Where are we? Investigating how inexpensive technology can mitigate GPS spoofing

Michael Benjamin Sammueller
Department of Computer Science
University of Essex Online

CSPROJ: Dissertation
Registration Number:
Supervisors: Dr. Oliver Buckley & Dr. Samuel Danso

Date of Submission: December 2024
Word Count: 15,338

Acknowledgements

I would like to thank my supervisors, Dr. Oliver Buckley and Dr. Samuel Danso, for their guidance and direction throughout this project. I also want to thank my wife for encouraging me to pursue this degree and being very patient and supportive throughout the past two years.

Table of Contents

Introduction

Background

GPS, a fundamental backbone of civil aviation, enables efficient airspace use, precision approaches, and low-visibility operations (Corraro et al., 2022). Its importance cannot be overstated, as it allows airlines to provide and air traffic control to receive aircraft position estimates through ADS-B, a crucial function for air navigation service providers (ANSPs) (Figuet et al., 2022). The introduction of services such as the “Galileo High Accuracy Service” (HAS) has further improved GPS accuracy to decimeter levels (Portelli et al., 2023).

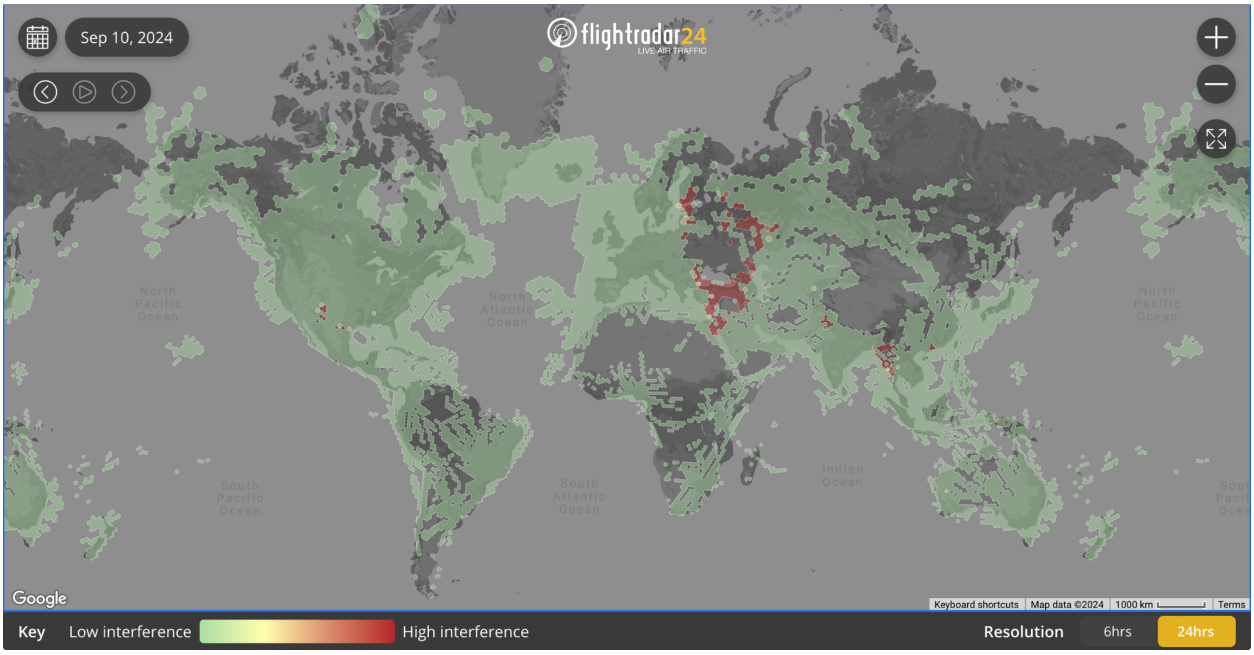
Problem Statement

This reliance on GPS exposes the aviation industry to security risks that need immediate attention. GPS receivers are susceptible to various forms of radio frequency interference, including GPS spoofing, where a malicious entity broadcasts fake GPS signals. Figuet et al. (2022) report that radio frequency interference (RFI) affects up to 60% of air traffic in Eastern Europe daily under certain conditions. The rise of these types of incidents is not surprising - while equipment needed to conduct a spoofing attack would have cost anywhere between 50,000 to 500,000 U.S. dollars five years ago, anybody with a computer, an antenna, an RTL-SDR dongle and open-source software can conduct spoofing attacks for as little as 100 dollars today (Zangvil, N.D.).

Poor connectivity or electromagnetic interference poses a significant threat, especially in hostile environments like war zones (Corraro et al., 2022). Eurocontrol, the European Organisation for the Safety of Air Navigation, is actively researching methods to detect such interferences by attempting to understand how receivers behave under radio frequency interference (Nasser et al., 2022). In 2018, RFI incidents increased by over 2,000%, a percentage that has remained steady since (Eurocontrol, 2021). Given the sensitivity of these systems to spoofing, interference, or jamming attacks, the need for enhanced cybersecurity measures is not just critical; it’s urgent (Ostroumov & Kuzmenko, 2022). Although research has been done in the area of mitigation and prevention, such as implementing advanced filtering techniques to detect such signals (Lin, 2023), no commercial off-the-shelf solution is currently available to mitigate this problem.

Research Motivation

The significance of GPS in civil aviation cannot be overstated. Any disruption to the integrity of GPS, such as through spoofing, poses a direct threat to the safety and efficiency of air travel. GPS spoofing, once a rare and sophisticated attack, is now becoming more accessible to malicious actors.



Almost the entire globe experiences GPS interference (FlightRadar24, 2024)

The repercussions of this vulnerability include the potential for aircraft misrouting, loss of positional awareness, and, in extreme cases, safety-critical failures. Given the exponential growth of air traffic operations globally and the increasing complexity of airspace management, it is imperative to safeguard the integrity of GPS signals to ensure the continued safety and security of air travel. This research aims to address this challenge by developing a low-cost, scalable solution that can detect and mitigate GPS spoofing in real-time, thus contributing to the resilience of civil aviation systems.

Research Objectives

Despite the severity and frequency of GPS-spoofing attacks, no commercial off-the-shelf solution is currently available to counter this problem effectively. This gap in the market, coupled

with the limited research on low-cost hardware solutions for this problem, underscores the novelty and importance of this study. This project aims to build a solution that combines existing techniques with novel ideas. This solution should be tested to verify that it is accurate, reliable, and secure. The outcomes of these tests shall be recorded in this report to answer the question of whether it is possible to build a low-cost solution for GPS spoofing.

Research Question

Although the overarching question – “Where are we? Investigating how inexpensive technology can mitigate GPS spoofing.” – is the title of this project, there are several other questions which will be addressed throughout this study.

1. What are the current trends and patterns in GPS spoofing attacks targeting civil aviation?
2. How do these attacks impact aircraft systems, airline operations, and aviation authorities?
3. What are the existing countermeasures against GPS spoofing, and why have they proven insufficient?
4. Can low-cost hardware solutions be developed to detect and mitigate GPS spoofing attacks effectively?

Literature Review

Introduction

GPS, a fundamental backbone of civil aviation, enables efficient airspace use, precision approaches, and low-visibility operations (Corraro et al., 2022). Its importance cannot be overstated, as it allows airlines to provide and air traffic control to receive aircraft position estimates through ADS-B, a crucial function for air navigation service providers (ANSPs) (Figuet et al., 2022). The introduction of services such as the “Galileo High Accuracy Service” (HAS) has further improved GPS accuracy to decimeter levels (Portelli et al., 2023). However, this reliance on GPS exposes the aviation industry to security risks that need immediate attention. GPS receivers are susceptible to various forms of radio frequency interference, including GPS spoofing, where a malicious entity broadcasts fake GPS signals. Figuet et al. (2022) report that radio interference affects up to 60% of air traffic in Eastern Europe daily under certain conditions. The rise in these types of incidents is not surprising - while equipment needed to conduct a spoofing attack would have cost anywhere between 50,000 to 500,000 US dollars five years ago, anybody with a computer, an antenna, and open-source software can conduct spoofing attacks for as little as 100 dollars today (Zangvil, N.D.).

Especially in hostile environments, such as warzones, poor connectivity or electromagnetic interference pose a significant threat (Corraro et al., 2022). EUROCONTROL, the European Organisation for the Safety of Air Navigation, is actively researching methods to detect such interferences by attempting to understand how receivers behave under radio frequency interference (Nasser et al., 2022). In 2018, RFI incidents increased by over 2,000%, a percentage sustained ever since (Eurocontrol, 2021). Given the sensitivity of these systems to spoofing, interference, or jamming attacks, the need for enhanced cybersecurity measures is not just important; it's urgent (Ostroumov & Kuzmenko, 2022). Although research has been done in the area of mitigation and prevention, such as implementing advanced filtering techniques to detect such signals (Samalla & Kumar, 2024) or using deep learning to uncover hidden patterns in satellite data (Lin, 2023), there currently is no commercial off-the-shelf solution available to mitigate this problem.

This literature review aims to highlight the importance of GPS in civil aviation while also uncovering the threats and risks associated with its usage. Analysing current and past research in this area by contrasting different solutions should find gaps in existing research. These gaps present challenges and exciting opportunities for future research, paving the way for innovative solutions that can enhance and revolutionise GPS security in civil aviation.

Understanding GPS Spoofing

Key Concepts in GPS Technology

GPS, also known as GNSS or the “Global Navigation Satellite System,” is a satellite system that provides positioning, navigation, and timing data globally (Van Sickle, 2022). As a network, it transmits encoded data and makes it possible to pinpoint exact locations on Earth by measuring the distance between satellites and the receiver (Meral et al., 2021). Technology like ADS-B, the Automatic Dependent Surveillance-Broadcast, uses GPS to periodically determine and broadcast an aircraft's position (Yun et al., 2022). Simply put, a GPS receiver uses a combination of signal strength, correlation with known satellite data, precise timing, and ephemeris (orbital information) data to conduct a basic validation of the signals they receive.

Despite the benefits, GPS can be misused and weaponised by malicious third parties to perform GPS spoofing. Also known as GNSS spoofing, it is a technique used to deceive receivers by broadcasting false and manipulated GPS signals (Simak & Sedo, 2023). In specific scenarios, governments may employ the same method to deter the use of UAVs or GPS-guided missiles and to make them miss their intended target (Gebrekidan, 2024), which is why the frequency of GPS interference in and around warzones is exceptionally high (Mackinnon, 2024). As Minhas (2023) mentioned, spoofing attacks are launched with relative ease, allowing third parties to manipulate aircraft navigation systems, causing UAVs to crash into each other or, in some instances, even hijacking them.

GPS jamming, on the other hand, refers to the deliberate or unintentional blocking of GPS signals, preventing aircraft or other GPS-reliant vehicles from accurately determining their position. Similar to spoofing, such incidents can be caused by accidental radio frequency interference or deliberate attacks by malicious third parties or governments. The impact of GPS interference is underscored by a recent incident in Dallas-Fort Worth International Airport in October of 2022, where radio frequency interference caused significant disruptions, including several aircraft reporting their GPS receivers unserviceable within a 40 nautical mile radius around the airport, leading to runway closures and the rerouting of air traffic (Liu et al., 2023).

Although GPS systems are the main focus of this literature review and an invaluable tool inside any aircraft, they are part of larger aircraft navigation systems, primarily consisting of precise sensors, radio altimeters, barometric altimeters, and other inertial navigation systems (Vi et al., 2023). They are vital in ensuring safe and efficient flight operations by guiding manned and unmanned aircraft from one point to another (Kemkemian et al., 2022), optimising flight paths and reducing fuel consumption (Silveira et al., 2022).

Global aviation relies heavily on satellite communication (SATCOM) systems, facilitating ground-to-aircraft communication. Although both GPS and SATCOM rely on satellites and share similar vulnerabilities (Skelton, 2023), their purpose and functionality differ in that GPS is used to determine location and speed, whilst SATCOM is used purely for communication.

The term often mentioned in research regarding GPS spoofing is “Doppler Shift”. This term refers to the change in frequency or wavelength of a wave in relation to an observer moving relative to the wave source (Zhang et al., 2024). In the context of GPS, the Doppler shift occurs due to the relative motion between the satellite and the GPS receiver. It can be used to calculate the receiver's velocity to determine its position (Van Graas, 2023).
Closely related to this is the “Doppler Offset”, which describes the difference between the predicted Doppler shift and the actual measured Doppler shift. Regarding GPS, this offset can help detect inconsistencies or anomalies in the received signal (Zhou et al., 2022).

Another critical concept in understanding GPS positioning is pseudo-range. The term refers to the measured distance between a GPS satellite and a GPS receiver. It is called “pseudo-range” because it includes a range of errors and biases that must be corrected to obtain an accurate distance (Cheng et al., 2021 | McAlister, 2023). GPS satellites have very precise atomic clocks, but the clocks in GPS receivers are less accurate. This difference leads to a pseudo-range rather than an actual range, so GPS receivers correct this clock bias to accurately determine the receiver's location (McAlister, 2023).

In addition to these concepts, Signal-to-Noise Ratio (SNR) plays an essential role in assessing the quality of the GPS signal being received. SNR is a measure used in science and engineering to qualify how much noise has corrupted a signal. SNR is a critical parameter for GPS signals because it indicates the signal quality received from satellites. A high SNR means a clear, strong signal, whereas a lower SNR indicates a weaker signal, often more susceptible to errors and inaccuracies (Sun et al., 2019).

Threat Landscape in Civil Aviation

Although the threat of GPS spoofing is only now beginning to become public knowledge, the overall number of related incidents is astounding. Warfare is a primary driver and cause of GPS interference, with spoofing incidents spiking around war zones (Mackinnon, 2024). In early 2024, approximately 46,000 aircraft reported issues with GPS due to interference over Europe, especially in areas close to Russian territory (Dangwal, 2024), causing navigation systems to give false positioning data and guide aircraft hundreds of miles off course, leaving some aircraft with a total loss of navigational capability (Amaresh, 2024 | Dangwal, 2024). After the start of the Gaza war in October of 2023, reports of GPS spoofing across the Middle East skyrocketed. Aircraft departing from Israel’s Ben Gurion airport reported experiencing GPS interference upon takeoff (Thurber, 2024), suggesting this was an effort by the Israeli Defense Forces to thwart missile attacks (Mackinnon, 2024). Similarly, reports of GPS spoofing began to surge in 2022 into late 2023, directly following Russia’s invasion of Ukraine (Mackinnon, 2024).

Although commercial aircraft suffer the consequences of such activities, the primary military purpose appears to be the misguidance of drones and missiles (Warwick, 2024 | Wadhams, 2024). However, GPS spoofing can also be utilised to misguide and command aircraft purposely. According to some reports, Iranian military forces succeeded in steering and capturing a U.S. Lockheed Martin RQ-170 Sentinel stealth drone in 2011, utilising GPS spoofing

(Peterson & Faramarzi, 2011). Veillette (2023) discusses an incident which occurred in 1993, where Ethiopian forces shot down a Learjet 35A after it entered Ethiopian airspace accidentally because of GPS spoofing. Despite these incidents, Mackinnon (2024) states that aircraft systems are designed to be fail-safe, and multiple factors would have to coincide for a plane to crash due to a GPS spoofing attack.

Although it is one of today's most common (Iudice et al., 2024), particularly due to its lack of encryption and authentication (Liu et al., 2020), GPS spoofing is not the only threat aviation faces. In his paper about threats to civilian aviation, Kelly (2021) mentions five main threats: terrorist attacks, cyber-attacks, insider threats, organised crime, and accidental attacks. GPS spoofing mainly falls into two categories, as it can be a cyber-attack and an accidental attack, although it could be part of any of these categories. Accidental attacks and organised crime can take the form of other threats, such as ransomware malware attacks on airline systems. Ukwandu et al. (2022) discuss ten primary threats in their paper, including SATCOM, ADS-B-focused, and denial-of-service attacks.

Terrorism, which includes hijackings and bombings, aims to cause maximum damage and fear, often to make a political statement, whilst most incidents of GPS spoofing do not cause physical harm to people. Having said that, if a terrorist group were to use GPS spoofing to commit such an attack, they could employ spoofing to cause actual physical damage. However, aviation can also face threats from the inside, with individuals within the aviation sector causing harm. However, such threats are more difficult to detect, as it is challenging to detect such attacks amidst legitimate actions (Villarreal-Vasquez et al., 2021). For instance, Mackinnon (2024) mentions that, in some cases, military jamming or spoofing activities can affect civilian aircraft. However, they are not the intended target, underscoring a need for improved and increased communication between the military and civil aviation authorities.

On the other hand, a dedicated cyber-attack can control aviation systems in a way similar to a GPS spoofing attack (Lim et al., 2022). However, cyber-attacks can affect a broader range of systems, from check-in to air traffic control (Koroniotis et al., 2020). Air Traffic Management (ATM) systems, which are critical for aviation safety, are susceptible to cyber-attacks in the form of signal modification, jamming, and GPS spoofing due to their reliance on wireless technology, which often lacks a form of authentication or encryption (Murisa & Coetzee, 2024). Such attacks increase the workload of airline staff and air traffic control, leading to significant financial losses for airlines (Zmigrodzka, 2020).
Because of its interconnected nature and reliance on IT systems, the civil aviation industry is a prime target for DDOS attacks (Shah et al., 2024). Furthermore, the lack of standardised cybersecurity frameworks, together with the deployment of 5G and Internet of Things (IoT) infrastructure within airports, has expanded the attack surface, making airports, airlines, and air navigation service providers even more susceptible to sophisticated DDOS attacks (Whitworth, 2022).

Like GPS, SATCOM has one fundamentally insecure characteristic: its lack of encryption (Baselt et al., 2022). This vulnerability allows potential attackers to modify, inject, delete, or

spoof malicious messages over unencrypted SATCOM channels (Santamarta, 2014). Furthermore, because many legacy aircraft use dated SATCOM technology, they are vulnerable to additional risks, allowing attackers to easily intercept and eavesdrop on communications sent via this network. Just like SATCOM, ADS-B suffers from the same vulnerabilities. Because ADS-B broadcasts are unencrypted and unauthenticated, they are vulnerable to interception, eavesdropping, and manipulation (Wu et al., 2020). Furthermore, like GPS receivers, aircraft transponders will respond to ADS-B messages regardless of their validity due to a lack of verification (Dorland & Edmier, 2019).

Technological Impact and Vulnerabilities

As established in the previous paragraphs, GPS is paramount in civil aviation. If GPS equipment on board an aircraft were to be manipulated accidentally or with malicious intent, it could have catastrophic consequences. Aircraft navigation systems, which often rely on GPS, are essential for preventing mid-air collisions and ensuring that planes maintain a safe distance from each other while airborne (Minhas, 2023). Based on the FAA, the Federal Aviation Administration of the United States, over 90% of air traffic in the United States relies on GPS for navigation (Harris, 2021). Although modern aircraft maintain backup navigation systems, the primary tool for navigation is GPS (Firstpost, 2024). Despite having said backup systems, GPS spoofing can sometimes lead to complete navigational failure (Veillette, 2023).

Another concern, as mentioned by Vaddhiparthy et al. (2023), is that GPS spoofing can deceive the GNSS receivers of aircraft or, in their example, UAVs, causing them to misinterpret their location and movement. Furthermore, spoofing can lead to extreme deviation from the intended flight path, crashes, complete navigational failure, or, in some cases, re-routing of an aircraft, as proven by the Iran incident mentioned by Peterson & Faramarzi (2011). Most importantly, GPS receivers are especially susceptible to spoofing in areas with low satellite visibility. The effective spoofable distance increases when the visible satellite count is less than ten (Vaddhiparthy et al., 2023). Based on testing done with UAVs, dynamic spoofing, where the spoofed location changes over time, can make it more difficult for current solutions to detect spoofing attempts (Vaddhiparthy et al., 2023). This difficulty in detection, in particular, is an opportunity for future research and algorithm development.
Most authors mention that the underlying issue is the lack of authentication or verification of received signals (Islam et al., 2023). Spoofing stations often transmit a stronger GPS signal than satellites, causing receivers to accept the spoofed signal over a weaker, legitimate satellite signal (Islam et al., 2023), which is why it is easier to spoof a receiver in an area where fewer satellites are visible. Mackinnon (2024) argues that regulatory authorities should encourage investment in alternative navigation systems to reduce reliance on GPS and mitigate spoofing risk. However, they acknowledge that implementing such systems can be costly and time-consuming.

Spoofing and radio interference incidents, like the one at Dallas-Fort Worth International Airport in October 2022 (Liu et al., 2023), disrupt air traffic management systems, leading to flight delays, diversions, and financial losses for airlines and airports (Sathaye et al., 2022).

Furthermore, the increased fuel consumption caused by rerouting or holding patterns to correct an aircraft's course can lead to significant financial losses (Liu et al., 2020). Lastly, in extreme cases of spoofing, which lead to accidents (Khan et al., 2021), besides the loss of aircraft, the human loss would be incalculable. However, no specific monetary amounts are mentioned.

As the number of reported GPS spoofing cases rises and the industry attempts to cope with this threat, several international organisations, such as the International Civil Aviation Organisation (ICAO), the Radio Technical Commission for Aeronautics (RTCA), and the European Organisation for Civil Aviation Equipment (EUROCAE), are actively developing standards and monitoring anti-spoofing detection methods to enhance GNSS security (Kozovic & Durdevic, 2021). Together, these organisations aim to improve the resilience of next-generation aeronautical equipment against spoofing and are working on "Dual-Frequency Multi-Constellation (DFMC) GNSS" to replace current single-frequency GPS in the future (Kozovic & Durdevic, 2021). Additionally, the European Union Aviation Safety Agency (EASA) are developing guidelines and regulations to mitigate the risks of GPS spoofing and jamming by establishing reporting mechanisms, enhancing certification requirements of navigation systems, and creating an alerting system to inform stakeholders about GPS interference incidents (Villamizar, 2023). However, the guidance of ICAO is not binding, and implementation varies among member states (Mackinnon, 2024).

In a similar drive to mitigate the impact of spoofing, India's Directorate General of Civil Aviation (DGCA) has issued comprehensive guidelines to address the growing threat of GPS spoofing after increased incidents in Middle Eastern airspaces. The DGCA has mandated the establishment of a "Threat Monitoring and Analysis Network", together with other stakeholders, based on ICAO guidance, providing a practical roadmap to manage GPS interference effectively (Majumder, 2023). In a paper presented by the United Arab Emirates to ICAO, the UAE recommend collaboration between aviation and telecommunication authorities to manage radio frequencies effectively. They also suggest that all member states adopt and implement the measures provided by ICAO. They also call for developing technological solutions for effective GNSS interference mitigation (ICAO, 2023).

Furthermore, the aviation industry has begun introducing reactive, incident-driven policy shifts, such as those introduced after the GPS interference incident at Hanover Airport in Germany in 2010. In this incident, an aircraft received incorrect GPS location during taxi and takeoff, caused by interference from GPS repeaters used to test avionics in business planes in a nearby hangar (Kozovic & Durdevic, 2021). Although this appears to be a shift in the right direction, a 2019 assessment by ICAO found that many countries lack comprehensive strategies to address the threat of GPS spoofing (Mackinnon, 2024).

In addition to air traffic control policies and regulations, Veillette (2023) recommends that air crews receive specific training to help them detect error messages on flight instruments and how to solve these issues in flight, especially in high-risk regions like Middle Eastern airspaces. Furthermore, they mention that many aviation community members are awaiting guidance from the authorities responsible for them regarding this emerging threat.

Existing Solutions and Research

Detection Techniques

A recent increase in the sophistication of GPS spoofing attacks poses a threat to both military and civilian aviation. Although current literature is heavily based on spoofing detection in a military context, with a particular focus on UAVs, some techniques may be adapted for civilian use. The following chapter examines techniques for GPS spoofing detection mentioned in contemporary research.

Measurement-Based Detection

Minhas (2023) discusses measurement-based detection, where signals collected by sensors on several drones are analysed to detect inconsistencies. They propose utilising neural networks to identify GPS spoofing by analysing signal parameters like pseudo-range, Doppler shift, and signal-to-signal noise ratio (SNR). Leveraging the calculation of moving variance based on the Doppler offset and consistency test of PVT (Position, Velocity, Time) can aid in detecting spoofing attempts (Meng et al., 2023).

Game Theory and Machine Learning

Minhas (2023) also explores the application of game theory, where the interactions between attackers and defenders are modelled to predict spoofing attempts. However, Kanuri et al. (2023) highlight a significant limitation: location-based spoofing attacks can significantly degrade the performance of prediction models from an 80% to a 50% detection rate. In contrast, Li et al. (2023) propose using the AdaBoost algorithm for detecting GPS spoofing. The AdaBoost model aggregates multiple weak classifiers, like classification and regression trees (CART), to enhance detection accuracy. Despite Kanuri et al.'s (2023) concerns, Li et al. (2023) demonstrate that the AdaBoost model, when trained on public datasets, achieves a detection rate of approximately 97%, outperforming other machine learning models. Bose (2022) also explores using AdaBoost for this purpose, although he recommends using neural networks in general.

Dual Antenna and Sensor Fusion

Meng et al. (2023) and Mykytyn et al. (2023) suggest using dual antenna receivers to compare the carrier differences between antennas to detect spoofing. This technique is supported by Simak and Sedo (2023) and Srinivasan and Sathyadevan (2023), who recommend combining data from GNSS with other sensors to detect data mismatches, which may indicate spoofing.

Cryptographic Techniques and Anomaly Detection

Minhas (2023) advocates for using cryptographic techniques to verify and secure the authenticity of GPS signals and anomaly detection frameworks, such as the Maritime NMEA-

based Anomaly detection (MANA), to monitor and identify suspicious GPS data. Meng et al. (2023) support these approaches, emphasising the role of automatic gain control within the GPS receiver to detect and flag potential spoofing attacks with low computational complexity.

Predictive Mathematical Models and GNSS Services

Simak (2023) suggests using mathematical models to predict a vehicle's expected movement and speed, flagging improbable changes as suspicious. This method is complemented by cross-referencing data from multiple GNSS constellations, such as evaluating time differences in received signals (Simak, 2023 | Yang et al., 2023).

Advanced Analytical Techniques

Yang et al. (2023) propose using Kalman filters to estimate times and positions based on previous measurements. They also recommend using Long Short-Term Memory (LSTM) and deep neural networks to predict vehicle speed, direction, and position for enhanced spoofing detection.

Correlation with External Data

Mykytyn et al. (2023) suggest correlating UAV movements with onboard camera footage to identify spoofing. They further recommend utilising the cellular network to verify the validity of GPS data, effectively adding another layer of authentication.

Angle-of-Arrival (AoA) Detection

Yang and Chen (2022) propose using compressed sensing to estimate the power and direction of arrival (DOA) of satellite signals. This method would allow a receiver to identify single-source and multi-source spoofing attacks. According to Lubbers and Nikookar (2020), genuine satellite signals will have consistent AoA characteristics, whereas spoofed signals will exhibit anomalies due to the artificial nature of their origin.

Conclusions

The reviewed literature demonstrates various techniques and methods to detect GPS spoofing. Although most approaches are based on military applications, adapting them to a civilian use case holds promise for enhancing the security of GPS equipment.

Mitigation and Prevention Strategies

Villamizar (2023) describes several aviation industry strategies against GPS spoofing, including using decoy antennae and keeping GPS equipment offline when connectivity is unnecessary. StrategicRisk (2024) supports this, suggesting pilots may disconnect GPS from the flight

management system before entering known spoofing hotspots. Mackinnon (2024) highlights a collaborative workshop by EASA (European Union Aviation Safety Agency) and IATA (International Air Transport Association) on combating GPS jamming and spoofing, demonstrating international cooperation. However, despite acknowledging GPS vulnerabilities, the US government has not made any official efforts to address them (Mackinnon, 2024). The importance of having backup navigation systems is underscored by an incident at Tartu Airport in Estonia, where GPS interference led to flight cancellations due to the lack of ground-based navigational aids (Warwick, 2024).

MITRE Corporation, which operates federally funded research centres in the US, developed the Navigation Operational and Planning Agility Suite (NOPAS) for the FAA (Warwick, 2024). This tool measures GPS signal degradation using ADS-B data to identify issues, allowing the FAA to respond promptly (Warwick, 2024).

Military Applications

Anti-spoofing technology is vital for military operations. Precision-guided weapons, coordinated sea-land-air operations, and UAV command and control all rely on GPS (Junzhi et al., 2022). As discussed in previous chapters, most current research on GPS spoofing focuses on military applications, specifically UAVs.
Bose (2022) discusses a supervised learning approach for neural networks, leveraging historical data to improve detection accuracy, making it suitable for the dynamic and potentially hostile environments encountered in military operations. He demonstrates that this method achieves a detection probability exceeding 99%. This robustness is suitable especially for mission-critical applications in a military context. Zhou et al. (2023) emphasise that although existing technology, such as multi-antenna systems and adaptive beamforming, is effective in detection, further research to improve mitigation is required. They also highlight the need for autonomous systems which can operate without external information, as external support may not always be available in military operations.

Despite not acknowledging the issue officially (Mackinnon, 2024), the United States has responded to GPS threats by upgrading to third-generation GPS technology, enhancing jamming and anti-jamming capabilities, and focusing on research into deception jamming and anti-deception technologies (Junzhi et al., 2022).

Analysis of Existing Solutions

Datasets Used

The data sources used across the examined literature include a combination of controller laboratory experiments, real-world case studies, historical data, public datasets, and sensor fusion techniques. The authors of several studies have employed laboratory-based simulations with software-defined radios (SDRs) to generate spoofed GPS signals, allowing them to analyse

spoofing impacts in various controlled scenarios (Simak et al., 2023 | Vaddhiparthy et al., 2023 | Srinivasan & Sathyadevan, 2023).

Real-world incidents, such as the Black Sea spoofing event in 2017, were also referenced to validate findings and provide context (Junzhi et al., 2023). Public datasets, particularly those relating to GNSS and ADS-B data (Liu et al., 2020), were crucial for machine learning-based approaches, enabling the training and testing of models on extensive real-world data and in simulation software such as MATLAB (Meng et al., 2023). Additionally, some studies utilised multi-modal sensor data, combining GNSS inputs with data from inertial navigation systems (INS), barometers, and other onboard sensors to enhance the robustness of spoofing detection through cross-referencing (Vaddhiparthy et al., 2023). These diverse methodologies underscore the complexity and breadth of research addressing GPS spoofing in various contexts.

Strengths and Weaknesses

The solutions proposed by the authors quoted above form a broad foundation from which a smaller, lower-cost solution could be built. Each mitigation technique has strengths and weaknesses, reflecting the complexity of addressing this growing threat and the need for a more holistic solution.

While highly accurate, measurement-based detection demands sophisticated hardware and significant computational resources, which may limit its practicality, especially in cost-sensitive civilian contexts. Game theory and machine learning models, such as AdaBoost, show promise in prediction but suffer from degraded performance in location-based attacks and require high-quality training data. Dual antenna systems and sensor fusion provide robust detection, yet the complexity and cost of implementation may restrict their widespread use.

Cryptographic techniques offer strong security with low computational overhead but are challenging to implement in dynamic environments, and anomaly detection might miss subtle attacks or cause false positives. Predictive mathematical models, supported by GNSS services, provide reliable detection but rely on predictable movement patterns and consistent data, limiting their effectiveness in unpredictable scenarios.

Advanced analytical techniques, such as Kalman filters and deep learning, offer sophisticated detection capabilities but are computationally intensive and prone to overfitting. Lastly, methods such as angle-of-arrival detection and correlation with external data, though effective, require specialised hardware and integration with multiple systems, presenting practical challenges in real-world applications. These varied approaches highlight the need for a balanced solution that considers the specific demands of the operational environment.

Cross-Domain Applicability

Although much prior research has been conducted on GPS spoofing, with many techniques and methods that can be useful in mitigating GPS spoofing in civil aviation, the differences between UAV swarms and military usage, compared to civil aviation, are too significant in some areas, requiring substantial additional work to bridge the gap. Furthermore, current military-grade technology is expensive and challenging to implement in civilian contexts (Zhou et al., 2023).

For instance, UAV swarms have more dynamic and unpredictable flight paths than commercial aircraft, which follow predefined routes. Additionally, military GPS receivers often have access to encrypted signals and more advanced anti-spoofing features unavailable in civilian receivers (BAE Systems, N.D.). For example, military GPS receivers use “Selective Availability Anti-Spoofing Modules” (SAASM) to decrypt the precision GPS observations, providing satellite authentication, over-the-air rekeying, and contingency recovery features that enhance security against spoofing (US Air Force, N.D.).
Additionally, using aircraft camera feeds to verify geographical location is impractical, as commercial aircraft often fly at altitudes of up to 40,000 feet, with little to no ground visible below the aircraft, or at least not to a level where a person or machine learning model could recognise landmarks. Using cellular networks is similarly impractical for commercial aviation.

Furthermore, much of the current research does not account for modern location-based spoofing, where spoofed GPS signals overpower and replace legitimate signals entirely (Rados et al., 2024 | Mykytyn et al., 2023). The necessity for a device that can detect and reject spoofed signals (McAfee, N.D.), prevent navigational loss, and ensure continuous usage of legitimate GPS signals is evident.

Future Directions and Research Opportunities

Emerging Technologies

The rapid evolution of GPS spoofing necessitates continuous innovation in detection and mitigation technologies. Although some have already been touched upon, several promising areas for future research have emerged.

Artificial Intelligence and Machine Learning

Future research should focus on developing improved AI models capable of detecting sophisticated and subtle spoofing attacks in real-time, building upon Bose's (2022) and Li et al.'s (2023) work. Furthermore, additional research into using Long-Short-Term Memory (LSTM) networks, which show great promise in identifying patterns in GPS data, would be valuable.

Software-Defined Radios (SDRs)

As discussed by Simak et al. (2023), SDRs offer flexibility in signal processing, which could be used to develop more adaptive anti-spoofing techniques. Future research should focus on optimising SDRs for real-time spoofing detection in a civil aviation context.

Integration of Multiple Sensor Technologies

As recommended by Srinivasan & Sathyadevan (2023), future research should focus on integrating various sensors with GPS, allowing for a more resilient navigation system. Since modern aircraft are equipped with a plethora of onboard sensors, such as barometers and magnetometers, developing a solution that draws data from these sensors should be an achievable target.

Blockchain Technology

Implementing blockchain technology to create a distributed ledger of authentic GPS signals could provide further security against GPS spoofing. This approach could help verify the integrity of GPS signals across multiple trusted nodes (Baba et al., 2023).

Policy and Regulation Development

The increasing threat of GPS spoofing calls for a coordinated international policy and regulation development effort. As mentioned in this review, organisations such as ICAO, EASA, IATA, the FAA, and DGCA have begun making efforts. However, these entities should collaborate to develop comprehensive and internationally binding regulations for GPS security measures in civil aviation. These policies should include mandatory reporting and data sharing on GPS spoofing incidents. Global databases of such incidents, as suggested by the DGCA's guidelines (Majumder, 2023), could provide valuable data for research of countermeasures against GPS spoofing.
Furthermore, as highlighted by Villamizar (2023), regulatory bodies such as ICAO should establish more stringent certification requirements for GPS equipment, ensuring that all GPS equipment includes mandatory anti-spoofing capabilities. Finally, as suggested by Murisa & Coetzee (2024), GPS spoofing mitigation strategies should be integrated into broader aviation cybersecurity frameworks, which would include implementing Security Operations Centres for real-time threat monitoring.

Identified Gaps

Although GPS spoofing-related research is plentiful, there are several gaps which must be addressed by future research and solution development. Firstly, much of the current research focuses on military applications and UAVs. Further study is needed to address the unique challenges of GPS spoofing in civil aviation. Secondly, although sophisticated anti-spoofing technologies exist, more research must be conducted on how to implement those solutions cost-effectively across the commercial aviation sector. Furthermore, there needs to be more

research into how pilots and air traffic controllers could be trained to effectively recognise GPS spoofing incidents and how to react to them.
Finally, future research would benefit from investigating how new anti-spoofing technologies can be integrated into existing aviation navigation and communication systems without compromising the functionality of either system or introducing new vulnerabilities.

Conclusions

Summary of Findings

This literature review highlights the growing threat of GPS spoofing and its impact on civil aviation. Key findings include:

- GPS spoofing incidents have increased by 2000% annually since 2018 (Eurocontrol, 2021).
- GPS spoofing attacks have become more sophisticated and accessible, and the cost of spoofing equipment has dropped drastically (Zangvil, N.D.).
- Civil Aviation relies heavily on GPS for navigation, making it vulnerable to spoofing attacks.
- Various detection techniques have been proposed, such as AoA detection, machine learning, dual-antenna systems, and cryptographic techniques.
- Current mitigation strategies range from policy introduction to technological solutions. Despite this, there is yet to be a universally adopted solution.
- Much of the research has been conducted in military and UAV contexts. Adopting these solutions to civil aviation may be challenging due to differences in operational environments, regulatory requirements, and equipment.
- International organisations, like ICAO, EASA, and IATA, are working towards developing standards and guidelines. Despite this, there is a lack of internationally binding regulations addressing GPS spoofing in civil aviation.

As established throughout this literature review, each discussed technology has its benefits and drawbacks. Based on this, developing a solution incorporating several techniques may be beneficial in forming a holistic approach to this problem. Methods such as AoA, anomaly detection, and dual antenna arrays stand out as obvious choices for civil aviation. A more sophisticated solution may include elements of machine learning and correlation with external data. Furthermore, civil aviation may want to adopt a concept similar to UAV swarms, where the inter-communication between aircraft could be used to report heading, speed, and altitude, allowing any aircraft to dynamically triangulate its position based on the location of three other planes. Because this would require change or alteration to existing systems, developing an external “off-the-shelf” solution for spoofing seems preferable.

Methodology

Research Design

This project employs a Design Science Research (DSR) Paradigm to bridge the gap between theoretical research and practical application. DSR is inherently a problem-solving methodology that fits well with the objective of mitigating GPS spoofing in aviation through low-cost technology solutions. This paradigm allows researchers to investigate the problem and create tangible artefacts, such as the “Smart GPS Receiver”, which can be rigorously evaluated and iteratively improved.
The DSR approach ensures that the research outputs are theoretical contributions and practical innovations applicable to real-world scenarios. By iterating through design, implementation, testing, and evaluation cycles, the study demonstrates how technical solutions can address complex security problems in aviation, specifically the detection and mitigation of GPS spoofing.

Alongside DSR, this project adopts the Agile methodology. Agile offers a flexible and adaptive framework, which is crucial given the rapid pace of technological advancements in the aviation industry. Agile’s incremental and iterative nature allows for continuous feedback loops and refinement of hardware and software components. This is especially beneficial in handling the uncertainties and evolving requirements commonly faced during the development of advanced aviation systems.

The combination of DSR and Agile methodologies provides an optimal framework for this research. DSR focuses on delivering practical solutions and innovative technologies, while Agile ensures that the research remains flexible and responsive to new developments in GPS technology and aviation cybersecurity.

Justification for Methodology

The decision to use DSR is rooted in its ability to connect theory with practice. In aviation, where system reliability is paramount, creating functional prototypes that address real security threats is more valuable than abstract models alone. DSR supports the development of a concrete artefact, the “Smart GPS Receiver,” while also providing a structured way to evaluate its effectiveness through empirical studies and testing (Da Silveira & Henriqson, 2021 | Anthony et al., 2023).

Agile, on the other hand, is well-suited for projects like this, where rapid technological changes and new cybersecurity threats can quickly make rigid, waterfall-style development obsolete. The aviation industry is constantly innovating, and Agile allows the project to adapt to the latest developments, whether that be changes in GPS spoofing techniques or emerging mitigation strategies. Agile’s emphasis on short development cycles, known as sprints, ensures that the research can evolve with these changing dynamics while still delivering robust solutions.

The synergy of DSR and Agile thus provides the flexibility, responsiveness, and practical focus needed for the successful completion of this research. In sum, DSR grounds the research in solving real-world problems, and Agile provides the flexibility necessary to navigate a rapidly changing technological landscape.

Data Collection Methods

This project utilises both quantitative and qualitative data collection methods to collect data on the topic of GPS spoofing, as well as to design, build, and test the effectiveness of the proposed anti-spoofing solution. Data is collected through experiments, surveys, interviews with experts, and case studies. Each method provides a different insight into the problem of GPS spoofing in civil aviation, ensuring that the findings are well-rounded and comprehensive. Experimental data comes from the testing of the “Smart GPS Receiver” in simulated environments and real-world data. Surveys and interviews target aviation professionals, such as pilots and air traffic controllers, to gather practical insights on GPS spoofing threats.

Quantitative Methods

The primary quantitative method involves experimental research, where the “Smart GPS Receiver” undergoes rigorous testing under controlled conditions, both using mock data and simulated scenarios. The system’s performance is measured against several key metrics, including accuracy of spoofing detection, false positive rates, and response time. Additional quantitative data comes from the statistical analysis of survey responses, where participants are asked to provide insights into how GPS spoofing affects their professions.

Experimental Research

The “Smart GPS Receiver” is evaluated using both real and spoofed GPS signals in a controlled environment, using mock code and Matlab simulations. A set of scenarios, including legitimate satellite signals and spoofed signals originating from ground-based spoofing stations, are simulated. The experiment’s design replicates typical conditions in commercial airline operations, ensuring that the results are applicable to real-world scenarios. Data from these experiments are logged and analysed to determine the system’s effectiveness in identifying and mitigating spoofing attacks.

Statistical Analysis

To assess and enhance the performance of the “Smart GPS Receiver”, statistical analysis is performed on the data collected during the experiments, surveys, and interviews. Techniques such as Chi-Square and Kruskal-Wallis tests are used to evaluate whether the observed difference between legitimate and spoofed signals are statistically significant. The statistical

analysis also provides insights into the relationship between various factors, such as signal strength, signal-to-noise ratio, and the probability of detection.

Qualitative Methods

Qualitative data is obtained from interviews with aviation professionals and case studies. The interviews explore the challenges of GPS spoofing in aviation to gather feedback on the potential real-world application of the “Smart GPS Receiver”, as well as the existence and effectiveness of current solutions and procedures. Open-ended questions are employed to facilitate in-depth discussions on awareness of the problem, existence of training and procedures to handle this problem, and how the proposed system can be improved and integrated into existing aviation infrastructures.

Case Studies

Several case studies have been analysed during the literature review to gauge and contextualise the problem of GPS spoofing historically and contemporarily, by highlighting past and current occurrences and their impact on airline operations and air traffic management. By examining these incidents, the study identifies patterns and trends that inform the development of the “Smart GPS Receiver” and its relevance in real-world applications.

Surveys and Questionnaires

A survey is digitally distributed to several pilot platforms to gain insights into their experiences with GPS spoofing and its detection, as well as the impact on their day-to-day operations. The survey asks respondents to evaluate the impact of GPS spoofing on civil aviation, their own level of awareness, the level of training they have received, and current procedures that must be followed when GPS spoofing occurs. Multiple-choice questions are used to gather quantifiable data which will be analysed statistically.

Expert Interviews

To gather expert insights, semi-structured interviews are conducted with air traffic controllers. Similar to the pilot surveys, these interviews delve into the current levels of awareness and training, as well as asking for feedback and suggestions on what would improve current operations. This contributes to the overall design, testing, and evaluation of the proposed solution.

Participant Selection and Research Settings

The participants in this study include aviation professionals, air traffic controllers, and commercial pilots, all of which should have some level of familiarity with the concept of GPS

spoofing. Selection criteria focuses on individuals with relevant experience and knowledge of GPS spoofing and/or the importance of GPS systems in civil aviation. The experimental research is conducted in a controlled environment, utilising a simulated aircraft setting to ensure that the results are applicable to real-world scenarios.

Data Analysis Techniques

The collected data is analysed using a combination of descriptive and inferential statistics. Qualitative data from interviews and case studies is analysed using thematic analysis, where key themes and patterns are identified to provide deeper insights into the impact of GPS spoofing and the effectiveness of mitigation strategies. For the quantitative data, standard statistical techniques are employed to establish the validity and reliability of the experimental findings.

Ethical Considerations

The study follows strict ethical guidelines to protect participants' confidentiality and to ensure that the research complies with institutional and governmental standards. Informed consent is obtained from all interview and survey participants, and anonymity is maintained throughout the data collection process. Participants are made aware that they can withdraw from the study at any point in time and have their inputs deleted via a participant information sheet. As mentioned previously, the experiments involving GPS spoofing are conducted in a controlled environment, ensuring that no interference with actual aviation systems occurs. Approval from the university's ethics board, as well as from the employers whose employees are participating in this study have been obtained before commencing the research.

Development of the “Smart GPS Receiver”

Conceptual Design

As we have established, current research on GPS spoofing recommends various techniques for detecting spoofing. However, no commercial off-the-shelf solution exists for GPS spoofing today, and most receivers rely on one or two techniques instead of integrating as much as possible to form a holistic solution (Demir et al., 2020). Due to the critical nature of GPS in aviation, developing a solution for this growing threat is of utmost importance.

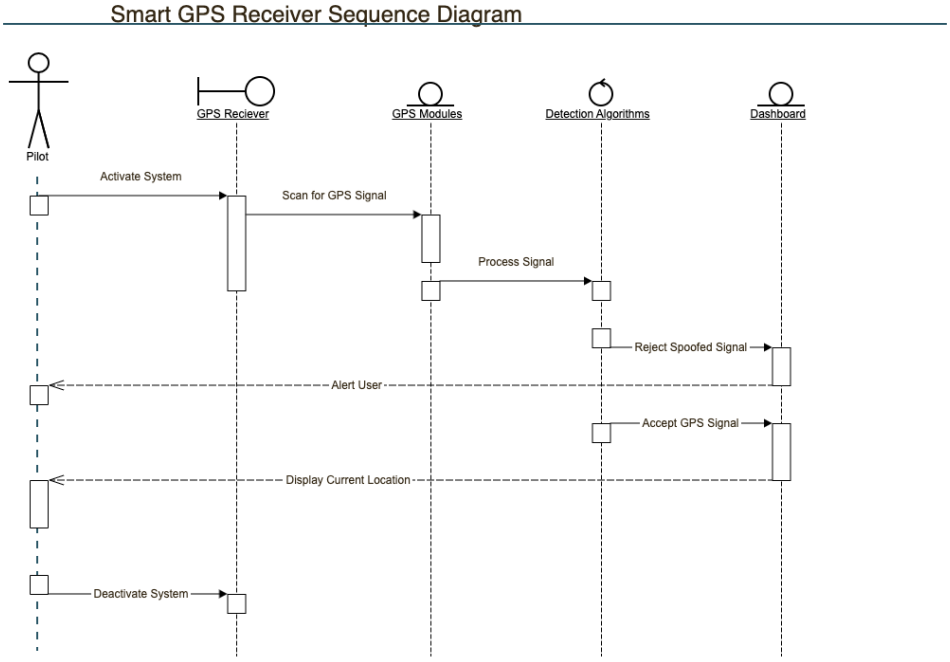
Design Philosophy

The “Smart GPS Receiver” is an advanced system specifically engineered to detect and mitigate GPS spoofing. It processes GPS signals using algorithms based on existing research explicitly tailored for the dynamic nature of civil aviation operations. The guiding design principles for this project are accuracy, reliability, and security.

- **Accuracy:** The receiver must demonstrate precise spoofing detection capabilities, minimising false positives to ensure continuous and reliable GPS coverage for the aircraft throughout the flight.
- **Reliability:** The system's integrity is crucial because pilots, the aircraft, and other associated systems rely on the receiver’s ability to correctly accept or reject GPS signals, ensuring the accurate determination of the aircraft’s geographical location.
- **Security:** The system must be robust against potential threats, ensuring that the GPS signals are protected from authorised interference or manipulation, thereby maintaining the integrity of the aircraft’s navigation system.

In addition to these principles, ensuring that the project’s hardware-related costs remain low is of utmost importance. The project intends to demonstrate that a receiver capable of mitigating spoofing risk can be constructed using inexpensive hardware components and custom software.

Overall System Architecture



UML Sequence Diagram demonstrating information flow in the "Smart GPS Receiver"

Hardware Components

The receiver's central computational unit will be an 8GB RAM Raspberry Pi 5 running a 64-bit 2.4 GHz quad-core ARM Cortex-A76 processor. The secondary unit will be a 4 GB RAM Raspberry Pi 5 running the same processor. Given their small size, Raspberry Pis are the perfect choice for a receiver intended to be used in an environment that values products with limited weight and size.

Most GPS receivers, like products from Garmin, rely on dedicated digital signal processors (DSPs) to process GPS signals (Garmin, N.D.). Due to their specialised architectures, DSPs outperform general-purpose CPUs for specific signal-processing tasks (Zhang et al., 2022). However, modern high-performance ARM cores like the Cortex-A76 have very capable SIMD (single instruction, multiple data) extensions and floating-point units, which allow them to handle DSP workloads well (Khadem et al., 2023). On the other hand, the Raspberry Pi 5 achieves 31.4 GFLOPS, meaning it can perform over 31 billion floating point calculations per second (University of Maine, N.D.). However, data on which specific chips and CPUs are used in current GPS receivers is limited, and the amount of GFLOPS in standard GPS receivers is not noted. Regardless, it is safe to assume that a standard GPS receiver would have less raw computing power than a Raspberry Pi 5 (Raspberry Pi, 2024 | UBlox, 2023). To put this into context, the Cortex-A76 CPU in the Raspberry Pi is a high-performance application processor, whilst chips like the Cortex-M series inside GPS receivers are built for efficiency and low-power

consumption. The Raspberry Pi achieves a clock speed of 2.4 GHz, compared to the Cortex-M's 200 MHz. The Raspberry Pi's CPU is Quad-core, whilst the processor inside a GPS receiver is typically limited to single-core (Raspberry Pi, 2024 | UBlox, 2023).

Overall, this makes the Raspberry Pi 5 a good and low-cost alternative to both control the GPS modules attached to it, as well as to perform data processing efficiently, whilst being widely available.

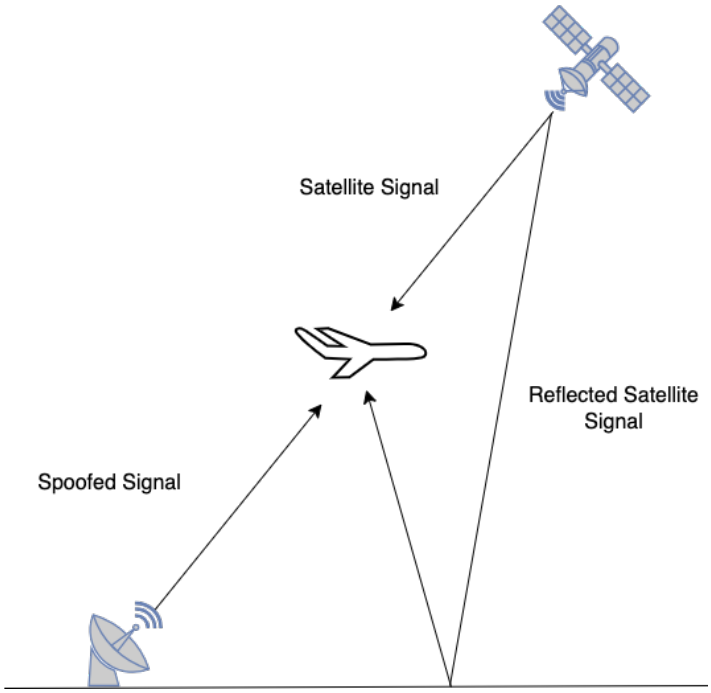
Each Raspberry Pi will be connected to an Adafruit GPS module to receive GPS signals. The Raspberry Pi 5 with 8 GB RAM will connect to the Adafruit Ultimate GPS HAT module with the following specifications:

- High-sensitivity receiver (-165 dBm)
- 10 Location updates per second (10 Hz)
- Up to 22 satellites on 99 channels
- GPS + GLONASS support
- Built-in real-time Clock
- 20 mA power draw

The Raspberry Pi 5 with 4 GB RAM will connect to the Adafruit Ultimate GPS Breakout V3 module with the following specifications:

- High-sensitivity receiver (-165 dBm)
- 10 Hz updates
- Up to 22 satellites on 66 channels
- 20 mA power draw

Both GPS modules on the receiver will be connected to an external GPS antenna, with one antenna mounted on the top of the unit facing upwards (designated to be the Stellar Unit) and the other mounted on the bottom facing downwards (designated to be the Terra Unit). Using dual antennas lets the receiver capture GPS signals through two independent modules. The received signals will be transmitted to the computing unit where anti-spoofing algorithms will process them to verify the authenticity of the GPS source.
Because most spoofing attacks originate from the ground (Brown, 2024), signals received by the stellar module are assumed to be inherently more authentic than signals received by the terra module. Signals received by the terra module are either reflections of satellite signals which are bouncing off the surface of the earth, or they are spoofed. Signals received mainly by the stellar module are assumed to be authentic.



The origin and reflection of GPS signals in terms of an aircraft.

Because there is always room for error, the algorithms conduct several tests to determine whether a signal is spoofed or authentic, and the code ensures that two or more checks fail before a signal is determined to be spoofed.

Each Raspberry Pi 5 requires a 27W power supply connected via USB-C. These power supplies will also power the GPS modules and antennas. They can be connected to a power bank or dedicated portable power supply in a portable environment. Both Pis will be connected via Ethernet to ensure fast and efficient data transmission. The Raspberry Pi 5 has a Gigabit Ethernet port, allowing for a fast and reliable connection between the two Pi's.

Software Architecture

This project follows an object-oriented paradigm to adhere to modern coding principles and ensure that it is scalable, reusable, and maintainable (Nagineni, 2021). The backend is written in Python and utilises the Flask framework for API and route management, as well as Javascript to provide the user interface and display data to the user.

Individual concerns, such as data collection and processing, have been coded in individual files to ensure maintainability and reusability further. The software consists of the following:

- Core modules

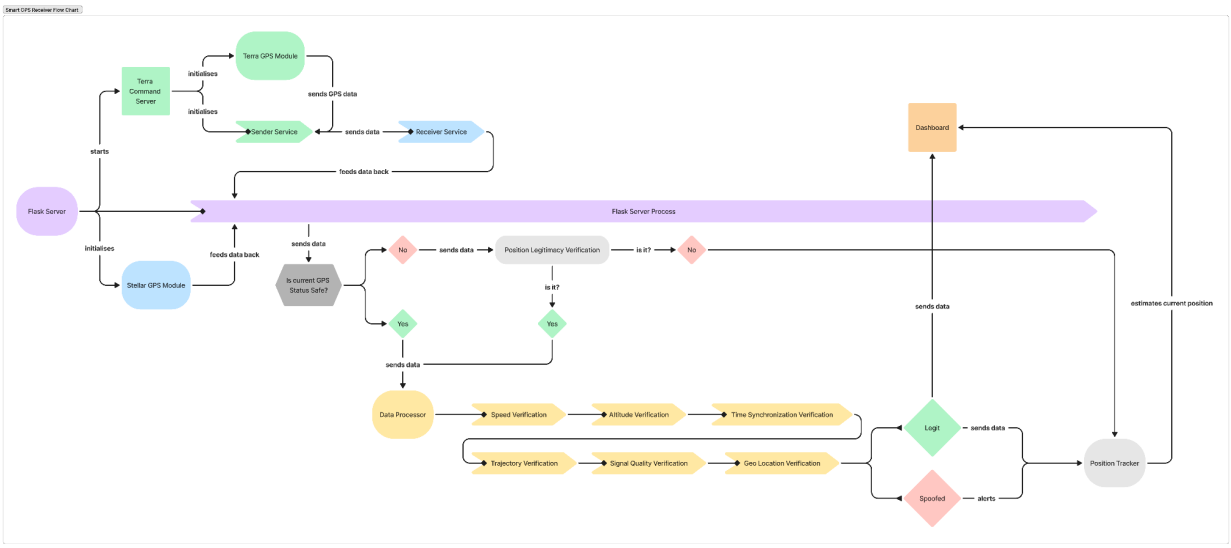
- Anti-spoofing algorithms
- Static files
- Templates
- Utility files

Core Modules

The core modules provide the functionality necessary to collect, process, and grade GPS signals, allowing the receiver to accept or reject them. They also pass the processed data to the dashboard front-end.

- **data_processor.py:** Applies below-mentioned anti-spoofing algorithms to data from two sources - the Stellar module and the Terra module.
- **gpsmodule.py:** Initialises the GPS module with specified serial ports, configures the GPS update rate and retrieves current GPS data. It returns a dictionary containing the fix status, date, time, latitude, longitude, fix quality, number of satellites, altitude, speed, track angle, horizontal dilution, and height above the geoid.
- **position_tracker.py:** Keeps track of the last legitimate position, speed, and heading of the receiver. It uses this information to estimate the receiver's current position in case the system flags current GPS signals as spoofed. It also has a method to determine whether the current GPS signals are legitimate, allowing the receiver to return to its normal status.
- **receiver.py:** Listens for incoming GPS data from the Terra module over a network socket (i.e. the ethernet cable). It processes and decodes the JSON data and allows this data to be returned to other methods.
- **sender.py:** Continuously retrieves and sends GPS data from the Terra module to the Stellar modules via network socket.
- **stellar_main.py:** Orchestrates the main operations for the receiver. It starts the server, receiver, and sender files to facilitate the exchange of data within the system. It also controls all the processing done by both the position tracker and the data processor.
- **terra_command_server.py:** Sets up a command server on the Terra module which listens for incoming socket connections. It facilitates the reception of commands from the Stellar module on the Terra module.
- **terra_main.py:** Initialises the Terra GPS module and orchestrates the sending of data to the receiver.
- **app.py:** Handles Flask-related processing and routing.

The signal processing algorithms are discussed in more detail below. The rest of the files in this project are front-end related.



Smart GPS Receiver flow chart demonstrating the logic of the software.

Signal Processing Algorithms

Most available solutions focus on a single comparison, algorithm, or method to detect spoofing (Septentrio, N.D. | Brown, 2024), and only some, like Honeywell and Rockwell Collins GPS receivers, use a combination of methods to detect spoofing (Brown, 2024 | Kozovic & Durdevic, 2021). Part of this thesis is to combine these methods to construct a holistic solution to spoofing detection, built on inexpensive technology. I have developed six primary algorithms, utilising the power of the hardware and the information it can collect to detect abnormalities, categorise, and rate them. This allows the system to determine whether to flag a signal as spoofed or legitimate.

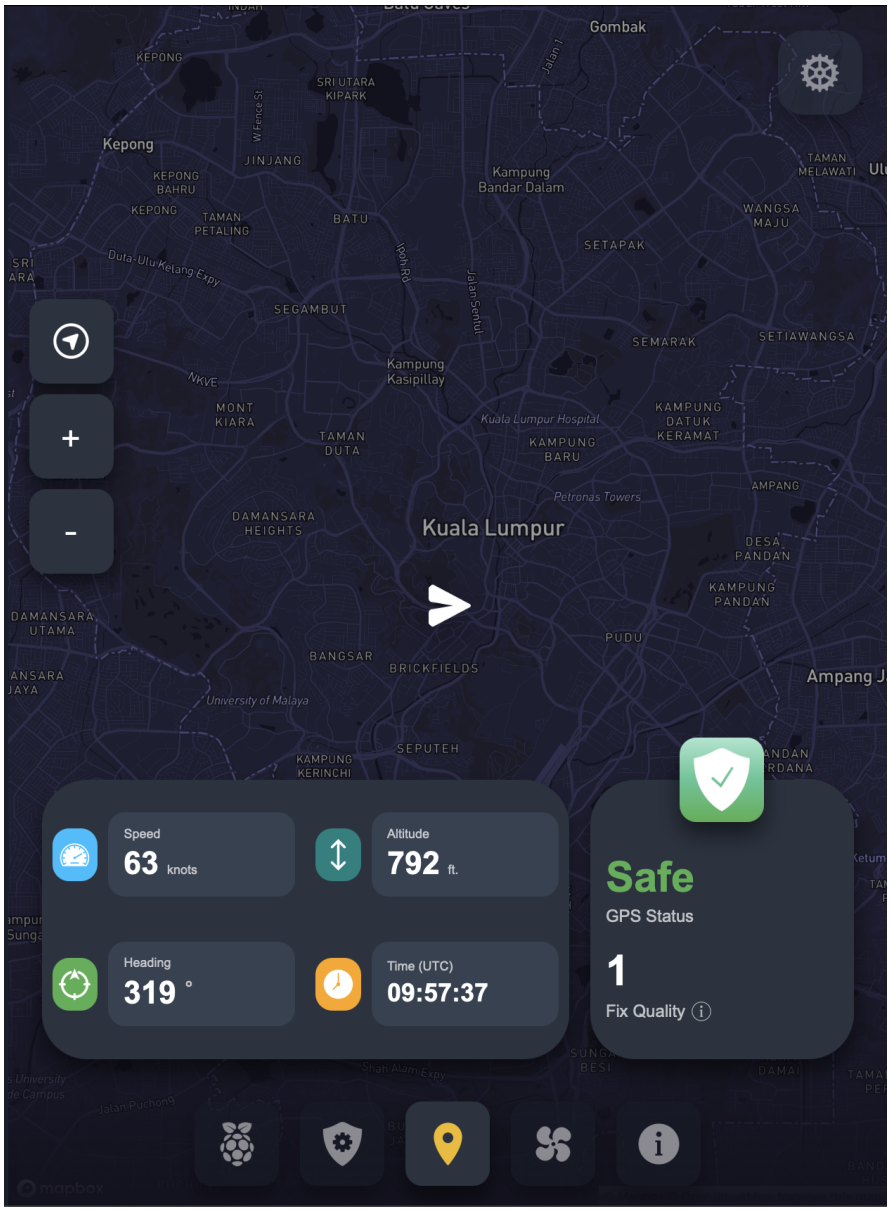
- **Altitude Checker (*Primary*):** Compares altitude information received by both GPS modules and checks for anomalies.
- **Geo Locator (*Primary*):** Compares the coordinate information received by both GPS modules and checks for anomalies. If either module reports a different country, this could be a sign of a spoofed signal.
- **Signal Quality Analyser (*Primary*):** Compares the signals of both modules in terms of GPS fix quality, amount of satellites visible and horizontal dilution.
- **Speed Verifier (*Primary*):** Compares the speed information received by both GPS modules and checks for anomalies.
- **Time Synchronisation Checker (*Primary*):** Checks the timestamps received by both GPS modules and checks for discrepancies.
- **Trajectory Analyser (*Primary*):** Analyses the geographical trajectory of the GPS receiver based on received data and flags any sudden increases in speed, jumps in speed, sharp turns, etc. as anomalies.

Each algorithm has predefined margins within which each calculation operates. For instance, the time synchronisation checker allows for a five second difference between the Stellar and

Terra timestamps, to avoid flagging a false positive. However, most importantly, the position tracker algorithm allows this GPS receiver to recover from a spoofing attack, something which current GPS receivers are unable to do.

User Interface Design

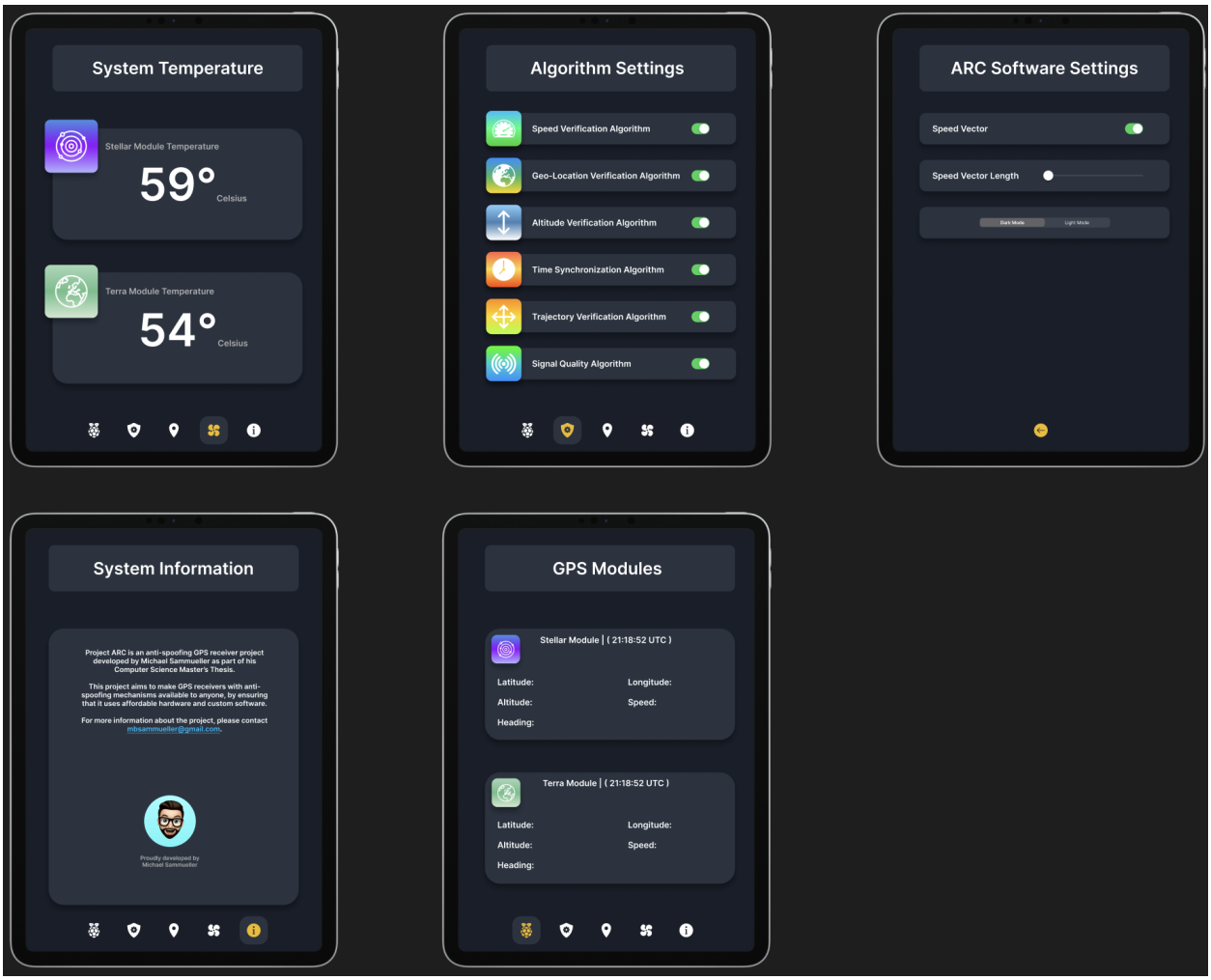
The development of the dashboards user interface for this project adhered to contemporary design principles, emphasising a modern aesthetic whilst prioritising usability and human factors. Drawing large inspiration from car dashboard designs (Dribbble, N.D.) and by state-of-the-art GPS systems, such as those produced by Garmin, the interface strikes a balance between sophistication and accessibility.



Main dashboard map view which displays vital information.

With its mobile-first design, the user interface has been designed for usage on iPads, which are commonly used in both private and commercial aircraft (VanHoenacker, 2022). Furthermore, all information has been arranged on the dashboard to draw attention to critical pieces of information with the live map which is updated every second, speed, altitude and heading information. Also displayed is the UTC time as received by the satellite. Additionally, visual elements have been incorporated to alert the user when the system detects a spoofing attempt, for instance, by changing the green square with the white shield and the "*GPS: Safe*" text to a red square with a corresponding red "*GPS: Unsafe*" text.

There have been additional designs for five additional pages, allowing the user to change settings and the configuration of the system. Although this added functionality would be helpful to the end user, but doesn't aid the goals of this study, the development on them has been shelved for future development.



Integration and Testing

The integration and testing of the GPS receiver followed a structured and iterative process aligned with the Agile methodology employed throughout this research project. The primary objective was to ensure that all hardware and software components functioned cohesively, providing accurate spoofing detection whilst maintaining low false-positive rates.

The integration of the dual GPS modules with their respective Raspberry Pi's (Terra and Stellar) was the first step. This involved connecting the Adafruit Ultimate GPS HAT and Ultimate GPS Breakout V3 modules to the respective Raspberry Pi units, ensuring that both modules could receive signals from the external antennas. As GPS antennas often struggle to receive signals inside buildings, this proved to be somewhat challenging at first. The antennas were carefully positioned - one facing upward to capture signals from satellites (Stellar) and the other facing downward to capture potential spoofed signals or signal reflections from the ground (Terra). The hardware integration involved soldering pins to the GPS modules, and tested by powering the units via USB-C power supplies and establishing an ethernet connection to ensure fast data transmission between the two Pi units.

The core software modules were integrated into a cohesive system. Special attention was given to the integration of the DataProcessor module, which determines the authenticity of received signals by comparing the strength and source of the signals between the Terra and Stellar units. The modules were designed to handle real-time data, ensuring that the system could process multiple signals and deliver results without significant delay. Additionally, error-handling and retry routines were incorporated to maintain system stability in the event of data inconsistencies or loss of satellite signal.

The testing phase involved subjecting the system to a variety of real and spoofed GPS signals in controlled environments. Python simulations were used to generate spoofing scenarios, including ground-based spoofing signals that mimicked legitimate satellite signals. These signals were transmitted to the system and its processing algorithms. Key performance metrics - accuracy of spoofing detection, false-positive rates, and system recovery time - were monitored and recorded.

Following Agile principles, the integration and testing process was iterative, with regular feedback loops to refine the system. During each sprint, any detected issues, such as delays in signal processing, inaccuracies in spoofing detection, or bugs and errors, were addressed and resolved. This process ensured that the system became progressively more robust, with each iteration improving its performance under both simulated and real-world conditions.

The final phase of testing involved a comprehensive evaluation of the system's ability to detect and mitigate spoofing in scenarios that closely replicated commercial airline operations. The results confirmed that the GPS receiver could accurately detect spoofed signals while maintaining a low false-positive rate, validating the system's effectiveness in real-world applications. This integration and testing phase demonstrated that the system not only meets its design specifications but also provides a cost-effective solution for GPS spoofing mitigation in

civil aviation. The recommended next step would be to integrate this receiver into a test aircraft to test it under operational conditions.

Results and Analysis

- Define the structure of the quantitative and qualitative analysis early in this section - this will add clarity.
- Consider creating a brief **Overview of Analytical Approach** where I explain how different data sources (e.g., experimental results, case studies) will contribute to my findings and enhance my understanding of GPS spoofing.

Overview of Analytical Approach

This section provides an outline of the analytical methods used to examine the various data sources in this study, including experimental results, case studies, survey responses, and expert interviews. The analysis is twofold, focusing on both quantitative and qualitative data to ensure a comprehensive understanding of GPS spoofing in aviation.

Quantitative Data Analysis

The primary focus of the quantitative analysis is to identify potential patterns and relationships in the data collected from surveys and experiments. Techniques such as Chi-Square tests and Kruskal-Wallis tests are employed to evaluate correlations between categorical variables, such as geographic regions, aircraft types, and the perceived importance of GPS. These statistical methods allow for an examination of whether the differences observed between groups are statistically significant, and thus provide evidence to support or reject the study's hypotheses.

In addition, the Kruskal-Wallis test was applied where data did not meet the normality assumptions required for parametric tests, ensuring robustness in the analysis of ordinal variables, such as pilots' perceptions of GPS importance across different regions.

Statistical Findings

Survey Results

Visualisation of pilot survey results

Based on the survey conducted for this study, as well as a GPS-spoofing workshop conducted by OPSGroup (OPSGROUP, 2024), the following potential relationships have been identified and analysed:

- Years of Experience vs. Preparedness
- Type of Operation vs. Suspected GPS Spoofing
- Geographic Region vs. GPS Importance
- Training vs. Familiarity with GPS Spoofing

Years of Experience vs Preparedness | Chi-Square Test

Chi-Square Statistic: 4.02
P-Value: 0.674
Degrees of Freedom: 6

There is no statistically significant association between the number of years of flight experience and preparedness to handle a GPS spoofing incident. This further underlines the importance of a technological solution or support tool which can aid pilots to overcome such attacks. This also matches the report by OPSGROUP, which highlights that many pilots feel unprepared to handle GPS spoofing incidents, even with years of experience (OPSGROUP, 2024).

A more shocking discovery lies in the fact that, out of 152 participants, **62** pilots did not feel adequately, and **40** only somewhat prepared to handle a GPS spoofing incident. Only **50** pilots felt that they would be prepared to handle such an incident.

Type of Operation vs. Suspected GPS Spoofing

Chi-Square Statistic: 6.73
P-Value: 0.347
Degrees of Freedom: 6

There is no statistically significant relationship between the type of aircraft operation (commercial, military, etc.) and suspected or confirmed spoofing attacks against them. This suggests that pilots experience a similar amount of spoofing attacks regardless of which type of aircraft they fly. This echoes the report by OPSGROUP (2024). As there are military solutions against GPS-spoofing, but a comparatively significant lack of commercial solutions, this further proves the need for a widely commercially available solution.

Aircraft Type vs. Preparedness to handle GPS Spoofing

Chi-Square Statistic: 1.69
P-Value: 0.945
Degrees of Freedom: 6

Since the p-value is greater than the common significance level, there is no statistically significant relationship between the type of aircraft operation and the pilots' preparedness to handle GPS spoofing, which is also underlined by the OPSGROUP (2024) report.

Geographic Region vs. GPS Importance | Kruskal-Wallis Test

This relationship was analysed using the Kruskal-Wallis test, as it is a non-parametric test that does not assume normality or equal variance, making it ideal for comparing the medians of ordinal data across multiple groups (Hoffman, 2019). The results of the test for this category were as follows:

Statistic: 24.79
P-Value: 0.847

Since the p-value is much greater than the common significance level, this indicates that there is no significant difference in how pilots across different geographic regions rate the importance of GPS in their daily flight operations. Again, this is supported by the OPSGROUP (2024) report.

Experimental Results

Several simulations were run to test the effectiveness and functionality of the GPS receiver, specifically the anti-spoofing algorithms. All simulations were based on actual flight plan data, specifically a flight from Doha, Qatar, to Manama, Bahrain. Real coordinates, altitudes, and speeds were passed to the anti-spoofing algorithms, combined with any other required data, to simulate a real flight.

The system has several fail safes that ensure the receiver does not operate using a spoofed signal. First, every received signal passes through the anti-spoofing algorithms. If the system deems the signal legitimate, the position tracker records the current position, speed, and heading. Once the system detects a signal as spoofed, it uses the recorded data in the position tracker to estimate the current position of the aircraft based on the last recorded coordinates, speed, and heading by using the Haversine formula:

$$a = sin^2\left(\frac{\Delta\phi}{2}\right) + cos(\phi_1) * cos(\phi_2) * sin^2\left(\frac{\Delta\lambda}{2}\right)$$

$$c = 2 * atan2\left(\sqrt{a}, \sqrt{1 - a}\right)$$

$$d = R * c$$

The system does not return to normal operations until the position tracker deems the signal to be legitimate again, by comparing the received location with the estimated location.

Initially, the plan was to utilise the simulation software MATLAB to conduct testing and simulations, however, it would serve no purpose other than overcomplicating the testing process. Furthermore, using the TEXBAT dataset, provided by the University of Texas, for testing was considered. However, the format of this data does adhere to the format of the Adafruit GPS modules, hence it would involve great work to convert the data into something that is readable by this projects' receiver. Using custom Python tests was deemed as sufficient to test the algorithms and the overall functionality of the software.

Simulation Setup

The Adafruit GPS modules capture NMEA (National Marine Electronics Association) sentences. These sentences are strings of information sent from satellites and captured by GPS receivers, like, for instance:

*$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A*

Each such message can be broken down into the following data (Adafruit, 2024):

- **$GPRMC:** Sentence identifier for Recommended Minimum sentence C
- **123519:** UTC Time in hhmmss format (12:35:19)
- **A:** Status (A = active or valid, V = void or invalid)
- **4807.038,N:** Latitude 48 deg 07.038' North
- **01131.000,E:** Longitude 11 deg 31.000' East
- **022.4:** Speed over ground in knots
- **084.4:** Track angle in degrees True (this is the direction of movement)
- **230394:** Date in ddmmyy format (23rd March 1994)
- **003.1,W:** Magnetic variation 3.1 degrees West
- ***6A:** Checksum data, always begins with *

Within the software for this project, Python is used to parse this information and store it in an easily accessible dictionary, one for each intercepted transmission. In this example, the dictionary would look as follows:

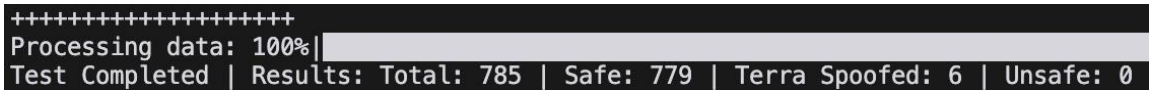
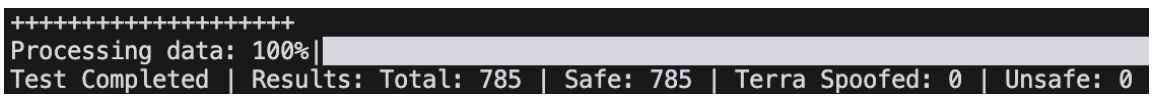
{"has_fix": true, "date": "01/01/2024", "time": "00:11:24", "latitude": 26.144166666666667, "longitude": 50.93383333333333, "fix_quality": 1, "satellites": 8, "altitude": 29629, "speed": 253, "track_angle": 288, "horizontal_dilution": 0.7373512806278844, "height_geoid": 35.329567655615165}

For the simulations, it was exactly such dictionaries which were passed to the system, in order to simulate a realistic flight between Doha, Qatar, and Manama, Bahrain. To further guarantee realism, the most common characteristics of spoofing attacks were considered during data preparation:

- **Timing Manipulation (Brown, 2024):** Spoofed signals are often pre-recorded and therefore have incorrect timestamps associated with the data that is being transmitted.
- **Deceptive Location Information ():** Most commonly, spoofed signals aim to falsify the receivers current location by sending false coordinates.
- **Signal Anomalies (Khoei et al., 2022):** In a culmination of the previous two points, spoofed GPS signals often include anomalous data, such as incorrect speeds and altitudes, or sudden “jumps” in speed and altitude.

The following scenarios were simulated to test the system:

<table>
<tr><th>Nr.</th><th>Description</th><th>Expected Outcome</th><th>Actual Outcome</th><th>System Response Time</th></tr>
<tr><td>1</td><td>Both the Stellar and Terra modules receive legitimate GPS data for a flight from Qatar to Bahrain</td><td>● Safe: 785
● Terra Spoofed: 0
● Unsafe: 0
● False Positive: 0</td><td>● Safe: 785
● Terra Spoofed: 0
● Unsafe: 0
● False Positive: 0</td><td>1 second</td></tr>
<tr><td></td><td colspan="4">++++++++++++++++++++
Processing data: 100%|
Test Completed | Results: Total: 785 | Safe: 785 | Terra Spoofed: 0 | Unsafe: 0</td></tr>
<tr><td></td><td colspan="4">All tests passed successfully with the expected outcomes matching the actual outcomes.</td></tr>
<tr><td>2</td><td>The Stellar module receives legitimate GPS data for a flight from Qatar to Bahrain, whilst the Terra module receives spoofed GPS data sporadically, indicating that it is located in Egypt and Sudan.</td><td>● Safe: 780
● Terra Spoofed: 5
● Unsafe: 0</td><td>● Safe: 779
● Terra Spoofed: 6
● Unsafe: 0
● False Positive: 1</td><td>1 second</td></tr>
<tr><td></td><td colspan="4">++++++++++++++++++++
Processing data: 100%|
Test Completed | Results: Total: 785 | Safe: 779 | Terra Spoofed: 6 | Unsafe: 0</td></tr>
</table>

	All tests passed successfully, but the actual outcomes do not match the expected outcomes. The system triggered one more spoofing alert for the Terra module, because it was recovering from being spoofed. After analysing this occurrence, it is understood that the system worked correctly and this is a symptom of spoofing.			
3	Both the Stellar and Terra modules receive spoofed data for a flight from Doha to Bahrain, indicating that the plane is now in Egypt & Sudan	• Safe: 780 • Terra Spoofed: 0 • Unsafe: 5	• Safe: 780 • Terra Spoofed: 0 • Unsafe: 5 • False Positive: 0	1 second
				
	All tests passed successfully. The system correctly identifies and flags the 5 spoofed coordinate pairs, and immediately recovers after receiving legitimate signals.			
4	Sudden mismatch in speed and altitude data between the two modules.	• Safe: 779 • Terra Spoofed: 6 • Unsafe: 0	• Safe: 779 • Terra Spoofed: 6 • Unsafe: 0 • False Positive: 0	1 second
				
	All tests passed successfully. The system correctly identifies and flags the 5 speed and altitude mismatches, and immediately recovers after receiving legitimate signals. It is also able to distinguish that the misinformation is coming from the terra module, and that the stellar module is authentic.			
5	Both modules receive legitimate data for a flight from Doha to Bahrain, but with different timestamps.	• Safe: 785 • Terra Spoofed: 0 • Unsafe: 0	• Safe: 785 • Terra Spoofed: 0 • Unsafe: 0 • False Positive: 0	1 second
				
	All tests passed successfully. Although the timestamps differ, this alone is not a reason for the system to trigger a “spoofing” flag, as at least two triggers are required for this to occur.			

Performance Evaluation of the "Smart GPS Receiver"

Initially, whilst testing the algorithms with simulated data, the system performed very well and was able to process and update data within one second. The same tests also concluded that a spoofed module will take one cycle (i.e. one second) after the spoofing is over to recover from being spoofed.

However, once the testing moved on to using real hardware, the software started to struggle a little bit, to the point where data wasn't being updated quickly enough, which, over time, led to significant drifts in the displayed time and other GPS data. To counteract this issue, threading was used to run each algorithm in its own thread, therefore being able to analyse GPS signals with each algorithm simultaneously instead of one after the other. This significantly increased the speed of the system, but didn't solve the problem in its entirety.

To further improve the performance of the system, the "main" function, as well as other important functions were reprogrammed to execute asynchronously, thereby significantly increasing the performance of the software. To benefit from the asynchronous execution of these methods and functions, the update rate of the GPS and the dashboard were programmatically increased, which allows the system to update every second without delay. Even if the system which is running the software causes the software to "pause" (i.e. by locking itself or by entering sleep mode), the software is able to recover and catch up in less than 30 seconds. Although this alleviated most performance problems, further integrating threading and asynchronous behaviour into the software would improve the performance for future releases.

Comparative Analysis with Existing Solutions

Information on existing solutions is limited, as they are either classified because of military usage, or because solutions that exist today are still experimental or in-development. Furthermore, there are no holistic off-the-shelf solutions available in the market today. Despite these difficulties, there are some comparisons we can draw.

Performance

The "Smart GPS Receiver" demonstrated robust performance in detecting GPS spoofing attacks through its multi-layered algorithmic detection. This holistic approach ensures high accuracy in identifying spoofed signals and maintaining navigational integrity. In comparison, military-grade receivers often use advanced anti-spoofing technologies like Selective Availability Anti-Spoofing Modules (SAASM), which provide high security but are not available for civilian use due to their cost and complexity (Defense Advancement, N.D. | Thales N.D.). Commercial solutions from companies like Honeywell and Rockwell Collins offer GPS receivers with integrated anti-spoofing technologies, typically relying on dual-antenna setups and advanced

signal processing techniques. While the “Smart GPS Receiver” achieves high level of accuracy in spoofing detection, it lacks the encrypted signal capabilities of military SAASMs. Although commercial solutions use similar dual-antenna and signal processing methods, the “Smart GPS Receiver” incorporates additional algorithms, enhancing its detection capabilities. Moreover, the position tracker algorithm in the “Smart GPS Receiver” allows it to recover from spoofing attacks, a feature not commonly found in existing commercial solutions (Thales, N.D.).

One of the primary objectives of this study was to develop a low-cost solution for GPS spoofing detection. The “Smart GPS Receiver” uses inexpensive hardware components like the Raspberry Pi and Adafruit GPS modules, significantly reducing the overall cost. Military-grade receivers are prohibitively expensive for civilian applications, often costing thousands or even tens of thousands of dollars per unit (Selinger, 2017 | Stratview Research, 2024). High-end commercial receivers with anti-spoofing capabilities also come at a premium price, making them less accessible for widespread civilian use. Based on the survey and interviews conducted for this study, most, if not all, commercial aircraft and air traffic control centres are not currently equipped with any solution.
In contrast, the “Smart GPS Receiver” can be easily scaled and deployed across multiple aircraft, providing a comprehensive solution to GPS spoofing at significantly lower costs.

Due to its highly modular nature, the “Smart GPS Receiver” can be easily configured to be integrated into existing aviation systems. Its modular design and use of standard interfaces ensures compatibility with current aircraft navigation systems. Military-grade receivers often require significant modifications to existing infrastructure, limiting their applicability in civilian contexts (GAO, 2021). While high-end receivers are more compatible with civilian systems, they may still require specialised installation and maintenance. In contrast, the “Smart GPS Receiver” is designed for easy installation and integration, making it accessible for airline operators as well as individual private pilots, without requiring extensive modifications to their existing systems. In fact, due to the hardware and software used, users could assemble such a receiver themselves if they really wanted to.
Additionally, its user-friendly dashboard provides intuitive controls and real-time alerts, enhancing its ability for pilots and air traffic controllers.

In conclusion, the “Smart GPS Receiver” offers a cost-effective, accurate, and easily scalable and integrable alternative solution for GPS spoofing detection in civil aviation. While it may not match the encrypted signal capabilities of military-grade systems, nor the highly advanced algorithms currently in development for commercial solutions, its multi-layered detection approach and low cost make it a highly competitive option compared. These results highlight the potential of the “Smart GPS Receiver” to enhance GPS security in the aviation industry, providing a scalable and practical solution to the growing threat of GPS spoofing.

Qualitative Data Analysis

In parallel to the quantitative analysis, qualitative data collected from expert interviews and case studies are analysed thematically. Key themes related to controllers’ awareness of GPS spoofing, their preparedness for handling such incidents, and their real-world experiences with

spoofed signals are extracted. This provides context and depth to the quantitative findings, enriching the study with practical insights from industry professionals.

Case Study Insights

The analysis of the case studies, including the recent incidents of GPS spoofing near the Iranian border, provides several critical insights into the nature, impact, and mitigation of GPS spoofing in civil aviation. These insights are crucial for understanding the broader implications of GPS spoofing and guiding the development of effective countermeasures.

Nature and Characteristics of GPS Spoofing Attacks

The case studies reveal that GPS spoofing is a sophisticated form of cyber-attack that involves broadcasting fake GPS signals to mislead aircraft navigation systems. Unlike GPS jamming, which blocks GPS signals, spoofing deceives the navigation systems into accepting false positional data. This can lead to significant deviations from the intended flight path, as evidenced by the incidents near the Iranian border where aircraft were misled to believe they were off-course by more than 60 nautical miles.

Impact on Civil Aviation

The impact of GPS spoofing on civil aviation is profound and multifaceted. The primary concern is the safety of air navigation. Spoofing can lead to unauthorised incursions into restricted airspace, posing a risk of military engagement, as nearly happened with the Embraer Legacy 650 (Veillette, 2023). Additionally, the loss of accurate navigation data can result in near-collisions, terrain warnings, and other critical safety incidents. Spoofing incidents cause significant operational disruptions. Pilots must rely on alternative navigation methods, such as ATC vectors and dead reckoning, which increases workload and stress. The Challenger 604 incident (Veillette, 2023) highlighted how crews had to navigate without reliable GPS data, leading to potential delays and increased fuel consumption, like in two recent incidents close to Qatari airspace (Anonymous, 2024). The economic impact includes increased operational costs due to rerouting, delays, and potential damage to aircraft. Moreover, the need for enhanced training and new technologies to counter spoofing adds to the financial burden on airlines and aviation authorities.

Detection and Mitigation Challenges

The case studies underscore several challenges in detecting and mitigating GPS spoofing. Current air traffic control systems and aircraft navigation systems lack advanced tools specifically designed to detect and mitigate GPS spoofing. This results in a reliance on manual cross-checks and pilot reports, which are not always reliable or timely. There is a notable gap in training for both pilots and air traffic controllers on how to handle GPS spoofing incidents. Many professionals feel unprepared to deal with such attacks, highlighting the need for dedicating training programs and resources. Existing navigation systems, including the Inertia Reference System (IRS), are not designed to counter spoofing attacks effectively. The spoofing incidents showed that the IRS could be disabled by false GPS signals, leading to a complete loss of navigational capability (Veillette, 2023).

Potential Solutions and Recommendations

The insights from these case studies point to several potential solutions and recommendations. Developing and deploying a multi-layered detection system that combines various techniques, such as signal strength analysis, angle-of-arrival detection, and anomaly detection, can enhance the ability to detect spoofing attacks. Investing in advanced navigation technologies, such as Vision Aided Navigation, Celestial Aided Navigation, and Magnetic Anomaly Aided systems (Veillette, 2023 | Honeywell, 2023), can provide alternative methods to verify positional data and ensure navigation accuracy. Aviation authorities need to establish stringent regulations and guidelines for GPS security. This includes mandatory reporting of spoofing incidents, certification requirements for navigation systems to include anti-spoofing capabilities, and the development of international standards for GPS security. Implementing comprehensive training programs for both pilots and air traffic controllers on GPS spoofing and its mitigation is essential. These programs should cover the identification of spoofing signs, use of alternative navigation methods, and protocols for reporting and responding to spoofing incidents.

Future Research Directions

The case studies highlight several areas for future research. Developing real-time algorithms that can detect and mitigate spoofing attacks as they occur is critical, which is the main purpose of this study. However, further improving these algorithms so that they are capable of processing large volumes of data and providing alerts to both pilots and controllers would be a possible area of improvement. Furthermore, research into integrating multiple sensor technologies, such as barometers, magnetometers, and optical sensors, with GPS systems can enhance the robustness of navigation systems against spoofing.

Expert Interview Findings

The expert interviews conducted for this research provided valuable insights into the practical challenges and strategies involved in dealing with GPS spoofing incidents within civil aviation. Participants consisted of air traffic controllers with significant experience, who have dealt with a variety of GPS-related disruptions. These interviews revealed recurring themes related to the awareness, preparedness, and mitigation strategies currently employed in air traffic control environments.

One of the most prominent findings from the interviews is the general awareness of GPS spoofing as a growing issue in aviation, particularly in regions prone to geopolitical instability. Multiple participants reported regular occurrence of suspected GPS spoofing incidents, with some controllers encountering multiple spoofing cases per week. Despite the high frequency, most controllers rely heavily on traditional radar systems to verify aircraft positions when GPS data appears unreliable. This reinforces the necessity of maintaining redundant systems, as GPS alone is not fully trusted in these environments. Controllers often described providing visual vectors to aircraft to mitigate the potential hazards of GPS inaccuracies. Pilots commonly receive a terrain warning, meaning the aircraft alerts the pilots to pull up because the aircraft is

about to hit terrain - fully caused by spoofed GPS signals. These statements highlight that, although experienced by air traffic controllers, GPS spoofing is primarily a radar controller issue, as no tower controller reported any GPS spoofing incidents during their watch (Anonymous 3, 2024)

Furthermore, the interviews highlighted a disparity in the availability of tools specifically designed to detect and mitigate GPS spoofing. Participants generally agreed that current air traffic control systems do not incorporate advanced GPS spoofing detection mechanisms, relying instead on manual cross-checks and pilot reports (Anonymous 1, 2024 | Anonymous 2, 2024). This results in increased workload and stress during suspected spoofing incidents, as controllers must take additional steps to ensure safety. The lack of specialised tools underscores a critical gap in current mitigation efforts.

Training was another key issue raised by the interviewees. While controllers undergo general emergency training, many expressed that training specific to GPS spoofing was either lacking or insufficient. The absence of dedicated resources for handling GPS spoofing incidents means that controllers often rely on experience and intuition rather than structured protocols. This points to the need for improved training programs that focus on GPS vulnerabilities and how to address them.

The interviews also revealed a strong desire among air traffic controllers for more sophisticated tools to assist in detecting and managing GPS spoofing. Participants suggested the development of monitoring systems capable of verifying GPS signal integrity and providing real-time alerts for suspected spoofing (Anonymous 2, 2024). Some also advocated for closer collaboration between radar engineers and radar controllers to enhance the overall resilience of the aviation navigation systems (Anonymous 1, 2024).

Furthermore, several interviewees anticipated that emerging technologies, such as artificial intelligence and advanced encryption methods, would play a significant role in future GPS spoofing mitigation. However, they noted that the implementation of these technologies would require considerable investment and regulatory support before they could be fully integrated into current air traffic control systems (Anonymous 1, 2024 | Anonymous 2, 2024).
In conclusion, the expert interviews provided a comprehensive view of the current state of GPS spoofing mitigation in civil aviation. While controllers are aware of the problem and adept at managing its effects, there is a clear need for enhanced tools, training, and system integration to better equip them for the increasing prevalence of spoofing incidents.

Discussion

Interpretation of Findings

The results presented in chapter 6 provide a comprehensive analysis of the effectiveness of the artefact in detecting and mitigating GPS spoofing attacks. The experimental data indicates that the receiver can accurately identify spoofed signals while maintaining a low false-positive rate. This finding is significant as it demonstrates the potential of a low-cost, scalable solution for GPS spoofing detection in civil aviation. The survey and interview data further support the need for such a solution, highlighting the current gaps in awareness, training, and technological capabilities among aviation professionals.

One unexpected but welcome result was the system's ability to recover from spoofing attacks within one cycle (approximately one second) after the spoofing ceased. This rapid recovery is crucial for maintaining navigational integrity and ensuring the safety of aircraft operations. The position tracker algorithm played a vital role in this capability, allowing the system to estimate the aircraft's position based on the last known legitimate coordinates, speed, and heading.

Implications for Civil Aviation

The implications of these findings for civil aviation are profound. The "Smart GPS Receiver" offers a practical and cost-effective solutions to a growing threat. By integrating this technology into existing aircraft navigation systems, airlines can enhance their resilience against GPS spoofing attacks, thereby improving safety and operational efficiency. The ability to detect and mitigate spoofing in real-time can prevent incidents that could lead to unauthorised airspace instructions, near-collisions, and other safety-critical hazards.

Additionally, the adoption of this technology could prompt regulatory bodies to update their guidelines and standards for GPS security in aviation. This would ensure a more robust and unified approach to tackling GPS spoofing, benefiting the entire industry.

Effectiveness of the Proposed Solution

The "Smart GPS Receiver" demonstrated several strengths during testing, including high accuracy in spoofing detection and the ability to recover quickly from spoofing attacks. The use of dual GPS modules and multiple anti-spoofing algorithms contributed to its robustness. However, there are areas for improvement. For instance, the system's performance could be further enhanced by optimising software for better handling of real-time data and reducing computational overhead. Furthermore, the introduction of even more advanced technologies, like artificial intelligence, could increase the systems ability to detect spoofing.

Compared to existing solutions, the artefact offers a more accessible and cost-effective alternative. While military-grade receivers provide high security, their cost and complexity limit their applicability in civilian contexts. The "Smart GPS Receiver" bridges this gap by providing a reliable solution that can be easily integrated into commercial aviation operations.

Limitations of the Study

Despite the promising results, there are several limitations to this study. The experimental setup, whilst designed to mimic real-world conditions, was conducted in a controlled environment. Real-world testing in operational aircraft would provide a more accurate assessment of the system's performance. Additionally, the study relied on simulated spoofing scenarios, which may not capture the full range of potential spoofing attacks encountered in practice.

The survey and interview data, while valuable, were limited to a relatively small sample size of 152 survey participants and 3 civilian air traffic controller interview participants. A broader sample size of interview participants across multiple aviation operations would provide a more comprehensive understanding of the industry's readiness to handle GPS spoofing.

Furthermore, the general lack of technical data available on existing military GPS receivers, civilian GPS receivers in development, and the complete lack of airline data proved to be somewhat of a hurdle in this study. However, the promising test results of this artefact may open the doors for future cooperation with airlines and other aviation stakeholders.

Future Research Directions

Future research should focus on addressing the limitations identified in this study. Conducting real-world tests in operational aircraft will be crucial to validate the system's effectiveness under actual flight conditions. Additionally, further development of the anti-spoofing algorithms, particularly in incorporating advanced machine learning techniques, could enhance the system's detection capabilities.

Exploring the integration of the "Smart GPS Receiver" with other navigational aids, such as inertial navigation systems and satellite-based augmentation systems, could provide a more comprehensive solution to GPS spoofing. Additionally, integrating other sensors, such as barometers, into the receiver will allow for the development of further algorithms to detect spoofing. Finally, expanding the survey and interview studies into much larger and more diverse groups of aviation professionals would offer deeper insights into the industry's needs and readiness.

Conclusion

Summary of Key Findings

This research project aimed to develop a low-cost, scalable solution to detect and mitigate GPS spoofing in civil aviation. The primary findings of this study are:

1. **Effectiveness of the "Smart GPS Receiver"**
    a. The artefact demonstrated high accuracy in detecting GPS spoofing attacks, with a low false-positive rate.
    b. The receiver's ability to recover from spoofing attacks within one second, using the position tracker algorithm, ensures continous navigationsl integrity.
2. **Technological Contributions**
    a. The integration of dual GPS modules and multiple anti-spoofing algorithms provided a robust framework for spoofing detection.
    b. The use of inexpensive hardware components, such as the Raspberry Pi and Adafruit GPS modules, proved that a cost-effective solution is feasible.
3. **Industry Gaps and Needs**
    a. Surveys and interviews revealed significant gaps in awareness, training, and technological capabilities among aviation professionals regarding GPS spoofing.
    b. There is a clear need for more advanced tools and structured training programs to prepare industry stakeholders for handling GPS spoofing incidents.

Contribution to the Field

Theoretical Contributions

This project contributes to the theoretical understanding of GPS spoofing and its mitigation in several ways:

- **Framework for Detection:** This study introduces a comprehensive framework for GPS spoofing detection that combines multiple algorithms and dual GPS modules. This framework can be used as a basis for future research and development in GPS security.
- **Algorithm Development:** The position tracker algorithm, which estimates the aircraft's position based on the last known legitimate coordinates, speed, and heading, offers a novel approach to maintaining navigational integrity during spoofing attacks.
- **Data-Driven Insights:** The survey and interview data provide valuable insights into the current state of awareness and preparedness within the aviation industry, highlighting areas that require further attention and development.

Practical Contributions

The practical implications of this research are significant for aviation authorities, policymakers, and technology developers:

- **Cost-Effective Solution:** The “Smart GPS Receiver” provides a low-cost, scalable solution that can be easily integrated into existing aircraft navigation systems. This makes it accessible to a wide range of aviation operators, from commercial airlines to private pilots.
- **Enhanced Safety:** By improving the detection and mitigation of GPS spoofing, the receiver enhances the overall safety and reliability of air navigation, reducing the risk of incidents caused by navigational errors.
- **Policy and Training:** The findings underscore the need for updated policies and comprehensive training programs. Aviation authorities and policymakers can use this research to develop guidelines and standards for GPS security, ensuring that all stakeholders are adequately prepared to handle spoofing incidents.

Recommendations for Stakeholders

Based on the findings of this research, the following recommendations can be made for industry stakeholders:

1. **Aviation Authorities and Policymakers**
    a. Develop and enforce regulations that require the integration of anti-spoofing technologies in all aircraft navigation systems.
    b. Establish mandatory reporting mechanisms for GPS spoofing incidents to create a comprehensive open-source database that can inform future research and policy development.
    c. Implement certification requirements for GPS equipment to ensure they include robust-anti spoofing capabilities.
2. **Airlines and Aviation Operators**
    a. Invest in the deployment of the “Smart GPS Receiver” or similar technologies to enhance the resilience of their navigation systems against GPS spoofing.
    b. Provide regular training programs for pilots and air traffic controllers on the identification and management of GPS spoofing incidents.
    c. Collaborate with technology developers to continuously improve and update anti-spoofing technologies.
3. **Technology Developers**
    a. Focus on developing real-time algorithms that can detect and mitigate spoofing attacks as they occur, enhancing the capabilities of existing GPS receivers.
    b. Explore the integration of multiple sensor technologies, such as inertial navigation systems and satellite-based augmentation systems, to provide a more comprehensive solution to GPS spoofing.
    c. Work closely with aviation authorities and operators to ensure that new technologies meet industry standards and address teh specific needs of the aviation sector.

Concluding Remarks

In conclusion, this project provides a significant contribution to the field of aviation cybersecurity by addressing the critical issue of GPS spoofing. The development of the “Smart GPS Receiver” demonstrates that it is possible to create a cost-effective, scalable solution that enhances the safety and reliability of air navigation. By combining theoretical insights with practical applications, this study offers valuable guidance for industry stakeholders, paving the way for improved GPS security in civil aviation. The continued collaboration between researchers, policymakers, and industry professionals will be essential in advancing this field and ensuring the resilience of global aviation systems against emerging threats.

Abstract

This thesis investigates the potential of using inexpensive technology to mitigate GPS spoofing, a critical threat to civil aviation. The research focuses on developing and testing a low-cost, scalable solution referred to as the “Smart GPS Receiver”. The study employs a Design Science Research (DSR) paradigm combined with Agile methodology to iteratively design, implement, and evaluate the receiver.

The “Smart GPS Receiver” integrates dual GPS modules and multiple anti-spoofing algorithms to detect and mitigate spoofing attacks. The system’s performance was tested through simulations and real-world data, demonstrating high accuracy in detecting spoofed signals and teh ability to recover from spoofing within one second. Survey and interview data from aviation professionals highlighted significant gaps in awareness, training, and technological capabilities regarding GPS spoofing.

The findings suggest that the “Smart GPS Receiver” offers a cost-effective, practical solution for enhancing GPS security in civil aviation. The study contributes to the theoretical understanding of GPS spoofing detection and provides practical insights for industry stakeholders, including recommendations for regulatory updates and training programs. Future research should focus on real-world testing and further development of advanced detection algorithms to ensure the continued resilience of aviation systems agains the ever developing threat of GPS spoofing.

Bibliography

Corraro, F., Cuciniello, G., Iudice, I., Ferraro, D. & Negro, G. (2022) 'Development and Experimental Validation of a GNSS Receiver Simulator for Flight Missions in Hostile Environments', *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*. Denver, Colorado. 19-23 September 2022. Online. Institute of Navigation. 2163 - 2177. DOI: https://www.doi.org/10.33012/2022.18336 [Accessed 08 July 2024].

Figuet, B., Waltert, M., Felux, M & Olive, X. (2022) 'GNSS Jamming and Its Effect on Air Traffic in Eastern Europe', *Proceedings of The 10th OpenSky Symposium*. Delft, Netherlands. 10-11 November 2022. Online: Engineering Proceedings. 1-10. DOI: https://www.doi.org/10.3390/engproc2022028012 [Accessed 08 July 2024].

Portelli, G., Angrisano, A., Cappello, G., Del Pizzo, S., Gioia, C., Troisi, S. & Gaglione, S. (2023) 'Enhancing navigation solution with Galileo HAS', *2023 IEEE International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea)*. La Valletta, Malta. 04-06 October 2023. Online: IEEE Explore. DOI: https://doi.org/10.1109/MetroSea58055.2023.10317475 [Accessed 24 July 2024].

Zangvil, Y. (N.D.) *Research on GPS Resiliency & Spoofing Mitigation Techniques Across Applications*. Available from: https://www.gps.gov/governance/advisory/meetings/2019-06/zangvil.pdf [Accessed 08 July 2024].

Nasser, H., Berz, G., Gomez, M., De la Fuente, A., Fidalgo, J., Li, W., Pattinson, M., Truffer, P. & Troller, M. (2022) 'GNSS Interference Detection and Geolocalization for Aviation Applications', *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*. Denver, Colorado. 19-23 September 2022. Online: Institute of Navigation. 192-216. DOI: https://www.doi.org/10.33012/2022.18358 [Accessed 08 July 2024].

Eurocontrol. (2021) *Does Radio Frequency Interference to Satellite Navigation pose an increasing threat to Network efficiency, cost-effectiveness and ultimately safety?* Online. Eurocontrol. Available from: https://www.eurocontrol.int/sites/default/files/2021-03/eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf [Accessed 08 July 2024].

Ostroumov, I. & Kuzmenko, N. (2022) 'Cybersecurity Analysis of Navigation Systems in Civil Aviation', *2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO)*. Kyiv, Ukraine. 10-14 October 2022. Online: IEEE Xplore. DOI: https://doi.org/10.1109/ELNANO54667.2022.9927038 [Accessed 08 July 2024].

Samalla, K. & Kumar, P. N. (2024) Global Navigation Satellite System in the Civil Surveillance. *ACS Journal for Science and Engineering* 4(1): 1-10. DOI: https://doi.org/10.34293/acsjse.v4i1.100 [Accessed 24 July 2024].

Lin, M. (2023) Civil Aviation Satellite Navigation Integrity Monitoring with Deep Learning. *Advances in Computer and Communication* 4(4): 260-264. DOI: https://www.doi.org/10.26855/acc.2023.08.008 [Accessed 24 July 2024].

Demir, M. O., Kurt, G. K. & Pusane, A. E. (2020) 'On the Limitations of GPS Time-Spoofing Attacks', *2020 43rd International Conference on Telecommunications and Signal Processing (TSP)*. Milan, Italy, 07-09 July, 2020. Online: IEEE. 313-316. DOI: http://dx.doi.org/10.1109/TSP49548.2020.9163444 [Accessed 12 August 2024].

University of Texas at Austin (N.D.) Texas Spoofing Test Battery (TEXBAT). Available from: https://radionavlab.ae.utexas.edu/texbat/ [Accessed 12 August 2024].

Garmin (N.D.) General Aviation Solutions - Setting The Course For Nextgen Air Navigation. Available from: https://www8.garmin.com/aviation/brochures/721_Gen_Aviation_Solutions.pdf [Accessed 12 August 2024].

Zhang, J., Wang, R., Liu, R., Guo, D., Li, B. & Chen, S. (2022) DSP-Based Traffic Target Detection for Intelligent Transportation. *IEEE Transactions on Intelligent Transportation Systems* 24(11): 13180-13191. DOI: https://doi.org/10.1109/TITS.2022.3225709 [Accessed 13 August 2024].

Khadem, A., Fujiki, D., Talati, N., Mahlke, S. & Das, R. (2023) 'Vector-Processing for Mobile Devices: Benchmark and Analysis', *Proceedings of the IEEE International Symposium on Workload Characterization (IISWC)*. Ghent, Belgium, 01-03 October 2023. Online: IEEE. 15-27. DOI: https://doi.org/10.1109/IISWC59245.2023.00036 [Accessed 13 August 2024].

University of Maine (N.D.) The GFLOPS//W of the various machines in the VMW Research Group. Available from: https://web.eece.maine.edu/~vweaver/group/green_machines.html [Accessed 13 August 2024].

Van Sickle, J. (2022) 'Satellite-Based Surveying Technology', in: Gillins, D. T. (eds) *Surveying and Geomatics Engineering: Principles, Technologies, and Applications*. Online: ASCE Library. Available from: https://ascelibrary.org/doi/10.1061/9780784416037.ch6 [Accessed 08 July 2024].

Meral, E., Guzel, M. S., Mehrubeoglu, M. & Sevinc, O. (2021) 'A New real-time Geolocation Tracking Tool Enhanced with Signal Filtering', in: Daimi, K., Arabian, H. R., Deligiannidis, L., Hwang, M. S. & Tinetti, F. G. (eds) *Advances in Security, Networks, and Internet of Things*. Online: Springer. 491-501. DOI: https://www.doi.org/10.1007/978-3-030-71017-0_35 [Accessed 08 July 2024].

Simak, V. & Sedo, J. (2023) GNSS Spoofing - Advanced Mechanizms of Detection. *Transport And Communication* 11(1): 41-44. DOI: https://www.doi.org/10.26552/tac.c.2023.1.8 [Accessed 08 July 2024].

Gebrekidan, S. (2024) An Israeli air base is a source of GPS 'spoofing' attacks, researchers say. *The New York Times*. Available from: https://www.nytimes.com/2024/07/03/world/europe/an-israeli-air-base-is-a-source-of-gps-spoofing-attacks-researchers-say.html [Accessed 25 July 2024]

Minhas, D. (2023) 'GPS Spoofing Attacks Detection Using Defensive Schemes in FANETs', *2023 International Conference on Data Science and Network Security (ICDSNS)*. Tiptur, India. 28-29 July 2023. Online: IEEE. 1-8. DOI: https://doi.org/10.1109/ICDSNS58469.2023.10245583 [Accessed 08 July 2024].

Vi, N. C., Giang, L. N. & Thong, N. V. (2023) Research and calculate flight navigation parameters using data from the angular speed sensor and long acceleration sensor. *International Journal of Multidisciplinary Research and Growth Evaluation* 4(1): 347-351. DOI: https://doi.org/10.54660/.IJMRGE.2023.4.1.347-351 [Accessed 08 July 2024].

Kemkemian, S., Nouvel, M. & Gilliot, A. (2022) 'Doppler Navigation for small Aircraft over Sea', *2022 23rd International Radar Symposium (IRS)*. Gdansk, Poland. 12-14 September 2022. Online: IEEE. 327-331. DOI: https://doi.org/10.23919/IRS54158.2022.9905060 [Accessed 08 July 2024].

Silveira, L., Rodrigues, M., Facial, B. S., Da Silva, A. S. Q., Marcondes, C., Maximo, M. R. O. A. & Verri, F. A. N. (2022) 'Navigation Aids Based on Optical Flow and Convolutional Neural Network', *2022 Latin American Robotics Symposium (LARS), 2022 Brazilian Symposium on Robotics (SBR) & 2022 Workshop on Robotics in Education (WRE)*. São Bernardo do Campo, Brazil. 18-21 October 2022. Online: IEEE. DOI: https://doi.org/10.1109/LARS/SBR/WRE56824.2022.9995889 [Accessed 08 July 2024].

Amaresh, P. (2024) GPS Spoofing in Aircrafts: The New Age Jeopardy in the Aviation Industry. Available from: https://www.cyberpeace.org/resources/blogs/gps-spoofing-in-aircrafts-the-new-age-jeopardy-in-the-aviation-industry [Accessed 29 July 2024].

Dangwal, A. (2024) GPS Jamming: When Russian Fighter Jet Shot Down '007 Aircraft' Due To Navigational Error, Killing 269 People. Available from: https://www.eurasiantimes.com/gps-spoofing-when-russian-fighter-jet-shot-down/ [Accessed 29 July 2024].

Thurber, M. (2024) GNSS Jamming and Spoofing Events Present a Growing Danger. Available from: https://www.ainonline.com/aviation-news/air-transport/2024-03-04/gnss-jamming-and-spoofing-events-present-growing-danger [Accessed 08 July 2024].

Goward, D. A. (2021) Top 10 GPS Spoofing Events in History - Threat Technology. Available from: https://www.linkedin.com/pulse/top-10-gps-spoofing-events-history-threat-dana-a-goward/ [Accessed 08 July 2024].

Mackinnon, A. (2024) War-Zone GPS Spoofing Is Threatening Civil Aviation. Available from: https://foreignpolicy.com/2024/03/19/war-zone-gps-spoofing-threat-civil-aviation-russia-iran/ [Accessed 08 July 2024].

Wadhams, J. (2024) The impact of GPS spoofing and jamming on aviation. Available from: https://www.wtwco.com/en-hk/insights/2024/06/the-impact-of-gps-spoofing-and-jamming-on-aviation [Accessed 08 July 2024].

Peterson, S. & Faramarzi, P. (2011) Exclusive: Iran hijacked US drone, says Iranian engineer. Available from: https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer [Accessed 31 July 2024].

Zee, M. (N.D.) Flights Misled Over Position, Navigation Failure Follows. Available from: https://ops.group/blog/gps-spoof-attacks-irs/ [Accessed 08 July 2024].

Kelly, L. (2021) *Threats to Civil Aviation Since 1975*. Available from: https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/15952 [Accessed 8th July 2024].
Zmigrodzka, M. (2020) Cybersecurity - One of the Greatest Challenges for Civil Aviation in the 21st Century. *Safety & Defense* 6(2): 33-41. DOI: https://www.doi.org/10.37105/SD.73 [Accessed 08 July 2024].

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I. & Bellekens, X. (2022) Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information 2022* 13(146): 1-22. DOI: https://doi.org/10.3390/info13030146 [Accessed 08 July 2024].

Vaddhiparthy, S. S., Garapati, S., Turlapati, P. R., Gangadharan, D. & Kandath, H. (2023) *A Comprehensive Evaluation on the Impact of Various Spoofing Scenarios on GPS Sensors in a Low-Cost UAV*. Available from: https://www.techrxiv.org/doi/full/10.36227/techrxiv.22709404.v1 [Accessed 08 July 2024].

Islam, S., Bhuiyan, M. Z. H., Paakkonen, I., Saajasto, M., Makela, M. & Kaasalainen, S. (2023). 'Impact analysis of spoofing on different-grade GNSS receivers', *2023 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. Monterey, CA, USA. 24-27 April 2023. Online: IEEE. 492-499. DOI: https://doi.org/10.1109/PLANS53410.2023.10139934 [Accessed 08 July 2024].

Sathaye, H., Noubir, G. & Ranganathan, A. (2022) *On the Implications of Spoofing and Jamming Aviation Datalink Applications*. DOI: https://doi.org/10.1145/3564625.3564651 [Accessed 08 July 2024].

Liu, G., Zhang, R., Yang, Y., Wang, C. & Liu, L. (2020) GPS spoofed or not? Exploiting RSSI and TSS in crowdsourced air traffic control data. *Distributed and Parallel Databases* 39: 231-257. DOI: https://www.doi.org/10.1007/S10619-020-07302-1 [Accessed 08 July 2024].

Khan, S. Z., Mohsin, M. & Iqbal, W. (2021) On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *PeerJ Computer Science* 7: 1-35. DOI: https://doi.org/10.7717/peerj-cs.507 [Accessed 08 July 2024].

Kozovic, D. V. & Durdevic, D. Z. (2021) Spoofing in Aviation: Security Threats on GPS and ADS-B Systems. *Vojnotehnicki glasnik* 69(2): 461-485. DOI: https://www.doi.org/10.5937/VOJTEHG69-30119 [Accessed 08 July 2024].

Majumder, A. (2023) DGCA brings guidelines against GPS spoofing. Available from: https://economictimes.indiatimes.com/industry/transportation/airlines-/-aviation/dgca-brings-guidelines-against-gps-spoofing/articleshow/105481750.cms [Accessed 08 July 2024].

Villamizar, H. (2023) The Impact of GPS Spoofing on Commercial Aviation. Available from: https://www.airwaysmag.com/legacy-posts/gps-spoofing-commercial-aviation [Accessed 08 July 2024].

ICAO (2023) Planning and Implementation Issues related to ATM/SAR - GNSS Interference & GPS Anomalies. Available from: https://www.icao.int/MID/Documents/2023/ATM%20SG9/WP21.pdf [Accessed 08 July 2024].

Veillette, P. (2023) The Serious Threat of GPS Spoofing: An Analysis. Available from: https://aviationweek.com/business-aviation/safety-ops-regulation/serious-threat-gps-spoofing-analysis [Accessed 08 July 2024].

Meng, L., Zhang, L., Yang, L. & Yang, W. (2023) A GPS-Adaptive Spoofing Detection Method for the Small UAV Cluster. *Drones 2023* 7: 461. DOI: https://doi.org/10.3390/drones7070461 [Accessed 08 July 2024].

Li, J., Chen, Z., Ran, Z., Xu, Y., Zhu, X. & Yuan, X. (2023) 'The GNSS Spoofing Detection Method Based on AdaBoost', *2023 6th International Symposium on Autonomous Systems (ISAS)*. Nanjing, China. 23-25 June 2023. Online: IEEE. DOI: https://doi.org/10.1109/ISAS59543.2023.10164411 [Accessed 08 July 2024].

Yang, Z., Ying, J., Shen, J., Feng, Y., Chen, Q. A., Mao, Z. M. & Liu, H. X. (2023) Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Learning From Demonstration. *IEEE Transactions on Intelligent Transportation Systems* 24(9): 9462-9475. DOI: https://doi.org/10.1109/TITS.2023.3269029 [Accessed 08 July 2024].

Mykytyn, P., Brzozowski, M., Dyka, Z. & Langendoerfer, P. (2023) 'GPS-Spoofing Attack Detection Mechanism for UAV Swarms', *2023 12th Mediterranean Conference on Embedded Computing (MECO)*. Budva, Montenegro. 06-10 June 2023. Online: IEEE. DOI: https://doi.org/10.1109/MECO58584.2023.10154998 [Accessed 08 July 2024].

Srinivasan, P. & Sathyadevan, S. S. (2023) 'GPS Spoofing Detection in UAV Using Motion Processing Unit', *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*. Chattanooga, TN, USA. 11-12 May 2023. Online: IEEE. DOI: https://doi.org/10.1109/ISDFS58141.2023.10131729 [Accessed 08 July 2024].

Yang, Q. & Chen, Y. (2022) 'A GPS Spoofing Detection Method Based on Compressed Sensing', *2022 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*. Xi'an, China. 25-27 October 2022. Online: IEEE. DOI: https://doi.org/10.1109/ICSPCC55723.2022.9984624 [Accessed 08 July 2024].

Lubbers, B. & Nikookar, H. (2020) 'A low complexity GNSS spoofing detection method for vehicular applications', *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. Antwerp, Belgium. 25-28 May 2020. Online: IEEE. DOI: https://doi.org/10.1109/VTC2020-Spring48590.2020.9128680 [Accessed 08 July 2024].

Bose, S. C. (2022) GPS Spoofing Detection by Neural Network Machine Learning. *IEEE Aerospace and Electronic Systems Magazine* 37(6): 18-31. DOI: https://doi.org/10.1109/MAES.2021.3100844 [Accessed 08 July 2024].

Zhou, W., Lv, Z., Wu, W., Shang, X. & Ke, Y. (2023) Anti-Spoofing Technique Based on Vector Tracking Loop. *IEEE Transactions on Instrumentation and Measurement* 72: 1-16. DOI: https://doi.org/10.1109/TIM.2023.3289551 [Accessed 08 July 2024].

Buske, I., Walther, A., Fitz, D., Acosta, J., Konovaltsev, A. & Kurz, L. (2022) 'Smart GPS spoofing to countermeasure autonomously approaching agile micro UAVs', *SPIE Security + Defence*. Berlin, Germany. 3-7 September 2022. Online: SPIE. Digital Library. DOI: https://www.doi.org/10.1117/12.2636236 [Accessed 08 July 2024].

Junzhi, L., Hairong, W., Jinfeng, G., Haitao, W. Huyong, L., Yuxiang, Z. & Jiaqi, T. (2022) 'Overview and Prospect of GNSS Anti-spoofing Technology', *2022 2nd International Conference on Computation, Communication and Engineering (ICCCE)*. Guangzhou, China. 04-06 November 2022. Online: IEEE. DOI: https://doi.org/10.1109/ICCCE55785.2022.10036172 [Accessed 08 July 2024].

StrategicRisk (2024) Spotlight on: GPS spoofing risks and what they mean for aviation security and supply chains. Available from: https://www.strategic-risk-global.com/emerging-risks/spotlight-on-gps-spoofing-risks-and-what-they-mean-for-aviation-security-and-supply-chains/1450903.article [Accessed 08 July 2024].

Zangvil, Y. (N.D.) *Research on GPS Resiliency & Spoofing Mitigation Techniques Across Applications*. Available from: https://www.gps.gov/governance/advisory/meetings/2019-06/zangvil.pdf [Accessed 08 July 2024].

Warwick, G. (2024) GPS Interference Grows As A Concern For Civil Aviation. Available from: https://aviationweek.com/aerospace/connected-aerospace/gps-interference-grows-concern-civil-aviation [Accessed 08 July 2024].

Villarreal-Vasquez, M., Model-Howard, G., Dube, S. & Bhargava, B. (2021) Hunting for Insider Threats Using LSTM-Based Anomaly Detection. *IEEE Transactions on Dependable and Secure Computing* 20(1): 451-462. DOI: https://doi.org/10.1109/TDSC.2021.3135639 [Accessed 01 August 2024].

Iudice, I., Pascarella, D., Corraro, G., & Cuciniello, G. (2024) A real/fast-time simulator for impact assessment of spoofing & jamming attacks on GNSS receivers. *Electrical Engineering and Systems Science*. DOI: https://doi.org/10.48550/arXiv.2405.17925 [Accessed 01 August 2024].

Liu, Z., Blanch, J., Lo, S. & Walter, T. (2023) 'Investigation of GPS Interference Events with Refinement on the Localization Algorithm', *Proceedings of the 2023 International Technical Meeting of The Institute of Navigation*. Long Beach, California, USA, 24-26 January 2023. Online: ION. 327-338. DOI: https://www.doi.org/10.33012/2023.18627 [Accessed 03 August 2024].

Murisa, W. & Coetzee, M. (2024) Strengthening Aviation Cybersecurity with Security Operations Centres. *Proceedings of the 19th International Conference on Cyber Warfare and Security* 19 (1): 481-489. DOI: https://doi.org/10.34190/iccws.19.1.2180 [Accessed 04 August 2024].

Lim, I. K., Cho, K. H., Oh, J. H. & Lee, J. R. (2022) Countermeasures against Cyber Threats to Aviation Systems. *Crisisonomy* 18: 21-31. DOI: https://doi.org/10.34190/iccws.19.1.2180 [Accessed 04 August 2024].

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P. & Janicke, H. (2020) A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. *IEEE Access* 8: 209802-209834. DOI: https://doi.org/10.1109/ACCESS.2020.3036728 [Accessed 04 August 2024].

Yun, D., Yong, Y., Kaijun, X. & Zhaoyu, X. (2022) 'Progress of ADS-B IN technology in civil aviation applications', *2022 7th International Conference on Communication, Image and Signal Processing (CCISP)*. Chengdu, China, 18-20 November 2022. IEEE: Online. DOI: https://doi.org/10.1109/CCISP55629.2022.9974442 [Accessed 04 August 2024].

Skelton, A. C. (2023) *Vulnerabilities in Satellite Communications Underscore Threat to Critical Infrastructure*. Available from: https://www.osti.gov/biblio/1992890 [Accessed 04 August 2024].

Shah, I. A., Jhanjihi, N. Z. & Brohi, S. (2024) *Cybersecurity in the Transportation Industry*. Online: Wiley Online Library. DOI: https://doi.org/10.1002/9781394204472.ch1 [Accessed 04 August 2024].

Whitworth, H., Al-Rubaye, S., Tsourdos, A., Jiggins, J., Silverthorn, N. & Khan, I. (2022) 'An Information Entropy and Ensemble Learning Approach for DR-DOS Detection within Aviation Networks', *2022 Integrated Communication, Navigation and Surveillance Conference (ICNS)*. Dulles, VA, USA, 05-07 April 2022. Online: IEEE. DOI: https://doi.org/10.1109/ICNS54818.2022.9771492 [Accessed 04 August 2022].

Baselt, G., Pavur, J., Martinovic, I. (2022) 'Security and Privacy Issues of Satellite Communication in the Aviation Domain', *14th International Conference on Cyber Conflict (CyCon) 2022*. Tallinn, Estonia, 31 May - 03 June 2022. Online: IEEE. DOI: http://dx.doi.org/10.23919/CyCon55549.2022.9811060 [Accessed 04 August 2024].

Santamarta, R. (2014) *A Wake-up Call for SATCOM Security*. Available from: https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf [Accessed 04 August 2024].

Wu, Z., Shang, T. & Guo, A. (2020) Security Issues in Automatic Dependent Surveillance - Broadcast (ADS-B): A Survey. *IEEE Access* 8: 122147-122167. DOI: https://doi.org/10.1109/ACCESS.2020.3007182 [Accessed 04 August 2024].

Dorland, K. & Edmier, T. (2019) 'Security Vulnerabilities in Flight Systems', *11th Annual Undergraduate Research Symposium*, Prescott, Arizona, USA, 04 September 2019. Online: Embry-Riddle Aeronautical University: Scholarly Commons. Available from: https://commons.erau.edu/pr-undergraduate-research-symposium/2019/presentations/4/ [Accessed 04 August 2024].
Harris, M. (2021) FAA Files Reveal A Surprising Threat To Airline Safety: The U.S. Military's GPS Tests. Available from: https://spectrum.ieee.org/faa-files-reveal-a-surprising-threat-to-airline-safety-the-us-militarys-gps-tests [Accessed 05 August 2024].

Firstpost (2024) What is GPS jamming, a growing concern for global aviation? Available from: https://www.firstpost.com/explainers/gps-jamming-aviation-aircraft-estonia-russia-13765939.html [Accessed 05 August 2024].

Kanuri, N. S., Chang, S., Park, Y., Kim, J. & Kim, J. (2023) 'Impact of Location Spoofing Attacks on Prediction in Mobile Networks', *Silicon Valley Cybersecurity Conference (SVCC 2022)*. Online, 17-19 August 2022. Springer Link. 107-119. Available from: https://link.springer.com/chapter/10.1007/978-3-031-24049-2_7 [Accessed 06 August 2024].

Rados, K. Brkic, M. & Begusic, D. (2024) Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors* 24(13): 1-28. DOI: https://doi.org/10.3390/s24134210 [Accessed 06 August 2024].

McAfee (N. D.) What is GPS spoofing? Available from: https://www.mcafee.com/learn/what-is-gps-spoofing/ [Accessed 06 August 2024].

BAE Systems (N. D.) GPS Products. Available from: https://www.baesystems.com/en/product/gps-products [Accessed 06 August 2024].

US Airforce (N. D.) *Global Positioning System (GPS) Selective Availability Anti-Spoofing Module (SAASM)*. Available from: https://www.dote.osd.mil/Portals/97/pub/reports/FY2011/af/2011gps.pdf?ver=2019-08-22-112333-690 [Accessed 06 August 2024].

Zhang, C., Jian, X. & Ta, D. (2024) Revealing the Incidence-Angle-Independent Frequency Shift in the Acoustic Rotational Doppler Effect. *Physical Review Letters* 132(11): 132. DOI: https://www.doi.org/10.1103/physrevlett.132.114001 [Accessed 06 August 2024].

Van Graas, F. (2023) 'Doppler Processing for Satellite Navigation', *2023 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. Monterey, CA, USA, 24-27 April 2023. Online: IEEE. 365-371. DOI: https://www.doi.org/10.1109/PLANS53410.2023.10140011 [Accessed 06 August 2024].

Zhou, Z., Li, H., Chen, Z., Zhong, M. & Lu, M. (2022) 'GNSS Spoofing Discrimination Based on Doppler Residual Monitoring', *Proceedings of the 2022 International Technical Meeting of The Institute of Navigation*. Long Beach, California, USA, 25-27 January 2022. Online: ION. 168-181. DOI: https://www.doi.org/10.33012/2022.18251 [Accessed 06 August 2024].

Cheng, L., Wang, W., Liu, J., Lv, Y. & Geng, T. (2021) GNSS Receiver-Related Pseudorange-Biases: Characteristics and Effects on Wide-Lane Ambiguity Resolution. *Remote Sensing* 13(3): 428. DOI: https://doi.org/10.3390/rs13030428 [Accessed 10 August 2024].

McAlister, C. (2023) *Lost Without It - How GPS is more than just navigation*. Online: University of Southern Queensland. Available from: https://usq.pressbooks.pub/gpsandgnss/ [Accessed 10 August 2024].

Sun, Z., Wang, T., Jiang, Z., Lin, P., Chen, J., Zhang, X., Chen, P. & Zhao, Y. (2019) A high SNR partially coherent beam source based on supercontinuum for free space data transmission. *Optics Communications* 450(1): 335-340. DOI: https://doi.org/10.1016/j.optcom.2019.05.063 [Accessed 10 August 2024].

Baba, A., Alothman, B. & Khattab, O. (2023) 'Blockchain-Based Heuristic Study to Secure UAVs From GPS Spoofing Signals and External Attacks', *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*. Kuwait, 24-26 October 2023. 377-379. Online: IEEE. DOI: https://doi.org/10.1109/BCCA58897.2023.10338915 [Accessed 10 August 2024].

Nagineni, R. B. (2021) A Research on Object Oriented Programming and Its Concepts. *International Journal of Advanced Trends in Computer Science and Engineering* 10(2): 746-749. DOI: https://doi.org/10.30534/ijatcse/2021/401022021 [Accessed 07 September 2024].

Brown, J. (2024) What is GPS Spoofing? … And How to Avoid It. Available from: https://flyapg.com/blog/what-is-gps-spoofing [Accessed 07 September 2024].

FlightRadar24 (2024) *GPS Jamming Map*. Online: FlightRadar24. Available from: https://www.flightradar24.com/data/gps-jamming [Accessed 11 September 2024].

Septentrio (2024) What is spoofing and how to ensure GPS security? Available from: https://www.septentrio.com/en/learn-more/insights/what-spoofing-and-how-ensure-gps-security [Accessed 14 September 2024].

Kozovic, D. V. & Durdevic, D. Z. (2021) *Spoofing in aviation: Security threats on GPS and ADS-B systems*. DOI: https://doi.org/10.5937/vojtehg69-30119 [Accessed 14 September 2024].

Raspberry Pi (2024) Raspberry Pi 5. Available from: https://www.raspberrypi.com/products/raspberry-pi-5/ [Accessed 14 September 2024].

UBlox (2023) NEO-M9N-00B. Available from: https://content.u-blox.com/sites/default/files/NEO-M9N-00B_DataSheet_UBX-19014285.pdf [Accessed 14 September 2024].

OPSGROUP (2024) *GPS Spoofing Final Report of the GPS Spoofing Workgroup*. Available from: https://ops.group/dashboard/wp-content/uploads/2024/09/GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24.pdf [Accessed 16 September 2024].

Anonymous (2024) Interview with Participant 1. 16 September 2024.

Anonymous (2024) Interview with Participant 2. 17 September 2024.

Anonymous (2024) Interview with Participant 3. 29 September 2024.

Honeywell (2023) Honeywell Alternative Navigation. Available from: https://aerospace.honeywell.com/content/dam/aerobt/en/documents/landing-pages/brochures/Aero-Honeywell-Alt-Navigation-Brochure.pdf [Accessed 23 September 2024].

VanHoenacker, M. (2022) Why the iPad is the pilot's new best friend. Available from: https://www.ft.com/content/9a23bcb5-b96b-4d64-8fac-8b53e474dba5 [Accessed 23 September 2024].

Dribbble (N.D.) Car Dashboard Display Transitions Design. Available from: https://dribbble.com/shots/16157449-Car-Dashboard-Display-Transitions-Design [Accessed 28 September 2024].

Adafruit (2024) Breakout Arduino Parsing. Available from: https://learn.adafruit.com/adafruit-ultimate-gps/parsed-data-output [Accessed 28 September 2024].

Khoei, T. T., Ismail, S. & Kaabouch, N. (2022) Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs. *Sensors* 22(2): 662. DOI: 10.3390/s22020662 [Accessed 29 September 2024].

Defense Advancement (N.D.) Military-Grade GPS Receivers & GNSS Receivers. Available from: https://www.defenseadvancement.com/suppliers/receivers/ [Accessed 29 September 2024].

Thales (N.D.) TopStar M, military GPS/GNSS receivers for mission success. Available from: https://www.thalesgroup.com/en/markets/aerospace/navigation-solutions/topstar-m-military-gpsgnss-receivers-mission-success [Accessed 29 September 2024].

Selinger, M. (2017) New GPS Receiver Cards To Exceed DoD Cost Estimate By Billions, GAO Says. Available from: https://www.defensedaily.com/new-gps-receiver-cards-exceed-dod-cost-estimate-billions-gao-says/congress/ [Accessed 29 September 2024].

Stratview Research (2024) Military GPS Receivers Market Analysis | 2024-2030. Available from: https://www.stratviewresearch.com/2882/military-gps-receivers-market.html [Accessed 29 September 2024].

GAO (2021) *GPS Modernization - DOD Continuing to Develop New Jam-Resistant Capability, But Widespread Use Remains Years Away*. Available from: https://www.gao.gov/assets/gao-21-145.pdf [Accessed 30 September 2024].

Hoffman, J. I. E. (2019) *Basic Biostatistics for Medical and Biomedical Practitioners*. 2nd ed. Online: Academic Press. DOI: https://doi.org/10.1016/B978-0-12-817084-7.00025-5 [Accessed 30 September 2024].
Da Silveira, G. A. & Henriqson, E. (2021) Design Science Research - Alternative Pathway for Aviation Training -Related Studies. *The Journal of Aviation/Aerospace Education & Research* 30(2): 1-19. DOI: https://doi.org/10.15394/jaaer.2021.1902 [Accessed 30 September 2024].

Antony, J., Sony, M., Lameijer, B., Bhat, S., Jayaraman, R. & Gutierrez, L. (2023) Towards a design science research (DSR) methodology for operational excellence (OPEX) initiatives. *The TQM Journal*. Available from: https://www.emerald.com/insight/content/doi/10.1108/TQM-01-2023-0017/full/html?skipTracking=true [Accessed 30 September 2024].

Appendix A

Participant Information Sheet

"Where are we? Investigating how inexpensive technology can mitigate GPS spoofing."

Invitation

You are invited to participate in a research project by Michael Sammueller, supervised by Dr. Oliver Buckley and Dr. Samuel Danso of the University of Essex. You have been selected to participate in this study based on your professional experience in aviation. Before participating, please ensure that you have read this sheet and fully understand the purpose of this research project and your involvement. If you have any questions after reading this sheet, please ask for clarification. Participation in this study is voluntary.

Purpose of the Research

According to a paper by Eurocontrol in 2021, radio interference incidents have increased by 2000% since 2018. Although significant prior research has been done regarding GPS spoofing and its impact on the military, especially UAVs, there is a considerable gap in research about it and its effects on civil aviation. Furthermore, there are no off-the-shelf solutions for GPS spoofing, and all existing mitigations used by the military are extremely expensive. This research project aims to address the pervasive and growing issue of GPS spoofing in aviation by developing a novel system that detects and rejects spoofed GPS signals, paving the way for future advancements in secure aerospace navigation.

Location and Time of the Research

Your involvement in this project is limited to a single interview or questionnaire. The interview or questionnaire will take an estimated 30 minutes to complete.

Your Involvement

You will be asked to answer questions on the issue of GPS spoofing in civil aviation, either in an interview or by filling out a questionnaire. If you choose to participate in this study, please answer these questions to the best of your abilities. You may choose to withdraw from this study at any point in time. You may also request that your personal information be anonymised.

Benefits

Participating in this study will aid in progressing research on the impact of GPS spoofing on civil aviation. Your input will also help in developing a potential solution for this issue. As a participant in this study, you may request a copy of the final dissertation.

Risks

There are no risks associated with participating in this study. The researcher will not discuss any sensitive topics with the participants. Personal data will be anonymised upon request, and you may withdraw from this study at any point.

Do you have to take part?

Participating in this study is entirely voluntary. Although you have been selected to participate in this study, you may choose not to. As mentioned, you may also choose to withdraw from the study at any time. You may also choose only to answer some questions and skip others.

Data Confidentiality

1) **How will my data be collected?**
   If you are participating in an interview, your data, such as your answers to the questions, will be written down on paper or recorded electronically in word processing software.
2) **How will my data be stored?**
   Electronic records will be stored on password-protected computers or in an encrypted and password-protected cloud environment. Physical records will be stored in a locked safe within the researcher's residence.
3) **How will my data be used?**
   Your data will support claims in the research paper, aid and guide the design of the final artifact and collect statistical data.
4) **Who has access to my data?**
   Access to your data is restricted to the researcher and the supervisors of this project.
5) **How long will my data be retained?**
   Your data is retained for the duration of the research project. If the dissertation is published in a journal, your data will be retained for seven years after the publication. You may request the deletion of your data at any point in accordance with GDPR.

Payment

You will receive no payment or any other financial benefits for participating.

Right of Withdrawal

You can withdraw from the study anytime, even after your interview or questionnaire. However, please remember that if you have asked for your data to be anonymised, there will be no way of tracing which data you have submitted. If you have any concerns regarding the study, please do not hesitate to ask questions. If you feel like you have been mistreated or your data is being misused, please contact the supervisors directly (see contact details below)

Ethical Review

The ethics board of the University of Essex has ethically reviewed this project. Permission to involve you in this project has been sought directly from your employer.

Results of the Project

The final results of this study will be presented to the computing faculty of the University of Essex. It may also be published in a scientific journal online. As a participant in this study, you may request a copy of the final dissertation to be emailed to you.

Contact Details

Researcher: Michael Sammueller
Email: mbsammueller@gmail.com
Tel: +97466409610

In case of concerns or complaints, please contact:

Supervisor: Dr. Oliver Buckley
Email: oliver.buckley@kaplan.com

Supervisor: Dr. Samuel Danso
Email: samuel.danso@kaplan.com

Thank you for taking the time to read this information sheet.

Research Project Participant Consent Form

"Where are we? Investigating how inexpensive technology can mitigate GPS spoofing."

Researcher: Michael Sammueller
Email: mbsammueller@gmail.com
Tel: +97466409610

Introduction

You are hereby invited to participate in a research project by Michael Sammueller, an MSc Computer Science student, which will be supervised by Dr. Oliver Buckley and Dr. Samuel Danso of the University of Essex.

Firstly, I would like to inform you that:

- Participating in this research project is voluntary
- You may choose to withdraw from this study at any point in time.
- You may request that your data be anonymised.
- Physical copies of your data will be stored in a locked safe at the researcher's residence
- Electronic copies of your data will be stored on a password-protected computer or in an encrypted and password-protected cloud environment.
- Your data will be retained for the duration of the study
- In case of publication, your data will be retained for 7 years following the publication.
- You may request that your data be deleted at any time in accordance with GDPR.
- You will receive no payment or other financial benefit from participating in this study.
- This research project has been reviewed by the ethics board of the University of Essex.
- The researcher is responsible for behaving ethically at all times.

Please contact me before signing this paper if you have any questions about these points.

Purpose of the study and your participation

You have been selected to participate in this study based on your professional experience in aviation. This research project aims to address the pervasive and growing issue of GPS spoofing in aviation by developing a novel system that detects and rejects spoofed GPS signals. This project addresses critical vulnerabilities and paves the way for future advancements in secure aerospace navigation.

The research will be conducted in person in a 30-minute interview/questionnaire session. Answers will be recorded on paper for the questionnaires and digitally in word processing

software for the interviews. Upon request, I will provide you with a copy of the final thesis.
Please note that you must be over 18 years of age to participate in this study.

I have understood my rights and voluntarily participate in this research project. I understand that I can withdraw my involvement at any project stage and request that my data be deleted.

Any information I provide will be solely used for the purposes of this research project, which may include publication. No individuals will be identified in the final publication.

Confidentiality will be respected by the researcher in relation to the information which I give.

Signature Print Name Date

Appendix B

GPS Spoofing in Aviation

Thank you for participating in this survey about GPS usage and spoofing in aviation. Your responses will contribute to a Master's thesis on improving GPS spoofing detection and mitigation. The survey should take about 5-10 minutes to complete.

Your responses will be completely anonymous and will play a crucial role in helping to improve aviation safety by informing the development of new technologies and protocols. The survey should take about 5-10 minutes to complete, and your participation is greatly appreciated. You can withdraw from this survey at any time before clicking "Submit" by closing this tab.

If you have any questions or would like to learn more about the research, please feel free to reach out at antispoofingresearch@gmail.com.

* Indicates required question

Background Information

In this section, we will ask a few questions about your experience as a pilot and the type of aircraft you fly. This helps us understand the context of your responses and ensures that the data we collect is relevant and meaningful.

1. How many years have you been flying as a pilot?*

- Less than 1 year
- 1-5 years
- 5-10 years
- More than 10 years

2. What type of aircraft do you primarily fly?*

- Commercial (e.g., airliners)
- Private (e.g., small planes, general aviation)
- Military
- UAV/Drone
- Other:

3.What regions do you typically fly in?*

Check all that apply.

- North America
- South America
- Europe
- Asia
- Africa
- Middle East
- Oceania
- Other:

GPS Usage and Awareness

Here, we would like to understand how you use GPS in your daily flight operations and your awareness of GPS spoofing. Your insights will help us gauge the importance of GPS and how familiar pilots are with potential GPS-related threats.

4. How important is GPS to your daily flight operations?

- Extremely important
- Very important
- Moderally important
- Slightly important
- Not important at all

5. How familiar are you with the concept of GPS spoofing (broadcasting false GPS signals to deceive GPS receivers?*

- Very familiar
- Somewhat familiar
- Heard of it, but not familiar
- Not familiar at all

6. Have you ever received training or briefings specifically about GPS spoofing?*

- Yes, in-depth training
- Yes, brief overview
- No, but I am aware of it
- No, not at all

Experience with GPS Issues

In this section, we will ask about any experiences you may have had with GPS reliability issues, including possible incidents of GPS spoofing. This will help us assess the frequency and nature of GPS-related challenges in aviation.

7. Have you ever experienced issues with GPS accuracy or reliability during a flight?*

- Yes, frequently
- Yes, occasionally
- Yes, but rarely
- No, never

8. If you have experienced GPS issues, what was the most likely cause in your opinion?

- Equipment malfunction
- GPS signal interference (e.g., jamming or spoofing)
- Poor signal coverage (e.g., mountainous regions)
- Not sure
- Other:

9. Have you ever suspected or confirmed that GPS spoofing was affecting your flight?*

- Yes
- No
- Not sure

10. If yes, how did you detect or suspect GPS spoofing?

Mitigation and Training

This section focuses on the training you have received and the actions you take if GPS spoofing or other issues occur. We are interested in understanding how prepared you feel to handle such situations and what additional resources might be beneficial.

11. What actions do you take if you suspect that the GPS signal is unreliable during a flight?

Check all that apply.

- Switch to backup navigation systems
- Contact air traffic control
- Continue flying with caution
- Other:

12. Do you feel adequately prepared to handle a GPS spoofing incident?*

- Yes
- Somewhat
- No

13. What additional training or resources would help you feel more confident in managing GPS spoofing risks?*

Suggestions for Improvement

We value your expertise and would love to hear your suggestions for improving GPS spoofing detection and mitigation in aviation. This is your opportunity to share any ideas or experiences that could help enhance aviation safety.

14. In your opinion, what could be done to improve the detection and mitigation of GPS spoofing in aviation?*

15. Is there anything else you would like to share about your experiences or thoughts on GPS spoofing and its impact on aviation?

Thank you!

Thank you for participating in this survey. By clicking "Submit," your responses will be securely transmitted to the research team. If you wish to withdraw from the survey, simply close this tab without clicking "Submit." Your responses will only be recorded upon submission.

Appendix C

Air Traffic Controller Interview Sheet

Introduction and Background

1. Can you tell me a little bit about your role as an air traffic controller and how long you have been in this position?

2. What type of sector do you typically manage? (Area, Approach, Director, Tower)

3. Have you had any experiences or been involved in incidents related to GPS failures or spoofing throughout your career? If so, could you describe them?

GPS Usage in Air Traffic Control

4. How integral is GPS to your daily operations?
5. What systems or tools do you rely on that are GPS-dependent?
6. How do you ensure the accuracy and reliability of GPS data when managing air traffic?

Impact of GPS Spoofing

7. Have you ever encountered a situation where GPS data was unreliable or potentially spoofed? How did you become aware of the issue?
8. What immediate actions do you take if you suspect GPS spoofing is affecting aircraft under your control?
9. How do you communicate with pilots during a suspected GPS spoofing incident?

Current Mitigation Strategies

10. What training have you received to handle GPS spoofing incidents?
11. Are there any specific tools or procedures that help you detect and respond to GPS spoofing?

12. What are your biggest challenges when dealing with GPS-related issues in air traffic management?

Suggestions for Improvement

13. What improvements could be made to better equip air traffic controllers to handle GPS spoofing?
14. How do you see the role of new technologies, such as Artificial Intelligence or enhanced satellite systems, in mitigating GPS spoofing in the future?
15. What additional support or resources would help you manage GPS spoofing risks more effectively?

Conclusion

16. Would you like to share anything else about your experiences or thoughts on GPS spoofing in air traffic control?
17. Would you be open to a follow-up discussion if additional questions arise as I progress with my research?