. they are related to the fact that messages are transmitted as text and have no encryption. Because of that, they are the main targets of malicious hackers (Kožović & Đurđević, 2019). Thus, the security risks faced by the ADS-B relate to ATC-aircraft connections, and if they are not secure, ADS-B messages may be hacked by authorized/unauthorized persons, especially when messages containing sensitive information are interrupted or eavesdropped.

Attacks on the ADS-B, which can have different levels of impact on aircraft systems, include eavesdropping, jamming, message insertion, message deletion, and message modification (Table 1) (Wang et al, 2020).

Table 1. Different types of attacks on the ADS-B system (Wang et al, 2020, p.3)

Таблица 1. Различные типы атак на систему ADS-B (Wang et al, 2020, p.3)

Табела 1. Различите врсте напада на АДС-Б систем (Wang et al, 2020, p.3)

Attack type	Purpose of attack	Way of attack
Eaves-dropping	Eavesdrop operating status information of aircraft (aircraft reconnaissance)	Obtain ADS-B data of the corresponding airspace through ADS-B In
Jamming	Jam the transmission of an ADS-B message in a specific airspace	By using an ADS-B transmitting device with sufficient high transmit power in the relevant frequency band
Message injection	Inject fake aircraft into a specific flight scenario, confusing ATC systems (aircraft target ghost injection/flooding)	By using a transmitting device with sufficient high transmit power in the relevant frequency band and capable of generating correct modulation and conforming to the ADS-B message format
Message deletion	Delete some or all of the information contained in a message (aircraft disappearance)	By implementation at the physical layer through constructive/destructive interference
Message modification	Modify the information contained in a message (virtual trajectory modification)	Realized by overshadowing and bit-flipping at the physical layer of the system and can also be achieved by combining two attack methods

Thus, eavesdropping causes minimal damage, because it does not directly damage the ATC system, while deleting messages affects the aircraft surveillance system (the aircraft temporarily disappears from the ATC map), but the aircraft can be identified by radar or multilateral systems. Message modification is a typical "spoofing" attack and has a major impact on the ATC system. For example, a spoofing attack, the so-called "boiled frog" (Chan-Tin et al, 2011), refers to a situation in which an attacker continuously, but to a small extent, changes the information about the position of the aircraft in the CSDP messages. In this case, it is difficult for surveillance technologies such as radar surveillance systems and positioning, to detect small differences which are within the accuracy of adjustment, resulting in inaccurate control of aircraft by air traffic control, as well as delayed system response to prevent collision in the air.

ADS-B spoofing

A spoofing attack on the ADS-B refers to an attack by modifying ADS-B messages, which is realized by inserting fake/falsified messages. It can be considered as an attack from both the ground and the air. An illustration of two different types of spoofing attacks on the ADS-B is given in Figure 2; namely, a spoofing attack by inserting messages and a spoofing attack on the ground station. In the first type of attack, the attacker uses a cheap SDR to re-broadcast a previously recorded message (so-called repeat attacks) or to transmit a newly generated and correctly modulated fake message (attack by introducing a ghost plane). The main goal of the attack is to falsify the presence of the non-existent, i.e. aircraft-ghost and to cause confusion of the ATC system. In the second type of attack, the attacker modifies the ICAO address in the ADS-B messages using the ADS-B transponder in the air posing as a known/reliable aircraft, thus bypassing surveillance.

Thus, depending on the way the spoofed messages are generated, ADS-B spoofing attacks can be divided into three types (Ying et al, 2019):

- message or IQ data⁷ replay attack,
- ghost aircraft injection attack, and
- aircraft spoofing attack.

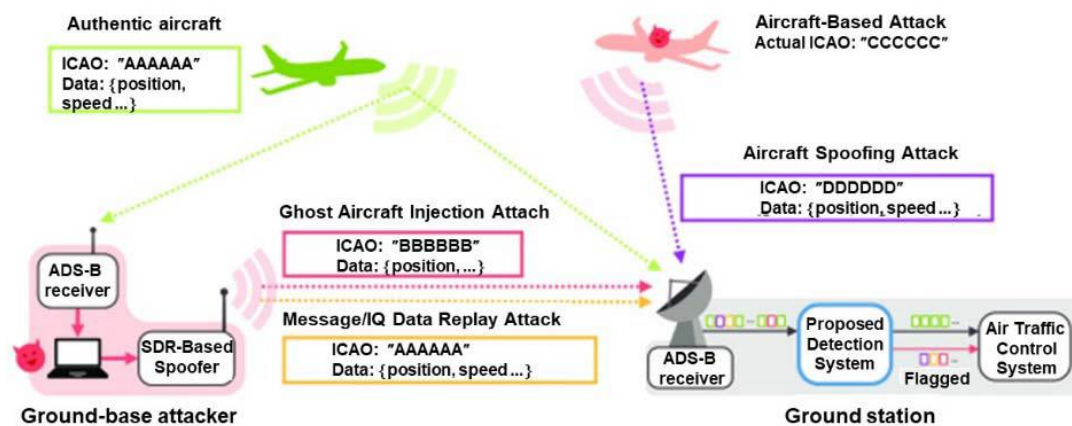


Figure 2.

Illustration of two types of attacks on the ADS-B: the ground-based attack, using a SDR spoofer and an aircraft-based attack where the attacker uses an ADS-B transponder with a changed ICAO address (Ying et al, 2019)

Рис. 2

Иллюстрация двух типов атаки на ADS-B: наземная атака с использованием спуфера SDR и воздушная атака, при которой злоумышленник использует транспондер ADS-B с измененным адресом ICAO (Ying et al, 2019)

Слика 2

Илустрација две врсте напада на АДС-Б: напад са земље, коришћењем СДР спуфера и напад из ваздушног простора (авиона), при чему нападач користи АДС-Б транспондер с измењеном ИЦАО адресом (Ying et al, 2019)

In a message/IQ data replay attack, an attacker from the ground records the content of the messages/IQ data of the received authentic ADS-B messages using an SDR, and then transmits the same messages at a later time without changing the message content. This attack is very sophisticated, because the recorded IQ data contains a lot of information, such as those related to the Doppler effect, the transmitter characteristics, and the channel characteristics, which is difficult to mimic otherwise. In a ghost aircraft injection attack, a ground-based attacker, using an SDR device, transmits fake ADS-B messages with arbitrary content of its choice. In particular, an attacker can simulate the trajectories of non-existent aircraft ("ghosts") and generate appropriate ADS-B messages by carefully selecting Doppler displacements, thus making these "aircrafts-ghosts" visible to earth stations. In an aircraft spoofing attack, an aircraft-based attacker (malicious aircraft) attempts to masquerade as a known or trusted aircraft by spoofing the ICAO address and hide its true identity. Since the aircraft is physically present, the masquerading attack will not be detected even if the secondary radar surveillance system is deployed

To detect spoofing, i.e. for the protection of wireless ADS-B communication, various security methods have been proposed, based on the existing cryptographic techniques (Finke et al, 2013; Alghamdi et al, 2018). An alternative to this are necryptographic approaches which are based on signal separation (PHY-layer signal separation) (Leonardi et al, 2017), time and position verification (Schäfer et al, 2015), Doppler shift (Schäfer et al, 2016), etc. The most recently developed methods for ADS-B system spoofing detection are based on the predictions of mathematically set models and network analysis. One of these is the method based on a SODA-DNN (Deep Neural Network) spoofing detector (Ying et al, 2019), whose application allows the detection of spoofing attacks with a very high probability and a very small proportion of false alarms, which is a significant improvement over other state-of-the-art detectors.

CONCLUSION

Systems based on satellite positioning techniques, such as the GNSS and the ADS-B, can be targets of various attacks, including the so-called spoofing attacks – a sophisticated form of attack in which false

signals (which imitate authentic satellite signals, but with higher power and different time delay in relation to authentic signals) are emitted. As a result, aircraft will send incorrect information about their position.

One of the most important steps in the modernization of ATC is the transition to the ADS-B wireless communication protocol, of which the GNSS is an integral part. In addition to its advantages, the ADS-B system also has several very important disadvantages, such as dependence on the satellite navigation system (which can be physically damaged, corrupt, or subject to interference) and a very simple protocol, which does not provide full authentication and encryption. All this increases the vulnerability of the ADS-B system to various types of cyber attacks, such as RFI, including spoofing, i.e. deliberately inducing RFI.

Also, the role of GPS/GNSS is constantly increasing, due to the increase in the use of UAV/drones, which is why new concepts of navigation and ATC will be necessary in a "crowded sky" situation, where many unmanned aerial vehicles will share airspace with crews. On the other hand, the increasing use of drones and the GPS for their navigation makes these systems interesting targets for the purpose of hijacking or distracting security/safety in airspace surveillance.

Although the spoofing of the GNSS system is a potential threat - there are still no confirmed reports of their exploitation in civil aviation, the technical feasibility of spoofing is realistic and the potential is great. Research in this area shows that almost every device that uses L1 civilian GPS is vulnerable to spoofing, and the application of spoofing is becoming more flexible and cheaper due to the very rapid advancement of SDR technology. Therefore, the issues of detection and prevention of spoofing attract the attention of researchers in the field of cyber security, and due to possible more sophisticated spoofing terrorist attacks on the aircraft system, ICAO, RTCA and EUROCAE are proactive in improving the robustness of GPS/GNSS to RFI.

However, the aircraft system is not helplessly exposed to spoofing attacks without any defense; by applying various anti-spoofing methods, GNSS receivers can detect spoofing by looking for signal anomalies or using signals designed to prevent spoofing, and advanced interference mitigation technologies use signal processing algorithms. Certainly, the effectiveness of the proposed antispoofing method depends on the level of sophistication of the device for generating false signals, i.e. scenarios of spoofing attacks, and tests in this area are performed in order to find sensitive, fast, as well as robust and reliable methods for detecting and mitigating spoofing.

Endnotes

¹GPS satellites are called NAVSTAR (Navigation Satellite Timing and Ranging).

²Control Center (the main checkpoint is Shriver Military Base, Colorado) checks the satellite condition, position, speed and altitude. The precise trajectory of the satellite is updated on average every 4 hours and the data on the updated orbits are sent to the satellites via terrestrial radio antennas.

³MFD – Multifunction Display

⁴EFB – Electronic Flight Bag

⁵GBT stations – Ground Based Transceivers stations.

⁶CDTI – Cockpit Display of Traffic Information

⁷IQ data/signals (samples or quadrature signals), are a pair of periodic signals which differ in a phase by 90°; designation I, refers to the in-phase (reference signal), while Q refers to the phase-shifted signal.

REFERENCES

- Alghamdi, F., Alshhrani, A., & Hamza, N. (2018). Effective Security Techniques for Automatic Dependent Surveillance-Broadcast (ADS-B). *Int J Comput Appl*, 180(26), 23-28. Retrieved from <https://www.ijcaonline.org/archives/volume180/number26/alghamdi-2018-ijca-916598.pdf> on 25 December 2020. [Crossref] [Google Scholar]
- Ali, B.S. (2016). System specifications for developing an Automatic Dependent Surveillance-Broadcast (ADS-B) monitoring system. *International Journal of Critical Infrastructure Protection*, 15, 40-46. [Crossref] [Google Scholar]
- Berz, G. (2018). GNSS spoofing and aviation: An evolving relationship. *Inside GNSS*. Retrieved from <https://insidegnss.com/gnssspoofing-and-aviation-an-evolving-relationship/> on 25 December 2020. [Google Scholar]
- Betz, J.W. (2002). Binary Offset Carrier Modulations for Radionavigation. *Navigation*, 48(4), 227-246. [Crossref] [Google Scholar]
- Borowski, H., Isoz, O., Eklof, F.M., Lo, S., & Akos, D. (2012). Detecting false signals with automatic gain control. *GPS World*. Retrieved from <https://www.gpsworld.com/detecting-false-signals-automatic-gain-control-12804/> on 1 April, 2012. [Google Scholar]
- Chan-Tin, E., Heorhiadi, V., Hopper, N., & Kim, Y. (2011). The frog-boiling attack: limitations of secure network coordinate systems. *ACM Transactions on information and system security (TISSEC)*, 14(3), 1-26. [Crossref] [Google Scholar]
- Costin, A., & Francillon, A. (2012). Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices. In: *BLACKHAT 2012, Las Vegas, NV, USA, July 21-26*. Retrieved from <https://www.eurocom.fr/publication/3788> on 25 December 2020.
- Enea, G., & Porretta, M. (2012). A comparison of 4D-trajectory operations envisioned for NextGen and SESAR, some preliminary findings. In: *Proceedings of the 28th International Congress of Aeronautical Sciences (ICAS), Brisbane, Australia, September 23-28*. (pp. 1-14). Retrieved from https://www.icas.org/ICAS_ARCHIVE/ICAS2012/PAPERS/310.PDF on 25 December 2020.
- Eurocontrol. (2011). Coding rules for 'Reserved Expansion Field' for ASTERIX Category 021: Apendix A. Retrieved from <https://www.eurocontrol.int/sites/default/files/2019-06/appendixcat021pt12aed11.pdf> on 25 December 2020.
- Eurocontrol. (2019). *EVAIR safety bulletin 20 (summer seasons and full years 2013-2017)*, Brussels, Belgium. Retrieved from <https://www.eurocontrol.int/publication/eurocontrol-voluntary-atm-incidentreporting-evair-safety-bulletin-20> on 25 December 2020.
- FAA. (2010). Automatic dependent surveillance broadcast (ADS-B) out performance requirements to support air traffic control (ATC) service (final rule). 14 CFR Part 91, *Federal Register*, 25 December 2020 | <https://www.govinfo.gov/content/pkg/FR-2010-05-28/pdf/2010-12645.pdf>, 30160-30195. [Google Scholar]
- Finke, C., Butts, J., Mills, R., & Grimaila, M. (2013). Enhancing the security of aircraft surveillance in the next generation air traffic control system. *International Journal of Critical Infrastructure Protection*, 6(1), 3-11. [Crossref] [Google Scholar]
- Galati, G., Piracci, E., & Leonardi, M. (2017). ADS-B jamming mitigation: A solution based on a multichannel receiver. *IEEE Aerospace and Electronic Systems Magazine*, 32(11), 44-51. [Crossref] [Google Scholar]
- Ghose, N., & Lazos, L. (2015). Verifying ADS-B navigation information through Doppler shift measurements. In: *IEEE/AIAA 34 th Digital Avionics Systems Conference (DASC), Praue, September 13-17*. (pp. 4A2-1-4A2-11). [Crossref] [Google Scholar]
- Hegarty, C., Odeh, A., Shallberg, K., Wesson, K., Walter, T., & Alexander, K. (2018). Spoofing detection for airborne GNSS equipment. In: *Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2018) (31st), Miami, FL, September 24-28*. (pp. 1350-1368). [Crossref] [Google Scholar]
- Hegarty, C.J., Ligler, G.T., Alexander, K., Chesto, L., Moses, H., Wichgers, J.M., Enge, P., Erlandson, B., van Dierendonck, A.J., Azoulai, L., Kalyanaraman, S., Heppe, S., Lee, J.C., Wesson, K., & Studenny, J. (2015). RTCA SC-159: 30 Years of Aviation GPS Standards. In: *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015), Tampa, FL, September 14-18*. (pp. 877-896). Retrieved from <https://www.ion.org/publications/abstract.cfm?articleID=13133> on 25 December 2020.
- Horton, E., & Ranganathan, P. (2018). Development of a GPS spoofing apparatus to attack a DJI matrice 100 quadcopter. *Journal of Global Positioning Systems*, 16(art.number:9). [Crossref] [Google Scholar]
- Humphreys Kintner, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W., & Kintner, P.M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In: *Proceedings of The International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008) (21st), Savanna, September 16-19*. (pp. 2314-2325). Retrieved from https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf on 25 December 2020.
- ICAO. (2006). Annex 10 to the Convention on International Civil Aviation: Aeronautical Telecommunications: Radio Navigation AIDS, 1(Radio Navigation Aids), Sixth Edition.

- ICAO. (2018). Concept of Operations (CONOPS) for Dual-Frequency Multi-Constellation (DFMC) Global Navigation Satellite System (GNSS).
- Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*. [Crossref] [Google Scholar]
- John A. Volpe National Transportation Systems Center. (2001). Vulnerability assessment of the transportation infrastructure relying on the global positioning system: Final Report. , 6-88, ES3. Retrieved from https://rntfnd.org/wp-content/uploads/Vople_vulnerability_assess_2001.pdf on 25 December 2020.
- Kožović, D.V., & Đurđević, D.Ž. (2019). Syber security in aviation. *Megatrend revija*, 16(2), 39-56. [Crossref] [SCIndeks] [PDF] [Google Scholar]
- Lohan, E.S., de la Fuente, A., Falletti, E., Richter, P., & Morales-Ferre, R. (2020). A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft. *IEEE Communications Surveys&Tutorials*, 22(1), 249-291. [Crossref] [Google Scholar]
- Magiera, J., & Katulski, R. (2015). Detection and mitigation of GPS spoofing based on antenna array processing. *Journal of Applied Research and Technology*, 13(1), 45-57. [Crossref] [Google Scholar]
- Nguyen, T.X. (2004). *Evaluation of a mobile phone for aircraft GPS interference*. Hampton, Virginia: Langley Research Center. Retrieved from <https://ntrs.nasa.gov/api/citations/20040040193/downloads/20040040193.pdf> on 25 December 2020.
- Nicola Falletti, M., Falco, G., Morales-Ferre, R., Lohan, E.S., Fuente, A., & Falletti, E. (2020). Collaborative Solutions for Interference Management in GNSS-Based Aircraft Navigation. *Sensors (Basel)*, 20(15), 4085-4108. [Crossref] [Google Scholar]
- Psiaki, M.L., O'Hanlon, B.W., Bhatti, J.A., Shepard, D.P., & Humphreys, T.E. (2011). Civilian GPS Spoofing Detection Based on Dual-Receiver Correlation of Military Signals. In: *ION GNSS 2011, Portland, September 20-23, Proceedings of*. (pp. 2619-2645). Retrieved from https://gps.mae.cornell.edu/Paper_E4_2_ION_GNSS_2011b.pdf on 25 December 2020.
- Sabatini, R., Moore, T., & Ramasamy, S. (2017). Global navigation satellite systems performance analysis and augmentation strategies in aviation. *Progress in Aerospace Sciences*, 95, 45-98. [Crossref] [Google Scholar]
- Sathaye, H., Schepers, D., Ranganathan, A., & Noubir, G. (2019). Wireless attacks on aircraft instrument landing systems. In: *USENIX Security Symposium (28th), Santa Clara, CA, USA, August 14-16*. (pp. 1-16). [Crossref]
- Schäfer, M., Lenders, V., & Martinović, I. (2013). Experimental analysis of attacks on next generation air traffic communication. In: M. Jacobson, M. Locasto, P. Mohassel, & R. Safavi-Naini, (Ed.). *Applied Cryptography and Network Security: ACNS 2013 (Lecture Notes in Computer Science)*. Berlin, Heidelberg: Springer. [Crossref] [Google Scholar]
- Schäfer, M., Lenders, V., & Schmitt, J. (2015). Secure track verification. In: *Proceedings of The 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, July 20*. (pp. 199-213). [Crossref] [Google Scholar]
- Schäfer, M., Leu, P., Lenders, V., & Schmitt, J. (2016). Secure motion verification using the Doppler effect. In: *Proceedings of The ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec'16) (9th), Darmstadt, Germany, July*. (pp. 135-145). [Crossref] [Google Scholar]
- Simsky, M. (2019). What is spoofing and how can you ensure GPS security? *Aerospace testing international*, 30 October [online]. Retrieved from <https://www.aerospacetestinginternational.com/features/what-is-spoofing-andhow-can-you-ensure-gps-security.html> on 25 December 2020. [Google Scholar]
- SkyBrary. (2020). Airborne Separation Assurance Systems (ASAS). Retrieved from [https://www.skybrary.aero/index.php/Airborne_Separation_Assurance_Systems_\(ASAS\)](https://www.skybrary.aero/index.php/Airborne_Separation_Assurance_Systems_(ASAS)) on 25 December 2020.
- Spilker, J.J., Axelrad, P., Parkinson, B.W., & Enge, P. (1996). *Global positioning system: Theory and applications*. Washington, DC: American Institute of Aeronautics and Astronautics. [Crossref] [PubMed] [Google Scholar]
- Steindl, E., Dunkel, W., Hornbostel, A., Haettich, C., & Remi, P. (2013). The impact of interference caused by GPS repeaters on GNSS receivers and services. In: *European Navigation Conference (ENC) GNSS 2013, Wien, April 22-25*. Retrieved from <https://elib.dlr.de/84739/> on 25 December 2020.
- Tippenhauer, N.O., Pöpper, C., Rasmussen, K.B., & Capkun, S. (2011). On the requirements for successful GPS spoofing attacks. In: *Proceedings of The ACM Conference on Computer and Communications Security (18th), Chicago, Illinois, USA, October 17-21*. (pp. 75-86). [Crossref] [Google Scholar]
- Turner, M., Wimbush, S., Enneking, C., & Konovaltsev, A. (2020). Spoofing Detection by Distortion of the Correlation Function. In: *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, Oregon, USA, April 20-23*. (pp. 566-574). [Crossref] [Google Scholar]
- Wang, J., Zou, Y., & Ding, J. (2020). ADS-B spoofing attack detection method based on LSTM. *Journal Wireless Communications and Networking*, art.number:160. [Crossref] [Google Scholar]
- Warner, J.S., & Johnston, R.G. (2002). A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *Journal of Security Administration*, 25(2), 19-27. [Google Scholar]

Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L., & Poovendran, R. (2019). Detecting ADS-B Spoofing Attacks Using Deep Neural Networks. In: *IEEE Conference on Communications and Network Security (CNS)*, Washington DC, USA, June 10-12. [[Crossref](#)] [[Google Scholar](#)]

Spufing u avijaciji - bezbednosne pretnje po GPS i ADS-B sisteme

Sažetak:

Uvod/cilj: U radu su ukratko opisana nedavna istraživanja u oblasti GPS i ADS-B spufinga/antispufinga. Ovi sistemi, koji se oslanjaju na tehnologiju satelitskog pozicioniranja, mogu biti meta spufing napada čiji je cilj generisanje pogrešnog pozicioniranja ili vremenskog određenja, tako što se u prijemnik "žrtve" ubacuju lažni signali. Naime, napadač pokušava da ubaci lažne informacije u sisteme koji, na primer, omogućavaju navigaciju aviona ili dronova radi otmice ili distrakcije bezbednosti/sigurnosti u nadzoru vazdušnog prostora. Zbog toga su neophodni novi koncepti navigacije i ATC-a. **Metode:** Primenom naučnog pristupa prezentovana je evaluacija GPS i ADS-B spufinga/antispufinga. Navedeno je kako spufing utiče na sajber bezbednost vazduhoplovnog sistema. **Rezultati:** Na osnovu korišćene metodološke analize objašnjen je značaj proučavanja spufinga/antispufinga u avijaciji. **Zaključak:** Iako spufing GNSS sistema predstavlja potencijalnu pretnju, njegova tehnička izvodljivost je realna, a potencijal veliki jer je fleksibilniji i jeftiniji zbog vrlo brzog napretka SDR tehnologija. Realan rizik predstavljaju potencijalni spufing napadi koji bi se mogli ostvariti iz vazdušnog prostora, uz korišćenje dronova/UAV. Međutim, primenom različitih antispufing tehnika prijemnici avionskog sistema mogu detektovati spufing. Zbog mogućih sofisticiranijih oblika spufing napada, međunarodne organizacije, poput ICAO, proaktivno se bave povećanjem otpornosti GPS i ADS-B sistema na spufing.

Ključne reči: ADS-B; avijacija; GPS; radio-frekvencijske interferencije; spufing; antispufing

Спуфинг в авиации: Угрозы безопасности систем GPS и ADS-B

Резюме:

Введение/цель: В статье представлен краткий обзор последних исследований в области спуфинга/антиспуфинга систем GPS и ADS-B. Системы, которые полагаются на технологию спутникового позиционирования, могут стать мишенью атак с использованием спуфинга, с целью внедрения неверного позиционирования/синхронизации при введении ложных сигналов в радиоприемник «жертвы». Таким образом летательный аппарат приближается к злоумышленнику, который пытается ввести ложную информацию о местоположении в системы, которые обеспечивают навигацию самолетов или беспилотников, с целью их угона или захвата, а также нарушения безопасности при наблюдении за воздушным пространством. В данной связи в ближайшее время потребуются разработки новых концепций как для навигации, так и УВД. **Методы:** Используя научный подход, в статье была дана оценка спуфинга / антиспуфинга GPS и ADS-B и того, как спуфинг влияет на кибербезопасность авиационных систем. **Результаты:** На основании проведенного методологического анализа доказана значимость изучения спуфинга/антиспуфинга в авиации. **Вывод:** Несмотря на то, что спуфинг в авиации представляет собой потенциальную угрозу, его техническая осуществимость вполне реальна и обладает большим потенциалом; он становится более доступным и дешевым вследствие быстрого развития технологий SDR. Реальный риск в будущем – это потенциальные атаки с использованием спуфинга с помощью дронов в воздушном пространстве. Однако авиационная система самолета оснащена антиспуфинг защитой и благодаря применению различных методов антиспуфинг защиты, радиоприемники могут обнаружить атаку. Кроме того, летчики проходят подготовку по обнаружению и решению проблем на каждом этапе полета. Однако в связи с возможностями более изощренных атак спуфинга международные организации, такие как ICAO, активно работают над повышением устойчивости систем GPS и ADS-B и предотвращением спуфинга.

Ключевые слова: ADS-B, авиация, GPS, радиочастотные помехи, спуфинг, антиспуфинг.