The Impact of GPS Interference in the Middle East

Vasilis Ieropoulos
School of Computer Science
Cardiff University
Cardiff, UK
Email: ieropoulosv@cardiff.ac.uk

***Abstract*—The use of Satellite Navigation Systems (SNS) has become indispensable for modern weather forecasting and aviation. However, the reliability of these systems is increasingly threatened by spoofing and jamming attacks, which can have severe consequences on weather balloon tracking networks and commercial flight paths. This paper focuses on the security implications of SNS spoofing and jamming in the Middle East region, examining how these types of attacks can impact weather forecasting models, air traffic control systems, and the overall safety of air travel. The study involves a comprehensive analysis using software-defined radio (SDR) systems to track planes and weather balloons, presenting detailed findings on the prevalence and characteristics of SNS spoofing attacks in the region. The manipulation or jamming of SNS signals severely compromises the reception of weather balloons, leading to inaccurate or incomplete atmospheric measurements and thus undermining weather forecasting accuracy. Furthermore, the navigation systems used by commercial airliners and private aircraft are also vulnerable to these attacks, potentially jeopardising the safety of passengers and crew. This paper discusses various mitigation measures to minimise the effects of these attacks on commercial flights and air traffic control systems. By analysing the data collected, this study aims to contribute to the ongoing debate about the security and reliability of SNS, especially in regions where the stakes are highest. The findings underscore the urgent need for robust countermeasures to detect and mitigate SNS interference, ensuring the continued reliability of critical infrastructure and the safety of air travel.**

I. Introduction

The Middle East region has witnessed an increasing number of attacks on Satellite Navigation Systems (SNS) in recent years, posing significant risks to the reliability of navigation systems that underpin various critical infrastructures. This has become even more prevalent in the last year, when fighting broke out between Isreal and Palestine. The reception of weather balloons, which transmit crucial data such as atmospheric pressure, temperature, and humidity readings, is severely compromised when SNS signals are manipulated or jammed. This can lead to inaccurate or incomplete measurements, compromising the integrity of weather forecasting models that rely on these data. Furthermore, the navigation systems used by commercial airliners and private aircraft are also affected by these attacks, potentially putting passengers and crew at risk. To better understand the scope and impact of SNS spoofing in the Middle East, we conducted a comprehensive analysis using our software-defined radio (SDR) system to track both planes and weather balloons. This paper presents the findings from this study, providing insights into the prevalence and characteristics of SNS spoofing attacks in the region. We focus specifically on the middle as this has become the highlight of spoofing and jamming attacks in the past year but also since we can verify our findings using our own equipment. By examining the data collected using our SDR system, we aim to contribute to the ongoing debate about the security and reliability of SNS systems, particularly in regions where the stakes are highest. This paper will serve as an assessment of the impact of SNS spoofing on weather balloon tracking networks and aviation navigation systems in the Middle East, informing strategies for improving the resilience of these vital infrastructure components.

II. Background

The following background section provides an overview of important technologies in aviation and meteorological science. Automatic Dependent Surveillance-Broadcast (ADS-B) and radiosondes with weather balloons. ADS-B has revolutionised aviation surveillance by using satellite communication to provide precise real-time tracking of aircrafts, thereby enhancing the efficiency and safety of air traffic management worldwide. Gleichzeitig, radiosondes, carried aloft by weather balloons, play a crucial role in meteorology by collecting detailed upper atmosphere data essential for accurate weather forecasting and climate research. This section explores the operational principles of these systems in their respective fields, highlighting their global impact on improving safety, efficiency, and scientific understanding.

A. What is ADS-B

ADS-B is an advanced aviation surveillance system that utilises satellite communication to track aircraft[1]. With ADS-B, planes equipped with this technology transmit crucial information such as their position, altitude, speed, and unique identification to Air Traffic Control (ATC). This continuous data exchange enhances the efficiency and safety of air traffic management by providing ATC with real-time updates on each aircraft's location and status[1].

In addition to transmitting data to ground stations, ADS-B also enables aircraft to receive real-time updates from other ADS-B-equipped planes in the vicinity. This feature significantly improves situational awareness for pilots, allowing them to monitor the positions and movements of nearby aircraft. Consequently, ADS-B contributes to collision avoidance and better-informed decision-making in the cockpit[2].

The ADS-B system operates globally on the 1090 MHz frequency, ensuring a standardised and reliable method of communication across different regions and airspaces. This global operability makes ADS-B a cornerstone of modern aviation safety and efficiency, facilitating seamless and coordinated air traffic management throughout the world[2].

B. The role of Radiosonde and WeatherBaloons

Radiosondes are compact instrument packages suspended beneath weather balloons, typically filled with hydrogen or helium.[3] As the balloon ascends through the atmosphere, the radiosonde measures key meteorological parameters such as atmospheric pressure, temperature, and relative humidity. These sensors are connected to a battery-powered radio transmitter, which continuously sends the collected data back to a ground-based receiver[3]. This real-time transmission of atmospheric data is essential for meteorology, as it provides vital upper-air observations that enhance weather forecasting accuracy and contribute significantly to atmospheric research. By reaching altitudes of up to 30 kilometres or more, radiosondes offer a detailed vertical profile of the atmosphere, capturing data that surface-based instruments cannot. This high-altitude information is crucial to understanding weather patterns, tracking storm development, and improving climate models[3]. Furthermore, radiosondes are indispensable for calibrating and validating data from satellites and other remote sensing instruments, ensuring that the global network of weather observation remains precise and reliable through their role in collecting and transmitting upper-air data; they provide the detailed insights necessary for predicting and understanding complex weather phenomena.

III. Incidents SNS Interferance

The European Union Aviation Safety Agency (EASA) works in collaboration with the airline industry to address the threat posed by interference with GPS signals. Increasing incidents of spoofing and jamming are endangering air travel safety. EASA and the International Air Transport Association (IATA) recently held a workshop to tackle this challenge[4]. They highlighted the need for short, medium and long-term measures to mitigate risks. Information sharing will occur through the European Occurrence Reporting scheme and the EASA Data4Safety programme[4]. In addition, traditional navigation aids will be retained as a backup for GNSS navigation, while aircraft manufacturers will guide the management of jamming and spoofing situations [5].

Multiple concerning reports have emerged from Iranian airspace regarding complex navigation failures caused by fake GPS signals. The FAA has issued a risk warning to civil air operators in Iraq and Azerbaijan, highlighting the recent threat to safety from GPS spoofing [6]. The Flight Data Intelligence website Ops Group identified 20 near-identical instances of GPS spoofing in Iranian airspace, affecting aircraft navigation systems and safety protocols[6].

According to reports, navigation systems of civilian aircraft flying over parts of the Middle East are being spoofed, posing a safety hazard[7]. The Indian civil aviation regulator, DGCA, has issued an advisory to Indian airlines, alerting them to this threat. The circular emphasizes the need for contingency measures to address jamming and spoofing of the GNSS[7]. Multiple incidents have been reported, including flights near Iran going off-course due to navigation system blindness caused by spoofed GPS signals.

Senior officer Andronikos Kakkouras, from the Deputy Ministry of Research and Innovation of Cyprus, explained that GPS systems in Cyprus are affected due to conflicts in Israel[8]. The interference is caused by electronic warfare tactics, specifically sending interference to the GPS frequency system. Cyprus, being close to Israel and the conflict zone, experiences disruptions in mobile telephony, digital terrestrial television, and other systems that use GPS, including drone applications[8].

In the midst of rising tensions with Iran, the Israel Defence Forces (IDF) have taken defensive measures by blocking GPS signals across swathes of Israel. This interference disrupts missiles and drones that rely on GPS for location settings [9]. The move comes after a strike on the Iran consulate building in Syria that killed 13 people, including a senior general. Israeli authorities believe that an Iranian response is imminent. Citizens reported GPS disruptions in major cities like Tel Aviv and Jerusalem, far from active combat zones. The IDF confirmed the use of GPS blocking, urging citizens to manually set their location on apps to ensure accuracy[9].

Instances of GPS jamming have increased in Lebanon due to concerns about a potential Israeli ground invasion against Hezbollah. Israel aims to disrupt Hezbollah attacks in northern Israel by interfering with GPS signals. This interference impacts civil aviation, as evidenced by a recent incident where a Turkish Airlines flight was unable to land in Beirut due to GPS disruption. In response, Lebanon plans to file a complaint with the United Nations against Israel for disrupting navigation systems.

Antonios Constantinides et al.[10] investigated interference within the high-frequency (HF) spectrum (3–30 MHz) resulting from long-distance propagation. The study focused on HF communication systems, which commonly experience spectral congestion due to interference from various sources. This congestion is notably significant during nighttime periods when solar activity is minimal. During a period exceeding one year, the researchers collected HF electric field data using a calibrated monopole HF antenna located in Cyprus. Some of the interference while not specifically mentioned in the study is documented to originate from the British RAF bases in Cyprus from the use of Over the Horizon radar[11]. The International Amateur Radio Union has set up multiple monitoring stations to investigate and identify spectrum interference, which they use to publish monthly reports on spectrum interference with the majority originating from military bases[12].

IV. Data Gathering

Our data collection process spanned one year, with a specific focus on the data obtained after October 20th 2023 when the

Israel-Palestine conflict escalated again. This coincides with reports emerging about jamming and spoofing attacks in the Middle East region[13][4].

To gather our data, we used two NooElec RTL SDRs[14], each configured for a different frequency range. These SDRs were equipped with custom-made 8-element ground-plane antennas, specifically designed to optimise reception at their corresponding frequencies.

As depicted in Figure 1, the ground-plane antenna is a monopole mounted above a conductive surface. This conductive plane reflects the signal, thereby enhancing it in the opposite direction. The lengths of the antenna and the ground plane are crucial for optimal performance, typically $\lambda/2$ (half wavelength) and $\lambda/4$ (quarter wavelength) respectively. This design enables omnidirectional radiation horizontally while focussing the signal vertically.

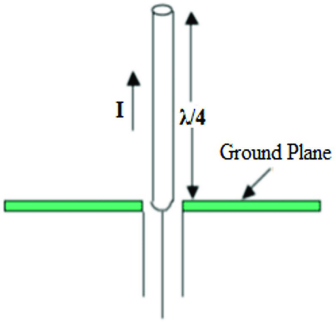


Fig. 1: Ground Plane Antenna

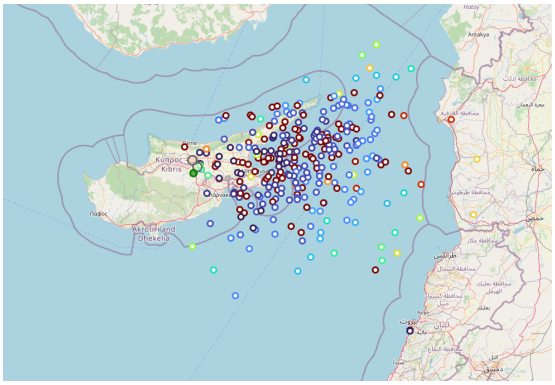
The first SDR was tuned to 400-406 MHz, allowing us to track weather balloons and feed their location data into SondeHub. This enabled us to monitor the trajectory of weather balloons in real-time and identify any potential anomalies or disruptions.

The second SDR was set to 1090 MHz, enabling us to decode ADS-B signals and send the resulting aircraft location data to FlightRadar24[15], FlightAware[16], and ADSBExchange[17]. These online platforms provide a wealth of information on commercial air traffic, including flight routes, altitudes, and velocities.

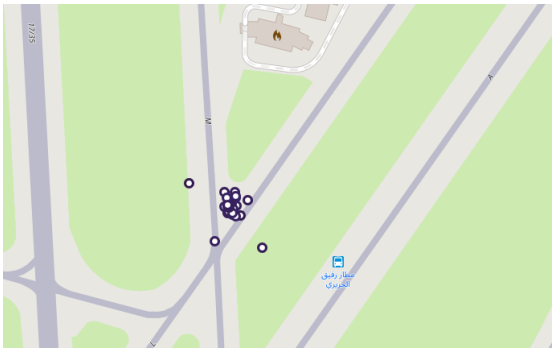
By analysing the data collected from these two SDRs, we were able to gain insight into the impact of jamming and spoofing attacks on weather forecasting models and air traffic control systems in the Middle East region.

A. Analysis of Weather Balloon Data

The impact of SNS interference is strikingly evident when examining the visualisation of the data presented in Figure 2a. A seemingly anomalous cluster has emerged, deviating from the typical distribution of weather balloons landing in the Mediterranean Sea. Upon closer inspection, as depicted in Figure 2b, it becomes clear that these ”balloons” are, in fact, nothing more than spoofed locations caused by interference in the region. This artificial clustering is a direct result of SNS interference, which has successfully manipulated the tracking data. The eastward movement of weather balloons is mainly influenced by Earth’s rotation and the Coriolis effect. As our planet spins from west to east, it imparts this motion to the atmosphere. The Coriolis effect arises due to varying rotational speeds across different latitudes, causing an apparent force that deflects moving air masses. In the Northern Hemisphere, this deflection results in an eastward bias for weather systems[18].



(a) Distribution of Weather Balloons from October 2023 to June 2024



(b) Weather Balloons that appear to be coming from Beirut

Fig. 2: Combined Figures

Furthermore, a deeper dive into the data reveals that this phenomenon did not occur overnight. Figure 3 illustrates the first recorded instance of this anomaly occurring on November 18th. This date marks the beginning of a prolonged period of SNS interference, which has continued to distort and mislead our understanding of the region’s weather patterns. The appearance of this anomalous cluster serves as a stark reminder of the far-reaching consequences of SNS interference in sensitive data sets like weather monitoring systems. It highlights the urgent need for robust measures to detect and mitigate such tampering, ensuring that we can rely on accurate and trustworthy information to inform our decision-making processes.

B. Analysis of ADSB data

To visualise the collected data, we utilised a colour-coded map overlay provided by FlightRadar24[19], representing varying levels of interference with global navigation satellite systems (GNSS), ranging from low (green) to high (red). This

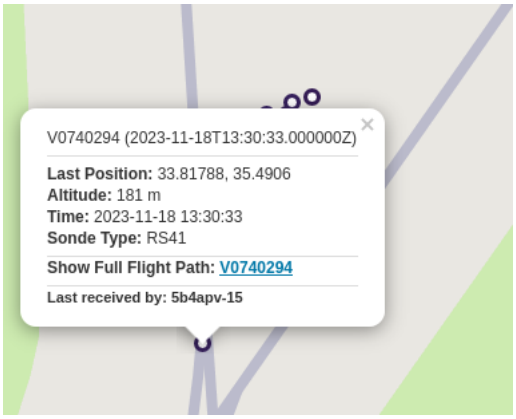


Fig. 3: The first "recorded" instance

interference affects not only the US GPS constellation but also other systems such as Russia's GLONASS, Europe's Galileo, and China's BeiDou.

The data, sourced from the FlightRadar24 website which aggregates data from multiple users, includes ADS-B messages received from aircraft. Within these messages, the Navigation Integrity Category (NIC) encodes the quality and consistency of the navigational data. The NIC value indicates the certainty of an aircraft's position by providing a radius of uncertainty; higher values signify greater uncertainty. By analysing the NIC values broadcast by aircraft over time in specific areas, we calculate the extent of GPS jamming and interference.

Upon examination of Figure 4, it is evident that the region encompassing Israel-Palestine, Jordan, and Cyprus experiences significant interference, which adversely affects flight tracking and overall aircraft positioning systems. The areas marked grey appear to lack active flight tracking equipment, possibly explaining their lack of data. This phenomenon is also observed in various parts of Africa and Asia, where stringent regulations can restrict the acquisition of such equipment.

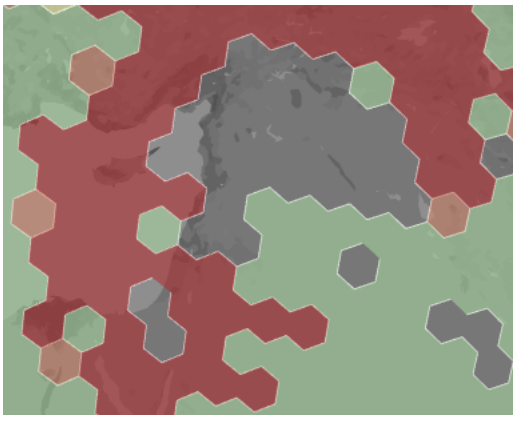


Fig. 4: GPS Interference map over the Middle East

V. Mitigation Strategies

In recent years, concerns have been raised regarding the vulnerability of aircraft navigation systems to Global Navigation Satellite System spoofing attacks. The potential for malicious tampering with GNSS signals poses a significant threat to the safety and integrity of commercial aviation. This section will discuss mitigation strategies that can be employed to counteract GPS and GNSS spoofing in aircraft navigation systems.

Some mitigation strategies are specific to certain aircraft as some technology is not available on every aircraft. **Hybridization within the ADIRS**: One effective strategy is to implement hybridization within the Aircraft Data Inertial Reference System (ADIRS) [20] this is specific to the Airbus A318/A319/A320/A321. This involves integrating inertial reference system data with other radio navigation systems, such as Distance Measuring Equipment (DME) and VHF Omnidirectional Range (VOR), to ensure continued navigation capabilities even in the presence of GNSS spoofing [20]. **IRS-based Positioning**: Another mitigation strategy is to rely on positioning based on the inertial reference system (IRS). In areas where IRS data is reliable, aircraft can switch from GPS-based navigation to IRS-based positioning, thereby ensuring continued safe flight operations[21]. This type of mitigation is also possible for UAVs and weather balloons as triagulation is used for location detection. **NAVAID-based Augmentation**: For regions with available Navigation Aids (NAVAIDs)[22], such as VORs and DMEs, augmenting the aircraft position using these signals can enhance the overall system integrity and availability. This approach enables pilots to maintain navigation capabilities even when GNSS signals are compromised or spoofed[22]. **Coasting Mode**: In situations where IRS data is unreliable or unavailable[23], implementing a coasting mode can ensure continued safe flight operations. This involves using the aircraft's momentum and other available navigation aids to guide the plane to its destination[23]. We suggest the implementation of Receiver Autonomous Integrity Monitoring (RAIM). Implementing RAIM techniques allows onboard receivers to detect anomalies in satellite signals by comparing redundant measurements. RAIM-enabled systems can autonomously identify and exclude spoofed signals, maintaining accurate navigation information[24]. Lastly, we also suggest the implementation of Multi-constellation GNSS Receivers. Deploying receivers capable of simultaneously utilising signals from multiple GNSS constellations (e.g., GPS, GLONASS, Galileo, BeiDou) enhances resilience against spoofing. By cross-verifying signals from different constellations, the system can detect and mitigate spoofed signals more effectively [25]. While this is not an extensive list, there are technical limitations to these approaches and it is up to the manufacturer's technical abilities to implement such approaches.

VI. Conclusion

The analysis of GPS interference in the Middle East reveals significant challenges to the integrity and reliability of satellite navigation systems, essential for weather forecasting and aviation. The prevalence of spoofing and jamming attacks poses severe risks to the accuracy of weather balloon data and the safety of commercial flights. Incidents of GPS signal

manipulation in Iranian airspace, the Eastern Mediterranean, and other areas prone to conflict illustrate the widespread impact of such interference. Our study, using software-defined radios to track weather balloons and aircraft, underscores the urgent need for robust countermeasures. The data highlights how these attacks distort weather forecasting models and compromise air traffic control systems. Mitigation strategies, such as hybridisation within the ADIRS, IRS-based positioning, NAVAID-based augmentation, and coasting mode, offer potential solutions to enhance navigation system resilience against spoofing and jamming attacks. To safeguard critical infrastructure and ensure air travel safety, it is imperative to implement these mitigation strategies, invest in advanced detection technologies, and promote international cooperation to address the threat of GPS interference. Future research should focus on developing more sophisticated methods for detecting and countering such attacks, ensuring the continued reliability of satellite navigation systems in response to evolving cyber threats.

REFERENCES

[1] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ads-b implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78–87, 2011.

[2] J. Zhang, L. Wei, and Z. Yanbo, "Study of ads-b data evaluation," *Chinese Journal of Aeronautics*, vol. 24, no. 4, pp. 461–466, 2011.

[3] (2024) Radiosondes — national oceanic and atmospheric administration. National Oceanic and Atmospheric Administration. [Online]. Available: https://www.noaa.gov/jetstream/upperair/radiosondes

[4] D. lole. (2023) Electronic warfare in middle east affecting cyprus air travel. Accessed on June 12, 2024. [Online]. Available: hhttps://cyprus-mail.com/2023/12/05/electronic-warfare-in-middle-east-affecting-cyprus-air-travel/

[5] E. U. A. S. A. (EASA) and I. A. T. A. (IATA), "Easa partners with iata to counter aviation safety threat from gnss spoofing and jamming," 2024, press release. [Online]. Available: https://www.easa.europa.eu/en/newsroom-and-events/press-releases/easa-partners-iata-counter-aviation-safety-threat-gnss-spoofing

[6] H. Davoren. (2023) Reports of gps spoofing in middle east rising, faa issues risk warning. Accessed on June 12, 2024. [Online]. Available: https://www.globalair.com/articles/reports-of-gps-spoofing-in-middle-east-rising-faa-issues-risk-warning?id=6435

[7] V. Som, "Planes losing gps signal over middle-east, indian regulator flags threat," 2023, news article. [Online]. Available: https://www.ndtv.com/india-news/planes-losing-gps-signal-over-middle-east-indian-regulator-raises-concern-4602298

[8] R. Gregoriades. (2024) Gps glitches from warzone 'manageable', electronics official says. Accessed on June 27, 2024. [Online]. Available: https://cyprus-mail.com/2024/06/20/gps-glitches-from-warzone-manageable-electronics-official-says/

[9] H. Bachega and S. Seddon. (2024) Israel: Gps disabled and idf leave cancelled over iran threat. Accessed on June 27, 2024. [Online]. Available: https://www.bbc.co.uk/news/world-middle-east-68734689

[10] A. Constantinides, H. Haralambous, H. Papadopoulos, and M. Makrominas, "Models of hf interference over cyprus," *Applied Sciences*, vol. 12, no. 22, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/22/11808

[11] I. A. R. U. I. R. 1, "Iarums region 1 newsletter, may 2024," 2024. [Online]. Available: https://www.iaru-r1.org/wp-content/uploads/2024/06/IARUMS-R1-Newsletter-2024-05.pdf

[12] I. A. R. U. (IARU). (2024) Iarums r1 newsletters. [Online]. Available: https://www.iaru-r1.org/spectrum/monitoring-system/iarums-r1-newsletters/

[13] A. Mitchell. (2024) Gps spoofing: A growing concern for global navigation security. Accessed on June 12, 2024. [Online]. Available: https://theatlasnews.co/analysis/2024/05/14/gps-spoofing-a-growing-concern-for-global-navigation-security/

[14] "Nooelec nesdr smart xtr sdr - premium rtl-sdr w/ extended tuning range, aluminum enclosure, 0.5ppm tcxo, sma input," premium software defined radio in a silver brushed aluminum enclosure. Fabricated by Nooelec in the USA and Canada.

[15] "Flightradar24," https://www.flightradar24.com/, accessed: 2024-06-26.

[16] FlightAware. (2024) Flightaware. [Online]. Available: https://www.flightaware.com/

[17] ADSB Exchange. (2024) Adsb exchange. [Online]. Available: https://www.adsbexchange.com/

[18] W. W. Hay, *The Coriolis Effect*. Cham: Springer International Publishing, 2021, pp. 575–596. [Online]. Available: https://doi.org/10.1007/978-3-030-76339-8_25

[19] I. Petchenik. (2024) Flightradar24's new gps jamming map. Accessed: June 28, 2024. [Online]. Available: https://www.flightradar24.com/blog/gps-jamming-map/

[20] Airbus, *Airbus A318/A319/A320/A321 Flight Crew Operating Manual*, 2021.

[21] X. Chen, Z. Chang, N. Zhao, and T. Hämäläinen, "Irs-based secure uav-assisted transmission with location and phase shifting optimization," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2023, pp. 1672–1677.

[22] I. C. A. O. (ICAO), *Global Navigation Satellite System (GNSS) Manual*, 2005, doc.9849 AN/457, First Edition. [Online]. Available: https://www.icao.int/Meetings/PBN-Symposium/Documents/9849_cons_en[1].pdf

[23] Airbus, *GNSS loss and GNSS Interferences on Airbus A/C*, 2019, document Number: 34.36.00049, First Issue Date: 22-FEB-2019. [Online]. Available: https://www.airbus-win.com/wp-content/uploads/2019/03/gnss-loss-and-gnss-interferences-on-airbus-ac-1.pdf

[24] S. Hewitson and J. Wang, "Gnss receiver autonomous integrity monitoring (raim) performance analysis," *GPS Solutions*, vol. 10, no. 3, p. 155–170, Dec 2005.

[25] K. Zhang and P. Papadimitratos, "Secure multi-constellation gnss receivers with clustering-based solution separation algorithm," in *2019 IEEE Aerospace Conference*, 2019, pp. 1–9.