

# The dark side of Radio Technology<sup>\*</sup>

Giorgi Tomadze<sup>1,\*</sup>, Ilia Lomidze<sup>1,†</sup>, Mikheil Kurashvili<sup>2,†</sup>, Giorgi Akhalaia<sup>3,†</sup> and Vladimer Svanadze<sup>4,†</sup>

<sup>1</sup> *Ivane Javakhishvili Tbilisi State University*

<sup>2</sup> *21<sup>th</sup> Public School*

<sup>3</sup> *Caucasus University, Caucasus School of Technology*

<sup>4</sup> *Business and Technology University*

## Abstract

Due to the fact that most modern technologies of the 21st century are based on radio signals, their safety is of utmost importance. The article presents common types of radio hacking, describes, and demonstrates some of them, and explains in detail how to spoof a GPS signal, as well as the associated dangers and ways to protect against them. Along with this, the purpose of ADS-B (a system installed on an aircraft that periodically broadcasts its location, altitude and other important details) and the importance of the safety of this system are discussed. The paper provides a comprehensive overview of GPS and ADS-B spoofing techniques, highlighting potential threats to navigation and airspace security. provides case studies and case studies of the changing landscape of navigation and aviation cyber threats.

## Keywords

ADS-B, Spoofing, GNSS, HackRF, Radio hacking

## 1. Introduction

In our present-day relocation of technology, the loud and unambiguous presence of radio waves have been vacant in paths of modern existence. A good example is the wireless communication devices that we heavily utilize everyday be it a call, a simple text or even a video chat. The radio waves may be invisible but they are the conduits that connect the world that is now complex with industries like aviation.[1] However, with this widespread reliance comes a new frontier of challenges: an effect of radio hacking.

The early 21st century was the almost immediate surge of the carrying online attacks by radio wave technologies, which are so significant and dangerous not only for private users, but also for critical infrastructure. This article takes a look at both sides of radio hacking which have serious consequences in our daily life, discuss current context, approaches and offer possible solutions.

Radio hacking, at its basis, comprises unauthorized uses, manipulations, and tempering of radio signals with a variety of techniques that target any weak link in the radio communication system. The advent of the digital age is coupled with the development of the cyber threat, as technology adapts so do the hostile elements that aim to use these newly made systems for bad intentions.[2]


Before delving into a discussion on the genesis of radio waves, it is important to traverse their beginning with German physicist Heinrich Hertz in the late 1800s. Hertz's unique experiments established the infrastructure for how our knowledge about electromagnetic waves came into being that gave rise to all the modern applications we so vividly witness around us.

<sup>\*</sup> *IVUS2024: Information Society and University Studies 2024, May 17, Kaunas, Lithuania*

<sup>1</sup>: Corresponding author

<sup>†</sup> These author contributed equally.

✉ [gio.tomadze@gmail.com](mailto:gio.tomadze@gmail.com) (G. tomadze); [ilikolomidze@gmail.com](mailto:ilikolomidze@gmail.com) (I. Lomidze); [misho.kurashvili789@gmail.com](mailto:misho.kurashvili789@gmail.com) (M. Kurashvili), [gakhalaia@cu.edu.ge](mailto:gakhalaia@cu.edu.ge) (G. Akhalaia); [vsvanadze@indein.net](mailto:vsvanadze@indein.net) (V. Svanadze).

 0000-0002-4194-2681 (G. Akhalaia)



The spin-off effect of radio waves, which enabled communication and connectivity, also ushered in new threat vectors that are gravely damaging in aviation safety systems. Because of its place of utmost importance, cybersecurity in the Aviation industry is a subject under the spotlights, the integrity of radio systems being pivotal for the safety of the passengers and crew. Using practical examinations, showcases, and involving interpretation, this article is committed to shining a light on all possible dynamics of radio jamming, thus helping readers to act safely and apprehensively in this digital duration. Through strengthening our awareness of the difficulties for adequately protecting the systems, we will continuously strive to shape a world where such cyber-attacks on radio systems would be a thing of the past.[2]

## 2. Literature Overview

The information we dig into entails a broad scope of technology and security concerns that border on aircraft technology, the incorporation of GPS systems with Global Navigation Satellite System Technology (GNSS) and the imminence of GPS spoofing.

The article How ADS-B Revolutionizes Air Traffic Surveillance and In-Cockpit Information Access examines its wholesome effect on air surveillance traffic and cockpit information access. ADS-B out and ADS-B in are the methods which are mainly used for more accurate tracking and real-time sharing of data with air traffic controllers and pilots respectively. With this breakthrough, the entire airspace management is bound to radically change and aviation authorities such as the FAA will undertake strict measures; possibly obligate ADS-B equipment in operating U.S. controlled airspace. Yet, doubts and skepticism about the cost-efficiency of such introduction remain among the air travel community that should be further controlled as the novel technology implementation on a wide scale seemed to be an ambitious goal. [2]

Whilst GNSS-based systems' precision location feature facilitates both long-term surveillance and real-time tracking of critical structures, such as buildings and bridges, the scope of improving cities' safety and security is undoubtedly augmented. Although the real-time kinematic (RTK) and precise point positioning (PPP) techniques have added new dimensions to the field for optimization of positioning accuracy, challenges still emerge due to atmospheric variability and observation noise. In spite of this, the provision of GNSS-based solutions with rapid data collection and analysis efficiency which leads to unique monitoring systems gives proof that their potential is in increasing the level of structural integrity and safety. [5]

During the same time the conversation about GPS spoofing gives a greater understanding of a mere danger of the unfriendly interference in navigation signals. Through the tampering of GPS signals such as simulators, Emulators, or Sentinels, which deceive receivers into believing

false signals, spoofing has detrimental repercussions in many sectors depending on the GPS technology. While protective measures consisting of technical countermeasures, policies, and frameworks exist, rather solving GPS spoofing is an intricate task hence. Patenting laws and strong measures of protection systems and integrity of data are the core pillars in the constantly evolving digital landscape.[7]

The three articles here may have different focuses but they all reach a conclusion that technology is moving forward, and the issue of security is one of these challenges. The field to be applied from aviation surveillance, hardware monitoring, to even internet security is the requirement of these systems for the connectivity between the modern architects and the securing procedures they have. It is through appreciating and resolving the deep rooted Disclosure: The past is often used to interpret the present, but it is important to keep in mind that each era had its own unique circumstances and challenges.

### **3. Radio hacking in aviation**

The modern aviation system relies heavily on radio technologies, which are essential for the efficient operation of this complex system. Most of these systems use the very high frequency range of radio signals, or VHF [1].

This system includes the following:

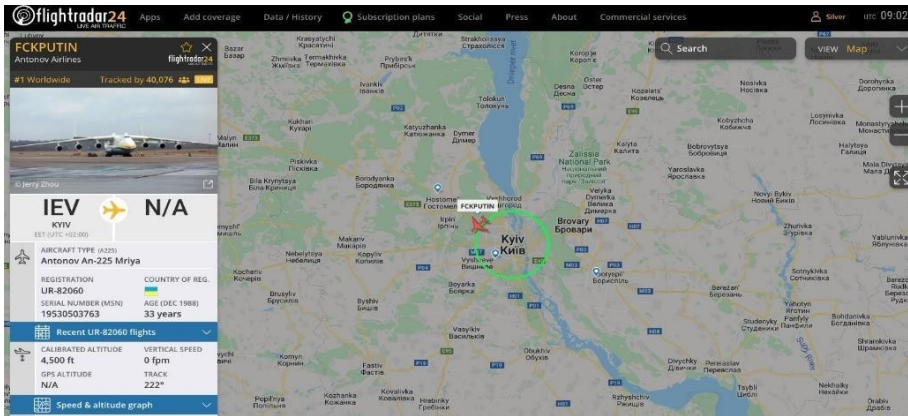
1. Voice and written communication between the air traffic controller and the pilots.
2. Use of ADS-B and its integral part – GNSS.

Using them, it becomes possible for the aircraft to broadcast its position, altitude, and other important data. This information is critical for air traffic controllers, as the above has serious vulnerabilities that could lead to dire consequences for an attacker. Cyber-attacks are carried out by a range of perpetrators. They include individuals, organized criminals, and state-sponsored entities.

An attacker can impersonate the signals transmitted by the aircraft and pretend to be a flying object or change the data transmitted by the authentic aircraft. This action could cause critical damage to aviation infrastructure and air flow.

In addition, other radio technologies are used in the aviation field, although they are beyond our research topic.

Picture 1, based on an ADS-B source, shows an aircraft that was destroyed by bombing on February 27, 2022, during the Russo-Ukrainian war. The photo was taken a few days later. It was an ideological cyber-attack [3].



Picture 1

## 4. Experimental Work

We used HackRF's hardware for the demonstration. HackRF is a versatile software-defined radio (SDR) platform known for its flexibility and open-source design. It allows users to explore and experiment with different radio frequencies and provides reception and transmission over a wide range of radio frequencies (1mHz to 6GHz) [4].



Picture 2




Picture 3

To generate fake ADS-B signals with a HackRF device, we start by encoding false aircraft data in protocol DO-260B. ADS-B messages follow the Mode S Extended Squitter protocol, using a 56-bit data frame to share details like position, altitude, and identification. Next, we modulate the encoded data into binary bits for the ADS-B message. The HackRF device then transmits these bits at a carrier frequency within the ADS-B band, at 1090 MHz. We then send these fake ADS-B signals sporadically to mimic a non-existent aircraft. Picture 2 and picture 3 demonstrate our experimental work.

To receive and prove the transmitted signal was encoded and transmitted correctly, we use receiver only software defined radio. We decode the signal using open-source software dump-

1090, [10] after the data is decoded live, we confirm that the transmitted and received data match.

The attack was performed in a controllable environment and transmitted signals did not exceed controlled premises. (picture N4).



Hex	Flight	Altitude	Speed	Lat	Lon	Track	Messages
000adb		36000	240	43.107	33.755		1

Picture 4

## 5. Global navigation satellite system (GNSS)

In the modern world it is extremely difficult to find a person without GPS. GPS is an American satellite system that belongs to GNSS, in fact we also use its other systems such as Galileo, Glonass, BeiDou etc. Many people use this navigation tool in their daily life, but only a few of them know how dangerous the cyberattack on it can be. The principle of its operation, at first glance, is quite simple. It works by using a network of satellites orbiting the Earth to pinpoint a position on the planet's surface by calculating the distance between a receiver and multiple satellites to determine a specific location in three-dimensional space based on the timing of the signal and the known positions of those satellites.

Today, a GNSS receiver is available to everyone. All types of GNSS satellites broadcast on different channels, namely: L1, L2, L3, L4, L5. Information from GNSS satellites is transmitted at a speed of 50 bits/sec. It transmits data about the satellite's orbit and satellite time, which in the case of civil aviation cannot be deciphered [5].

GNSS vulnerabilities coupled with radio frequency interference are a concern in the aviation industry. GPS signal loss is becoming increasingly common in civil aviation, especially in politically tense regions. There could be many reasons for this, but it is likely that they are provoked since signal suppression is no longer a problem today. While jamming is very dangerous and can happen from time to time, a spoofing attack is even more dangerous and predictable.

## 6. GNSS Spoofing

GNSS spoofing is a technique in which false signals are transmitted to the receiver, causing it to calculate an incorrect location. It can be spoofed by generating signals that mimic authentic GNSS signals, i.e. sending false information to the receiver. GNSS spoofing increases threat risks because it can be used to fool navigation systems, frustrate critical infrastructure, or disrupt the path of autonomous vehicles and aircraft [6,7]

In a noteworthy incident in 2010, Hanover Airport became an unintended target of a GNSS spoofing attack. Despite the seeming incredibility of such an event, a thorough investigation revealed that the false signals disrupting the aircraft's positioning system stemmed from an ongoing test conducted in a nearby hangar. This incident underscores the vulnerability of GNSS technology to manipulation and highlights the ease with which signals can be spoofed. The ramifications were far-reaching, as the falsified positioning data automatically altered the corresponding ADS-B information, emphasizing the potential implications of such attacks on aviation safety and security [2].

In 2018, Russia accused the US of faking the authenticity of the drone and using it to attack a Russian air base in Syria. Also, in the past few years, there have been many location spoofing incidents near the Russian border, and drones are believed to have been "placed" at nearby airports [8].

This incident sparked significant geopolitical tension between Russia and the United States. Russia leveled accusations against the US, alleging that the authenticity of a drone used in an attack on a Russian air base in Syria had been falsified. This accusation underscored the deep-seated mistrust and rivalry between the two nations, particularly in the context of the complex and volatile Syrian conflict.

Moreover, the claim that drones have been involved in location spoofing incidents near the Russian border raises concerns about the security of airspace and critical infrastructure. These alleged incidents suggest a deliberate attempt to manipulate location data for strategic or nefarious purposes. The suspicion that drones may have been clandestinely placed at nearby airports adds another layer of complexity to the situation, highlighting the potential vulnerabilities in aviation security and the challenges faced in safeguarding against emerging threats. Such accusations and incidents not only exacerbate tensions between nations but also raise broader questions about the integrity of military operations, the reliability of surveillance and monitoring systems, and the need for enhanced cybersecurity measures in an increasingly interconnected world. [13] As technology continues to advance, the potential for misuse and manipulation of drones and other unmanned systems underscores the importance of international cooperation and robust security protocols to mitigate risks and maintain stability. Simple and relatively complex attacks are possible on GNSS. In a simple attack, the attacker suppresses the authentic signal and broadcasts his own fake signal, causing the receiving device to tune in to his signal. Detecting and avoiding such a simple attack is not very difficult, since the fake and real signals will not be synchronized, and this can be easily detected by software. [11] In the case of more complex attacks, the attacker tries to covertly convert the receiver from an authentic signal to a fake one, for this he must first mask the authentic signal with a fake signal so that all indicators are initially like the authentic one, and then change it in his favor [9].

## 7. GNSS Spoofing Prevention Methodology

The greater the involvement of technology in modern life, the greater the probability of insecurity increases, naturally, technological regression cannot help us in this, although there must be certain aspects that must be strictly protected.

We have already explained the dangers of these attacks. And now we can talk about the methods of solving them.

First, to prevent GNSS spoofing, we all think of encrypted data exchange, but with today's technology, this is practically impossible.

Because of the distance, they have to broadcast at a low frequency, which does not allow the implementation of mass encryption. Unlike the military unit.

The military sector is capable of encrypted communication only because they use the same encryption algorithm that the receiver uses to decode the signal. All receivers use the same key. Current GNSS systems only allow communication to be encrypted with a symmetric algorithm. It is unsuitable for civilian use, as storage, distribution and management of different encryption keys is practically impossible.

In fact, one of the appropriate ways of protection may be a verification mechanism.

Additional sensors will be used such as inertial navigation systems (INS) or alternative positioning technologies, which play a critical role in the protection of navigation systems. By combining data from multiple sensors, including GPS, these systems can maintain accurate positioning information even in difficult environments or when the GPS signal is interrupted. Additional sensors provide a backup mechanism that is responsible for the continuity of navigation and protects against potential threats such as GPS spoofing or blocking.

We can consider multi-frequency receivers as another protection mechanism.

Multi-frequency authentication in GNSS allows us to use different frequency signals such as L1, L2 and L5. This approach enhances accuracy by reducing the effects of environmental factors such as the ionosphere, blurring the signal, and resisting interference and spoofing attempts. Multi-frequency authentication contributes to the reliability and security of GNSS, making it valuable for applications that require accurate and reliable positioning information.

We may also have active monitoring of signal quality as a version, which ensures detection of signal changes, anomalies, and unauthorized interference.

## **8. ADS-B Spoofing Prevention Methodology**

By using message authentication, we can make sure that the data is not forged. Authentication of the message can mean an electronic (cryptographic) signature, with which the recipient will confirm the integrity of the message. Or the easiest way, let's go back to the compass methodology.

Amplitude sensing techniques leverage the diverse signal strengths received by various antenna elements. By tapping into the distinct directivity features offered by each antenna's

gain pattern, we can assign a distinct signal signature to every direction from which a signal arrives. One notable method in this category is the Watson-Watt (Adcock) antenna approach. In the realm of signal authentication, the precision of angular measurements required hinges upon the spatial configuration among the transmitting source, the receiving end, and any simulated or phantom aircraft falsely indicated by a spoofed signal. Achieving a desired confidence level in position estimation demands a keen eye on the quality of angular data, ensuring accurate localization despite potential deceptive signals.[12]

## 9. Conclusion

In this elaborate presentation we analyzed the dark side of radio technology leaving no stone unturned on the danger involved in GNSS and ADS-B spoofers. Our foray into this domain underlined the immediate need of heightened readiness and reinforced policies to strengthen the safety, dependability of these indispensable systems.

It seems that most criticism of ADS-B stems from its weak electronic security which was demonstrated in our own testing. It was a wake up call to air traffic controllers, unveiling its vulnerabilities and ease by spoofing. Not only we pointed out the risks but also discussed possible defense measures providing a comprehensive tactical guide for protection against malicious behavior. Against the backdrop of a geopolitical environment characterized by lingering symptoms dating from times gone with cyberspace escalates into an inner shell that commands dangerous amounts, any close examination remains relevant as a shroud against attempts to exert pressure or undermine our systems and institutions.

Through collaboration and vigorous mechanisms put in place for cyber security, we can all work together to navigate through the complex world of radio technology ensuring it remains a force good then an instrument which people use as instruments. By ensuring vigilance, inventiveness and unified political will for cyber security we can reduce the chances lurking in spoofing practices to achieve a secure technology future.

## References

- [1] Dejan V. Kozovic et al., Spoofing in aviation: Security threats on GPS and ADS-B systems. April 2021, Vojnotehnicki glasnik 69(2):461-485 DOI:10.5937/vojtehg69-30119 [https://www.researchgate.net/publication/350481235\\_Spoofing\\_in\\_aviation\\_Security\\_threats\\_on\\_GPS\\_and\\_ADS-B\\_systems](https://www.researchgate.net/publication/350481235_Spoofing_in_aviation_Security_threats_on_GPS_and_ADS-B_systems)
- [2] Federal Aviation Administration: "Ins and Outs". February 7, 2023 [https://www.faa.gov/air\\_traffic/technology/equipadsb/capabilities/ins\\_outs](https://www.faa.gov/air_traffic/technology/equipadsb/capabilities/ins_outs)
- [3] James Field. Ukraine Crisis: FlightRadar24 User Provides Fake Data on Antonov AN-225 Mriya With Expletive Towards President Vladimir Putin. March 11, 2022 <https://www.key.aero/article/225-airborne>



- [4] HackRF: “Great Scott Gadgets” (Hardware). [https://greatscottgadgets.com/hackrf/?fbclid=IwAR118kAxZmfu\\_cDPFRp0KbPOVL\\_fqg31\\_khssQZsLzXzaNqBQ1OTPgZio](https://greatscottgadgets.com/hackrf/?fbclid=IwAR118kAxZmfu_cDPFRp0KbPOVL_fqg31_khssQZsLzXzaNqBQ1OTPgZio)
- [5] Nan Shen, Liang Chen et al. A Review of Global Navigation Satellite System (GNSS)-Based Dynamic Monitoring Technologies for Structural Health Monitoring. 26 April 2019 [https://www.mdpi.com/2072-4292/11/9/1001?fbclid=IwAR3rd9kf98ptWCrwTO2G0rk2Ohamjq0m0Pd2aPk5NR66Z3r\\_ZCdqT8dT6nek](https://www.mdpi.com/2072-4292/11/9/1001?fbclid=IwAR3rd9kf98ptWCrwTO2G0rk2Ohamjq0m0Pd2aPk5NR66Z3r_ZCdqT8dT6nek)
- [6] FAA Officially Launches Radar’s Replacement. March 9, 2009 <https://www.flyingmag.com/gear-avionics-faa-officially-launches-radars-replacement/>
- [7] What is GPS spoofing? <https://www.mcafee.com/learn/what-is-gps-spoofing/>
- [8] Russia Claims U.S. Led Drone Attack on Russian Air Base In Syria. October 25, 2018 <https://www.rferl.org/a/russia-claims-u-s-led-drone-attack-on-russian-air-base-in-syria/29563585.html>
- [9] Gustavo Lopez, Maria Simsky. What is GNSS Spoofing? March 8, 2021 [https://www.gim-international.com/content/article/what-is-gnss-spoofing?fbclid=IwAR0Xb\\_QyGURQC-vQrUdh9dyTmbY99hHUjubOAVrwRBEoNba\\_CjJSEnfbYOA](https://www.gim-international.com/content/article/what-is-gnss-spoofing?fbclid=IwAR0Xb_QyGURQC-vQrUdh9dyTmbY99hHUjubOAVrwRBEoNba_CjJSEnfbYOA)
- [10] Antirez: “dump1090” (Software Package). <https://github.com/antirez/dump1090>. Accessed 12.02.2024
- [11] Seco-Granados, G., Gómez-Casco, D., López-Salcedo, J.A. et al. Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability. *GPS Solut* 25, 33 (2021). <https://doi.org/10.1007/s10291-020-01049-z>
- [12] Jeong, S., Lee, J. Synthesis Algorithm for Effective Detection of GNSS Spoofing Attacks. *Int. J. Aeronaut. Space Sci.* 21, 251–264 (2020). <https://doi.org/10.1007/s42405-019-00197-y>
- [13] Lebrun, S., Kaloustian, S., Rollier, R., Barschel, C. (2021). GNSS Positioning Security: Automatic Anomaly Detection on Reference Stations. In: Percia David, D., Mermoud, A., Maillart, T. (eds) *Critical Information Infrastructures Security. CRITIS 2021. Lecture Notes in Computer Science()*, vol 13139. Springer, Cham. [https://doi.org/10.1007/978-3-030-93200-8\\_4](https://doi.org/10.1007/978-3-030-93200-8_4)