# Assessing the Effectiveness of ADS-B Mitigations

**Heinke Lubbe, Rudi Serfontein and Marijke Coetzee**
School of Computer Science and Information Systems, North-West University, Potchefstroom, South Africa

lubbeheinke7@gmail.com
Rudi.Serfontein@nwu.ac.za
Marijke.Coetzee@nwu.ac.za

**Abstract:** The rise in aerial traffic necessitates aircraft localisation methods that go beyond radar technology's built-in capabilities. The Automated Dependent Surveillance-Broadcast (ADS-B) system is a novel aircraft localisation method that promises to provide the necessary precision to handle the current air traffic surge. The Federal Aviation Administration has, therefore, enforced ADS-B's deployment. However, the architecture of the ADS-B system holds several vulnerabilities. Most of these vulnerabilities are because ADS-B is designed to rely on wireless networks. This paper provides an in-depth analysis of the ADS-B threat landscape and potential mitigations to better understand their distinct characteristics and impact on the ADS-B system. Addressing these security concerns is imperative to ensure ADS-B systems' robustness and trustworthiness and safeguard the aviation industry from potential cyber threats. The paper concludes with a critical review of how well the proposed mitigations address the identified security threats.

**Keywords:** Automated Dependent Surveillance-Broadcast (ADS-B), Threats, Vulnerabilities, Mitigations, Critical Infrastructure

## 1. Introduction

The Automated Dependent Surveillance-Broadcast (ADS-B) system is a novel air traffic surveillance technology employed by aircraft and air traffic controllers. ADS-B allows aircraft to autonomously determine their position using a Global Positioning System (GPS) or Global Navigation Satellite System (GNSS). The ADS-B avionics then combines the data with data gathered from other aircraft systems, such as the Flight Management System (FMS), altimeter, and Traffic Collision Avoidance System (TCAS) units to construct a set of information for the aircraft (Mirzaei et al, 2019). The aircraft automatically broadcasts this information once every second to an ADS-B ground station. Ground stations send the information to an Air Traffic Controller (ATC) for reliable aircraft monitoring (Hasin et al, 2021), resulting in enhanced situational awareness and improved safety and efficiency of air traffic management. Aircraft can also communicate with one another to determine precise positions. In this regard, ADS-B IN and ADS-B OUT are the two functions that make up ADS-B (Hasin et al, 2021). ADS-B OUT is used to broadcast ADS-B data while ADS-B IN is used to receive any ADS-B broadcasted data. Figure 1 shows how ground control stations and aircraft use ADS-B IN and ADS-B OUT to exchange information.

In Figure 1, the transmitting aircraft at the top left corner uses ADS-B OUT (1) to broadcast its location, identification, velocity, and other GNSS related data through a data link (Khandker et al, 2021). There are primarily two types of data links for ADS-B data transmission: the 1090ES and UAT978 (Blåberg et al, 2020). However, 1090ES is the most widely used of these two (Khandker et al, 2022a) and operates on a frequency of 1090 MHz. Ground stations, depicted at the bottom left corner, can receive the broadcasted information using ADS-B IN (4), after which it can process the received information and then broadcast it to all other nearby aircraft using ADS-B OUT (3). Receiving aircraft equipped with ADS-B IN (2), depicted at the top left corner, can immediately receive, process, and display ADS-B signals from all other ADS-B OUT-equipped aircraft and ground stations (Khandker et al, 2021).

This research aims to unveil the ADS-B threat landscape, potential mitigation strategies, and underlying challenges. The paper contributes by not only classifying the threats according to the first two layers of the OSI model but also by critically reviewing how well the potential mitigation addresses the identified threats. In this regard, the paper identifies key areas that need to be addressed.

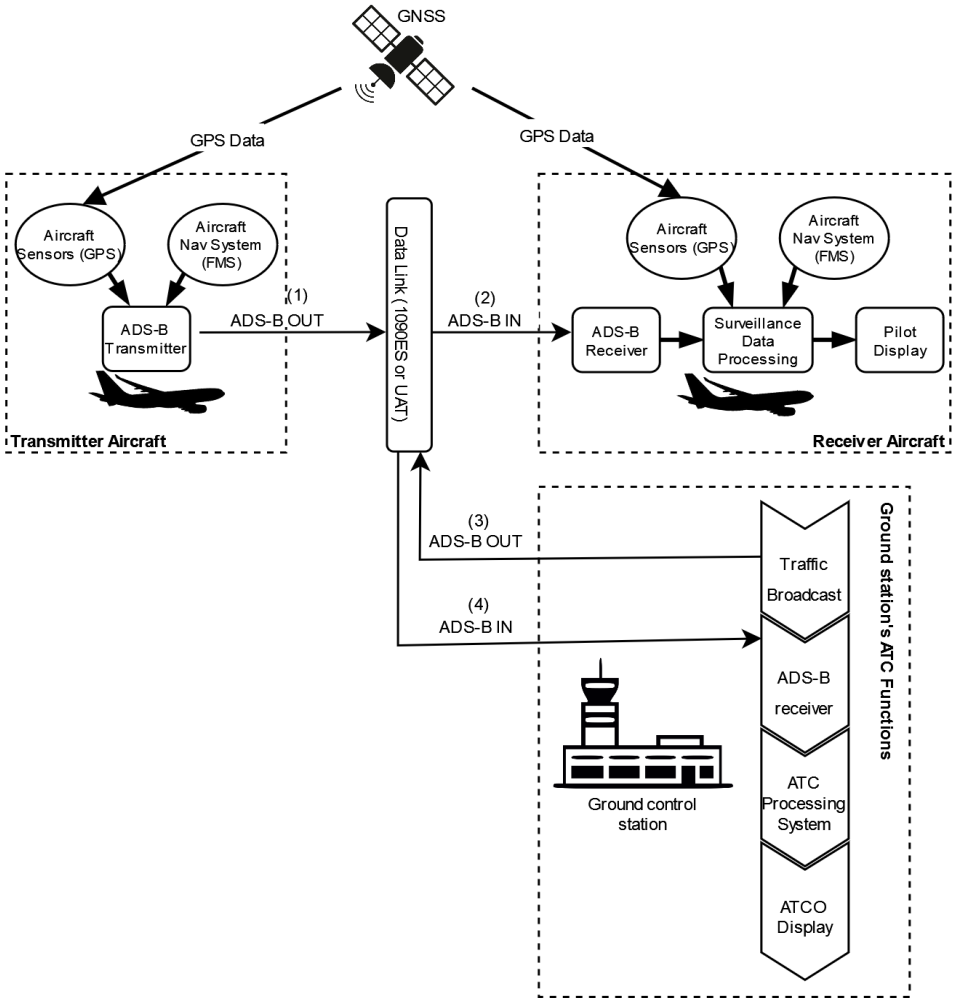


**Figure 1: The ADS-B system**

The following section delves into a threat analysis of the ADS-B technology to provide a better understanding of its distinct characteristics, potential ramifications, and the extent of its impact on the ADS-B system.

## 2. ADS-B Threats

Most ADS-B vulnerabilities result from the nature of the ADS-B architecture, as ADS-B is designed to rely on wireless networks. ADS-B's dependence on wireless networks, GPS, and low-power signals renders ADS-B more vulnerable to security vulnerabilities than radar systems (Li & Kamal, 2011). According to Manesh and Kaabouch (2017), these security vulnerabilities include message interception, injection, modification, and deletion. Figure 2 provides a classification of attacks according to the OSI model's physical and data link layers. While threats can potentially exist at higher layers, they are often less impactful to the core functionality of ADS-B compared to threats at the two lowest layers, which are critical to the system's operation. The threats are discussed in the order in which they appear in Figure 2.

### 2.1 Physical Layer

#### *2.1.1 Flooding*

ADS-B receivers (ASD-B IN) are designed to be sensitive. While this does allow ADS-B receivers to detect weak signals, it poses a security concern. Due to this phenomenon, ADS-B receivers are generally prone to flooding attacks whereby an attacker can flood the screen of an aircraft, or Air Traffic Control, with fake airplanes (Naganawa & Miyazaki, 2018). Flooding attacks may disrupt or overwhelm regular air traffic monitoring systems with a large volume of fabricated messages. According to Khandker et al (2021), these attacks do not require high-end equipment. However, flooding requires a high level of bandwidth in the spectrum in accordance with

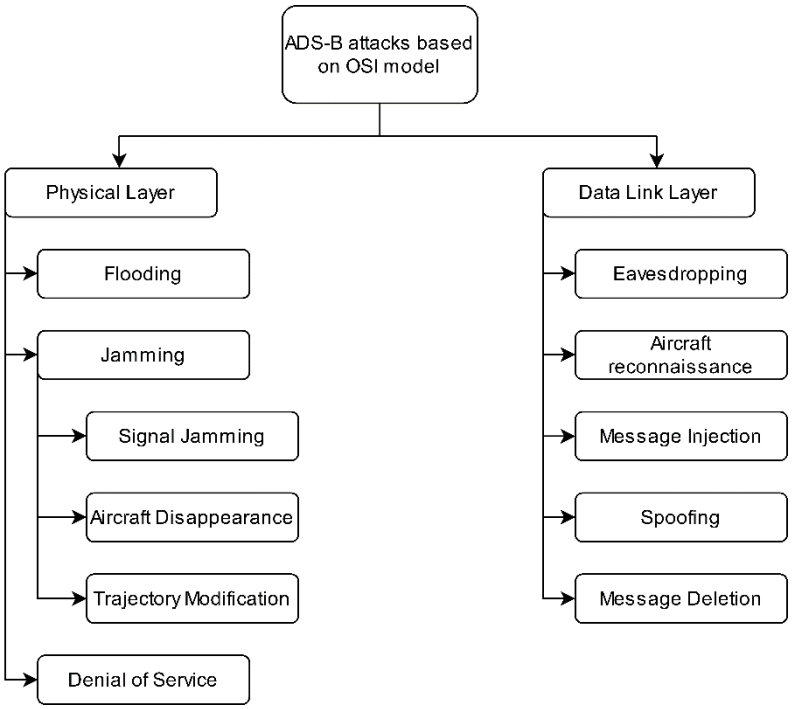


**Figure 2: ADS-B Attacks categorised by OSI Model layers**

It is impossible for the system to pinpoint the location of a potential attacker since ADS-B receivers have omnidirectional antennae that cannot distinguish the direction of the information they receive (Schäfer et al, 2013).

### *2.1.2 Jamming*

According to Khandker et al (2021), an attacker can use a powerful RF signal to cause destructive interference. In this case, the attacker can deny service to wireless nodes within the interference range by overwhelming the system's spectrum. This type of attack is generally referred to as jamming.

Khandker et al (2021) outline several types of ADS-B attacks that utilise this technique:

- **Signal Jamming**: During this attack, an attacker would use a high-power RF noise transmission to block ADS-B traffic channels.
- **Aircraft Disappearance**: An attacker blocks the targeted aircraft's signal through destructive signal interference.
- **Trajectory Modification**: An attacker replaces a part of, or even the entire message, of a low-power signal using a high-power signal. The high-power signal superimposes the fake information by flipping the bits in the real message (Wu et al, 2020).

A jamming attack can either be carried out against the ground station or an aircraft (McCallie et al, 2011). When carried out against a specific ground control station, an attacker would use a low-power jamming device to overwhelm all incoming aircraft transmissions. Of importance to note is that the impact is limited to a confined area due to the jamming signal's range and proximity to the ground station. Alternatively, an attacker could perform an attack against an aircraft. An attack against an aircraft requires a high-power jamming device, as it is very challenging to get in close contact with an aircraft that is moving or flying. An attacker would consequently be more likely to launch the attack from inside an aeroplane.

### *2.1.3 Denial of Service (DoS)*

According to Mirzaei et al (2019), no physical barrier controls access to the data link. An attacker can, therefore, send data at the same 1090MHz radio frequency to real communicating entities. ADS-B receivers can easily detect these signals since they are designed to be inherently sensitive. An attacker can consequently send a large number of fictitious signals in the form of white noise to a particular aircraft. Should the number of signals exceed the ADS-B IN capacity, the ADS-B might become unresponsive or deliver incorrect information (Khandker et al, 2021).

## 2.2 Data Link Layer

### *2.2.1 Eavesdropping and aircraft reconnaissance*

The ADS-B service relies on radio communication that is not encrypted. Unencrypted radio transmissions give rise to eavesdropping as yet another security concern (Blåberg et al, 2020). According to Khandker et al (2021), unencrypted ADS-B broadcasts are accessible to everyone, making aircraft reconnaissance possible. To perform this attack, one can acquire any commercially available ADS-B receiver to intercept ADS-B OUT messages (Viveros, 2016). Wu et al (2020) extend this statement by pointing out that one can use a mobile app or public website to see real-time ADS-B information. Viveros (2016) names several public websites from which real-time ADS-B information can be obtained. The websites include www.flightradar24.com, www.radarvirtuel.com, and www.flightaware.com. The ADS-B information is accessible in real-time since the ADS-B allows aircraft to periodically broadcast information, in the form of plaintext, on a fixed frequency.

### *2.2.2 Message injection*

The ADS-B network does not incorporate authentication in the data link layer (Manesh and Kaabouch, 2017). It is, therefore, possible to inject pseudo-legitimate messages into air traffic communications, referred to as message injection. Khandker et al (2021) state that attackers can launch such attacks using a transmission-enabled SDR-coupled device with power amplifiers. During message injection attacks, attackers construct and broadcast fake ADS-B messages with the same, but less realistic, data as real ADS-B messages, such as velocity, position, and identification number. Aircraft and Air Traffic Control systems in the vicinity receive these ADS-B messages using ADS-B IN and process the messages. As a result, a fake aircraft starts to appear among the real aircraft in the network. The goal of these types of attacks is to inject false information and disrupt the system (Khandker et al, 2021).

### *2.2.3 Spoofing*

The ADS-B service cannot block a malicious transmission source since it relies on radio communication. In other words, the ADS-B service does not implement any form of authentication, which enables an attacker to perform a spoofing attack. These attacks are also called replay attacks and ghost aircraft injection attacks. The primary goal is to confuse the ATC system into recognising ghost planes as real planes (Ying et al, 2019). An attacker can introduce a ghost aircraft on the ATC screens by transmitting a fake signal that matches the required messaging protocol (Khandker et al, 2021). Or, more simply put, the signal must have the same attributes as an authentic ADS-B message (Wu et al, 2020). Ying et al (2019) classify spoofing attacks into the following two categories: aircraft-based and ground-based.

- **Aircraft-based:** In aircraft-based, an attacker operating from an aircraft alters the ICAO address in the ADS-B messages sent by the airborne ADS-B transponder, posing as a known or trusted aircraft to avoid detection.
- **Ground-based:** With ground-based, a ground-based attacker uses an SDR to transmit newly created and properly modulated fake messages or to retransmit previously recorded messages.

Spoofing attacks are, to a large extent, the same as message injection attacks. The only difference lies in the attack's nature and the attacker's intent. Spoofing aims to impersonate legitimate aircraft and transmit false ADS-B signals that appear authentic. Message injection, on the other hand, does not involve impersonation. Instead, the attacker injects false or unauthorised messages directly into the system without necessarily pretending to be a specific aircraft.

### *2.2.4 Message deletion*

The fact that the ADS-B service relies on an unencrypted communication channel and cannot block a malicious transmission source allows an attacker to exploit ADS-B's CRC error handling. Attackers can exploit these 24 bits through constructive interference (Manesh & Kaabouch, 2017). The ADS-B protocol messages include 24 bits of parity (CRC error handling), which can fix up to five bits of errors. Any message with more than five incorrect bits is regarded as corrupted and dropped.

Alternatively, in destructive interference, the attacker creates a time-synchronised signal that inverses the ADS-B signal and reduces or destroys the ADS-B message (Mirzaei et al, 2019). The result is that the ADS-B signal gets destroyed while in transit. However, this approach requires the attacker to eavesdrop on the 1090 MHz extended squitter channel and create a destructive interference with the time-synchronised message that the attacker wants to delete before the message reaches the ground station (Schäfer et al, 2013). The complexity of

time synchronisation makes this kind of message deletion attack more challenging to carry out and less effective (Manesh & Kaabouch, 2017).

It becomes clear that ADS-B holds several security concerns. Addressing these security concerns is imperative to ensure ADS-B systems' robustness and trustworthiness and safeguard the aviation industry from potential cyber threats. As such, the following section discusses potential mitigations for the above-identified security concerns.

## 3. Mitigations

The following section provides a comprehensive analysis of the literature on potential solutions for safeguarding ADS-B systems against the threats identified in Section 2. This section aims to offer insights into techniques and strategies for enhancing the integrity and resilience of ADS-B networks.

Over the past decade, numerous studies have proposed methods for securing ADS-B communications. According to both Wu et al (2020) and Khandker et al (2021), ADS-B security solutions can be divided into two main categories: secure broadcast authentication and secure location verification. Wu et al (2020) provide an ontological tree in Figure 3 to graphically depict the security methods for ADS-B.

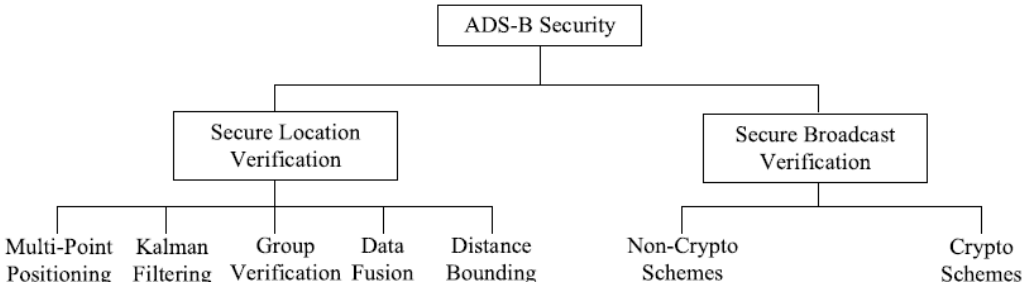


**Figure 3: Classification of ADS-B mitigations (Wu et al, 2020)**

The following sections discuss each category and its associated methods independently. An in-depth discussion follows the analysis of these methods.

### 3.1 Secure Location Verification

Secure location verification aims to determine how authentic an aircraft's position or that of another communication participant is (Wu et al, 2020). Manesh and Kaabouch (2017) state that secure location verification can be divided into two categories: secure location determination and in-region verification. Secure location determination solutions find the sender's physical location information and use that information to cross-validate the message's legitimacy (Wu et al, 2020). Conversely, in-region verification uses an estimation algorithm to calculate the likelihood that the reported position is true. In other words, in-region verification tries to assess the reliability of a stated location in an ADS-B message that has been received (Manesh & Kaabouch, 2017). The techniques used in secure location verification are analysed in the order presented in Figure 3.

#### *3.1.1 Multi-point positioning*

In multi-point positioning, an aircraft broadcasts signals to several ground stations. Each ground station receives an identical signal with a different time stamp. A hyperbolic equation calculates the aircraft's position based on the delay in the signal received (Wu et al, 2020).

#### *3.1.2 Kalman filtering*

Kalman filtering, also known as linear quadratic estimation, determines unknown variables to produce estimates that are likely more correct than estimates based solely on observations of individual measurements. The algorithm consists of three steps: Prediction, observation, and update (Manesh & Kaabouch, 2017). The system's state variables and any resulting uncertainties are anticipated in the prediction process. The forecasts rely on the system's present condition, state transitions from earlier states to its current state, and system inputs. The algorithm adjusts its estimates in the observation phase by computing the error as the difference between the current measured state measurements and the projected values derived in the previous step. The weights are updated and distributed among the estimates in the update step, with greater weights going to the estimates that have a higher probability (Bishop & Welch, 2001). The Kalman filtering can produce ideal and accurate flight status values, clear incorrect data, smooth all missing data, and filter signal noise and instability. It primarily serves the ground system's ADS-B validation needs (Wu et al, 2020).

### *3.1.3 Group verification*

Group verification primarily uses multi-alteration technology amongst group members to confirm the location declaration information of the non-group members, hence ensuring the ADS-B IN communication security. Before joining a group, four or more aircraft must authenticate one another to establish trusted actors (Manesh & Kaabouch, 2017). The air position of non-group members can then be determined using multi-alteration techniques based on signal strength or signal arrival time differential. The aircraft in the opposite group is alerted, and the proper course of action is implemented as soon as a false location report is discovered (Wu et al, 2020).

### *3.1.4 Data fusion*

With data fusion, data from various sources are combined and correlated to produce more accurate and trustworthy results than those from a single source (Wu et al, 2020). This technique can help mitigate attacks such as malicious data injection.

### *3.1.5 Distance bouncing*

Distance bouncing is one of the in-region location verification methods (Manesh & Kaabouch, 2017). The basis of this method is that a signal's transmission speed (speed of an electromagnetic wave) is equal to the speed of light. Any signal delay means the message has been spoofed (Wu et al, 2020). Consider a transmitting aircraft A and a receiving aircraft B. Aircraft A becomes the prover node in distance bouncing and Aircraft B the verifier node. Aircraft B typically sends a message to Aircraft A, to which Aircraft A must respond to prove that it is in range of Aircraft B. For this reason, aircraft A is referred to as the prover node. Aircraft B, the verifier node, then considers the messages' round-trip times plus some processing time to compute the distance between the two aircraft. This information can be used to verify the correctness of the claimed location of a node (Manesh & Kaabouch, 2017).

### *3.1.6 Traffic modelling*

Modelling is done using data mining techniques to spot inaccurate location data or other malicious behaviour. For instance, as the received signal strength is inversely proportional to the distance, one can determine whether the position data is accurate (Wu et al, 2020).

This section analysed some of the Secure Location Verification methods that are aimed at mitigating several prominent ADS-B threats. The next section examines Secure Broadcast Authentication techniques shown in Figure 3.

## 3.2 Secure Broadcast Authentication

Secure broadcast authentication has the security requirement that no attacker may fake a legitimate broadcast. Secure broadcast authentication seeks to offer ADS-B with an authentication method that still ensures the preservation of ADS-B's openness (Wu et al, 2020). However, Manesh and Kaabouch (2017) state that ADS-B message authentication is more challenging than for a standard point-to-point network due to the lack of two-way communications and reliable transmission between ADS-B communicating entities. There are two types of secure broadcast authentication: crypto and non-crypto schemes.

### *3.2.1 Crypto schemes*

Symmetric and asymmetric approaches for message authentication form part of cryptographic schemes to authenticate ADS-B messages. However, the application of symmetric and asymmetric systems has several challenges due to the features of ADS-B broadcast. This seems to be particularly true concerning key management and distribution. Additionally, the frequencies designated for ADS-B technologies - 978 MHz for UAT and 1090 MHz for 1090ES - cannot support a significant number of nodes when channel interference is considerable (Manesh & Kaabouch, 2017). Cryptographic techniques that lengthen ADS-B messages result in more significant interference and constrained capacity.

Asymmetric encryption, also known as Public Key Infrastructure (PKI), is a scalable and systematic way to distribute keys. Asymmetric encryption, as an ADS-B solution, has two significant drawbacks. First, the length of sent ADS-B signals increases because current asymmetric systems lack compact encryption structures. Second, each receiver needs to receive distinct encrypted ADS-B messages (Manesh & Kaabouch, 2017). Furthermore, PKI must maintain and store certificates to assure the validity and authenticity of the public key. The revocation, updating, and storage operations involving the certificates necessary for the functioning of PKI setups will

become increasingly frequent as the number of planes rises, which is expensive and less scalable (Wu et al, 2020).

The Aircraft Address Message Authentication Code (AA-MAC) is an alternative cryptographic security solution. This specific security solution performs message integrity using a common hash technique, such as MD5 or SHA, and a private authentication key on the current aircraft address (AA) (Giannatto Jr, 2015). As such, an ADS-B message's current aircraft address (AA) field is replaced with the newly calculated AA-MAC. The rest of the message remains the same. This is required for the AA-MAC message source integrity scheme to work correctly. As with public key infrastructure, secret key distribution is also one of the difficulties that AA-MAC faces.

### *3.2.2 Non-crypto schemes*

The above-discussed cryptographic solutions are highly dependent on key distribution and management. This requirement makes cryptographic solutions incompatible with the existing ADSB infrastructure and challenging to employ (Manesh & Kaabouch, 2017). Non-cryptographic network security strategies, however, avoid the issue of key management or distribution by primarily using fingerprinting technology and spread spectrum.

Fingerprinting, as a non-cryptographic approach to authentication and identification, is based on software or hardware errors or features of frequency channels that are difficult to replicate. By utilising fingerprinting, network intrusions can be recognised using the distinctive qualities of genuine network nodes (Zeng et al, 2010). Zeng et al (2010) outline three methods, namely software-based fingerprinting, hardware-based fingerprinting, and channel-based fingerprinting, that can be used to improve or even supplant conventional encryption.

- Software-based fingerprinting is based on the distinctive characteristics of networking software that runs on hardware from a specific vendor. These variations can be grouped and used to recognise network devices.
- Hardware-based fingerprinting rely on variations in network hardware. Hardware-based fingerprinting methods, such as radiometric fingerprinting, can take advantage of these variations in the modulation of radio waves to identify devices.
- Location-based fingerprinting use of the inherent qualities of communication channels. It has been used to replace conventional authentication and verification approaches with procedures that rely on signal intensity, channel impulse response, and carrier phase (Manesh & Kaabouch, 2017).

Each method has specific benefits and drawbacks. Some methods require considerable infrastructure, while others are relatively practical (Khandker et al, 2021).

## 4. ADS-B Countermeasure Gaps

The following section critically reviews the solutions discussed in this paper. In Table 1, ADS-B countermeasures are compared regarding their ability to address security threats. Jamming attacks remain the biggest concern on the physical layer, with multi-point positioning currently being the only solution. As for the data link layer, eavesdropping and aircraft reconnaissance remains a major concern. The Public Key Infrastructure (PKI) solution is the only solution to address these concerns. In fact, the PKI solution handles most security concerns despite being the most challenging and expensive. However, spoofing attacks are fully covered, followed by flooding and message deletion attacks. It should also be noted that the majority of the other defences, such as distance bounding and Kalman filtering, only address a specific attack approach and are ineffective as stand-alone remedies.

The ADS-B countermeasures are compared in Table 2 to the security services. For instance, the public key infrastructure solution guarantees data integrity, location integrity, authentication, and data confidentiality, but it cannot provide ADS-B network availability. Data fusion can ensure availability, authenticity, and location fidelity. However, the integrity and confidentiality of ADS-B transmissions are not guaranteed with data fusion.

**Table 1: Comparison of ADS-B countermeasures to threats addressed**

| | Method | Flooding | Jamming | Denial of Service | Eavesdropping | Aircraft reconnaissance | Spoofing | Message Deletion |
|---|---|---|---|---|---|---|---|---|
| Secure location verification | Multi-point positioning | No | Yes | Yes | No | No | Yes | Yes |
| | Kalman filtering | Yes | No | No | No | No | Yes | No |
| | Group verification | Yes | No | No | No | No | Yes | Yes |
| | Data fusion | Yes | No | Yes | No | No | Yes | Yes |
| | Distance bouncing | Yes | No | No | No | No | Yes | No |
| | Traffic modelling | Yes | No | No | No | No | Yes | No |
| Secure Broadcast Authentication | PKI | Yes | No | No | Yes | Yes | Yes | Yes |
| | Message authentic-cation code | Yes | No | No | No | No | Yes | Yes |
| | Fingerprinting | Yes | No | Yes | No | No | Yes | Yes |

Other methods, such as distance bounding and message authentication codes, solely address a single security need and are unacceptable as stand-alone security solutions. When considering the two tables as a whole, it should be noted that none of the proposed secure location verification mitigation strategies currently addresses eavesdropping and aircraft reconnaissance. Location verification mitigation strategies, when compared to secure broadcast authentication, are more orientated towards verifying the legitimacy of an aircraft's claimed position. In other words, it ensures location integrity. Secure Broadcast Authentication, on the other hand, are focused on authentication.

**Table 2: Comparison of ADS-B countermeasures with security services**

| | Method | Authentication | Confidentiality | Data Integrity | Location Integrity | Availability |
|---|---|---|---|---|---|---|
| Secure location verification | Multi-point positioning | No | No | Yes | Yes | Yes |
| | Kalman filtering | Yes | No | Yes | Yes | No |
| | Group verification | No | No | No | No | No |
| | Data fusion | Yes | No | No | Yes | Yes |
| | Distance bouncing | No | No | No | Yes | No |
| | Traffic modelling | No | No | No | Yes | No |
| Secure Broadcast | PKI | Yes | Yes | Yes | Yes | No |
| | Message authentication code | Yes | No | No | No | No |
| | Fingerprinting | Yes | No | No | No | Yes |

Maintaining confidentiality remains a challenge due to the lack of mitigation strategies that address eavesdropping and aircraft reconnaissance. Maintaining confidentiality is not as simple as one might expect. According to the US Federal Aviation Administration (FAA), operational requirements make unencrypted data links vital to ensure compatibility and global interoperability (Khandker et al, 2022b). Operational requirements for that reason make unencrypted messages and the lack of authentication one of ADS-B's primary flaws. The lack of fundamental security safeguards makes tampering with ADS-B signals easy, impacting the confidentiality, integrity, and availability of the transmitted aircraft data (Wu et al, 2020). Furthermore, only multi-point

positioning, data fusion and fingerprinting address Denial of Service attacks. As such, these are the only solutions addressing the availability of ADS-B messages and services.

Based on this analysis, it is clear that no holistic solution exists. This paper addresses this research gap by proposing a hybrid solution. Message authentication code, which is a crypto scheme more practical than PKI, should be integrated with underlying cross-verification techniques used for secure location verification. The hybrid solution would consequently address most of the ADS-B threats and thereby security services, rendering the solution acceptable as a stand-alone security solution. Furthermore, such an approach should satisfy the FAA's operational requirements. Although confidentiality is still not fully covered, it will be to a larger extent as threat actors might still intercept transmission and extract certain information. However, threat actors will not be able to tell from which aeroplane the transmission originated. The only drawback is that this solution has an underlying requirement to overcome secret key distribution challenges. That is, an aeroplane should be provided with a secret key when the specific aeroplane desires to access the air traffic control system and ADS-B network. It seems feasible since AA-MAC only needs one key to identify a sender uniquely.

## 5. Conclusion

The primary contribution of this paper is to not only classify the threats according to the OSI model but also to critically review how well the potential mitigation addresses the identified threats. This is accomplished by analysing both the security concerns and solutions related to ADS-B. ADS-B system attacks and mitigations have been extensively covered in published research studies. Based on the literature, ADS-B is vulnerable to cyber-attacks in multiple ways. Most of these attacks try to exploit the 1090 MHz communication channel. As such, most security solutions also relate to the 1090 MHz communication channel. Many of the proposed solutions address either a single or a small number of security concerns at a time. Furthermore, many of the solutions do not consider the limitations of the ADS-B architecture, the dense traffic on the 1090 MHz channel, or compatibility with current communications hardware and software. Consequently, the suggested countermeasures are often impractical. According to Wu et al (2020), many of the proposed solutions are only in an experimental phase. Manesh and Kaabouch (2017) continue by stating that the recommendations also call for considerable improvements. This paper addresses this research gap by proposing an alternative solution. Future research will focus on the development of the hybrid solution presented in Section 4.

## References

Bishop, G. & Welch, G. (2001) *An introduction to the kalman filter*. SIGGRAPH, Course, 8(27599-23175):41.

Blåberg, A., Lindahl, G., Gurtov, A. & Josefsson, B. (2020) *Simulating ADS-B attacks in air traffic management*. 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC). IEEE. pp. 1-10.

Giannatto Jr, C.J. 2015. *Challenges of implementing automatic dependent surveillance broadcast in the nextgen air traffic management system*.

Hasin, F., Munia, T.H., Zumu, N.N. & Taher, K.A. (2021) *ADS-B based air traffic management system using ethereum blockchain technology*. 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD). IEEE. pp. 346-350.

Khandker, S., Turtiainen, H., Costin, A. & Hämäläinen, T. (2021) *Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures*. IEEE Transactions on Aerospace and Electronic Systems, 58(4):2702-2719.

Khandker, S., Turtiainen, H., Costin, A. & Hämäläinen, T. (2022a) *On the (in) security of 1090ES and UAT978 mobile cockpit information systems–an attacker perspective on the availability of ADS-B safety-and mission-critical systems*. IEEE Access, 10:37718-37730.

Khandker, S., Turtiainen, H., Costin, A. & Hämäläinen, T. (2022b) *Cybersecurity attacks on software logic and error handling within ais implementations: A systematic testing of resilience.* IEEE Access, 10:29493-29505.

Li, W. & Kamal, P. (2011) *Integrated aviation security for defense-in-depth of next generation air transportation system*. 2011 IEEE International Conference on Technologies for Homeland Security (HST). IEEE. pp. 136-142.

Manesh, M.R. & Kaabouch, N. (2017) *Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system*. International Journal of Critical Infrastructure Protection, 19:16-31.

McCallie, D., Butts, J. & Mills, R. (2011) *Security analysis of the ADS-B implementation in the next generation air transportation system*. International Journal of Critical Infrastructure Protection, 4(2):78-87.

Mirzaei, K.F., De Carvalho, B.P. & Pschorn, P. (2019*) Security of ADS-B: Attack scenarios*. EasyChair, Tech. Rep,

Naganawa, J. & Miyazaki, H. 2018. *A method for accurate ads-b signal strength measurement under co-channel interference*. 2018 Asia-Pacific Microwave Conference (APMC). IEEE. pp. 354-356.

Schäfer, M., Lenders, V. & Martinovic, I. (2013) *Experimental analysis of attacks on next generation air traffic communication*. Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28, 2013. Proceedings 11. Springer. pp. 253-271.

Viveros, C.A.P. (2016) Analysis of the cyber attacks against ADS-B perspective of aviation experts.

Wu, Z., Shang, T. & Guo, A. (2020) *Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey*. IEEE Access, 8:122147-122167.

Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L. & Poovendran, R. (2019) *Detecting ADS-B spoofing attacks using deep neural networks*. 2019 IEEE conference on Communications and Network Security (CNS). IEEE. pp. 187-195.

Zeng, K., Govindan, K. & Mohapatra, P. (2010) *Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]*. IEEE Wireless Communications, 17(5):56-62.