CyCon 2025: The Next Step
17th International Conference on Cyber Conflict
C. Kwan, N. Gratzer, K. Podiņš, M. Tolppa (Eds.)
2025 © NATO CCDCOE Publications, Tallinn

Navigating Turbulence: Understanding New GNSS Risks in Conflict Zones

Michael Felux
School of Engineering
Zurich University of Applied Sciences
Winterthur, Switzerland
michael.felux@zhaw.ch

Benoit Figuet
SkAI Data Services
Zurich University of Applied Sciences
Winterthur, Switzerland
benoit.figuet@skai-data-services.com

Vincent Lenders
Cyber-Defence Campus
armasuisse
Thun, Switzerland
vincent.lenders@armasuisse.ch

Raphael Monstein
SkAI Data Services
Zurich University of Applied Sciences
Winterthur, Switzerland
raphael.monstein@skai-data-services.com

Martin Strohmeier
Cyber-Defence Campus
armasuisse
Thun, Switzerland
martin.strohmeier@armasuisse.ch

Abstract: Aviation's dependency on global navigation satellite systems (GNSSs) has highlighted the vulnerability of aircraft to jamming and spoofing attacks, which pose significant safety and security challenges. These threats, created and exacerbated by recent geopolitical conflicts, underscore the necessity for monitoring and mitigating GNSS interference to ensure the integrity of aviation systems. This paper examines the impact of GNSS interference on civil and military aviation, focusing on its operational and safety implications. By building a new tool that exploits Automatic Dependent Surveillance-Broadcast (ADS-B) data, we identify hotspots of GNSS jamming and spoofing in conflict zones during 2024 in regions such as the Black Sea, Eastern Mediterranean, and the India–Pakistan border during peak periods. Daily detections peaked at 1,500 flights, declining to about 500 flights by late 2024.

Finally, we discuss the applicability of existing countermeasures, such as cryptographic authentication, multi-constellation GNSS usage, and data fusion with inertial systems. While promising, these methods face challenges in widespread adoption due to technical, operational, and regulatory constraints.

Our results contribute to understanding the evolving nature of GNSS threats and demonstrate the need for collaborative international efforts to develop resilient aviation navigation systems. By prioritizing GNSS interference monitoring and mitigation, the aviation sector can enhance safety, operational reliability, and preparedness against future threats.

Keywords: *GNSS, GPS, jamming, spoofing, aircraft*

1. INTRODUCTION

The insecurity of global navigation satellite systems (GNSSs), such as the Global Positioning System (GPS) and the European Galileo, has been known since at least the early 1990s [1]. A combination of a weak received signal strength and a lack of authentication (apart from the recently introduced Galileo Open Service Navigation Message Authentication, OSNMA [2]) makes it an easy target for both accidental and malicious interference, including jamming and spoofing. Despite many warnings from security researchers and increasing numbers of reported interference incidents across different applications [3], [4], [5], the global dependency on GNSSs has grown significantly during the past decade, simply due to their high utility in all sectors of life and industry.

While it has always been an open secret that GNSS interference could also impact the aviation sector, specifically aircraft navigation systems, until recently, it was restricted to a few known areas and limited to jamming, and as such was considered an occasional fact of pilot life [6]. With the Ukraine–Russia war and escalating tensions in the Middle East, this changed fast, and malfunctioning GNSS systems became a common and significant issue for both military and civil aircraft [7], [8].

A prominent example came in May 2024, when Tartu airport in Estonia was affected by interference (according to the Estonian government, the source was inside Russia), rendering its GPS-based approach procedures unavailable [9], [10]. This potentially lethal damage shut down all commercial flight services to the airport for weeks, until a GPS-free approach procedure based on ground-based distance measuring

equipment (DME) could be enabled. Other incidents in civil aviation have involved spurious alerts from the ground proximity warning system, causing sudden and unsafe maneuvers [3].

In [11], the authors analyzed the evolution of GNSS jamming over one year after the onset of the war in Ukraine, which showed that the effect varied significantly regionally and over the year. Recent efforts from different researchers have focused on methods to detect the evolving threat of GNSS spoofing and its localization based on ADS-B data [12], [13], [14]. In this paper, we conduct a comprehensive analysis of GNSS interference on aircraft in various conflict zones in 2024. To do this, we exploit the information on the estimated quality and accuracy of the GNSS positions broadcast by civil and military aircraft using the Automatic Dependent Surveillance-Broadcast (ADS-B) technology to a large network of more than 7,000 ground-based receivers globally.

Our analysis shows that, at its peak, more than 1,500 flights have been affected daily near conflict regions from the Black Sea to the Eastern Mediterranean to the India–Pakistan border. Beyond the impact on the affected aircraft, this approach provides insights into the conflict areas subject to jamming and spoofing, the types of interference techniques used, and the origins of the interferences.

To summarize, this paper makes the following contributions:

- We present a new tool to detect GNSS interference, both jamming and spoofing, on a global scale. The tool exploits the ADS-B technology widely deployed in civil and military aircraft worldwide.
- We analyze one year of incidents using crowdsourced open ADS-B data. We find hotspots in war and crisis areas.
- We analyze the impact on civil aviation in these airspaces by quantifying the interference, including the approximate origin, and discussing several safety-relevant case studies.
- Finally, we discuss possible avenues forward to secure GNSS. This includes academic proposals to strengthen its security and the countermeasures Galileo has deployed against spoofing.

2. BACKGROUND

We briefly describe the use of GNSS in aviation and its known security issues. We go on to explain the concept of aircraft transponder data that can be used to detect

attacks on GNSSs at a global scale. We refer to the civilian version of GPS unless noted otherwise.

A. GNSSs in Aviation

Among the major global navigation satellite constellations (GPS, Galileo, GLONASS, and BeiDou), relevant standards have only been developed for GPS and GLONASS. All major aircraft manufacturers only use avionics that rely solely on GPS, leveraging its ability to determine position, velocity, and precise time. The onboard receiver estimates its position by measuring so-called pseudoranges (i.e., ranges determined based on signal propagation time measurements with a user clock unsynchronized to GPS time) from multiple satellites with known positions to an unknown user location, whether on land, at sea, or in the air. Based on this information, a set of equations with four unknowns can be formulated: the three-dimensional coordinates of the receiver and the offset of the receiver's clock relative to GPS time. By applying numerical methods, these equations are solved to determine the receiver's position and time.

For air navigation, the integrity of GPS data is continuously monitored to ensure safety. Aircraft-based integrity monitoring can be categorized into two types: receiver autonomous integrity monitoring (RAIM), which relies solely on GNSS data, and aircraft autonomous integrity monitoring, which incorporates additional sensors such as barometric altimeters, clocks, or inertial navigation systems. In RAIM, a minimum of six satellites is required to detect and exclude a faulty satellite by testing all possible combinations of satellite subsets.

1) GNSS Security Issues

In this section, we discuss the two main threat vectors to GNSSs: jamming and spoofing.

As GNSS satellite signals are extremely weak, reaching Earth below the noise floor, they can be easily interfered with even over long distances. Fundamentally, an attacker is only constrained by their power budget and line of sight to the target. Aircraft, particularly at cruising altitudes, can thus be targeted at long distances, in extremis up to the radio horizon of about 300 miles.

Jamming

Jamming involves the intentional transmission of radio frequency signals that disrupt the reception of legitimate GNSS signals. Concretely, such interference causes the receiver to lose its lock on legitimate satellites and leaves it unable to determine its position. This will typically show in the aircraft's flight instruments as "no GPS position." The position will then be estimated with less accurate means, such as conventional ground-based navigation aids like DME, VHF Omnidirectional Range

(VOR), and/or the aircraft's onboard inertial sensors, which can drift over time and can thus deviate substantially from the true position. While aircraft were designed to and are perfectly able to continue navigating without GPS, the use of precise and reliable GNSS-based navigation is a key enabler for providing airspace capacity. Given current and expected future traffic volumes, the unavailability of GNSSs can have a significant impact on capacity. Figure 1 shows the impact of jamming on an Airbus A350.

FIGURE 1: GPS JAMMING AS SEEN ON AN SAS AIRBUS A350 FROM COPENHAGEN TO BANGKOK. INTERFERENCE WAS REPORTED FROM POLAND TO THE PERSIAN GULF [15], [16]

Spoofing

A step up in complexity from jamming, we define spoofing as manipulating or overshadowing GNSS signals to deceive receivers into calculating incorrect positions. Growing in accessibility since the early 2000s, commercial products and open-source software enable cheap, easy, and widespread execution of various spoofing techniques for many actors.

Pilots on aircraft subject to spoofing may be shown the wrong position on their flight instruments if the aircraft does not detect the GPS position error and reject it. Most passenger aircraft have proven to be effective in detecting spoofing and excluding GPS information when determining the aircraft's position. However, in less well-equipped (usually smaller) aircraft, position information may not be based on hybridization

with inertial sensors and/or may be based on GPS only. An example from an avionics security laboratory experiment is shown in Figure 2.

FIGURE 2: AVIONICS SECURITY LABORATORY UNDER GPS SPOOFING. THE GARMIN SYSTEM SHOWS ITS GPS POSITION IN SCANDINAVIA DESPITE BEING LOCATED IN SWITZERLAND

B. ADS-B

The ADS-B protocol enables aircraft to broadcast their ID, position, velocity, and additional information, such as intent or urgency codes. These broadcasts occur twice per second for position and velocity updates and once every five seconds for identification. Mandated for use in U.S. and European airspace since the early 2020s, ADS-B is intended to improve the accuracy of air traffic control's (ATC) situational awareness, and it reduces system costs by replacing traditional radar systems. This protocol represents the shift toward cooperative, digital data communication networks in the next generation of ATC, enhancing and eventually replacing analog methods.

In addition to position information, parameters describing the estimated quality of the transmitted position are included in the ADS-B messages. These parameters include the Navigation Integrity Category (NIC). The Navigation Accuracy Category for Position

(NACp) indicates the maximum radius of a circle centered at the transmitted position within which the actual position is expected to be with a high probability, while the NIC specifies an integrity containment radius around the transmitted position. Both parameters are further described in the RTCA DO-260B standard document.

Most aircraft transmit ADS-B position messages based on GPS data alone, typically without hybridization or data fusion with inertial reference units, making them a particularly effective method to detect spoofing.

C. OpenSky: Crowdsourcing Air Traffic Data for Security

The OpenSky Network[1] (OSN) is a crowdsourced sensor network that collects ATC surveillance data for public access and research. Since 2013, it has continuously gathered data, offering a vast historical database of individual aircraft messages, unlike commercial flight tracking services, which aggregate them. This resource supports advancements in ATC technologies and research across various fields, from air traffic management and earth science to cybersecurity.

Starting with just eight sensors in Switzerland and Germany, the network now includes over 7,000 registered receivers worldwide. As of 2025, it has accumulated more than 12 years of data, covering over 35 trillion aircraft messages. Initially focused on ADS-B, OpenSky expanded to include further air traffic communication technologies such as Mode S, VHF, and FLARM.

The network relies on enthusiasts, academics, and institutions, with coverage limited by the line-of-sight range of individual sensors, typically 400–500 km. Growth has mirrored population density and economic development, with saturation reached in regions like Europe and the U.S. by 2024. However, significant coverage improvements continue in areas such as the Middle East, South Asia, and New Zealand, particularly at lower altitudes. OpenSky remains a vital tool for enhancing air traffic research and technologies globally, with over 650 publications depending on its data to date [17].

OpenSky provides convenient interfaces to both historical and live data for us to retrieve the necessary position and accuracy information we require for efficient detection of GNSS interference, as described in the next section.

3. IMPACT OF GNSS INTERFERENCE ON AIRCRAFT

GNSS jamming and spoofing can have severe implications for modern aircraft operations, as many aviation systems rely heavily on accurate GNSS signals for navigation, communication, time, and situational awareness. The effects and severity

1 https://opensky-network.org

vary widely between aircraft and avionics types, and spoofing is generally more disruptive than jamming. The reason is that, whereas jamming causes the receiver to be unable to determine its position, spoofing causes the receiver to determine a faulty position. If undetected, this can cause contamination of the hybrid navigation—that is, the fused navigation obtained from multiple sources, such as inertial navigation. Below, we discuss some of the main ways in which GNSS interference can negatively impact an aircraft's systems and safety:

1. **Steering Off Course**
   The most immediate and obvious consequence of GNSS interference may be the aircraft deviating from its intended flight path if it is following a spoofed false position. This can result in the aircraft entering restricted, dangerous, or politically sensitive airspace, posing risks to operational safety and security, as has reportedly happened previously with a business jet almost entering Iranian airspace without clearance [18]. In extreme cases, this could escalate to airspace violations or military interventions. Such deviations could also lead to increased fuel consumption and delays, further compounding operational issues. It should be noted, however, that significant deviations from the intended trajectory have been very rare.

2. **Spurious Ground Proximity Warnings**
   GNSS interference can cause errors in Enhanced Ground Proximity Warning Systems (EGPWS) that rely on GNSS data to determine the aircraft's position relative to the terrain. This has reportedly already resulted in erroneous ground proximity warnings [8], [19], prompting unnecessary and potentially hazardous reactions from the flight crew. Frequent false alarms can also degrade trust in these critical safety systems, leading to delayed or complete lack of response in genuine emergencies.

3. **Reduced Navigation Performance Post-Interference**
   Even after leaving the area of direct GNSS interference, negative effects can persist as some avionics systems are seemingly unable to recover without a restart, which causes operational overheads. As a result, the aircraft may be unable to comply with the required navigation performance (RNP) standards even outside the immediately affected conflict zones, which may cause complications regarding aircraft separation and terminal navigation. We analyzed a sample of 397 transatlantic flights from Europe to America that were spoofed over the Black Sea in the summer of 2024. Of this sample, 10% were still broadcasting severely reduced navigation performance as they entered oceanic airspace.

4. **Unavailability of Approach Procedures Requiring GNSS and Precision Approaches Using GBAS/SBAS**
   GNSS-based augmentation systems, such as the Ground-Based Augmentation System (GBAS) and Satellite-Based Augmentation System (SBAS), are required for certain precision approaches. Interference can disrupt these systems and render approach procedures unavailable, as seen in incidents like the ones in Denver and Dallas in 2023.

5. **Loss of Datalink/CPDLC Capability**
   Beyond confusing the aircraft position, GNSS spoofing can lead to discrepancies between GPS time and an aircraft's internal clock. This misalignment can disrupt datalink communications, including controller–pilot data link communications (CPDLC), which require accurate time synchronization. Loss of CPDLC capability compromises efficient communication between pilots and ATC, particularly in oceanic and remote airspace, increasing workload and reliance on voice communications. This degradation in communications efficiency poses potential risks in high-traffic areas or during emergencies.

4. DETECTING GPS JAMMING AND SPOOFING USING ADS-B DATA

A. GPS Jamming

To identify GPS jamming events, two parameters from ADS-B data can be used: the NIC parameter and the NACp (similar approaches were previously discussed, for example, in [20], [21]). NIC is embedded within position messages and provides an indicator of the integrity of the navigation solution, while NACp is included in status messages and reflects the positional accuracy of the aircraft. For this analysis, NIC is preferred because it is directly embedded in position messages, which also contain the aircraft's latitude, longitude, and altitude. This makes it simpler to evaluate navigation integrity with NIC than with NACp.

In scenarios where GPS jamming is present, the NIC value typically decreases, often dropping from values above 6 (indicating reliable GPS availability) to 0 (indicating compromised navigation integrity). By monitoring NIC values, we can identify instances of GPS interference. Specifically, we aggregate the percentage of flights within a defined geographical area reporting a low NIC (NIC < 4) relative to those reporting a high NIC (NIC > 6). This ratio is calculated as follows:

$$\text{ratio} = \frac{\text{Number of flights with NIC} < 4}{\text{Number of flights with NIC} > 6 + \text{Number of flights with NIC} < 4}$$

This ratio is computed hourly to allow for temporal analysis of jamming incidents. By mapping these ratios spatially, we can identify regions affected by GPS interferences.

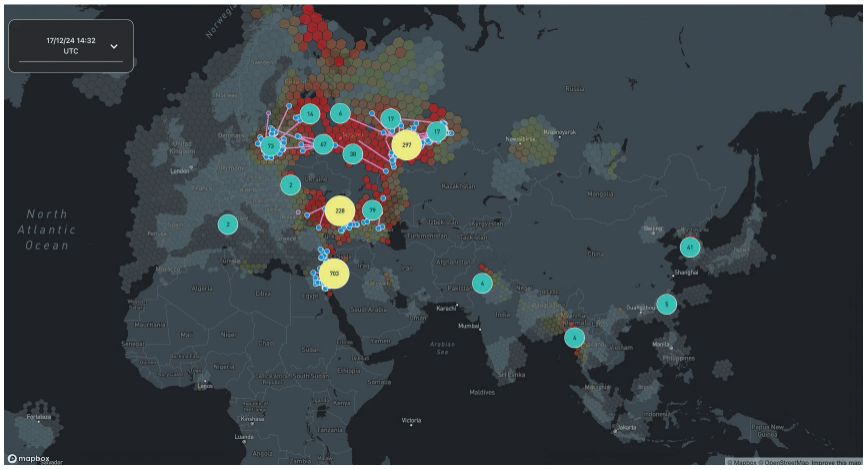
B. GPS Spoofing

We detect anomalies in the transmitted positions, such as position jumps, unrealistic speeds, or incoherent altitudes, to detect aircraft affected by spoofing. Our methodology assumes that GPS spoofing is not targeted at individual aircraft but affects multiple aircraft in the same area. To reduce noise and improve detection accuracy, we cluster the reported spoofed positions, retaining only locations reported by multiple aircraft as spoofed. This clustering approach allows us to filter out isolated anomalies and focus on genuine spoofing events that impact broader airspace regions.

C. A Tool to Monitor GPS Jamming and Spoofing Almost in Real Time

Using the techniques presented above, we have developed a website[2] that ingests ADS-B data from the OpenSky Network, identifies GPS spoofing events almost in real time, and displays GPS jamming incidents with a delay of less than two hours. Figure 3 shows the interface and display of our tool, illustrating detected jamming and spoofing interference on a single day in December 2024.

FIGURE 3: SCREENSHOT OF GPS JAMMING AND SPOOFING DETECTION MAP ON DECEMBER 17, 2024



Note: Clusters show spoofed GPS positions of aircraft, with numbers indicating the count of spoofed flights per location. Blue markers represent aircraft positions before spoofing, connected by lines to their spoofed locations. Colored hexagons indicate GPS jamming intensity, with red denoting higher levels of interference.

2 Publicly accessible at https://spoofing.skai-data-services.com

5. EXPERIMENTAL DESIGN

A. Global Analysis

To analyze global GPS spoofing activity, we used ADS-B data from the OSN spanning January 1 to December 12, 2024. The global analysis is not geographically restricted but is limited to OSN's ground-based receiver coverage, which is more dense in regions such as Europe, North America, and parts of Asia and sparse in areas such as the polar regions and oceans. Using this dataset, we identified and characterized spoofing events using the method introduced in section 4.B.

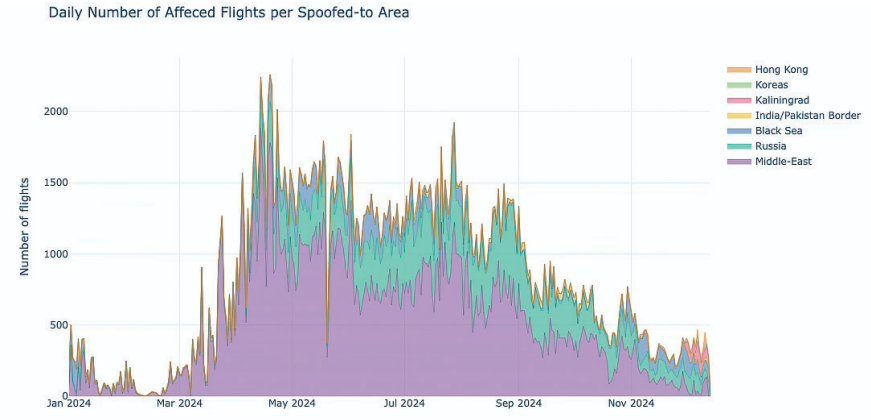
B. Kaliningrad Case Study

To analyze GPS spoofing activity around the Kaliningrad exclave, we focused on the period from December 1 to December 30, 2024, corresponding to the initial emergence of the spoofing activity in this region, which began in late November. For each identified affected flight, we also retained the last valid observation recorded before the onset of GPS spoofing.

6. QUANTITATIVE RESULTS: GNSS INTERFERENCE IN CONFLICT ZONES

While GPS jamming has been observed widely for almost two decades [22], widespread GPS spoofing affecting aviation is a relatively new phenomenon and began in earnest in the autumn of 2023. Figure 4 illustrates the rise of spoofing globally, with incidents grouped by geographical location. The daily number of detected flights plateaued around May 2024, with between 1,000 and 1,500 flights affected daily. The number decreased around September 2024 to under 500 fights affected daily. The decrease is mainly due to the decreased spoofing activities in two locations that see relatively large amounts of aircraft traffic: the Middle East and the Black Sea. Both locations have a relatively high air traffic density; thus, many aircraft are affected by it. The decrease in affected flights in the Middle East is due to the more limited operation of the spoofer. During the summer, the spoofer was active almost all day, every day. Since then, it appears that the spoofer has been active intermittently, for shorter periods of time.

FIGURE 4: NUMBER OF DETECTED UNIQUE FLIGHTS PER DAY



Note: The colors indicate the geographical region.

Individual events, such as the destruction of an oil platform in the Black Sea by the Ukrainian armed forces at the beginning of August can lead to a change in spoofing patterns. A Ukrainian spokesperson stated that the platform hosted a GNSS spoofer and was a danger to civil navigation. After the strike, the detected spoofing patterns in the area changed. While the daily number of affected aircraft decreased, it did not reduce to zero. Instead, other spoofers at different locations continued to disrupt civil air traffic.

Spoofers affecting large amounts of air traffic simultaneously, such as the ones in the Middle East and Russia, are well-known, so flight crews can be briefed and prepared for a potential impact on the aircraft. However, smaller and less frequently active spoofers also pose a danger to air traffic. They might not be known to the flight crew and might take them by surprise, increasing the workload and the risk of loss of situational awareness. A noteworthy example is the GPS interference on the southern border of North Korea. On May 28–29 and June 1–2, North Korea launched hundreds of balloons filled with trash and feces toward South Korea. At the same time, GPS interference at the border was detected at scale. It started on May 28 with GPS jamming, followed by spoofing from May 30 to June 2. Even aircraft on the ground at Incheon International Airport were affected during that period. After that initial period, little interference was detected until November 5, when both jamming and spoofing activities increased again, and have continued intermittently since.

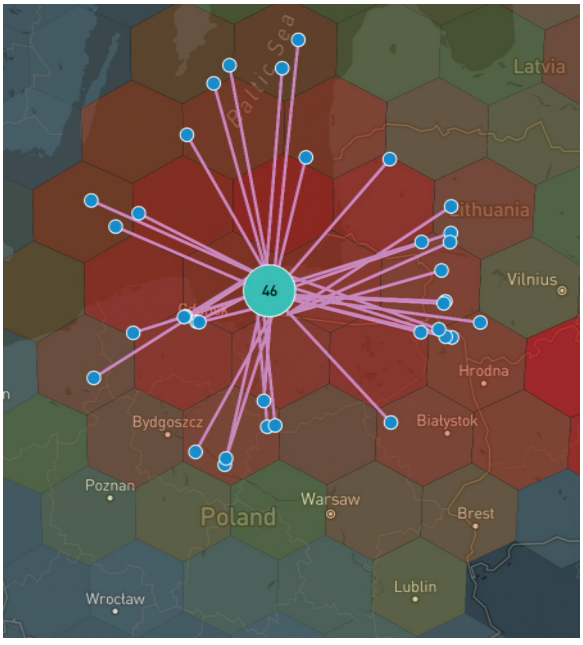
It is worth noting that GNSS interference is not limited to active conflict zones. For example, spoofing was detected on December 18 around Hong Kong and Macau. On

that day, China's President Xi Jinping arrived in Macau to mark 25 years of Chinese rule over the former Portuguese enclave. This visit coincided with spoofing activities in the area on that day. In our data sample, aircraft in this area were usually not affected by spoofing, and only experienced issues on December 7 and 9.

7. CASE STUDY

Since late November 2024, we have observed significant GPS spoofing activity impacting aircraft operating over Poland, Finland, Lithuania, and Belarus. Affected aircraft reported erroneous positions localized within the Kaliningrad exclave. Figure 5 illustrates December 8, when the Live GPS Spoofing Tracker identified spoofing incidents involving 46 aircraft.

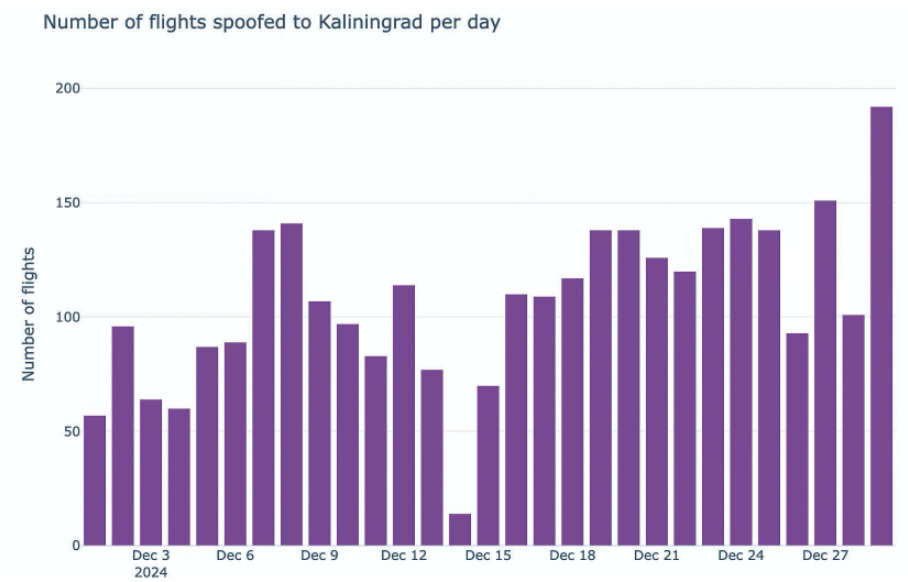
FIGURE 5: SPOOFING ACTIVITY ON DECEMBER 8, 2024, WHEN 46 AIRCRAFT WERE SPOOFED FROM KALININGRAD



Note: Blue markers represent the actual positions of the aircraft before spoofing occurred. The intensity of GPS interference is depicted by the color of the hexagons, with red indicating higher levels of detected interference.

By analyzing the historical database of the OSN, we identified over 3,000 flights affected by this spoofing activity, with as many as 150 aircraft impacted on December 30 alone. Figure 6 presents the daily count of flights detected as spoofed.

FIGURE 6: THE DAILY NUMBER OF UNIQUE FLIGHTS SPOOFED TO KALININGRAD BASED ON THE OSN HISTORICAL DATABASE



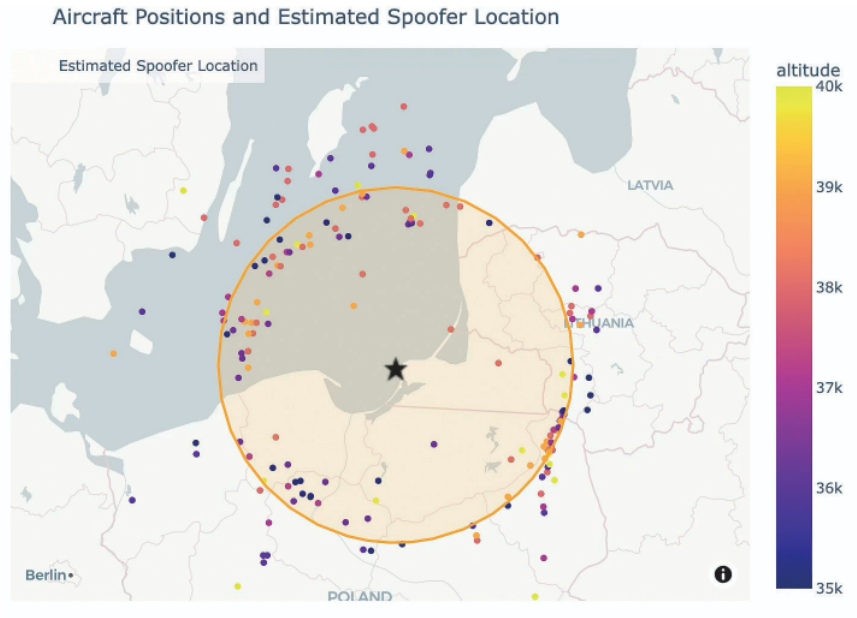
In addition to using ADS-B data to detect spoofing activity, it is also possible to approximate the location of the spoofer. By assuming a single spoofer operating from the ground and considering that radio wave propagation follows a line-of-sight principle, we infer that aircraft at the same altitude will be affected at similar distances from the spoofer.

To estimate the spoofer's position, we analyze the last valid positions of affected aircraft immediately before they were spoofed. By fitting a circle to these positions, we hypothesize that the spoofer's approximate location corresponds to the center of the fitted circle. This method provides a rough but effective estimate of the interference source.

To apply this method to our dataset, we first filter the data to include only position reports from aircraft flying at altitudes between FL350 and FL400. This altitude range is chosen to ensure that the selected aircraft are at similar flight levels, thereby maintaining consistency in their line-of-sight distance to the spoofer. Furthermore, this altitude range was selected because it contains a high density of aircraft in our

dataset. Additionally, we retain only position reports where the time difference between the last valid position and the first spoofed observation is less than 5 minutes. The filtered latitude and longitude coordinates are then projected onto a Cartesian coordinate system using the EuroPP projection.

FIGURE 7: VISUALIZATION OF FILTERED AIRCRAFT DATA DEPICTING THE LAST VALID POSITIONS OF AFFECTED AIRCRAFT (MARKERS)



Note: The orange fitted circle represents the estimated range of the spoofer for aircraft flying at altitudes between 35,000 and 40,000 feet, and the circle's center (star), indicates the estimated spoofer location. The markers' colors correspond to the altitude of the aircraft at the time they were spoofed.

In total, we obtained 284 data points for this analysis. The estimated spoofer location is at latitude 54.84 and longitude 19.83, in Kaliningrad, with the fitted circle having a radius of 220.4 km. This is illustrated in Figure 7, where the markers represent the last valid positions of the aircraft, and the star indicates the center of the circle, representing the likely location of the spoofer.

8. DISCUSSION

In this section, we discuss the results, their limitations, and potential countermeasures against GNSS interference in aviation.

A. The Imperative of Monitoring GNSS Interference

We argue that monitoring GNSS interference in aviation is of increasing importance, for both civil and military stakeholders. This importance is illustrated by the rapidly growing interest in up-to-date information on GNSS interference. In December, we observed almost 10,000 active users on our interference detection website, a significant amount for such a niche website that is less than a year old. At the same time, new and established organizations, such as gpsjam.org and Flightradar24,[3] have similar offerings, and the number of providers is increasing. In civil aviation, including up-to-date information in pre-flight briefings can prepare the crew for GNSS interference, reduce the surprise factor, prepare procedures to address radio frequency interference (RFI) and its associated effects, and increase situational awareness. Additionally, understanding the nature and impact of GNSS interference on aviation and all other users enables the development of technological and procedural mitigations. These advancements can make flying in the vicinity of conflict zones safer and help prevent incidents and accidents. From a military perspective, monitoring GNSS interference is essential for understanding and adapting to evolving jamming and spoofing strategies, ensuring preparedness and resilience in the face of these challenges. By prioritizing GNSS interference monitoring, aviation stakeholders can enhance safety, security, and operational effectiveness in increasingly complex environments.

B. Limitations

Detecting GNSS RFI using ADS-B data has many advantages but also several limitations.

First, it cannot detect interference in regions lacking either ADS-B coverage or active air traffic. While more and more receivers go online every day, uninhabited areas over oceans and mountain ranges are naturally difficult terrain to cover. Further, ADS-B ground receivers cluster in wealthy, industrialized regions and countries, leaving many African countries, for example, uncovered. Some of this can be mitigated using satellite-based ADS-B receivers. However, these systems cannot offer the same sensitivity and update rate [23].

Second, it should be noted that the effectiveness of this approach is contingent on aircraft flying in regions susceptible to interference, posing limitations when restricted by no-fly zones, such as those enforced by the International Civil Aviation Organization in conflict zones like Ukraine. However, open aviation data is often the

3 https://www.flightradar24.com/data/gps-jamming

best tool available, and it is being used widely by everyone from academic researchers to air traffic controllers to mainstream data journalists.

Third, the proposed methodology cannot identify targeted spoofing attacks affecting a single aircraft. Suppose a strong military attacker focuses on a particular, high-value aircraft. In that case, they can orchestrate the signals such that only that target is affected and slowly steered off course. Here, local countermeasures on the aircraft need to be deployed to detect the attack.

Fourth, the inherent noise in ADS-B data makes it challenging to eliminate false positives and false negatives entirely. As discussed by [19], many deliberate and non-deliberate sources of interference can influence the crowdsourced air traffic data underlying our approach. While such noise makes up only a small fraction and can be filtered out in post-processing, false positives can happen. We prevent this through carefully adjusted thresholds in our algorithms and by examining interference incidents over longer periods, which increase confidence in our analysis.

C. Countermeasures

Identifying GPS interference in the cockpit of a modern airliner with its complex avionics is not always straightforward. This is because the information displayed to the pilots is often a fused position estimate drawing from various sources. Flight crews unaware of the potential of GPS interference can be caught by surprise and might need time to track the issue. This can be mitigated by providing up-to-date information to prepare the crew for such a case. Additionally, recovery of the position estimate is a crucial second step after jamming and spoofing.

We detail the state-of-the-art countermeasures grouped into approaches leveraging data fusion with other GNSS or navigation aids, cryptographic solutions, and physical and application layer solutions. The aviation sector, with its long certification and deployment timelines, faces challenges in implementing updates quickly. Modifying the Minimum Operational Performance Standards for GNSS receivers to improve (or even just begin to address) security is a significant undertaking.

1) Data Fusion

Using multiple GNSS constellations (e.g., GPS and Galileo) at the same time increases resilience against certain naive spoofing threats that only target one system. However, it is straightforward to target several systems at the same time.

Integrating GNSS data with inertial navigation systems, DME, or other ground-based systems such as VOR or non-directional beacons can provide better layers of resilience. Indeed, instead of potentially phasing out the older technologies, several

European air navigation service providers are increasing investment in them in order to reduce reliance on GPS.

2) Message Encryption and Authentication

Cryptographic approaches such as [24], [25], [26] involve encrypting and authenticating navigation messages, making it infeasible for attackers to forge GNSS signals for arbitrary spoofing. While fundamentally the best approach to securing wireless systems, standard methods are difficult to deploy in a global and open system. Military GPS does employ encryption and spread-spectrum techniques to protect against spoofing and jamming. While effective, these techniques rely on secret keys that must be securely exchanged and managed, making them infeasible for shared and global civilian systems.

The European GNSS system, Galileo, implements anti-spoofing measures based on timed efficient stream loss-tolerant authentication (TESLA) [27]. While not similarly effective as military encryption, these measures provide some authentication of the navigation data, offering enhanced protection for civilian use.

3) Physical and Application Layer Countermeasures

Techniques from the literature at the physical layer focus on detecting anomalies in radio frequency properties of the GNSS signals, such as signal strength [28] and auxiliary peaks [29], angle and direction of signal arrival [30], and validation of satellite ephemeris and timing data [29]. Using multiple antennae or receivers enhances the ability to detect interference by analyzing the spatial properties of incoming signals.

Beyond mere detection, several approaches can recover the true GNSS signal and allow the navigation system to provide the correct position. Successive interference cancellation techniques involve iterative removal of spoofed signals to isolate and recover legitimate GPS signals [31], [32]. Antenna arrays can spatially filter signals, enhancing resilience against interference and spoofing. Peripheral anti-jamming devices such as described in [16] are designed to filter out jamming signals. They are commercially available and provide protection up to certain signal strengths. However, no wireless system is entirely immune to sufficiently strong jamming attacks, particularly in contested environments or over hostile territory.

9.CONCLUSION

The escalation of GNSS interference, particularly spoofing, poses a severe threat to civil aviation safety and efficiency as increasingly severe and common recent incidents

show. Urgent research is needed to enhance awareness, detection, localization, and mitigation strategies.

In this paper, we have described a novel tool that exploits ADS-B data sent by aircraft and received by crowdsourced receivers around the world to demonstrate how widespread the issue of GNSS interference is for aviation. We have identified hotspots of GNSS jamming and spoofing in several conflict zones during 2024, in particular in regions such as the Black Sea, Eastern Mediterranean, and the India–Pakistan border during peak periods. Daily detections peaked at 1,500 flights, declining to about 500 flights by late 2024.

We believe that more research is needed to better understand the potential impact of GPS interference on autopilot and autolanding systems. The impact is likely to be greatest and most direct when there are no humans in the loop. Without adequate measures, the risk of severe accidents looms large, emphasizing the imperative need for awareness, education, and proactive intervention.

REFERENCES

[1] J. R. Vasquez, "Detection of spoofing, jamming, or failure of a global positioning system (GPS)," M.S. thesis, Air Force Institute of Technology, 1992.

[2] A. Pirsiavash, A. Broumandan, and S. Kennedy, "Galileo open service navigation message authentication (OSNMA): Benefits, challenges, and limitations," in *Proc. 37th Int. Tech. Meeting Satellite Division Inst. Navig. (ION GNSS+)*, 2024.

[3] A. Morrison, N. Sokolova, and A. Diez, "The evolving GNSS RFI threat space," in *Proc. 36th Int. Tech. Meeting Satellite Division Inst. Navig. (ION GNSS+)*, 2023, pp. 4197–4208.

[4] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *NAVIGATION*, vol. 64, no. 1, pp. 51–66, 2017.

[5] A. Konovaltsev et al., "Interference detection and characterization with an array-based GNSS receiver using conformal antennas in maritime environments," in *Proc. 30th Int. Tech. Meeting Satellite Division Inst. Navig. (ION GNSS+)*, 2017, pp. 2795–2811.

[6] O. Osechas, F. Fohlmeister, T. Dautermann, and M. Felux, "Impact of GNSS-band radio interference on operational avionics," *J. Inst. Navig.*, vol. 69, no. 2, 2022.

[7] M. Felux, V. Fischer, S. Jochems, B. Figuet, and R. Monstein, "Navigating interference—Examining in-flight GNSS spoofing patterns and signal disruptions," in *Proc. 2025 Int. Tech. Meeting Inst. Navig.*, 2025, pp. 443–452.

[8] GPS Spoofing WorkGroup, *GPS Spoofing: Final Report*, OPSGROUP, 2024.

[9] S. Jacobsen and A. Kauranen, "Estonia says Russia violates international rules with GPS interference," *Reuters*, Apr. 30, 2024. [Online]. Available: https://www.reuters.com/world/europe/estonia-says-russia-violates-international-rules-with-gps-interference-2024-04-30/

[10] Reuters, "Finnair pauses some Estonia flights due to GPS interference," *Reuters*, Apr. 29, 2024. [Online]. Available: https://www.reuters.com/world/europe/finnair-pauses-flights-tartu-estonia-amid-gps-interference-2024-04-29/#:~:text=%22Finnair%20will%20suspend%20its%20daily,GPS%20disruptions%20in%20the%20past

[11] M. Felux, P. Fol, B. Figuet, M. Waltert, and X. Olive, "Impacts of global navigation satellite system jamming on aviation," *J. Inst. Navig.*, vol. 71, no. 3, 2024.

[12] SkAI Data Services, "Live GPS spoofing and jamming tracker map," 2025. Accessed: Feb. 25, 2025. [Online]. Available: https://spoofing.skai-data-services.com/

[13] Z. Liu, S. Lo, J. Blanch, and T. Walter, "GNSS spoofing detection and localization using ADS-B data," in *Proc. 37th Int. Tech. Meeting Satellite Division Inst. Navig. (ION GNSS+)*, 2024, pp. 796–803.

[14] Kai Jansen, Matthias Schäfer, Daniel Moser, Vincent Lenders, Christina Pöpper, and Jens Schmitt, "Crowd-GPS-Sec: Leveraging crowdsurfing to detect and localize GPS spoofing attacks", IEEE Symp. on Security and Privacy (S&P), San Francisco, CA, USA, May 2018.
[15] Flightradar24, "Flightradar24 blog," Apr. 5, 2024. Accessed: Jan. 7, 2025. [Online]. Available: https://www.flightradar24.com/blog/videos/a350-longhaul-behind-the-scenes-in-the-cockpit-with-sas/
[16] Infinidome, "GPSdome2." Accessed: Jan. 7, 2025. [Online]. Available: https://infinidome.com/gps-dome-2/
[17] J. Sun, X. Olive, E. Roosenbrand, C. Parzani, and M. Strohmeier, "OpenSky report 2024: Analysis of global flight contrail formation and mitigation potential," in *Proc. Dig. Avion. Syst. Conf. (DASC)*, 2024.
[18] J. Kupietzky, "Why 20 aircraft went off course over Iraqi airspace," *Simple Flying*, Oct. 1, 2023.
[19] M. Schäfer, M. Strohmeier, M. Smith, M. Fuchs, V. Lenders, and I. Martinovic, "OpenSky report 2018: Assessing the integrity of crowdsourced Mode S and ADS-B data," in *IEEE/AIAA 37th Dig. Avion. Syst. Conf. (DASC)*, 2018.
[20] Z. Liu, S. Lo, and T. Walter, "GNSS interference detection using machine learning algorithms on ADS-B data," in *Proc. 34th Int. Tech. Meeting Satellite Division Inst. Navig. (ION GNSS+)*, 2021.
[21] B. Figuet, M. Waltert, M. Felux, and X. Olive, "GNSS jamming and its effect on air traffic in Eastern Europe," in *Proc. 10th OpenSky Netw. Symp*., 2022.
[22] D. L. Wu, C. Csar, and J. H. Salinas, "GPS jamming: A historical record from global radio occultation (RO) observations," in *37th Int. Tech. Meeting Satellite Division Inst. Navig. (ION GNSS+)*, 2024.
[23] M. Strohmeier, D. Moser, M. Schäfer, V. Lenders, and I. Martinovic, "On the applicability of satellite-based air traffic control communication for security," *IEEE Commun. Mag*., no. 9, pp. 79–85, 2019.
[24] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *J. Inst. Navig*., vol. 59, no. 3, pp. 177–193, 2012.
[25] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the Galileo open service," *J. Inst. Navig*., vol. 63, no.1, pp. 85–102, 2016.
[26] S. C. Lo and P. K. Enge, "Authenticating aviation augmentation system broadcasts," in *Proc. IEEE/ION Position, Location and Navigation Symp*., 2010.
[27] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. IEEE Symp. Secur. Priv. (S&P)*, 2000.
[28] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *J. Inst. Navig*., vol. 59, no. 4, pp. 281–290, 2012.
[29] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, "SPREE: A spoofing resistant GPS receiver," in *Proc. 22nd Annu. Int. Conf. Mobile Comput. Netw.*, 2016.
[30] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz, "Direction-of-arrival assisted sequential spoofing detection and mitigation," in *Proc. 2016 Int. Tech. Meeting Inst. Navig*., 2016.
[31] M. Eichelberger, F. Von Hagen, and R. Wattenhofer, "A spoof-proof GPS receiver," in *19th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, 2020.
[32] H. Sathaye, G. LaMountain, P. Closas, and A. Ranganathan, "SemperFi: Anti-spoofing GPS receiver for UAVs," in *Netw. Distrib. Syst. Secur (NDSS) Symp*., 2022.