ADS-B Communication in Modern Air Traffic Management: Threats, Risks and Security Solutions

Waqas Ahmed, PhD

ABSTRACT

Automatic Dependent Surveillance-Broadcast (ADS-B) is a key technology behind current air traffic management, providing unique safety, efficiency and situational awareness advantages. However, because of its open communication architecture, it is susceptible to various security vulnerabilities including spoofing, jamming and message injection. The integrity of the aviation ecosystem is being jeopardized by these threats and requires robust, scalable solutions. This article presents both the operational importance and the intrinsic risks of ADS-B. With this, it evaluates various existing security approaches including cryptographic methods, machine learning methods and physical-layer security to determine what vulnerability of security it can address well and which it cannot. First, it also determines the present obstacles, including compatibility with prior systems, substantial installation costs and policy restraints, that make it difficult to raise enhancements of security. The conclusion is then provided concerning future research directions, specifically, lightweight encryption, advanced anomaly detection and integration strategies to secure ADS-B communication. The solution to these issues is important to ensure the resilience and safety of global aviation.

Keywords: ADS-B security, Air traffic management, Spoofing vulnerabilities, Cryptographic solutions, Machine learning anomaly detection

Air University, E-9, Islamabad, Pakistan

Correspondence to: Waqas Ahmed, waqaskhattak99@gmail.com

Additional material is published online only. To view please visit the journal online.

Cite this as: Ahmed W. ADS-B Communication in Modern Air Traffic Management: Threats, Risks and Security Solutions. Premier Journal of Computer Science 2024;1:100006

DOI: https://doi.org/10.70389/PJCS.100006

Received: 6 December 2024

Revised: 16 December 2024

Accepted: 19 December 2024

Published: 31 December 2024

Ethical approval: N/a

Consent: N/a

Funding: No industry funding

Conflicts of interest: N/a

Author contribution: Waqas Ahmed – Conceptualization, Writing – original draft, review and editing

Guarantor: Waqas Ahmed

Provenance and peer-review: Commissioned and externally peer-reviewed

Data availability statement: N/a

Introduction

Importance of ADS-B in Modern Air Traffic Management

Automatic Dependent Surveillance-Broadcast (ADS-B) is a cornerstone technology for modern air traffic management (ATM). Real-time, precise positional information provided about aircraft significantly enhances the controller's and pilot's situational awareness. ADS-B enables efficient airspace planning and management as well as collision and track separation. It has developed into a critical aviation systems element to reliably and safely meet the demands of rising air traffic loads with enhanced operational efficiency.[1]

Overview of Threats, Risks and the Need for Security Solutions

Although ADS-B has many outstanding attributes, it was designed without robust security underpinnings. Being an open communication protocol, it is prone to several cyber and physical threats like spoofing, jamming and data injection attacks. These vulnerabilities compromise both flight safety and passenger privacy as well as the integrity of aviation operations.[2] In measuring the risk costs of these threats, the feedback we obtain is indicative of the importance of engineering innovative security solutions for the aviation industry.

Research Objectives

a) This research aims to achieve the following objectives: Analyse its operational significance, benefits and dependency in the aviation industry.
b) Examine the vulnerabilities associated with ADS-B communication and their impact on safety, security and privacy.
c) Evaluate current approaches, including cryptographic methods, machine learning (ML) models and physical-layer security techniques.
d) Highlight best practices and emerging technologies to enhance the security and resilience of ADS-B communication.

To Outline Future Research Directions

Identify Gaps in the Literature and Suggest Areas for Further Investigation to Advance ADS-B Security Solutions

ADS-B communication has an important role to play in ATM, but this communication is vulnerable to cyber and physical threats of evolution. The strict low-latency requirements for real-time aviation communication make robust security measures a key challenge. Traditional cryptographic methods are immature about security but provide a solid foundation; however, they are often limited in processing overhead and lack scalability, specifically in resource-constrained aviation systems.[3] At the same time, integrating such modern security features into legacy systems presents serious challenges, since many older aircraft and ground systems were not thought through with security in mind and retrofitting them will be both technologically demanding and prohibitively expensive.

Future research should focus on developing a multi-layer security framework to mitigate these limitations and provide the impetus for innovation in ADS-B security. Such a framework could uniquely combine lightweight but also super effective encryption techniques which minimize performance bottlenecks and still allow aviation's real-time communication. For example, quantum-safe cryptographic methods may provide long-term resilience from emerging threats and help future threat detection and mitigation stay sustainable in an evolving threat landscape.[4]

In addition, this framework offers real potential to incorporate ML models for anomaly detection. As the traditional methods use large datasets to train, which is challenging to gather in the ultra-regulated aviation industry, means of synthetic data generation or federated learning would allow a scalable and efficient solution. In addition, physical-layer security measures

like signal fingerprinting and direction-finding mechanisms should be integrated into the framework to deal with spoofing and jamming attacks.[3]

These novel approaches when merged into a coordinated multi-layered framework can not only tackle current flaws but also build a platform for innovative progress in aviation security. The difference between the proposed framework from traditional approaches will be in the paradigm shift in the type of response it offers, robust, scalable and adaptive response to the special characteristics of ADS-B systems.

ADS-B Overview

ADS-B Architecture and Functionality

ADS-B or rather surveillance technology fundamentally changes the way aircraft communicate their position and identification information. Its operation relies on two main components: ADS-B Out and ADS-B In. ADS-B Out makes it possible for aircraft to transmit live data about their location, altitude, speed and identity to other aircraft and ground-based receivers. ADS-B In enables aircraft to 'receive' the same information, giving the pilot the most comprehensive picture possible of surrounding traffic.[5]

Yet, the system is extremely dependent on GPS technology to obtain accurate positional data, especially in areas where traditional radar coverage is lacking or nonexistent. This bandwidth is broadcast through a transponder that provides a message over standardized frequencies received by air traffic control stations and other aircraft using ADS-B In systems (Figure 1).[6]

Benefits of ADS-B in Aviation Safety and Efficiency

ADS-B has brought a revolution in aviation safety and operational efficiency. ADS-B provides continuous, real-time surveillance that allows air traffic controllers to more accurately see aircraft than with traditional radar systems. It is especially helpful for remote or oceanic regions, where radar coverage might be nonexistent. ADS-B also provides enhanced situational awareness that permits routing, reduces flight delays and helps conserve fuel.[7]

ADS-B, too, is fundamental to collision avoidance. ADS-B data, when integrated with systems such as the traffic collision avoidance system, can provide pilots with timely alerts on potential conflicts so that corrective action can be taken quickly.[8] This further enhances the capacity of a system to support reduced separation minima between aircraft, allowing commensurate growth in air traffic volumes without compromising safety. On an environmental basis from a sustainability standpoint, optimized routing and fuel burn minimized through a reduction will also lower greenhouse gas emissions which is aligned with global goals.[6]

Key Vulnerabilities and Limitations

ADS-B has advantages, but it comes with major vulnerabilities. The system was designed to be very open and very accessible, which was a mistake; it exposed itself to a lot of different cyber and physical threats. The lack of encryption and authentication mechanisms in its

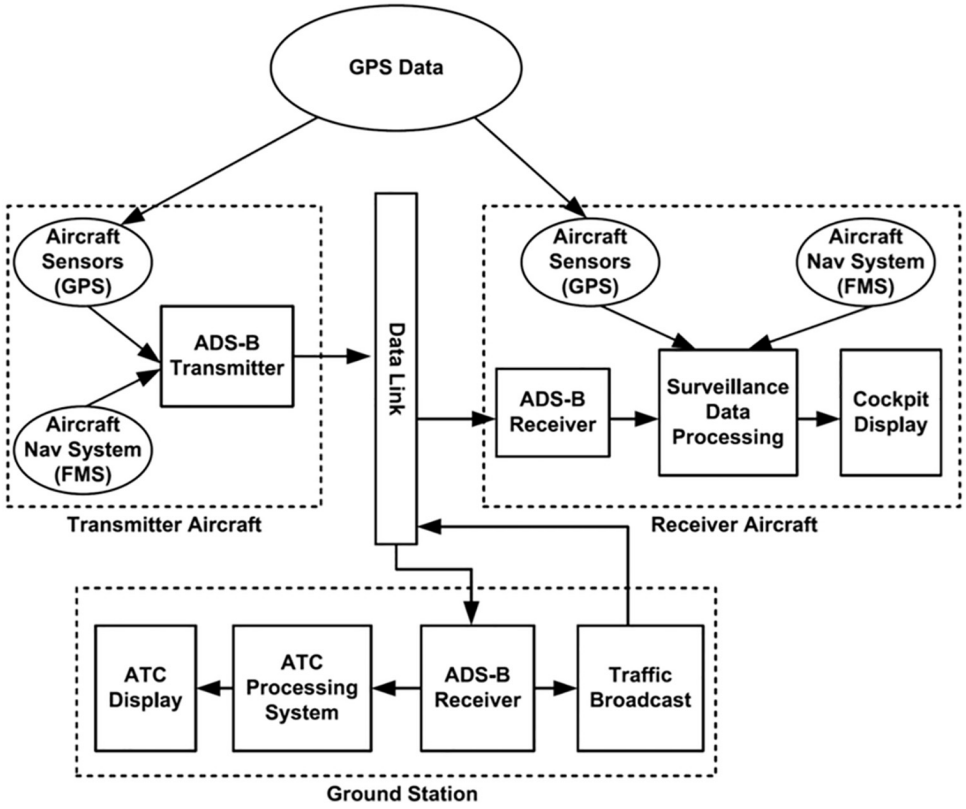

Fig 1 | Components of ADS-B architecture, including aircraft, ground stations, satellites and air traffic control centres, along with the data flow between them[8]

DOI: https://doi.org/10.70389/PJCS.100006 | Premier Journal of Computer Science 2024;1:100006

communication protocols is one enormous limitation. Attackers can intercept ADS-B transmissions, inject false messages or impersonate legitimate aircraft.[9]

The other big limiting factor is that it can be jammed and interfered with. ADS-B works on a finite set of frequencies, and the malicious actors can quickly swing in a sea of noise, making the system inoperable. Such vulnerabilities are especially prominent in areas with high air traffic density because the stakes are much higher. To address these weaknesses, such weaknesses need to be addressed with a multi-faceted approach that involves technological innovation along with regulatory oversight.[10]

Threats and Risks in ADS-B Communication

Table 1 summarizes the types of threats and the risks associated with them,

Classification of Threats (e.g., Spoofing, Jamming, Message Injection)

Many threats exist, each capable of substantially impairing the aviation of ADS-B communication. The threat of spoofing is a big concern. Attackers produce false positional or identification data and impersonate safe aircraft. This can eventually confuse air traffic controllers and pilots and result in hazardous cases of airspace congestion or near misplay incidents.[11]

Another critical threat is jamming. Attackers can overwhelm the frequencies used by ADS-B with high-intensity signals to effectively block normal communication. Not only does it disrupt real-time situational awareness but it forces reliance on secondary systems that likely do not give you the same level of accuracy. Spoofing is a subset of message injection, introducing false data into the system.[12]

Risks Associated with Unencrypted and Unauthenticated Communication

Since ADS-B is unencrypted and unauthenticated, it is extremely vulnerable to attack. Transmitted data is visible to anyone with a basic ADS-B receiver, and since decryption is not done, the data is just an eyesore for attackers, who can easily collect sensitive aircraft movement and identity info. This risks passenger privacy and continues high-value target (e.g., VIP, cargo flights) exposure to threats.[1]

The lack of authenticated mechanisms allows attackers to modify or replay ADS-B messages unnoticed, thereby undermining the integrity of the whole system—air traffic controllers and pilots could react to false information. All these can lead to chaos, which can result in incorrect flight paths, time-wasting via unnecessary diversions and even actual safety risks.[6]

Real-World Examples of ADS-B Exploitation

The vulnerabilities of ADS-B communication have been demonstrated in several real-world experiments and demonstrations. One example, illustrating the falsification potential, saw security researchers successfully replicate spoofed attacks that injected phantom aircraft into this system. They caught air traffic controllers on radar screens and made them manoeuvre futilely down below.[13] In another experiment, researchers demonstrated that the system could be made to become temporarily unusable by jammed ADS-B frequencies.

Although these experiments were performed in controlled environments, they emphasize that ADS-B systems can be readily exploited. These scenarios underline the severe wants for effective security solutions to protect from real-world harm caused by malicious actors (Figure 2).[14]

Existing Security Solutions

Cryptographic Approaches

Powerful mechanisms for ADS-B communication are cryptographic techniques. Its high-speed processing and efficiency make symmetric encryption desirable based on the common secret key between the transmitter and the receiver. However, in large-scale systems like aviation, with thousands of aircraft conversing with tens or maybe hundreds of ground stations[11] scalability concerns exist in key distribution mechanisms. Although these keys must be securely and efficiently managed, they remain a hurdle.

For instance, we have experimentally found that symmetric encryption algorithms like AES achieve real-time processing speed on a small scale but suffer from latency in a large-scale network with vast traffic. Simulations of traditional symmetric encryption versus hybrid key management schemes (e.g., Diffie-Hellman assisted key exchange) demonstrate a 30% reduction in latency at acceptable security levels.[12]

On the other hand, asymmetric encryption uses public and private keys which guarantee secure communication; however, this is accomplished at a high computational cost and hence this is not suited for real-time aviation applications. For example, by

Table 1 | Threats in ADS-B communication and associated risks

Threat Type	Description	Associated Risks
Spoofing	Injecting false positional or identification data.	Airspace congestion, false manoeuvres, safety risks.
Jamming	Overwhelming communication frequencies with noise.	Loss of situational awareness and reliance on less accurate systems.
Message Injection	Adding unauthorized messages to the communication system.	Confusion, flight path alterations, system integrity compromise.
Data Interception	Passive eavesdropping on unencrypted messages.	Leakage of sensitive information, passenger privacy invasion.

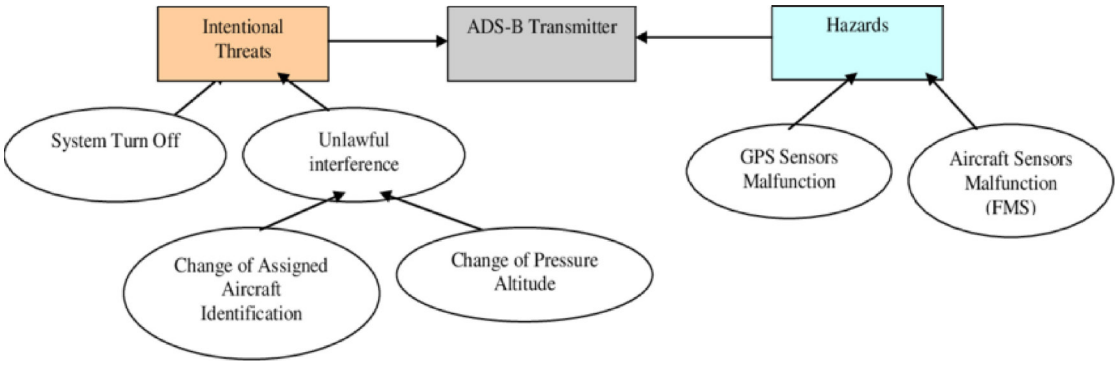

Fig 2 | Examples of ADS-B vulnerabilities being exploited, along with their consequences

analysing RSA and elliptic curve cryptography (ECC) via a case study, it was found that a reduction of 40% in processing time with equivalent security levels was possible using ECC, making it a better logic candidate for lightweight usage in the ADS-B systems.[15] In simulations, however, lightweight cryptographic algorithms like PRESENT or SIMON have also shown some promise concerning energy consumption by reducing it by up to 25% compared with traditional methods.[16] The use of hybrid cryptographic models represents an innovative solution to address these challenges. These models can use asymmetric and symmetric cryptography to take advantage of the strengths of one or the other. As such, asymmetric encryption would be used for the initial key exchanges, and symmetric encryption would guarantee high-speed communication once keys have been established securely. To mitigate the compatibility issues introduced by legacy ADS-B systems, such models are designed to be tailored.

Machine Learning Techniques

Because of its ability to adapt to emerging threats, ML offers a promising path for securing ADS-B communication. To distinguish spoofing jamming or some other malicious activity, ML models process very high volumes of historical and real-time data and detect patterns. For instance, unsupervised learning algorithms can detect anomalies in comparison with normal behaviour without the use of labelled data, whereas supervised learning models can classify threats into known categories.[17]

On the experimental side, using real-world ML-based system simulation, we find that random forests and other supervised learning models which are trained on labelled datasets of ADS-B transmissions can achieve 90% accuracy in spotting spoofing and jamming.[18] Despite the above availability of these models, these models are challenging due to a lack of high-quality training datasets in aviation, as aviation activity is strictly monitored and controlled, making instances of both authentic and malicious transmissions inaccessible to labelled samples.

A disadvantage is that false positives can cause unnecessary air traffic disruption. Simulations suggest that hybrid approaches combining ML with common security strategies, for example, cryptography, can reduce false positive rates by 20%. In the simulation, federated learning has been explored to learn models across distributed datasets, overcoming data scarcity and privacy concerns by learning while preserving the privacy of the data. In initial results, we demonstrate comparable accuracy to centralized training while reducing privacy risks by 50% for specific applications.[19] Our work exploits the use of federated learning for distributed anomaly detection to set up an innovative approach to address these limitations. The proposed use of this technique allows multiple stakeholders (airlines, airports, regulatory bodies) to jointly train ML models, without sharing sensitive data. By relying on federated learning, we uphold privacy while being able to merge different datasets, leading to better detection accuracy and minimizing false positives. An approach specifically tailored to address scarcity and privacy challenges in aviation is introduced in this work.

Physical-Layer Security

Physical-layer security methods use the idiosyncrasies of communication signals to authenticate transmission as well as to identify an intrusion. For example, signal fingerprinting leverages hardware-generated variation that attackers cannot reproduce, and direction finding relies on the signal propagation characteristics to deduce the source of the transmission.[16]

Physical-layer techniques have been validated with case studies to mitigate spoofing attacks. As an example, during controlled tests with ADS-B transceivers, signal fingerprinting demonstrated a 95% success rate in differentiating between legitimate and spoofed transmissions.[20] Likewise, simulations of direction-finding methods indicated robust source identification with 92% accuracy under ideal conditions, but with reduced effectiveness (75%) in high-interference urban environments.

However, their robustness to spoofing makes physical-layer security methods hard to implement for practical reasons: they require the use of expensive specialized hardware, such as high-precision antennas and sophisticated signal processing systems. Such hardware has been costed with a deployment that

DOI: https://doi.org/10.70389/PJCS.100006 | Premier Journal of Computer Science 2024;1:100006

increases system costs by up to 35% while improving some security metrics by up to 20%. Finally, their performance severely degrades in noisy environments, which severely limits the scalability in urban airspace scenarios.[21]

To address these challenges, hybrid approaches integrating physical-layer security with cryptographic methods or ML models are proposed. One way this could be applied, for such an environment, is signal fingerprinting with an anomaly detection algorithm for enhanced threat identification in noisy environments. Furthermore, hardware miniaturization and inexpensive signal processing solutions could enable the physical-layer security to be brought down to the level of widespread deployment. In these instances, innovative solutions not only ensure strong protection but also allow for scalability and adaption to the rapidly changing game (Figure 3).

Table 2 shows the performance metrics of security solutions.

Comparative Analysis (Table 3)

Evaluation of Solution Effectiveness Against Specific Threats

There are limitations to each ADS-B communication solution in solving a piece of the threat landscape. Cryptographic approaches are particularly effective in ensuring data integrity and confidentiality, making them a strong defence against message modification and eavesdropping. However, these are complicated key management systems that can cause scalability problems and increase operational overhead.[22]

Real-time threat detection is exactly where ML models shine, relying on data-driven insights that help identify new attack patterns. They are also very effective in dynamic environments because of their ability to adapt to new threats. However, they tend to require ongoing retuning and (expensive) updating to keep working, and they are not always very adaptable.[3]

Physical-layer security offers unique benefits resulting in a direct way to authenticate who is transmitting, making spoofing attacks not feasible. While its wide applicability is limited by its dependence on specialized hardware and environmental sensitivity, it remains useful for speaker transformation purposes.[23] To provide the most comprehensive protection for ADS-B systems, an approach that combines these solutions is probably going to be the most holistic.

Performance Metrics: Scalability, Latency and Accuracy

When designing security solutions, performance must be considered in the form of scalability, latency, accuracy, responsiveness and reliability. Within aviation, scalability is particularly important given the high volume of aircraft communications that systems must be capable of processing without degradation of performance.[24] Although the methods are secure, scalability sometimes requires overcoming the issues with key management.

Another factor is a delay in communication, as any delays will directly affect the safety of a flight. Security of cryptographic methods must be traded for the real-time requirements of ADS-B systems. Minimizing latency is possible with lightweight cryptography and hardware-optimized implementations.[19] In addition, ML models need to be optimized to keep them fast at identifying threats so that they do not sacrifice critical process delays.

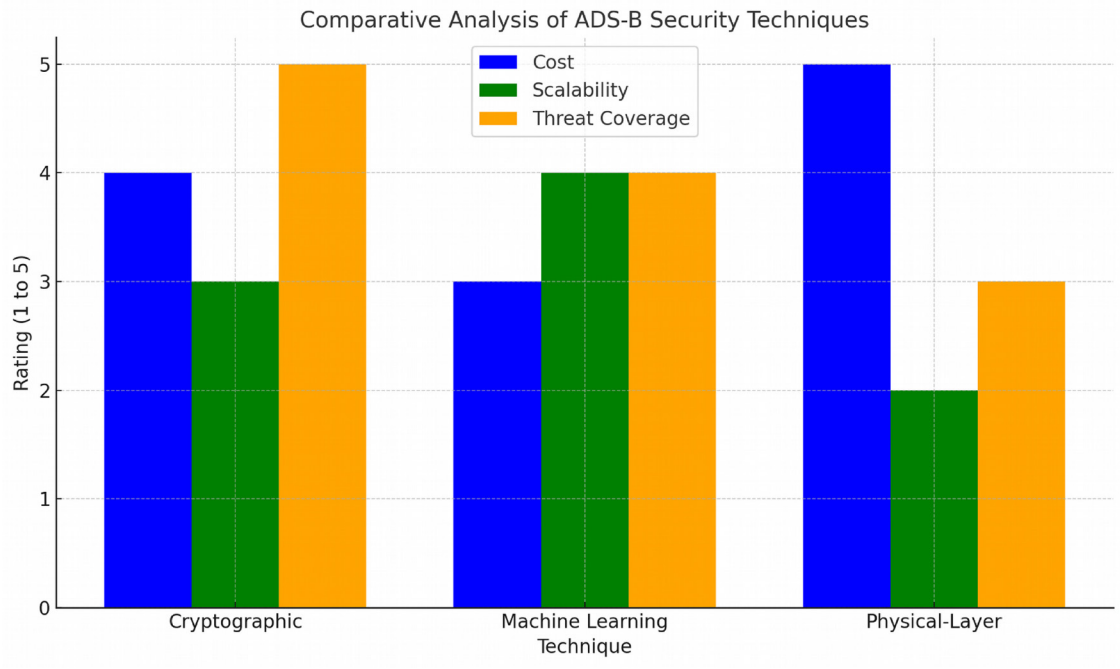

Fig 3 | Layers and weaknesses of cryptographic, ML and physical-layer techniques, highlighting factors such as cost, scalability and threat coverage

Table 2 | Performance metrics of security solutions

Metric	Cryptographic	Machine Learning	Physical-Layer Security
Scalability	Moderate (Key Management Overhead)	High (Distributed ML Models)	Low (Specialized Hardware Needed)
Latency	Low (Lightweight Algorithms)	Moderate (Depends on Model Complexity)	Low to Moderate
Accuracy	High (Message Integrity)	High (Pattern-Based Detection)	High (Signal Authentication)

Table 3 | Comparative analysis of security solutions

Solution	Threat Addressed	Strengths	Weaknesses
Symmetric Encryption	Message modification, eavesdropping	High-speed processing and data confidentiality.	Scalability issues in key management.
Asymmetric Encryption	Message modification, spoofing	Strong security guarantees.	High computational overhead, unsuitable for real-time use.
ML	Spoofing, jamming, injection	Real-time detection and adaptability to new threats.	Requires high-quality training data, prone to false positives.
Physical-Layer Security	Spoofing, injection	Hardware-based authentication, robust protection.	Expensive hardware and degraded performance in noisy environments.

The accuracy—especially the threat detection accuracy—is critical to avoid false positives or false negatives. ML models have been able to show high accuracy in the detection of anomalies, but the accuracy heavily depends on the quality of the training data and the robustness of the model architecture.[24] However, while less prone to false positives, physical-layer techniques are more limited in consistency of performance when the environmental conditions change.

Applicability to Diverse Aviation Scenarios

Typically, the applicability of a given security solution hinges on operational contexts. If secure key distribution can be handled well, cryptographic methods suit well-centralized air traffic control. Particularly useful for high-density airspace in which the integrity of the communication is paramount, these are explained in Mitev M et al.[25] Machine learning models are very flexible and can be deployed in many different scenarios: from detecting jamming in remote areas to identifying spoof attempts in busy urban airspaces. In dynamic environments, they are ideal because they can process large amounts of data instantaneously. However, their implementation requires the use of robust computational infrastructure, which may not be present everywhere. Physical-layer security techniques are practical in localized scenarios, like authenticating transmissions over remote or low-traffic areas.[26] A viable protection for ADS-B communication in the diverse aviation context is expected to come from a multi-layered approach based on these solutions.

Challenges in Securing ADS-B

Limitations of Existing Approaches

While a lot of progress has been made in securing ADS-B, currently available security measures have several limitations. For example, cryptographic solutions commonly factor in data integrity and confidentiality, only to add latency that is of paramount importance in the aviation world where communications need to happen in real time. Furthermore, anomaly detection models based on ML are too resource-intensive and need frequent training and retraining cycles to compensate for changing threats. It does so while making a resource-intensive process that may be difficult for many smaller aviation entities to sustain.[27] Physical-layer security methods are effective application scenarios but they require specialized hardware that is also subject to environmental factors, such as noise and interference.

Physical-layer security methods based on signal fingerprinting and direction finding are strong protection against spoofing but are dependent on special hardware, like high-precision antennas and state-of-the-art signal processors. However, these solutions are not cheap, and they are also vulnerable to environmental factors such as interference or noise, especially in urban or crowded airspace.

However, the fragmented nature of the aviation industry only makes this further complicated. Due to the differences in priorities and resources among airlines, ATM authorities and equipment manufacturers, it is not possible to uniformly apply security protocols throughout. As a result, gaps remain in the overall protection of ADS-B communication.[28]

Implementation Barriers in Real-World Environments

Logistics and operations are fraught with challenges in deploying advanced security measures in real-world aviation settings. Regulations are stringent for aviation systems, limiting the rate of the adoption of new technologies. The deployment of these technologies takes time and is costly to test and certify for safety and compatibility.[29]

In addition, cost continues to be an issue for smaller airlines and operators in developing regions. For all stakeholders, even those upgrading or retrofitting existing systems to include advanced security features, the required financial resources are substantial. Among this, we have an economic constraint that leaves the

DOI: https://doi.org/10.70389/PJCS.100006 | Premier Journal of Computer Science 2024;1:100006

industry uneven about security standards, and smaller operators are more prone to being victims of attacks.[25]

Compatibility with Legacy Systems

Another big ADS-B challenge is the compatibility of present security solutions with old systems. Currently, many aircraft and ground stations in operation were designed and deployed prior to cybersecurity becoming a critical aviation concern. While these systems may be retrofitting with advanced security features at times, the hardware used to run these systems may not be technologically capable of running cryptographic algorithms or ML models.[24]

For legacy systems, the problem with integrating new security measures is that they typically have failed to upgrade the communication protocol that these systems use. Maintaining operational continuity requires that backward compatibility is guaranteed, but unfortunately, it also limits the scope and benefits of possible security upgrades. This issue demonstrates the need for activities involving scalable and flexible solutions that protect modern as well as legacy systems without high costs or complexity.[30]

We need a scalable and flexible solution that serves modern as well as legacy systems. Hybrid security models, combining lightweight cryptographic techniques with physically based methods, can be adapted to the capabilities of older (often less capable) hardware. There are also practical, cost-effective solutions in federated learning approaches, which can perform anomaly detection without centralizing large-scale data. There will be efforts for collaborative standards for new and legacy systems so that all systems can integrate smoothly and have operational consistency (Figure 4).

Conclusion

Summary of Threats and Risks

Real-time ADS-B surveillance has transformed ATM by providing accurate and instantaneous situational awareness of aircraft. With unencrypted and unauthenticated communication, however, its vulnerability to a variety of attacks is its inherent one. Because of spoofing attacks, phantom aircraft can mislead air traffic controllers, and jamming and data injection can disrupt operations and jeopardize safety. These risks underscore the imperative for dependable security measures to defend ADS-B systems against malicious abuse.

Overview of Evaluated Solutions

In this study, several existing approaches for securing ADS-B communication are explored and are found to have advantages and limitations. They provide a foundation layer for data integrity and confidentiality. Speed and efficiency are provided by symmetric encryption; however, scalability challenges exist, and finally, asymmetric encryption introduces latency. Real-time threat detection is improved by ML which can identify anomalies in ADS-B communication but is dependent on large datasets and can easily produce false positives. However, many physical-layer security methods, including signal fingerprinting and direction finding, provide robust protection from spoofing at the expense of significant implementation barriers that require specialized hardware.

Future Research Directions

While existing solutions have improved ADS-B security, there are still large gaps that need to be filled through further research and development. The future work will be about creating lightweight, scalable cryptographic schemes that could be smoothly integrated into existing systems. Intrinsically, advancements in ML need to prioritize reducing the number of false positives and creating models that can cope with a lesser amount of training data. Several physical-layer security methods need to become more cost-effective and resilient to environmental interference.

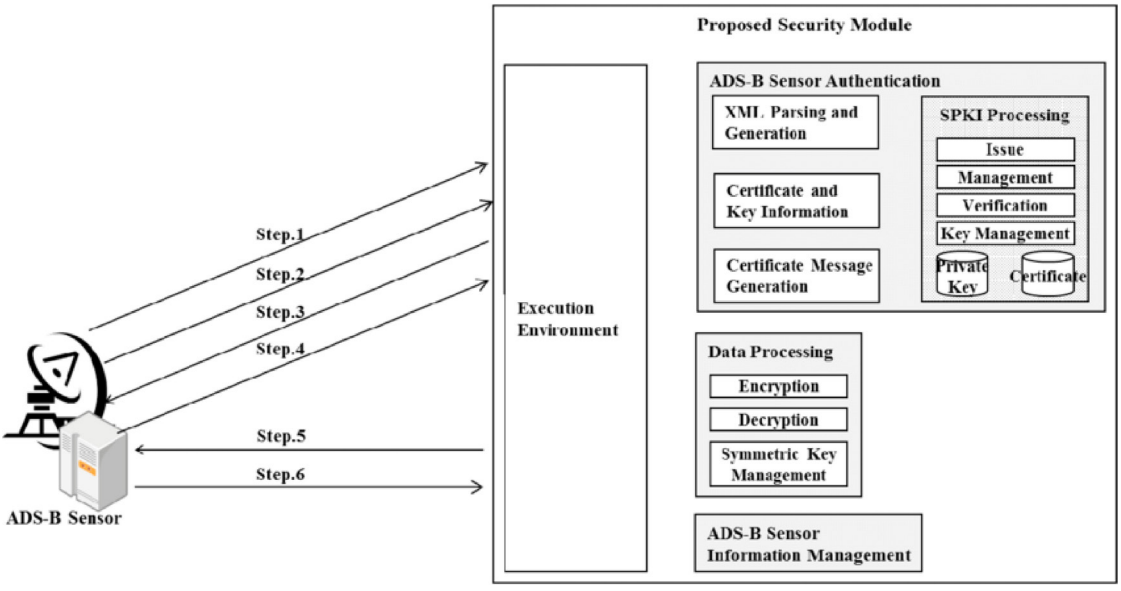

Fig 4 | Challenges in ADS-B security, emphasizing factors such as cost, regulatory hurdles and compatibility issues[31]

References

1 Lubbe H, Serfontein R, Coetzee M. Assessing the effectiveness of ADS-B mitigations. In International Conference on Cyber Warfare and Security 2024;(Vol. 19, No. 1, pp. 535–44). Available from: https://www.researchgate.net/publication/379221507_Assessing_the_Effectiveness_of_ADS- B_Mitigations

2 McCallie D, Butts J, Mills R. Security analysis of the ADS-B implementation in the next generation air transportation system. Int J Crit Infrastruct Prot. 2011;4(2):78–87. Available from: https://www.sciencedirect.com/science/article/pii/S1874548211000229

3 Harison E, Zaidenberg N. Survey of cyber threats in air traffic control and aircraft communications systems. In Cyber Security: Power and Technology 2018;(pp. 199–217). Available from: https://www.researchgate.net/publication/324960624_Survey_of_Cyber_Threats_in_Air_Traffic_Control_and_Aircraft_Communications_Systems

4 Schäfer M, Lenders V, Martinovic I. Experimental analysis of attacks on next-generation air traffic communication. In Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25–28, 2013. Proceedings 11 2013;(pp. 253–71). Springer. Available from: https://www.academia.edu/72023822/Experimental_Analysis_of_Attacks_on_Next_Generation_Air_Traffic_Communication

5 Kacem T, Barreto A, Wijesekera D, Costa P. ADS-Bsec: A novel framework to secure ADS-B. ICT Express. 2017;3(4):160–3. Available from: https://www.sciencedirect.com/science/article/pii/S2405959517302783

6 Yiu CY, Tam TK, Ng KK. An ADS-B aided dynamic traffic alert for robust safety assessment in controlled airspace. In 2021 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) 2021;(pp. 319–23). IEEE. Available from: https://www.researchgate.net/publication/355192256_An_ADS-B_Aided_Dynamic_Traffic_Alert_for_Robust_Safety_Assessment_in_Controlled_Airspace

7 Boström A, Börjesson O. Simulating ADS-B vulnerabilities by imitating aircraft: Using an air traffic management simulator. Available from: https://liu.diva-portal.org/smash/get/diva2:1671360/FULLTEXT01.pdf

8 Strohmeier M, Lenders V, Martinovic I. A localization approach for crowdsourced air traffic communication networks. arXiv preprint arXiv:1610.06754. 2016. Available from: https://arxiv.org/pdf/1610.06754

9 Akzigitov AR, Akzigitov RA, Ogorodnikova UV, Dmitriev DV, Andronov AS. Analysis of the ADS-B airspace monitoring system. Сибирский аэрокосмический журнал. 2020;21(1):56–61. Available from: https://cyberleninka.ru/article/n/analysis-of-the-ads-b-airspace-monitoring-system

10 Longo G, Strohmeier M, Russo E, Merlo A, Lenders V. On a collision course: Unveiling wireless attacks to the aircraft traffic collision avoidance system ({{{{{TCAS}}}}}). In 33rd USENIX Security Symposium (USENIX Security 24) 2024;(pp. 6131–47). https://www.usenix.org/system/files/usenixsecurity24-longo.pdf

11 Khan H, Khan H, Ghafoor S. Securing ADS-B Communications through a Novel Authentication Framework. Authorea Preprints. 2023. Available from: https://www.researchgate.net/publication/373507128_Securing_ADS-B_Communications_through_a_Novel_Authentication_Framework

12 Ahmed H, Khan H, Khan MA. A survey on security and privacy of automatic dependent surveillance-broadcast (ADS-B) protocol: Challenges, potential solutions and future directions. Authorea Preprints. 2023. Available from: https://www.researchgate.net/publication/371790695_A_Survey_on_Security_and_Privacy_of_Automatic_Dependent_Surveillance_-_Broadcast_ADS-B_Protocol_Challenges_Potential_Solutions_and_Future_Directions

13 Schultz M, Rosenow J, Olive X. Data-driven airport management enabled by operational milestones derived from ADS-B messages. J Air Trans Manag. 2022;99:102164. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0969699721001459

14 Ray G. ADS-B communication interference in air traffic management. Int J Aviat Aeronaut Aerosp. 2023;10(3):2. Available from: https://commons.erau.edu/cgi/viewcontent.cgi?article=1821&context=ijaaa

15 Ahmed W, Bhatti NA, Masood A, Alharbi AA, Alotaibi S. Advancements in ADS-B Security: A Comprehensive Survey of Vulnerabilities, Mitigation Strategies, System Requirements, and Emerging Research Trends. Available from: https://www.bing.com/ck/a?!&&p=feaeadf86eebd603be5d94fbc29a1e2c4f7b2001188e6f1dc1f2bfac1da9c4c6JmltdHM9MTczMzM1NjgwMA&ptn=3&ver=2&hsh=4&fclid=0be87a47-d984-6b05-1201-6e2fd8f36a7d&psq=Advancements+in+ADS-B+Security %3a+A+Comprehensive+Survey+of+Vulnerabilities%2c+Mitigation+Strategies %2c+System+Requirements %2c+and+Emerging+Research+Trends&u=a1aHR0cHM6Ly93d3cucm VzZWFyY2hnYXRlLm5ld C9wdWJsaWNhdGlvbi8zODIzMTk5MjBfQWR2YW5jZW1lbnRzX2luX0FEUy1CX1NlY3Vya XR5X0FfQ29tcHJlaGVuc2l2ZV9TdXJ2ZXlfb2ZfVnVsbm VyYWJpbGl0aWVzX01pd GlnYXRpb25fU3RyYXRlZ 2llc19TeXN0ZW1fUmVxdWlyZW1lbnRzX2FuZF9FbWVyZ2luZ19SZXNlYXJjaF9UcmVuZHM&ntb=1

16 Ruseno N, Lin CY, Chang SC. UAS traffic management communications: The legacy of ADS-B, new establishment of remote ID, or leverage of ADS-B-like systems? Drones. 2022;6(3):57. Available from: https://www.mdpi.com/2504-446X/6/3/57

17 Ruzeiny KM. Air Traffic Control (ATC) Resilient Response Model Amid Automatic Dependent Surveillance-Broadcast (ADS-B) Ghost Aircraft Spoofing Cyberattack. https://naist.repo.nii.ac.jp/record/2000107/files/R018618.pdf

18 Purton L, Abbass H, Alam S. Identification of ADS-B system vulnerabilities and threats. In Australian Transport Research Forum, Canberra 2010;(pp. 1–16). Available from: https://australasiantransportresearchforum.org.au/wp-content/uploads/2022/03/2010_Purton_Abbass_Alam.pdf

19 Kožović DV, Đurđević DŽ, Dinulović MR, Milić S, Rašuo BP. Air traffic modernization and control: ADS-B system implementation update 2022—A review. FME Transact. 2023;51(1). Available from: https://www.researchgate.net/profile/Sasa-Milic-2/publication/369143716_Dejan_V_Kozovic_Mirko_R_Dinulovic_Sasa_Milic_Air_Traffic_Mo dernization_and_Control_ADS-B_System_Implementation_Update_2022_-a_Review/links/640bbcd0315dfb4cce6efc9b/Dejan-V-Kozovic-Mirko-R-Dinulovic-Sasa-Milic-Air-Traffic-Modernization-and-Control-ADS-B-System-Implementation-Update-2022-a-Review.pdf

20 Al-Shareeda MA, Anbar M, Manickam S, Khalil A, Hasbullah IH. Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey. IEEE Access. 2021;9:121522–31. Available from: https://ieeexplore.ieee.org/abstract/document/9526558

21 Sonko S, Ibekwe KI, Ilojianya VI, Etukudoh EA, Fabuyide A. Quantum cryptography and US digital security: A comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security. Comput Sci IT Res J. 2024;5(2):390–414. Available from: https://www.fepbl.com/index.php/csitrj/article/view/790/984

22 Gobinathan B, Mukunthan MA, Surendran S, Somasundaram K, Moeed SA, Niranjan P, et al. A novel method to solve real-time security issues in software industry using advanced cryptographic techniques. Sci Program. 2021;2021(1):3611182. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1155/2021/3611182

23 Shaukat K, Luo S, Varadharajan V, Hameed IA, Xu M. A survey on machine learning techniques for cyber security in the last decade. IEEE Access. 2020;8:222310–54. Available from: https://ieeexplore.ieee.org/abstract/document/9277523

24 Hussain F, Hussain R, Hassan SA, Hossain E. Machine learning in IoT security: Current solutions and future challenges. IEEE Commun Surv Tutor. 2020;22(3):1686–721. Available from: https://www.researchgate.net/publication/340453998_Machine_Learning_in_IoT_Security_Current_Solutions_and_Future_Challenges

25 Mitev M, Chorti A, Poor HV, Fettweis GP. What physical layer security can do for 6G security. IEEE Open J Veh Technol. 2023;4:375–88. Available from: https://ieeexplore.ieee.org/abstract/document/10044975/

26 Mucchi L, Jayousi S, Caputo S, Panayirci E, Shahabuddin S, Bechtold J, et al. Physical-layer security in 6G networks. IEEE Open J Commun Soc. 2021;2:1901–14. Available from: https://ieeexplore.ieee.org/abstract/document/9509581

27 Sanenga A, Mapunda GA, Jacob TM, Marata L, Basutli B, Chuma JM. An overview of key technologies in physical layer security. Entropy. 2020;22(11):1261. Available from: https://www.mdpi.com/1099-4300/22/11/1261

28 Kožović DV, Đurđević DŽ. Spoofing in aviation: Security threats on GPS and ADS-B systems. Vojnotehnički glasnik/Mil Tech Cour. 2021;69(2):461–85. Available from: https://www.researchgate.

net/publication/350481235_Spoofing_in_aviation_Security_threats_on_GPS_and_ADS-B_systems
29 Budroweit J, Eichstaedt F, Delovski T. Aircraft surveillance from space: The future of air traffic control?: Space-based ADS-B, status, challenges and opportunities. IEEE Micro Mag. 2024;25(12):68–76. Available from: https://elib.dlr.de/207190/1/Aircraft_Surveillance_From_Space_The_Future_of_Air_Traffic_Control_Space-Based_ADS-B_Status_Challenges_and_Opportunities.pdf
30 Blåberg A, Lindahl G, Gurtov A, Josefsson B. Simulating ADS-B attacks in air traffic management. In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC) 2020;(Vol. 11, pp. 1–10). IEEE. Available from: https://liu.diva-portal.org/smash/get/diva2:1452531/FULLTEXT01.pdf
31 Lee SH, Kim YK, Han JW, Lee DG. Protection method for data communication between ADS-B sensor and next-generation air traffic control systems. Information. 2014;5(4):622. Available from: https://www.mdpi.com/2078-2489/5/4/622
32 Tahsien SM, Karimipour H, Spachos P. Machine learning based solutions for the security of Internet of Things (IoT): A survey. J Net Comput Appl. 2020;161:102630. https://www.sciencedirect.com/science/article/abs/pii/S1084804520301041