PREMIER JOURNAL OF COMPUTER SCIENCE REVIEW

State-of-the-Art Security Measures for ADS-B Analyzing Current Protocols and Future Directions

Waqas Ahmed, PhD

Air University, 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. State-of-the-Art Security Measures for ADS-B Analyzing Current Protocols and Future Directions. Premier Journal of Computer Science 2024;1:100005

DOI: https://doi.org/10.70389/PJCS.100005

Received: 7 December 2024
Revised: 16 December 2024
Accepted: 19 December 2024
Published: 30 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

ABSTRACT

ADS-B offers aircraft situational awareness and real-time tracking. Despite its operational advantages, its absence of built-in security measures leaves it open to injection, jamming, and spoofing assaults, endangering privacy and safety. This article examines the weaknesses present in ADS-B systems and evaluates the most recent security solutions, such as machine learning, cryptography, and physical-layer security. A comparative study highlights the advantages, disadvantages, and trade-offs of various strategies in terms of cost, latency, and scalability. New technologies like explainable AI, blockchain, and quantum cryptography are emphasized as possible ways to get beyond current protocol restrictions. The result calls for lightweight cryptographic protocols to be integrated with advanced anomaly detection models and regulatory collaboration to strengthen ADS-B.

Keywords: ADS-B vulnerabilities, Aviation cybersecurity, Spoofing attacks, Cryptographic protocols, Machine learning security

Introduction

ADS-B has changed the world of the aviation industry. It remains the basis for the current forms of air traffic management: accurate and real-time aircraft tracking to enhance safety and efficiency in global airspace. Compared to traditional radar systems, it depends on satellite navigation and onboard broadcasting systems that can communicate flight data to air traffic controllers and other aircraft.[1]

Significance of ADS-B in Modern Air Traffic Management

Traditional radar systems used in air traffic control have been phased out by ADS-B, which has replaced them with a more precise and effective aircraft tracking technology. It does this by broadcasting key flight data, including position, altitude, and speed, to ground stations and other nearby aircraft. This real-time exchange of data improves pilots' and air traffic controllers' situational awareness, minimizing the risk of collisions.[1,2] In addition, ADS-B enables fuel-saving routes and optimal routes that reduce environmental effects as well as operational expenses. Federal Aviation Administration studies indicate a 12% increase in efficiency on any route for planes equipped with ADS-B flying in the airspace within the United States.[3]

Overview of Vulnerabilities and Security Challenges

The transparency that gives effectiveness to ADS-B to enhance situational awareness brings many cyber threats upon itself.[4] The main weakness of ADS-B is that it is a completely unencrypted communication through which flight data is sent into open space in plaintext. It would, therefore, allow someone ill-intentioned to intercept that and extract sensitive information, for instance, an aircraft's location, heading, or even altitude. There is also no authentication protocol in the ADS-B messages, hence making the system vulnerable to spoofing attacks, which include injecting fake messages into the air traffic controllers or pilots in order to deceive them. The attacks may create phantom aircraft or manipulate real flight data, thus causing operational chaos. The other major vulnerability identified is susceptibility to jamming. The ADS-B makes use of radio frequency communications, which can be deliberately interfered with. Jamming might lose the ADS-B signals that give both controllers and pilots much-sought situational awareness, while message injection attacks raise even higher risks due to their capability to inject malicious messages into a flight, disrupting normal flight operations.[5]

Research Objectives and Scope

a) Examine the architecture, operational benefits, and inherent vulnerabilities of ADS-B in modern air traffic management.
b) Provide an in-depth evaluation of cryptographic methods, machine learning techniques, and other advanced solutions implemented to address ADS-B security challenges.
c) Identify key threats, including spoofing, jamming, and message injection, and their impact on aviation safety and privacy.
d) Compare current solutions based on performance metrics like scalability, latency, accuracy, and computational efficiency.
e) Highlight emerging technologies such as blockchain, quantum cryptography, and explainable AI for developing robust and scalable security frameworks.

ADS-B System Overview

Functional Architecture and Working Principles

The fundamental components of the ADS-B system include Aircraft Transponders, Ground Stations, and Air Traffic Management Systems. Aircraft equipped with ADS-B Out broadcast key flight parameters such as position, altitude, velocity, and identification over radio frequencies. These broadcasts are received by ADS-B ground stations and other aircraft with ADS-B In capabilities, allowing for real-time tracking and collision avoidance.[6] Figure 1 below illustrates the functional workflow of ADS-B.

The data exchange in ADS-B systems is through two frequency bands: 1,090 MHz ES (Extended Squitter)

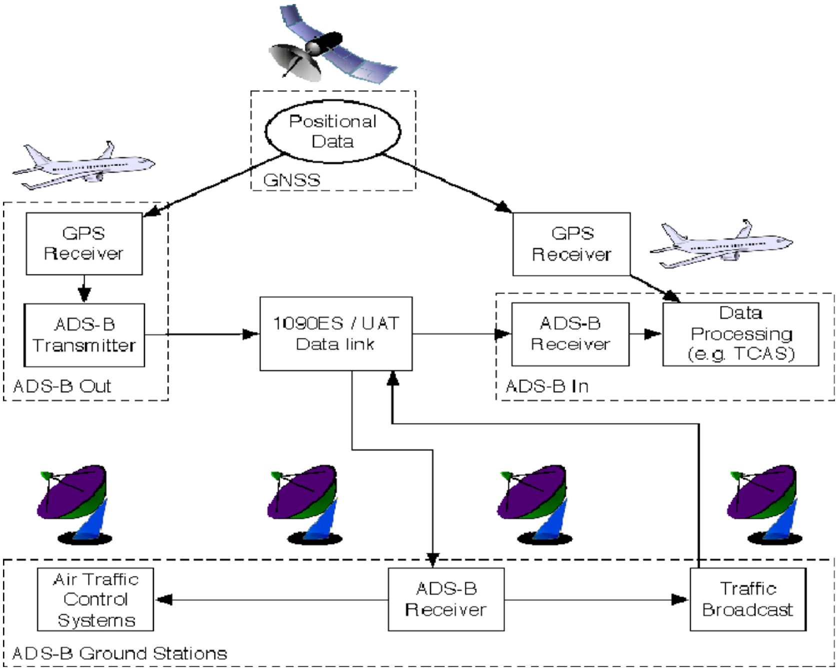

Fig 1 | Working architecture of ADS-B[7]

Table 1 | Security standards and limitations in ADS-B systems

Feature	Current Standard	Limitation
Encryption	None	Exposes data to interception and analysis.
Authentication	None	Enables spoofing and injection of false messages.
Signal Integrity Checks	Basic Error Checking (CRC)	Insufficient for mitigating malicious attacks.
RF Signal Protection	Open Broadcast	Prone to jamming and interference.

and 978 MHz UAT (Universal Access Transceiver). The 1,090 MHz frequency is used worldwide for high-altitude flights, and 978 MHz is mainly used in the United States for general aviation below 18,000 feet.[8] ADS-B expands the message elements of Mode S to include data about the aircraft and its location. This extended squitter is called 1090ES. An international technical advisory committee selected 1090ES as the worldwide standard for ADS-B.

The ground networks have been systematically upgraded and deployed.[9] UAT is approved for use at altitudes below 18,000 feet. UAT provides free graphical weather and traffic information to ADS-B In-equipped aircraft. It does not supersede the requirement for transponders. The rest of the world intends to use the 1,090 MHz link for ADS-B.[10]

Current Security Standards and Limitations

The current standards of ADS-B focus more on operational efficiency and interoperability, as determined by the International Civil Aviation Organization (ICAO) and other bodies regulating aviation. However, these standards do not have strong security mechanisms within them, which would open the system to abuse. Situational awareness is enhanced, and infrastructure cost is reduced with the use of ADS-B protocol; however, encryption and authentication are not part of this system.[11] The ICAO emphasizes in its ADS-B standards, worldwide interoperability, such that any aircraft system will always seamlessly communicate with the different regions' air traffic management systems.[12] This has facilitated widespread adoption, however; it has also increased vulnerabilities in the system because this open nature of the communication of ADS-B naturally does not align with what needs to be done and guaranteed in secure and private data exchange (Table 1).

Operational Benefits vs. Vulnerabilities

Operational Benefits: Increased Situational Awareness: ADS-B offers real-time, accurate information on aircraft locations, altitude, and speed, to both air traffic controllers and pilots. The potential for mid-air collision is greatly reduced, and there is better coordination during takeoffs, landings, and en route operations.[13]

Enhanced Operational Performance: The accuracy and timeliness of ADS-B data enable the optimal planning of routes, thus reducing flight times and fuel consumption. ADS-B eliminates reliance on radar systems, making airspace more efficient, especially in congested or remote regions where radar coverage is limited.[13]

Cost-Effectiveness: Unlike traditional radar infrastructure, with its high investment and maintenance needs, ADS-B operates at relatively low cost by using satellite navigation as well as off-the-shelf receivers. Both industrialized and emerging regions' air traffic management systems that desire modernization would find this to be a workable answer.[14]

Global Interoperability: ADS-B facilitates cordial communication between international skies while adhering to ICAO regulations to guarantee uniformity across borders. This indicates that maintaining uniform air traffic control procedures and overseeing cross-country flights depend heavily on interoperability.[15]

Operational Vulnerabilities: Spoofing Vulnerability: Because ADS-B lacks message authentication, it is simple for attackers to insert fictitious data, generating phantom aircraft or altering the locations of actual ones. Air traffic controllers and pilots may become confused by spoofing assaults, which could result in delays, rerouting, or even collisions.[16]

Risks to Privacy: Anybody with a compatible receiver can access sensitive flight information through the unencrypted broadcast of ADS-B data. Military and VIP flights, which often require discretion, are particularly vulnerable to tracking and surveillance by adversaries or malicious entities.[16]

Jamming Threats: Being an RF-based system, ADS-B has an enormous vulnerability to jamming. In fact, any sort of jamming may jeopardize communication and even compromise situational awareness. This may pose more risk in areas having significant interference with RF or in conflict regions, as there might be deliberate jamming.[17]

Table 2 | Key security vulnerabilities in ADS-B systems

Vulnerability	Description	Impact
Lack of Encryption	Unencrypted messages expose sensitive data.	Compromises aircraft privacy.
No Message Authentication	False messages cannot be identified.	Enables spoofing and data manipulation.
Susceptibility to Jamming	RF communication is easily disrupted.	Leads to a loss of situational awareness.
Message Injection	Unauthorized data insertion disrupts ATM.	Causes safety and operational risks.

Table 3 | Operational benefits and vulnerabilities

Aspect	Operational Benefit	Operational Vulnerability
Situational Awareness	Real-time, accurate data improves safety.	Spoofing attacks can introduce false or misleading data.
Efficiency	Optimized routing reduces fuel and time costs.	Jamming can disrupt operations, negating efficiency gains.
Cost-Effectiveness	Low infrastructure costs compared to radar.	Adding security measures increases implementation costs.
Interoperability	Seamless global communication in aviation.	Open design compromises security and privacy.

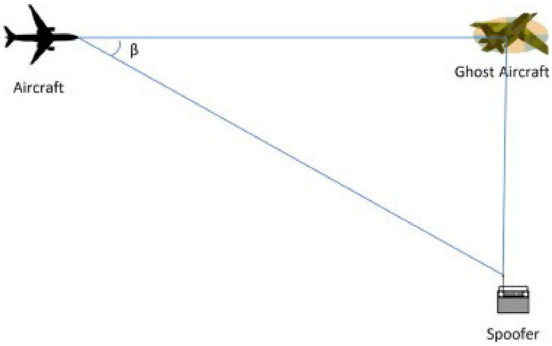

Fig 2 | Spoofing and jamming in ADS-B[20]

Table 2 below outlines the key operational benefits and vulnerabilities of ADS-B systems (Table 3):

Threats and Risks to ADS-B Communication

Classification of Threats: Spoofing, Jamming, Injection Attacks, etc.

Spoofing: Spoofing refers to an attack wherein adversaries transmit false ADS-B messages for the purpose of deceiving air traffic controllers or onboard systems.[18] In this type of attack, fake "ghost" aircraft can be created, legitimate aircraft's locations can be obscured, and radar displays can become confusing. High-traffic airspace is more dangerous with spoofing because a collision or rerouting could easily happen because of false data.[15,20]

Jamming: Jamming refers to the deliberate interference with the radio frequencies of ADS-B. Such an attack may interfere with the transmission of vital data, leading to disruptions in air traffic management (Figure 2).[19]

Message Injection Attacks: In message injection attacks, an attacker inserts false data into ADS-B transmissions in order to manipulate flight paths or create erroneous situational awareness. In contrast to spoofing, injection attacks focus on corrupting the data flow rather than creating phantom aircraft, resulting in operational inefficiencies and safety risks (Figure 3).[4]

Replay Attacks: Replay attacks represent intercepting and retransmitting legitimate ADS-B messages sometime later. Such an attack can easily mislead air traffic control through the presentation of the outdated positions of aircraft and confusing navigational mistakes (Table 4; Figure 4).[21]

Table 5 shows the ADS-B threats and its corresponding security measures:

Risks to Aviation Safety, Privacy, and Reliability

The most significant implication of ADS-B threats is on aviation safety. Spoofing or injection attacks can create false flight paths and mislead pilots and controllers, increasing the risk of mid-air collisions or runway incursions.[14] Jamming disrupts communication entirely, making reliance on backup systems a necessity that may not even provide the same level of accuracy. The open broadcast nature of ADS-B allows anyone with the right equipment to intercept and track aircraft in real time. This poses significant privacy risks, especially for sensitive flights involving military operations, VIPs, or corporate executives. Air traffic management system reliability is affected if the ADS-B message gets interfered or spoofed. In the case of replay and man-in-the-middle attacks, inconsistency in flight data causes delay, rerouting, or even a shutdown of an airspace management system.[22]

Phantom Aircraft in Europe: A Case of ADS-B Spoofing

The phantom aircraft were created by transmitting false ADS-B messages that used legitimate aircraft data. These false signals were then received by the ground-based ADS-B receivers, which interpreted and exhibited this as a real aircraft. The above scenario was possible because ADS-B broadcasts are transmitted in plaintext with no built-in authentication mechanisms to establish the legitimacy of the messages. This spoofed aircraft was usually spotted in high-traffic airspaces, making the task for air traffic controllers a little more complicated. At times, controllers had to

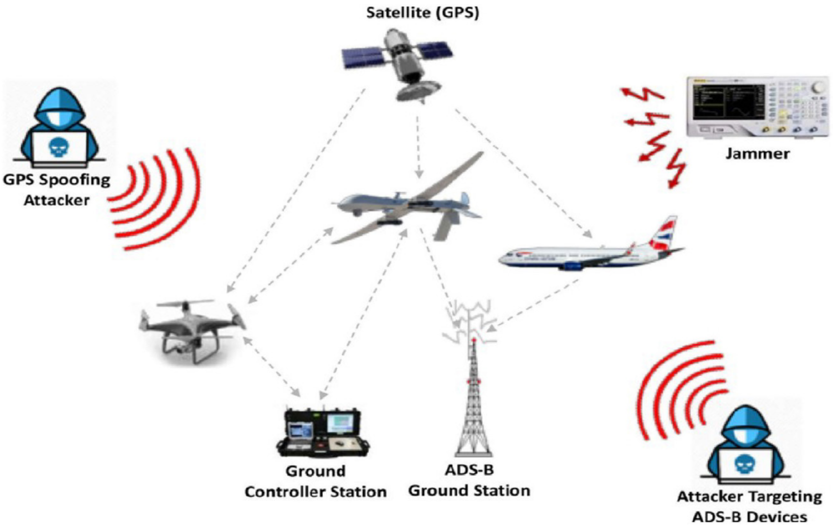

Fig 3 | Message injection attack[4]

Table 4 | Threats and impacts		
Threat Type	**Mechanism**	**Impact on Aviation**
Spoofing	False message creation	Phantom aircraft, collision risks, confusion in airspace.
Jamming	RF signal interference	Loss of communication, situational awareness disruptions.
Message Injection	False data insertion	Erroneous flight paths, inefficiencies, safety risks.
Replay Attacks	Reuse of intercepted data	Confusion from outdated or duplicated messages.

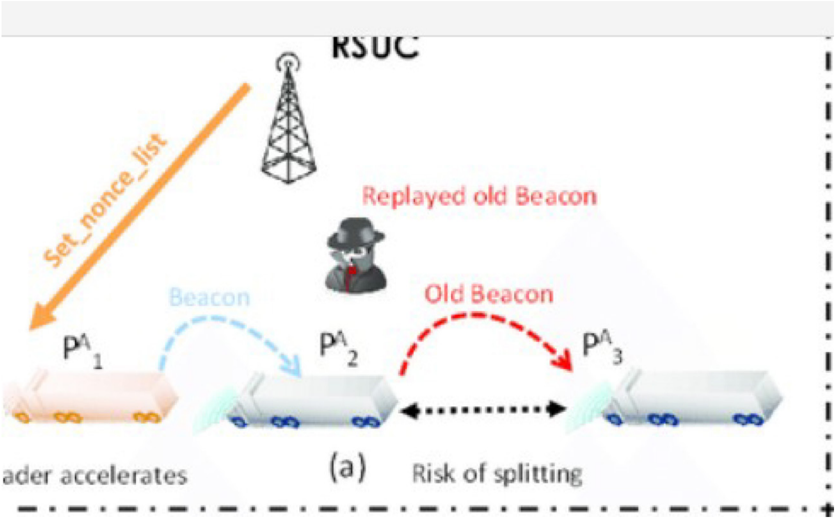

Fig 4 | Replay attacks[21]

Table 5 | ADS-B threats and corresponding security measures		
Threat	**Proposed Solution**	**Implementation Feasibility**
Spoofing	Digital Signatures, ML Models	High
Jamming	Signal Authentication	Moderate
Injection Attacks	Lightweight Cryptography	High
Privacy Risks	Blockchain	Moderate

reroute genuine flights just to avoid collisions with such nonexistent aircraft, causing undue delay and disruptions.[23]

Post-incident investigations found that these spoofing attacks could be implemented with fairly inexpensive, commercially available equipment. This means of access to attack tools revealed how easily ADS-B vulnerabilities could be exploited by malicious actors, such as hobbyists, cybercriminals, or even entities with bad intent.[24]

State-of-the-Art Security Measures

As the vulnerabilities in ADS-B systems have become better known, several advanced security methods have been proposed to ward off the potential threats that may arise.

Cryptographic Solutions

Symmetric and Asymmetric Encryption

Encryption is key to securing ADS-B communications. Here, symmetric encryption uses the same key for encryption as well as decryption, and asymmetric encryption uses a pair of public and private keys. Symmetric encryption algorithms, such as AES, offer high efficiency in terms of speed and computational resources, which makes them very suitable for real-time applications like ADS-B. AES supports processing 10,000 messages per second with a latency as low as 5 ms per message, evidencing its scalability in high-volume environments, but symmetric encryption has the flaw of difficulty in keying distribution and management.[25]

Asymmetric encryption, for example, RSA, can be useful when symmetric encryption is not able to solve the problem of key distribution and management. The public key infrastructure makes possible secure communication in asymmetric encryption, allowing data integrity during transmission and sender identity verification.[26] Digital signatures along with public-key cryptography is probably one of the most promising cryptographic methods for ADS-B, allowing ADS-B message authentication and preventing spoofing attacks.[27] By stopping attempts at spoofing, asymmetric encryption ensures only authentic airplanes broadcast accurate data.

Lightweight Encryption Protocols

Aviation systems have limited bandwidth and processing capacity. Thus, lightweight encryption techniques are needed. These protocols are designed to be as secure as possible without being too slow for real-time communication. Because they can provide strong encryption with less computational and bandwidth overhead than more traditional techniques like RSA, lightweight algorithms such as ECC are becoming increasingly popular.[28] ECC promises well in ADS-B data settings with high volume and low latency when conventional encryption methods may not be effective.

Machine Learning Approaches

Anomaly Detection and Predictive Models

An excellent method for finding strange behavior within the ADS-B data which would identify possible security threats is using machine learning. Anomaly detection models detect ordinary communication patterns and recognize anomalous signals that may indicate a potential jamming, spoofing, or other kinds of attack.[29] By training the algorithms using past ADS-B data, anomalies in the characteristics of aircraft velocity, trajectory, and altitude can be detected as probable threats. Using supervised learning to detect spoofing attempts in ADS-B messages achieved a 95% accuracy rate with a false-positive rate of 2%.[30] Predictive models can be applied to foresee aircraft movements and identify instances where the incoming ADS-B data does not follow the expected pattern. These models also rely on time series analysis and regression approaches.[31]

Supervised and Unsupervised Learning Technique

Supervised learning methods are particularly effective for security applications in ADS-B, where models are trained using labeled datasets. Such datasets contain instances of normal and abnormal data. Using techniques such as random forests and SVM, communications of ADS-B can be classified as either legitimate or suspect.[32] When no labeled data is available, unsupervised learning methods like density estimation and clustering perform well. Clustering algorithms identified previously unseen attack patterns with a 90% success rate in an experimental dataset of anomalous ADS-B messages.[33] These algorithms can successfully detect attack patterns that were previously unknown by grouping signals that exhibit similar patterns or outliers.[34] A viable solution for real-time security monitoring of ADS-B systems may be achieved by combining supervised and unsupervised learning techniques.

Physical-Layer Security

Authentication and Fingerprinting

By protecting the actual transmission medium, the physical-layer security technique makes sure that ADS-B signals are genuine and impenetrable. Signal authentication allows receivers to verify the signal's origin by adding unique identities or cryptographic keys into the physical layer of communication.[35] Signal fingerprinting, which identifies a unique characteristic of each transmitter derived from the signal's signature, successfully identified spoofed ADS-B signals in 98% of test scenarios with minimal false positives.[36]

Challenges in Practical Implementation

Although promising, the physical-layer security approach has several challenges with its implementation in real ADS-B systems. For one, fingerprinting of signal requires quite sensitive equipment in capturing and analyzing unique aspects of signals transmitted. Therefore, not all air traffic management systems may be accessible to this kind of setup.[37] Second, integration with existing ADS-B infrastructure will have huge costs and may demand system upgrades of legacy systems that can be difficult to implement, in terms of both feasibility and regulatory approval.[38]

Comparative Analysis

Performance Evaluation of Different Security Measures

In evaluating the performance of different security measures proposed for ADS-B, there are several key metrics at play: security, efficiency, scalability, and ease of integration into existing systems. Cryptographic solutions, such as symmetric encryption and digital signatures, offer robust security by preventing unauthorized access and spoofing.[39] However, they incur latency due to computational overheads, especially asymmetric encryption methods like RSA and ECC, which take a considerable amount of processing time for key generation and verification. Anomaly detection and supervised learning algorithms-based approaches are promising for ML-based identification of potential threats and deviations from normal operating patterns.

Strengths, Weaknesses, and Applicability of Each Approach

Cryptographic Solutions

Cryptographic methods, especially asymmetric encryption, ensure message authenticity and confidentiality, providing strong security against spoofing and message injection attacks. The computational burden can introduce latency in such solutions, particularly in low-processing-power and low-bandwidth environments such as those found in aviation systems.[40] Applications for cryptographic solutions include high-security air traffic management systems and commercial aviation communications, where security is crucial and computational cost can be weighed against the necessity for strong protection.[41]

Machine Learning Approaches

Because of their great flexibility and adaptability, ML-based anomaly detection systems are able to identify new patterns that have never been seen before. With them, real-time threat detection is also possible, and the overhead is minimal. The performance of an ML model is very much dependent on the dataset being used. Poor model performance and false positives could arise from inadequate training data.[32] These techniques are very applicable in dynamic environments such as air traffic control, where the monitoring is constant and requires real-time responses to threats that are dynamically changing. They are very useful when detecting advanced or new forms of attack vectors.[34]

Physical-Layer Security

Physical-layer security provides another layer of protection by utilizing the inherent characteristics of the transmission medium to prevent spoofing or injecting malicious signals undetected.[38] Implementing physical-layer security calls for specialized gear and a lot of resources. When aircraft are located far from ground stations or in severely interfering conditions, fingerprinting and authentication might not be feasible.[38] This approach is applied in areas where high-level security is required, with the extra costs and complications being worthwhile.

Trade-Offs in Terms of Scalability, Latency, and Cost

Each security mechanism has its drawbacks in scalability, latency, and costs. Scalability is particularly a concern while implementing such security mechanisms on ADS-B systems, which are always increasing with more aircraft spread across the world. It is difficult to scale with cryptographic methods while maintaining acceptable security because such methods require computationally expensive means for large quantities of aircraft.[42] While scalable, these machine learning models will likely need extensive retraining given newly developed attack patterns, and the requirement for significant datasets may also limit scalability.[35]

Latency is another critical parameter in ADS-B systems because delays in message transmission affect situational awareness and safety. Cryptographic methods, such as asymmetric encryption, incur latency in the processing time for key management and message verification.[43] Machine-learning-based anomaly detection can be very efficient but still incur latency in processing large datasets in real time. Physical-layer security techniques may incur delays during signal authentication processes, but their impact on overall latency is generally lower than that of cryptographic methods.[38]

Cost is always a concern when deploying security measures in large-scale systems. Cryptographic solutions, particularly those based on asymmetric encryption, may require significant computational resources and infrastructure, raising both initial and ongoing costs.[43] Machine learning models also require a significant investment in data collection, model training, and infrastructure, though their long-term costs can be lower as they scale with automated updates and learning.[34] Physical-layer security approaches, while highly secure, often require specialized hardware and signal processing equipment, which increases both initial and operational costs.[38]

Challenges and Gaps

Limitations of Existing Protocols and Solutions

Current security solutions for ADS-B still face some limitations despite the improvements made. In the original ADS-B design, there is no message authentication, which leaves the system vulnerable to spoofing and jamming. It is also dependent on the use of cryptographic protocols that might not be able to deal with all types of cyberattacks, especially in limited computational resource environments.

Barriers to Real-World Implementation in Aviation Systems

Advanced security measures in real-world aviation systems are difficult to implement. The most important hurdles have been related to cost, most of which is in relation to the security mechanism—including advanced encryption and physically layered security technologies—which calls for a highly up-to-date infrastructure.[14] With specific reference to developing regions, which most of Africa would consider, it might not afford upgrading this equipment which poses possible cybersecurity vulnerability. According to a report from ICAO, the total investments, over $1 billion globally, would be needed across all regions for modernized ADS-B security standardizations.[44]

Another significant hurdle is backward compatibility. Many legacy ADS-B systems do not have hardware and software in place to support modern security technologies, including digital signatures or blockchain-based authentication, without major redesigns. In some places, due to the lack of well-defined international standards for aviation cybersecurity, it has taken time to integrate lightweight cryptographic protocols into existing systems.[27]

Compatibility Issues with Legacy Systems

Since many historical ADS-B systems were not created with security in mind, they might not support contemporary security protocols like machine-learning-based anomaly detection or digital signatures.[45] This makes maintaining the safety of the entire aviation network extremely difficult, particularly when new security measures are implemented without interfering with ongoing operations.

Conclusion

Summary of Findings from the Review

According to the analysis, ADS-B has transformed air traffic control by increasing situational awareness and operational effectiveness, but it is vulnerable to serious threats such as message insertion, jamming, and spoofing. Existing technologies provide useful protection, including physical-layer security measures, machine-learning-based anomaly detection, and cryptographic protocols. However, scalability, latency, expense, and compatibility with existing systems are all drawbacks of these approaches. High security is provided by the cryptographic method, although computational overheads are incurred. Large training datasets are essential to the machine learning approach's effectiveness in real-time threat identification. Even though physical-layer security provides a layer of protection, it is resource-intensive and impractical to implement in real life.

Improvement Recommendations for ADS-B Security

- Enhance Integration of Cryptography: A lightweight cryptographic algorithm should be employed in multitudes; this would include the employment of elliptic curve cryptography to ensure that both aspects are balanced.

- Improve Machine Learning Models: Anomaly detection should be enhanced through the training of robust supervised and unsupervised machine learning models with diverse, high-quality datasets. Further enhancement of the transparency and trustworthiness of these systems can be achieved using explainable AI.
- Hybrid Conceptual Framework: A hybrid conceptual framework combining cryptographic techniques, machine learning models, and blockchain technology is proposed.
    - Cryptographic Layer: Lightweight algorithms such as ECC for secure and efficient data encryption and authentication.
    - Machine Learning Layer: Supervised and unsupervised anomaly detection models enhanced by explainable AI for real-time identification of threats.
    - Blockchain Layer: Decentralized, tamper-proof data verification and transaction logging for security and data integrity and accountability.

Final Remarks

The safety and effectiveness of contemporary air traffic control depend heavily on the integrity and dependability of ADS-B systems. The dangerous landscape is constantly changing as the aviation sector depends more and more on digital communication systems. To proactively address these difficulties, it is necessary to strike a balance between operational limitations, cost considerations, and technology improvements. In addition to being an operational requirement, creating and putting into place strong, scalable, and affordable security procedures are a critical first step in safeguarding aviation's future.

References

1 Wu Z, Shang T, Guo A. Security issues in automatic dependent surveillance - broadcast (ADS-B): a survey. IEEE Access. 2020;8:122147–67. https://doi.org/10.1109/ACCESS.2020.3007182

2 Zhang X, Zhang J, Wu S, Cheng Q, Zhu R. Aircraft monitoring by the fusion of satellite and ground ADS-B data. Acta Astronautica. 2018;143:398–405. https://doi.org/10.1016/j.actaastro.2017.11.026

3 Airspace Federal Aviation Administration. Faa.gov. 2022. https://www.faa.gov/air_traffic/technology/equipadsb/research/airspace

4 Ahmed W, Bhatti NA, Masood A, Alharbi AAK, Alotaibi S. Advancements in ADS-B security: A comprehensive survey of vulnerabilities, mitigation strategies, system requirements, and emerging research trends. 2024. https://doi.org/10.20944/preprints202405.0586.v1

5 Abu Al-Haija Q, Al-Tamimi A. Secure aviation control through a streamlined ADS-B perception system. Appl Syst Innov. 2024;7(2):27. https://doi.org/10.3390/asi7020027

6 Ali BS, Ochieng WY, Schuster W, Majumdar A, Chiew TK. A safety assessment framework for the Automatic Dependent Surveillance Broadcast (ADS-B) system. Saf Sci. 2015;78:91–100. https://doi.org/10.1016/j.ssci.2015.04.011

7 Strohmeier M. Security in next generation air traffic communication networks. 2016. https://www.researchgate.net/publication/313376223_Security_in_Next_Generation_Air_Traffic_Communication_Networks

8 Cessna. ADS-B Out Explained. txtav.com. 2024. https://txtav.com/en/journey/articles/articles/adsb-out-explained

9 FAA. Ins and Outs Federal Aviation Administration. Faa.gov. 2016. https://www.faa.gov/air_traffic/technology/equipadsb/capabilities/ins_outs

10 Skybrary. Automatic Dependent Surveillance Broadcast (ADS-B). SKYbrary Aviation Safety. 2021. https://skybrary.aero/articles/automatic-dependent-surveillance-broadcast-ads-b

11 Amin S, Clark T, Offutt R, Serenko K. Design of a cyber security framework for ADS-B based surveillance systems. In 2014 Systems and Information Engineering Design Symposium (SIEDS) 2014;(pp. 304–9). IEEE. https://doi.org/10.1109/sieds.2014.6829910

12 ICAO, Automatic Dependent Surveillance -Broadcast (ADS-B) Implementation and Regulation Meeting for the NAM/CAR/SAM Regions ADS-B/LEG Final Summary of Discussions. 2018. Available from: https://www.icao.int/NACC/Documents/Meetings/2018/ADSB/ADS-B-LEG-FinalSummaryofDiscussions.pdf

13 Federal Aviation Administration. Automatic Dependent Surveillance - Broadcast (ADS-B). Federal Aviation Administration. Faa.gov. 2022. https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs/afs400/afs410/ads-b

14 Manesh MR, Kaabouch N. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. Int J Crit Infrastruct Prot. 2017;19:16–31. https://doi.org/10.1016/j.ijcip.2017.10.002

15 Strohmeier M, Lenders V, Martinovic I. On the security of the automatic dependent surveillance-broadcast protocol. IEEE Commun Surv Tutor. 2014;17:1066–87. Available from: https://www.researchgate.net/publication/305720556_On_the_Security_of_the_Automatic_Dependent_Surveillance-Broadcast_Protocol

16 Kim Y, Jo J-Y, Lee S. ADS-B vulnerabilities and a security solution with a timestamp. IEEE Aerosp Electron Syst Mag. 2017;32(11):52–61. https://doi.org/10.1109/MAES.2018.160234

17 CISA. Radio Frequency Interference Best Practices Guidebook. CISA. 2020. Available from: https://www.cisa.gov/sites/default/files/publications/SAFECOM-NCSWIC%20RF%20Interference%20Best%20Practices%20Guidebook_3.16.20%20-%20FINAL%20%28508c%29.pdf

18 Fried A, Last M. Facing airborne attacks on ADS-B data with autoencoders. Comput Secur. 2021;109:102405. https://doi.org/10.1016/j.cose.2021.102405

19 Sciancalepore S, Alhazbi S, Pietro RD. Reliability of ADS-B communications. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing 2019; Association for Computing Machinery. https://doi.org/10.1145/3297280.3297518

20 Rudys S, Aleksandravicius J, Aleksiejunas R, Konovaltsev A, Zhu C, Greda L. Physical layer protection for ADS-B against spoofing and jamming. Int J Crit Infrastruct Prot. 2022;38:100555. https://doi.org/10.1016/j.ijcip.2022.100555

21 Di Maio A, Palattella MR, Soua R, Lamorte L, Vilajosana X, Alonso-Zarate J, et al. Enabling SDN in VANETs: What is the impact on security? Sensors. 2016;16(12):2077. https://doi.org/10.3390/s16122077

22 Ronen R. Ben-Moshe B. Cyberattackson flight safety: detection and mitigation using LoRa. Sensors. 2021;21(13):4610. https://doi.org/10.3390/s21134610

23 Zaidi D. ATSEP Use Cases: Impact of False Targets on Air Traffic Control. www.skyradar.com. 2023. https://www.skyradar.com/blog/atsep-use-cases-impact-of-false- targets-on-air-traffic-control

24 ICAO. ADS-B SITF/15 -IP/15 Agenda Item 4 14/04/16 Agenda Item 4: Review States' activities and interregional issues on implementation of ADS-B and multilateration ADS-B FAILURES IN CERTAIN A330 AIRCRAFT. 2023. Available from: https://www.icao.int/APAC/Meetings/2016%20ADSB%20SITF15/IP15_AUS%20AI.4%20-%20ADS-B%20failure%20in%20A330.pdf

25 Khan H, Khan H, Ghafoor S. Securing ADS-B Communications through a Novel Authentication Framework. 2023. https://doi.org/10.36227/techrxiv.24043494

26 Al-Shabi MA. A survey on symmetric and asymmetric cryptography algorithms in information security. Int J Sci Res Publ (IJSRP). 2019;9(3):8779. https://doi.org/10.29322/ijsrp.9.03.2019.p8779

27 Ukwandu E, Amine Ben Farah M M, Hindy H, Bures M, Atkinson R, Tachtatzis C, et al. Cyber-security challenges in aviation

industry: A review of current and future trends, NASA ADS. 2021. Accessed Sep 13, 2023. https://ui.adsabs.harvard.edu/abs/2021arXiv210704910U/abstract

28 Shamala LM, Zayaraz G, Vivekanandan K, Vijayalakshmi V. Lightweight cryptography algorithms for internet of things enabled networks: An overview. J Phys Conf Ser. 2021;1717:012072. https://doi.org/10.1088/1742-6596/1717/1/012072

29 Lok LK, Hameed VA, Rana ME. Hybrid machine learning approach for anomaly detection. Indones J Electr Eng Comput Sci. 2022;27(2):1016–24. https://doi.org/10.11591/ijeecs.v27.i2.pp1016-1024

30 Ying X, Mazer J, Bernieri G, Conti M, Bushnell L, Poovendran R. Detecting ADS-B spoofing attacks using deep neural networks. 2019 IEEE Conference on Communications and Network Security (CNS) 2019;(pp. 187–95). IEEE. Accessed Apr 12, 2022. https://ieeexplore.ieee.org/document/8802732

31 Taşdelen O, Çarkacioglu L, Töreyin BU. Anomaly Detection on ADS-B Flight Data Using Machine Learning Techniques. In Lecture Notes in Computer Science. 2021;(pp. 771–83). Springer. doi: https://doi.org/10.1007/978-3-030-88081-1_58

32 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. https://doi.org/10.1109/access.2020.3041951

33 Kamarudin MH, Maple C, Watson T, Safa NS. A new unified intrusion anomaly detection in identifying unseen web attacks. Secur Commun Netw. 2017;2017:1–18. https://doi.org/10.1155/2017/2539034

34 Kaliyaperumal P, Periyasamy S, Thirumalaisamy M, Balusamy B, Benedetto F. A novel hybrid unsupervised learning approach for enhanced cybersecurity in the IoT. Future Internet. 2024;16(7):253. https://doi.org/10.3390/fi16070253

35 Prakash P, Abdelhadi A, Pan M. Secure authentication of ADS-B aircraft communications using retroactive key publication. arXiv (Cornell University). 2019. https://doi.org/10.48550/arxiv.1907.04909.

36 Rzemyk TJ. Chapter 10 - Biometrics in the criminal justice system and society today. In Fennelly LJ, ed. Effective Physical Security 2017;(5th ed., pp. 249–54). Butterworth-Heinemann. https://www.sciencedirect.com/science/article/abs/pii/B9780128044629000105

37 Strohmeier M, Schafer M, Lenders V, Martinovic I. Realities and challenges of nextgen air traffic management: the case of ADS-B. IEEE Commun Mag. 2014;52(5): 111–8. https://doi.org/10.1109/mcom.2014.6815901

38 Cepheli Ö, Kurt GK. Physical layer security in wireless communication networks. In Advances in Information Security, Privacy, and Ethics Book Series 2013;(pp. 61–81). IGI Global. https://doi.org/10.4018/978-1-4666-4691-9.ch004

39 Dawood M, Tu S, Xiao C, Alasmary H, Waqas M, Rehman SU. Cyberattacks and security of cloud computing: a complete guideline. Symmetry. 2023;15(11):1–33. https://doi.org/10.3390/sym15111981

40 Hassan N, Aazam M, Tahir M, Yau K-LA. Floating fog: extending fog computing to vast waters for aerial users. Cluster Comput. 2022;26:181–95. https://doi.org/10.1007/s10586-022-03567-6

41 Yang H, Zhou Q, Yao M, Lu R, Li H, Zhang X. A practical and compatible cryptographic solution to ADS-B security. IEEE Internet Things J. 2018;6:3322–4. https://doi.org/10.1109/jiot.2018.2882633

42 Markani JH, Amrhar A, Gagné J-M, Landry RJ. Security establishment in ADS-B by format-preserving encryption and blockchain schemes. Appl Sci. 2023;13(5):3105. https://doi.org/10.3390/app13053105

43 Pouyan A, Parham M. Performance-analysis-of-cryptography-methods-for-secure. 2023;5(2). Available from: https://www.researchgate.net/publication/373649405_Performance-Analysis-of-Cryptography-Methods-for-Secure

44 ICAO. Whereas the future development of international. Accessed Dec 14, 2024. [Online]. Available from: https://www.icao.int/publications/Documents/9921_en.pdf

45 Kocaaga E, Kulekci MO. Security analysis on the ADS-B technology. 2022 30th Signal Processing and Communications Applications Conference (SIU) 2017;(pp. 1–4). https://doi.org/10.1109/siu.2017.7960506