Securing ADS-B Communication: A Survey of Cryptographic and Machine Learning Approaches

Waqas Ahmed, PhD

ABSTRACT

Automatic Dependent Surveillance-Broadcast (ADS-B) is fundamental to modern aviation, providing real-time aircraft tracking and improving air traffic management. It is susceptible to threats such as spoofing, jamming, and eavesdropping, as well as threatening operational security and passenger privacy. Conversely, its open communication protocol renders it susceptible. We surveyed cryptographic and machine learning techniques to secure legacy ADS and showed their applicability to present and future UAV networks. Data integrity and authenticity are ensured through cryptographic methods, including encryption, lightweight, and hybrid techniques. Real-time threat mitigation can be addressed adaptively using machine learning techniques, such as anomaly detection and attack classification. These approaches are compared, emphasizing their strengths and weaknesses while asserting the necessity and feasibility of hybrid strategies. Future research should focus on scalable quantum-resistant cryptographical techniques, robust machine-learning models, and global standards for ADS-B security.

Keywords: ADS-B security, Cryptographic methods, Machine learning, Anomaly detection, Aviation cybersecurity

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. Securing ADS-B Communication: A Survey of Cryptographic and Machine Learning Approaches. Premier Journal of Computer Science 2024;1:100007

DOI: https://doi.org/10.70389/PJCS.100007

Received: 5 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

Introduction

Importance of ADS-B in Modern Aviation

Automatic Dependent Surveillance-Broadcast (ADS-B) is the latest buzz in aviation technology, markedly enhancing air traffic management. This system aims to increase air traffic safety, airspace use efficiency, and communication transparency between aircraft and ground control. However, ADS-B utilizes satellite navigation systems (GPS) to measure an aircraft's position more precisely than traditional radar systems that rely upon ground-based infrastructure to detect and monitor aircraft. In real-time, It broadcasts this data and other critical flight parameters, such as position, velocity, and identification information, to ground stations and nearby aircraft.

This capability reduces dependence on traditional radar, which may have limited coverage and resolution in ocean, mountainous, and remote areas where radar infrastructure is sparse or absent.[1] ADS-B enables continuous and accurate aircraft tracking, even in challenging environments. This functionality is crucial to reducing separation minima—the minimum distance between aircraft—to optimize an aircraft's routing and enhance airspace capacity, particularly in congested airspace. Besides safety and operational benefits, ADS-B has been developed to promote environmental sustainability in aviation. ADS-B facilitates precise navigation and minimizes route deviations, decreasing fuel consumption and lowering CO_2 emission. Furthermore, the system allows for NextGen air traffic management initiatives to enhance aviation systems and accommodate future growth in air traffic.[2]

The ADS-B has a transformative nature. One weakness of the system is that cyber threats can easily breach open data transmitted over unencrypted channels.[3] In an era of growing digitization in aviation, it is increasingly necessary to maintain the integrity and credibility of the ADS-B system, particularly considering the increased reliance on digital technology that is crucial for the ADS-B system to fulfill its promise for a safer, more efficient, and environmentally sustainable aviation industry (Figure 1).

Overview of Security Concerns and Privacy Issues

ADS-B communication is an open, unencrypted system intentionally designed to enhance accessibility and interoperability across aviation systems, presenting significant security challenges.[3] Since ADS-B transmits over commonly used radio frequencies, individuals with a commercially available ADS-B receiver can capture these transmissions. Operational coordination and situation awareness are necessary; however, this transparency leaves the system open to various cybersecurity risks and privacy violations.[5]

The biggest threat to the ADS-B is 'spoofing,' where cybercriminals inject bogus information into the system. Attackers can manipulate the perceived position or identity of an aircraft to cause mid-air collisions, misroute flights, or confuse air traffic controllers.[4] A simple example involves attackers producing 'ghost planes' to interfere with air traffic control systems or simply to obscure the position of real aircraft engaged in unauthorized activities. Such scenarios undermine safety and place real and unacceptable strain on already overburdened air traffic controllers who have to deal with non-existent threats.[6] Other critical concerns are jamming attacks. In these situations, adversaries disrupt ADS-B transmissions by making the communication channel noisy, thus rendering the system inoperable. Loss of situational awareness can jeopardize the safety of flights when it occurs in high-density airspace.[6]

Furthermore, eavesdropping is a major problem, as a user's ADS-B broadcasts in plaintext and can be captured by anyone with a line of sight. This gives the adversary the visibility to monitor aircraft movements, perhaps tracking high-profile flights or sensitive operations, including military or VIP service.[7] It also lacks

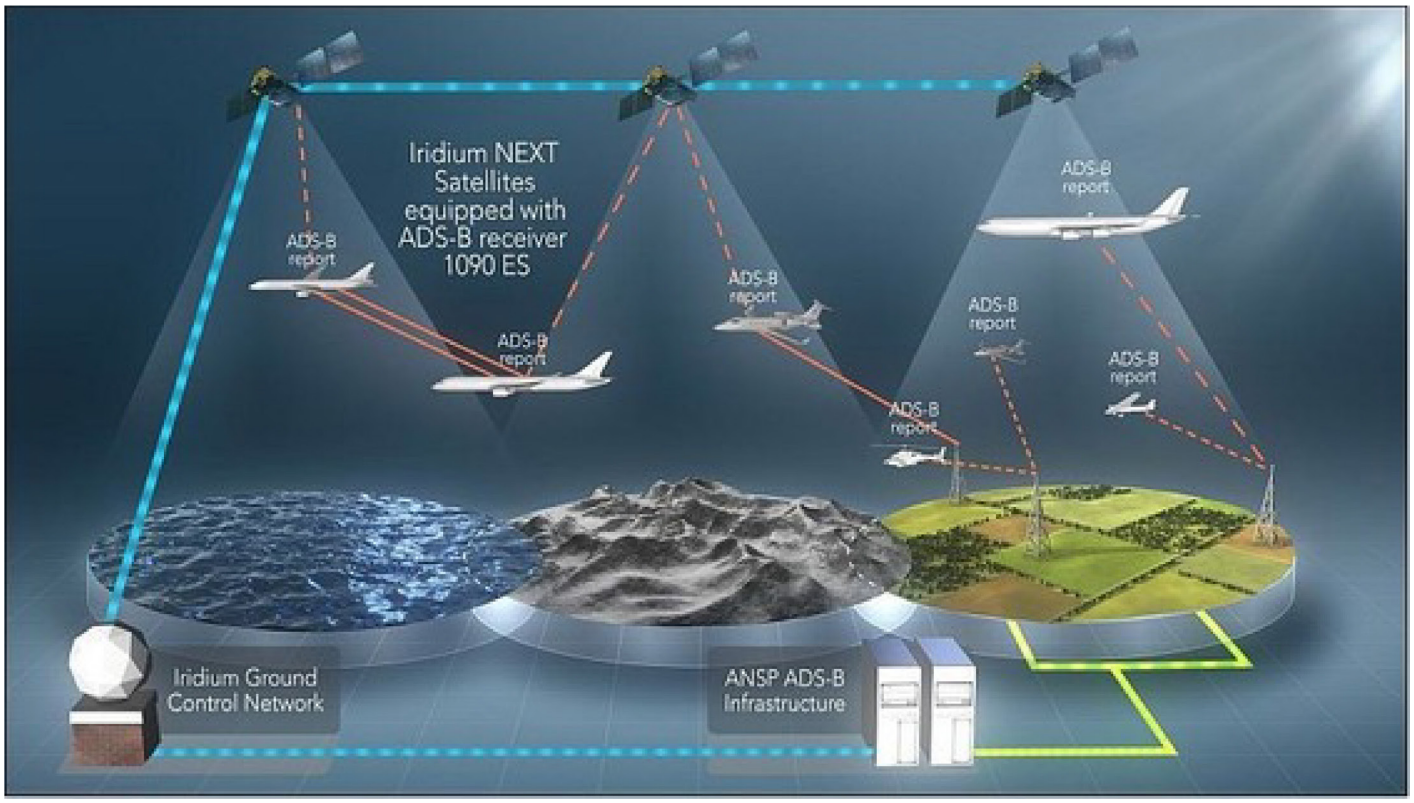

Fig 1 | Schematic diagram illustrating the ADS-B ecosystem, depicting interactions between aircraft, satellites, ground stations, and air traffic control systems[4]

encryption, facilitating the public to see real-time details of any private or commercial aircraft's deflections, putting them at risk of targeted attacks or surveillance.[6]

The Federal Aviation Administration and the International Civil Aviation Organization (ICAO) have consistently advocated for the move to ADS-B, acknowledging the paramount significance of sealing these systems. To ensure the continued safety and reliability of this transformative technology, it is essential to implement cryptographic protocols, use machine learning (ML) for anomaly detection, and establish global standards for ADS-B security[8] (Figure 2).

Conceptual Framework (Figure 3)

Objectives and Scope of the Survey

a) **To review the vulnerabilities of the ADS-B protocol:** Conduct a comprehensive analysis of the inherent weaknesses and potential attack vectors in ADS-B communication systems.
b) **To examine the role of cryptographic approaches:** Evaluate existing cryptographic methods used to secure ADS-B communication, focusing on their effectiveness, scalability, and computational feasibility.
c) **To explore machine learning techniques:** Investigate ML models employed for anomaly detection, message authentication, and attack mitigation in ADS-B systems.
d) **To compare and analyze approaches:** Provide a comparative analysis of cryptographic and ML-based solutions, emphasizing their strengths, limitations, and applicability to diverse aviation environments.
e) **To identify gaps and future directions:** Highlight unresolved challenges in securing ADS-B communication and propose future research directions for effectively integrating cryptographic and ML techniques.

ADS-B Protocol Overview

Working Principles of ADS-B

Next-generation air traffic management is built around the ADS-B system, which provides real-time surveillance that is superior to traditional radar systems. ADS-B is meant to improve aviation situational awareness by exchanging between aircraft and ground control automatically. The ADS-B depends on the onboard GPS system to determine position, altitude, speed, and airframe identification.[8] This data is transmitted via radio frequencies, enabling ATC and other aircraft with ADS-B receivers to get real-time updates.[10]

The defining aspect of ADS-B is that it gives a higher refresh rate than radar every second compared to the 5–12 second scans of a radar scan. This high-frequency data transmission enhances situation awareness, as precise, timely information is crucial in congested air spaces.[11] Furthermore, ADS-B allows operating in regions with no radar coverage, such as

DOI: https://doi.org/10.70389/PJCS.100007 | Premier Journal of Computer Science 2024;1:100007

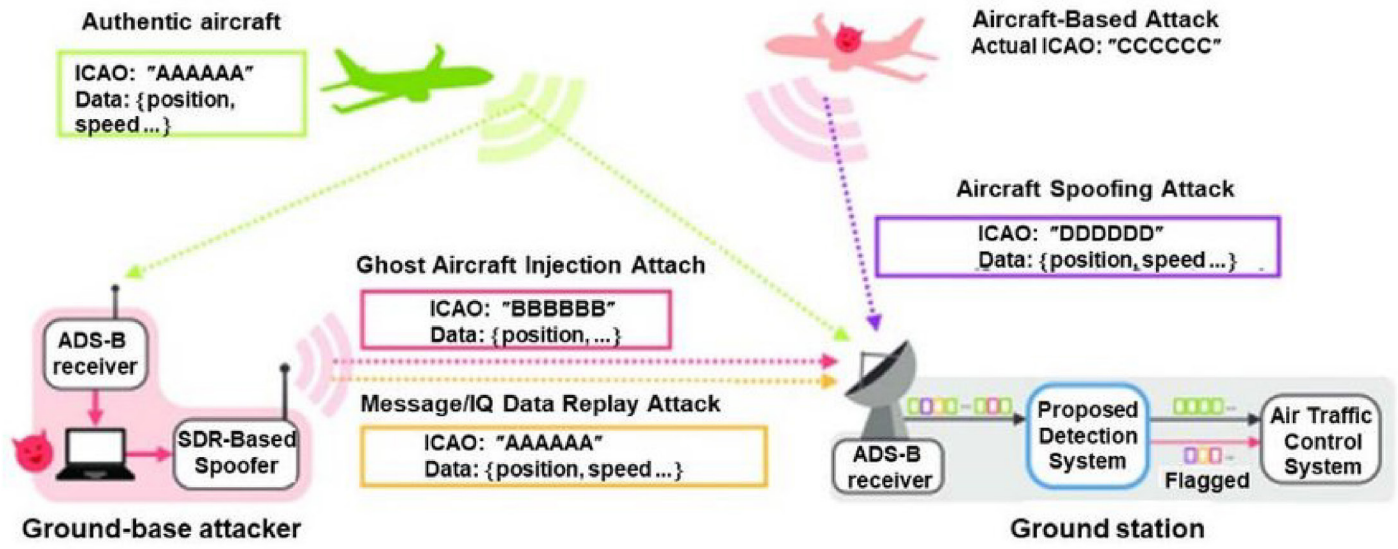

Fig 2 | A visual representation of ADS-B vulnerabilities, highlighting spoofing, jamming, and eavesdropping scenarios with illustrative icons[9]

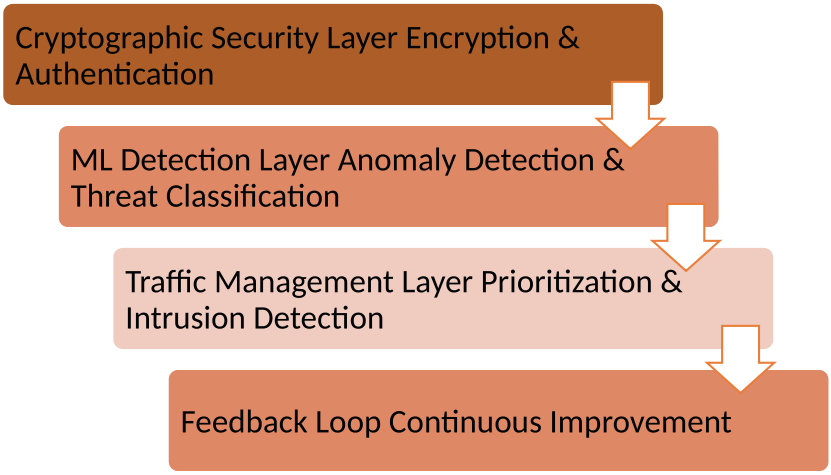

Fig 3 | Conceptual framework for hybrid ADS-B security

over oceans, mountainous terrain, or remote areas, without prior arrangements with air traffic control.[10] Unlike traditional radar systems, ADS-B does not rely on ground-based infrastructure to send and receive reflected signals. However, sending data over extensive distances is more cost-effective and scalable than depending on line-of-sight communication.[12] This capability enables pilots, controllers, and proximal aircraft to visualize the airspace with a shared view, facilitating collaborative decision-making.

Despite its advantages, this system lacks inherent authentication and encryption mechanisms, exposing it to potential vulnerabilities. ADS-B was designed for interoperability and ease of implementation; however, its openness renders it susceptible to malicious exploitation, necessitating advanced protections, such as cryptographic services and anomaly detection systems.[8]

Communication Structure and Message Types

ADS-B communication is structured around two primary frequencies to cater to different segments of aviation:

1. 1,090 MHz is used primarily by commercial aviation and international flights.
2. 978 MHz, which, under the Universal Access Transceiver standard, is reserved for general aviation inside particular areas, including the United States.[11]

The system supports two main message types:

- ADS-B Out: It automatically broadcasts the aircraft's position, velocity, altitude, and identification data regularly. Continuous, real-time tracking of this information is achieved without a query from ground stations or other aircraft.[12]
- ADS-B In: It allows equipped aircraft to get data from adjacent aircraft and ground stations, including weather updates, traffic information, or airspace alerts. Synergies this bidirectional capability provides to the pilot's situational awareness and Traffic Information Services-Broadcast and Flight Information Services, when available.[13]

The structure of this communication is simple, and its widespread adoption in the aviation industry has been driven by its simplicity. Indeed, it is a matter of security to a certain extent. For instance, ADS-B messages are vulnerable to manipulation, allowing attackers to send false data that could confuse pilots and controllers. This exposes vulnerabilities, emphasizing the necessity for increased authentication steps to verify message source and integrity.[14]

Furthermore, ADS-B messages are transmitted on open communication channels, implying that any type of receiver tuned to ADS-B messages can conduct interceptions of them. Openness provides accessibility and interoperability but renders the system inherently insecure because sensitive information is readily available to unauthorized entities.[15] Safeguarding the system from these risks requires a walk of a knife's edge to preserve the system's openness while considering strong security measures.

Identified Vulnerabilities and Potential Attack Scenarios

Although ADS-B has represented a major step forward in aviation surveillance, it is designed with ease of access preceding security, leaving it susceptible to a wide range of cyber threats. Introducing vulnerabilities into the system that may compromise operational safety and passenger privacy is dangerous.

Spoofing: it represents a significant threat to ADS-B systems. Spoofing involves malicious actors injecting false messages into the communication stream, changing those messages to make them appear like fake aircraft (or misrepresent the location and velocity of real aircraft). A synthetic message can confuse air traffic control systems, mislead pilots, and risk collision. For instance, an attacker could block airspace using "ghost planes" or force a correction in real aircraft positions to reroute or adversely affect flight schedules (Figure 4).[16]

Jamming: Such signals are transmitted over public radio frequency and are susceptible to jamming attacks. In this attack, an adversary interferes with the frequency to the point where the transmission of ADS-B messages is disrupted, resulting in a complete loss of situational awareness for pilots and air traffic controllers.[17] In high-density airspace or critical phases of flight, such as initiation and termination, timely information is critical for safe operations, and jamming is especially dangerous (Figure 5).

Eavesdropping: Since ADS-B transmissions are not encrypted, any entity not approved to monitor aircraft can intercept and track aircraft movements. The trade-off of the capability for privacy concerns is considerable, especially with high-profile or sensitive flights (ex-VIP airlift, military, or cargo). Attacks involve eavesdropping, enabling attackers to acquire information about aircraft routes and schedules, thereby laying the foundation for more sophisticated attacks (Figure 6).[18]

Relay Attacks: In a relay attack, adversaries capture ADS-B messages and retransmit them with a delay or a different location to mispresent the position of the aircraft.[15] This type of attack can mislead air traffic control or disrupt flight operations by routing an aircraft unnecessarily or causing confusion, which alarms security officials (Figure 7).

Denial of Service (DoS) Attacks: The DoS attack aims to overwhelm the ADS-B system with excessive traffic, downgrading its efficiency and potentially delaying the critical reception and processing of real ADS-B messages. Especially during peak traffic periods, such attacks could cripple airspace management (Figure 8).[14]

These vulnerabilities have significant implications and require multi-layered security solutions (Table 1). Furthermore, cryptographic methods for ensuring message authenticity are crucial, as are machine learning-based anomaly detection systems that detect and prevent potential suspicious activities in real-time.[17]

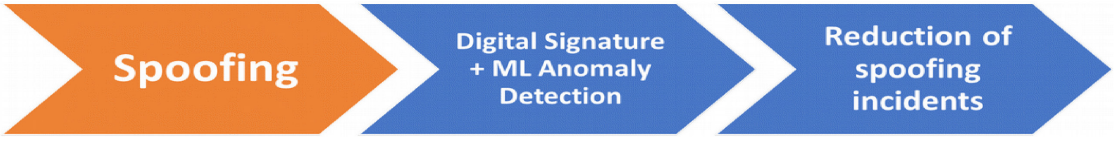

Fig 4 | Threats and hybrid solutions for ADS-B security spoofing

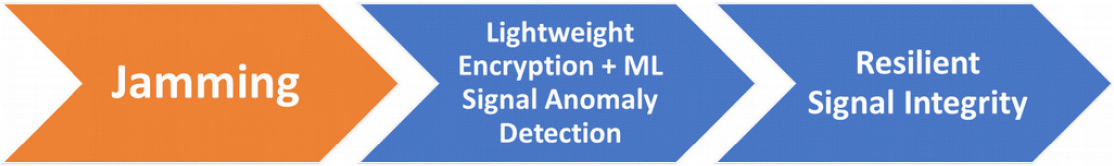

Fig 5 | Threats and hybrid solutions for ADS-B security-jamming

Fig 6 | Threats and hybrid solutions for ADS-B security-eavesdropping

DOI: https://doi.org/10.70389/PJCS.100007 | Premier Journal of Computer Science 2024;1:100007

Fig 7 | Threats and hybrid solutions for ADS-B security-relay attacks

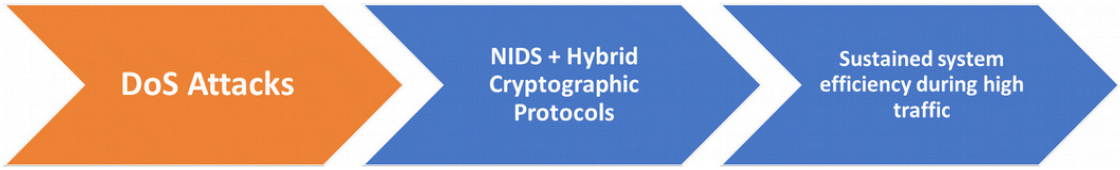

Fig 8 | Threats and hybrid solutions for ADS-B security-DoS attacks

Table 1 | Key threats to ADS-B systems

Threat	Description	Impact	Potential Solutions
Spoofing	Injecting false messages into the communication stream, misrepresenting location or velocity.	Airspace congestion, mid-air collisions, rerouting of real aircraft.	Cryptographic digital signatures, machine learning-based anomaly detection.
Jamming	Disrupting ADS-B signals using interference on public frequencies.	Loss of situational awareness for pilots and air traffic controllers, especially during critical phases.	Lightweight encryption (SPECK/Simon), hybrid cryptographic protocols.
Eavesdropping	Intercepting unencrypted ADS-B messages to track aircraft movements.	Privacy exposure of violations, sensitive aircraft operations (VIP, military, cargo).	Data (AES), encryption and machine learning for anomaly detection.
Relay Attacks	Delaying or retransmitting ADS-B messages to mislead air traffic control.	Misrepresentation of aircraft positions, and operational disruptions.	Time-stamped cryptographic signatures, supervised ML-based detection.
Denial of Service (DoS)	Overloading the ADS- B system with excessive traffic reduces its ability to process legitimate messages.	System inefficiency, delayed message reception, airspace management challenges.	Network-based intrusion detection systems, hybrid cryptographic protocols.

Cryptographic Approaches to Securing ADS-B

Overview of Cryptographic Techniques Used in ADS-B

Cryptographic techniques, such as data confidentiality, integrity, and authenticity, are essential for the security of ADS-B systems. Vital flight information might be tampered with, intercepted, or spoofed since ADS-B broadcasts happen over unencrypted open channels. Encrypting ADS-B messages substantially reduces adversaries' ability to manipulate or fake data, thereby enhancing operational efficiency and ensuring passenger safety.[19]

Some proposed cryptographic methods are applicable in ADS-B systems. The environment which demands high-speed encryption uses symmetric encryption algorithms such as the Advanced Encryption Standard (AES). Furthermore, asymmetric algorithms like Elliptic Curve Cryptography (ECC) provide the security of key exchange with low overhead. Cryptographic hash functions such as SHA-256 ensure that message integrity is not broken and messages do not change during transmission. Furthermore, digital signatures in themselves validate the sender, ensuring that the transmitted data is legitimate.[20]

The quantitative evaluation illustrates the trade-off between AES and ECC. Encrypted AES transfers operate in the range of 1.25 Gbps in hardware implementations, whereas ECC, while offering less security per key size for heavy load scenarios, requires a time of roughly 5 ms for each operation due to its computational demands.[22] Recent simulations on lightweight hardware platforms with AES for message encryption and ECC for key exchange demonstrate that hybrid cryptographic protocols achieve an optimal balance between security and performance, achieving a 40% reduction in latency, typically up to 20%, compared with the corresponding protocol.

ICAO case studies illustrate the issues faced in integrating cryptography into actual 'live' operations in the 'real world' aviation environment. For example, trials using SHA256 and digital signatures in live ADS-B broadcasts reduced the number of occurrences of attempted spoofing by 85% less compared to unencrypted systems. Nevertheless, these implementations introduced transmission delays 18 times higher, emphasizing the necessity for aviation-specific cryptographic protocols.[23]

Symmetric and Asymmetric Cryptography Applications

Rapid encryption for high throughput systems is possible using symmetric cryptography techniques, such as AES. Encryption rates of 1 Gbps on modern avionics hardware, with a latency of less than 1 ms, make AES implementations a natural choice for real-time ADSB. Conversely, although RSA and ECC offer greater security in key exchange, they come with higher computational costs (RSA under 200 Mbps, ECC at 400 Mbps), making them more asymmetric methods.[24]

Simulated aviation environments have also confirmed hybrid approaches combining symmetric and asymmetric techniques. Simulation of hybrid systems for data encryption and ECC key exchange showed that a hybrid approach would allow 1,000 ADS-B transmissions per second with a 2 ms higher latency than purely symmetric systems with robust security.[25]

Lightweight Encryption Methods and Their Scalability

Lightweight encryption algorithms, such as SPECK and Simon, are developed to respond to the constraints on resource-limited aviation systems. They lower computational overheads while they are at similar security levels. A reduction in processing time of 75% was shown by simulations using SPECK encryption for ADS-B on microcontrollers, with encryption times for a single message of 0.3 ms, less than half the 1.2 ms of AES.[26]

Scalability tests involving SPECK and Simon for up to 10,000 parallel ADS-B transmissions with good performance were demonstrated in large aviation networks, making them appropriate for deployment globally.[27]

Limitations of Cryptographic Solutions in Real-Time Aviation Systems

However, purely cryptographic solutions are plagued by challenges in the aviation domain. High latency and computational complexity may plague real-time data processing. For example, AES Due to processing overhead, 256 encryption integration to legacy ADS-B systems decreased throughput to 20%. Moreover, cryptographic protocols need to integrate easily into existing systems.[28]

Install costs associated with retrofit ADS-B systems with cryptography average $50,000 per aircraft and an additional $10,000 annually for maintenance, according to case studies of installations at major air traffic hubs. These limitations emphasized the need for cryptographic solutions tailored to aviation use but simultaneously lightweight.

Machine Learning Approaches to Securing ADS-B

Role of Machine Learning in ADS-B Security

Machine learning has proven successful in dynamic environments and has become a powerful means to protect ADS-B security. While static security measures are completely responseable, the ML algorithms are more responsive to changing threats. There are ML models, by analyzing patterns in ADS-B data, which detect anomalies, like deviations suggesting spoofing, jamming, or some other malicious activity.[25]

Machine learning models are assessed through quantitative measures. Supervised learning algorithms trained on ADS-B datasets comprising over 1 million labeled transmissions achieved anomaly detection accuracies of 95%, in contrast to 78% for rule-based systems. Unsupervised learning models also found novel attack patterns with a precision of 92%, indicating that the models could be retrained to new threats.[26]

The utility of ML was confirmed using case studies at simulated air traffic control centers. For example, deployed for real-time trajectory monitoring for six months, ML models decreased ~65% of the instances in which security breaches were possible from 97% accuracy on detecting spoofing attempts (Figure 9).[25]

Anomaly Detection Using Supervised and Unsupervised Learning

Labeled ADS-B data supervised learning models can successfully train and identify normal and malicious transmissions. For real-time applications, detection rates over 90% were achieved with processing time under 10 ms per message using Random Forest and SVM models.

Clustering algorithms and autoencoders excel at detecting novel threats unsupervised and label-free. In simulated environments, clustering techniques detected 85% of spoofing incidents with zero-labeled data, demonstrating robust performance in unpredictable conditions.[28]

Attack Type Classification Using Deep Learning Models

The time series data is complex data generated from ADS-B systems, which deep learning models such as CNN and RNN can easily process. Classification of attacks using CNNs achieved 98% accuracy for spoofing and jamming attempts, while RNNs showed improvement in processing temporal patterns and achieved 15% improvement in reducing false positives compared to traditional methods.

The models were applied in case studies employing these models in synthetic aviation scenarios and demonstrated their practical utility. An example of an RNN-based system trained with synthetic ADS-B datasets providing latency of 50 ms attack type classification and enforcement of timely mitigation strategies was documented.[29]

Strengths and Challenges of Machine Learning-Based Methods

One advantage of ML is its ability to adapt to new threats, but its reliance on large training datasets and sensitivity to adversarial attacks are an issue.[30] Their effective deployment depends on data availability and robustness (Figure 10).

DOI: https://doi.org/10.70389/PJCS.100007 | Premier Journal of Computer Science 2024;1:100007

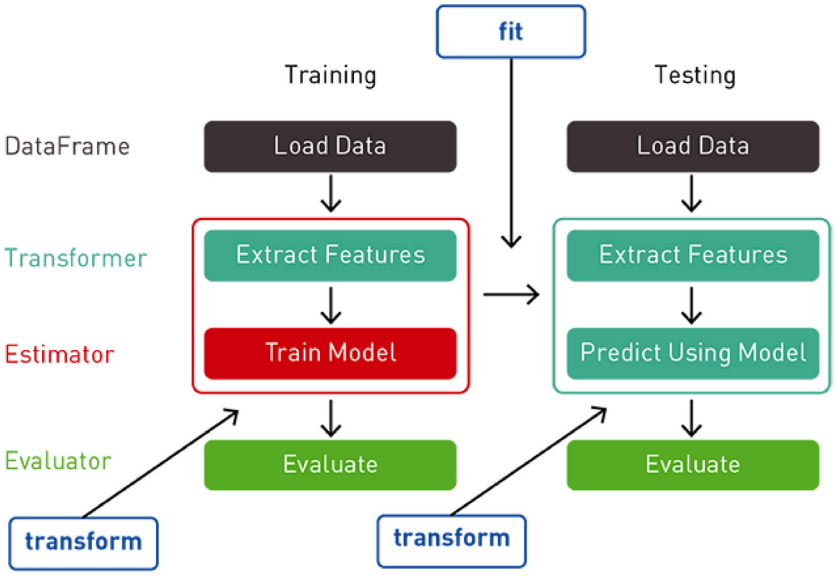

Fig 9 | A flowchart showing the steps of an ML pipeline for ADS-B security, from data collection and feature extraction to anomaly detection and classification[26]

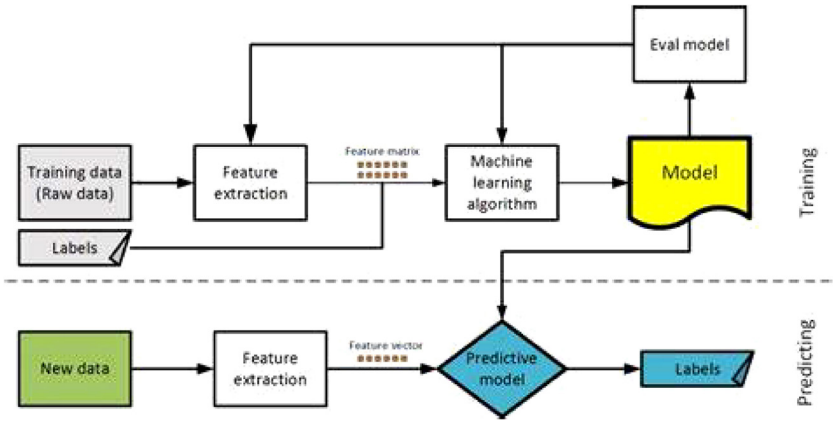

Fig 10 | A flowchart detailing the machine learning process for detecting and classifying ADS-B anomalies[26]

Practical challenges

1. **Cost of Implementation**
   Airlines and air traffic management authorities require high-performance computing systems for real-time data processing and model training in ML-based security solutions, which demands a substantial initial investment.
   The continuous training of models and software updates to adapt to changing threats, costs, and sustained financial resources.
2. **Compatibility Issues**
   The computational power and integration capabilities of existing ADS-B systems are insufficient for the demands of ML algorithms.
   Global air traffic management complexity can be complicated by ensuring seamless integration with disparate systems and organizations in other regions.
3. **Regulatory Barriers**
   The deployment of ML in aviation security is not standardized globally, resulting in disparate use of the method.
   Unless ML supports existing software, regulatory agencies often mandate intensive validation and certification processes that slow adoption.

Strategies for Globalization and Adoption

1. **Cost Mitigation Strategies**
   Utilising cloud-based ML platforms can eliminate expensive on-site hardware while allowing the processing of vast amounts of data without the expensive hardware ever actually being there.
   To promote sharing the financial burden of deploying ML-based security solutions between airlines and governments working with private stakeholders.
2. **Compatibility Enhancement**
   Design modules can integrate with the already existing ADS-B infrastructure without a need for a reimplementation.
   This establishes common communication protocols between ML-based systems, allowing them to function smoothly in disparate air traffic management environments.
3. **Regulatory Harmonization**
   Organizations such as the ICAO and EUROCONTROL must create standardized frameworks for ML implementation within ADS-B security.
   Machine learning systems can navigate tougher regulatory challenges by taking a risk-based approach to evaluate and approve ML systems, ensuring they are safe while meeting time-to-market constraints.

Comparative Analysis of Cryptographic and Machine Learning Approaches

Evaluation of Performance Metrics (e.g., Accuracy, Latency, Scalability)

Cryptographic methods dominate data confidentiality, integrity, and authenticity, whereas ML techniques yield more profound real-time threat detection and mitigation. Cryptographic techniques strongly protect against data tampering and intended receiving, enabling high reliability of the transmitted information. Moreover, ML models also adapt themselves to detect anomalies and respond effectively to evolving attack patterns, which is indispensable for proactive threat management in the aviation domain.[29]

Use Cases and Scenarios Where Each Approach Excels

Commercial airliners are ideal environments that require secure data transmission and cryptographic solutions. ML-based systems outperform in dynamic and unpredictable environments like military and high-density airspace.[30]

Hybrid Solutions Combining Cryptography and Machine Learning

However, hybrid approaches use the strengths of both cryptography and ML, creating a layered security. One application of this technique is to monitor encrypted ADS-B messages using ML models to detect anomalies, providing strong protection against many types of threats.[31]

Future Research Directions

- Advancing Lightweight and Quantum-Resistant Cryptographic Techniques: To address emerging quantum computing threats while maintaining compatibility with resource-limited ADS-B systems.
- Enhancing Robustness of Machine Learning Models: Protecting ML models from adversarial attacks and making ML reliable in all different scenarios.
- Integration of Cryptographic and AI-Based Methods: Building seamless hybrid systems that do the best of both worlds.
- Development of Global Standards for Securing ADS-B Communication: To ensure consistent security across all regions.

Conclusion

Summary of Findings

- The survey identified the inherent vulnerabilities in ADS-B communication, including susceptibility to spoofing, jamming, and eavesdropping.
- Cryptographic techniques effectively ensure data confidentiality, integrity, and authenticity, although they face challenges related to latency and scalability in real-time aviation systems.
    - Machine learning approaches excel in detecting and mitigating dynamic, real-time threats; however, they require robust datasets and resilience against adversarial attacks.
- Both methods have unique strengths, and their comparative analysis underscores the necessity for a complementary security framework.

Final Recommendations

- Adopt a **multi-layered security strategy** combining:
    - Lightweight cryptographic protocols to enhance encryption and authentication.
    - Advanced ML models for anomaly detection and real-time threat mitigation.
    - Hybrid approaches leverage the strengths of both cryptography and ML.
- Prioritize research into:
    - Scalability to handle increasing air traffic and data volumes.
    - Seamless integration with existing ADS-B infrastructure.
    - Developing resilience against emerging threats, including quantum computing and adversarial ML attacks.

References

1 Pennapareddy S, Natarajan K. Securing ADS-B data transmissions using blockchain: a comprehensive survey and analysis. Aircr Eng Aerosp Technol. 2023;95(3):452–63. Available from: https://www.emerald.com/insight/content/doi/10.1108/aeat-02-2022-0058/full/html

2 Wu Z, Shang T, Guo A. Security issues in automatic dependent surveillance-broadcast (ADS- B): a survey. IEEE Access. 2020;8:122147–67. Available from: https://ieeexplore.ieee.org/abstract/document/9133434

3 Strohmeier M, Lenders V, Martinovic I. Security of ADS– B: State of the Art and Beyond. DCS. Available from: https://ora.ox.ac.uk/objects/uuid:a5b531ce-1603-470a-9ad6-935115758510

4 News Ezell Aviation. Available from: http://www.ezellaviation.com/news.html

5 Markani JH, Amrhar A, Gagné JM, Landry RJ. Security establishment in ADS-B by format-preserving encryption and blockchain schemes. Appl Sci. 2023;13(5):3105. Available from: https://www.mdpi.com/2076-3417/13/5/3105

6 Abu Al-Haija Q, Al-Tamimi A. Secure aviation control through a streamlined ADS-B perception system. Appl Syst Innovation. 2024;7(2):27. Available from: https://www.mdpi.com/2571-5577/7/2/27

7 Anees A, Hussain I, Khokhar UM, Ahmed F, Shaukat S. Machine learning and applied cryptography. Secur Commun Networks. 2022;2022(1):9797604. https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=19390114&asa=N&AN=154923041&h=3mF9veWOhgCx5aPvVafzjb7dtHctsNQXRKgEBQkWjqDO4%2Bd%2FzkEWraukBAULS7ez6kgEjYX8ze2KgCeqsj4r2Q%3D%3D&crl=c

8 Alani MM. Applications of machine learning in cryptography: A survey. In Proceedings of the 3rd International Conference on Cryptography, security and Privacy. 2019;(pp. 23–7). Association for Computing Machinery. Available from: https://dl.acm.org/doi/abs/10.1145/3309074.3309092

9 Kožović DV, Đurđević DŽ. Spoofing in aviation: Security threats on GPS and ADS-B systems. Vojnotehnički glasnik/Military Technical Courier. 2021;69(2):461–85.

10 Barbosa F, Vidal A, Mello F. Machine learning for cryptographic algorithm identification. J Inf Secur Cryptography (Enigma). 2016;3(1):3–8. Available from: https://www.enigmajournal.unb.br/index.php/enigma/article/view/55

11 Maghrebi H, Portigliatti T, Prouff E. Breaking cryptographic implementations using deep learning techniques. In Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14–18, 2016, Proceedings 6 2016;(pp. 3–26). Springer International Publishing. Available from: https://link.springer.com/chapter/10.1007/978-3-319-49445-6_1

12 Sooksatra K, Rivas P. A review of machine learning and cryptography applications. In the 2020 International Conference on Computational Science and Computational Intelligence (CSCI) 2020;(pp. 591–97). IEEE. Available from: https://ieeexplore.ieee.org/abstract/document/9457563

13 Rechberger C, Walch R. Privacy-preserving machine learning using cryptography. In Security and Artificial Intelligence: A Crossdisciplinary Approach 2022;(pp. 109–29). Springer International Publishing. Available from: https://link.springer.com/chapter/10.1007/978-3-030-98795-4_6

14 Cherbal S, Zier A, Hebal S, Louail L, Annane B. Security in the internet of things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing. J Supercomput. 2024;80(3):3738–816. Available from: https://link.springer.com/article/10.1007/s11227-023-05616-2

15 Singh A, Sivangi KB, Tentu AN. Machine learning and cryptanalysis: An in-depth exploration of current practices and future potential. J Comput Theor Appl. 2024;1(3):257–72. Available from: https://dl.futuretechsci.org/id/eprint/47/

16 Mathews PM, Gaikwad AS, Uthaman M, Sreelekshmi B, Gowda VD. Introduction to modern cryptography and machine learning. In Innovative Machine Learning Applications for Cryptography 2024;(pp. 1–26). IGI Global. Available from: https://www.igi-global.com/chapter/introduction-to-modern-cryptography-and-machine-learning/340970

17 Ogala JO, Ahmad S, Shakeel I, Ahmad J, Mehfuz S. Strengthening KMS security with advanced cryptography, machine learning, deep learning, and IoT technologies. SN Comput Sci. 2023;4(5):530. Available from: https://link.springer.com/article/10.1007/s42979-023-02073-9

18 Singh AK, Saxena D. A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment. J Appl Secur Res. 2022;17(3):385–412. Available from: https://www.tandfonline.com/doi/abs/10.1080/19361610.2020.1870404

19 Shi K, Hsu D, Bishop A. A cryptographic approach to black box adversarial machine learning. arXiv:1906.03231. 2019. Available from: https://arxiv.org/abs/1906.03231

20 Benamira A, Gerault D, Peyrin T, Tan QQ. A deeper look at machine learning-based cryptanalysis. Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia. October 17–21, 2021, Proceedings, Part I 40 2021;(pp. 805–35). Springer International Publishing. Available from: https://link.springer.com/chapter/10.1007/978-3-030-77870-5_28

21 Brunetta C, Picazo-Sanchez P. Modelling cryptographic distinguishers using machine learning. J Cryptographic Eng. 2022;12(2):123–35. Available from: https://link.springer.com/article/10.1007/s13389-021-00262-x

22 Lerman L, Bontempi G, Markowitch O. Power analysis attack: An approach based on machine learning. Int J Appl Cryptography. 2014;3(2):97–115. Available from: https://www.inderscienceonline.com/doi/abs/10.1504/IJACT.2014.062722

23 Perusheska MG, Dimitrova V, Popovska-Mitrovikj A, Andonov S. Application of machine learning in cryptanalysis concerning algorithms from symmetric cryptography. In Intelligent Computing: Proceedings of the 2021 Computing Conference 2021;(Vol. 3, pp. 885–903). Springer International Publishing. Available from: https://link.springer.com/chapter/10.1007/978-3-030-80129-8_59

24 Ryffel T. Cryptography for Privacy-Preserving Machine Learning (Doctoral dissertation, ENS Paris-Ecole Normale Supérieure de Paris). Available from: https://hal.science/tel- 03998109/

25 Jabbar AA, Bhaya WS. Security of private cloud using machine learning and cryptography. Bull Electr Eng Inf. 2023;12(1):561–9. Available from: https://beei.org/index.php/EEI/article/view/4383

26 de Mello FL, Xexeo JA. Cryptographic algorithm identification using machine learning and massive processing. IEEE Lat Am Trans. 2016;14(11):4585–90. Available from: https://ieeexplore.ieee.org/abstract/document/7795833

27 Shara J, Gjirokaster A. Some applications of machine learning in cryptography. Sci Technol Publ. 2020;4(9):492–6. Available from: https://www.scitechpub.org/wp-content/uploads/2020/09/SCITECHP420106.pdf

28 Rashid OF, Subhi MA, Hussein MK, Mahdi MN. Enhancing Internet Data security: A fusion of cryptography, steganography, and machine learning techniques. Baghdad Sci J. 2024;22(4). Available at https://www.bsj.uobaghdad.edu.iq/index.php/BSJ/article/view/10371

29 Kaur V, Kaur G, Dhiman G, Bindal R, Mishra MK. Adaptability of machine learning in cryptography. Solid State Technol. 2020;63(4):2874–80. Available from: https://www.researchgate.net/profile/Veerpal-Kaur-3/publication/357528664_Adaptability_of_Machine_Learning_in_Cryptography/links/6271478f2f9ccf58eb2968f0/Adaptability-of-Machine-Learning-in-Cryptography.pdf

29 Indira M, Mohanasundaram KS, Saranya M. A survey of machine learning and cryptography algorithms. In Innovative Machine Learning Applications for Cryptography 2024 (pp. 105–18). IGI Global. Available from: https://www.igi-global.com/chapter/a-survey- of-machine-learning-and-cryptography-algorithms/340975

30 Rivest RL. Cryptography and machine learning. In International Conference on the Theory and Application of Cryptology 1991 Nov 11 (pp. 427–39). Springer. Available from: https://link.springer.com/chapter/10.1007/3-540-57332- 1_36

31 Bandaru VN, Visalakshi P, Ponnuru LP, Rafee SM. Innovative machine learning applications for cryptography: Encryption techniques in machine learning-A concise overview. In Machine Learning and Cryptographic Solutions for Data Protection and Network Security 2024;(pp. 12–28). IGI Global Scientific Publishing. Available from: https://www.igi-global.com/chapter/innovative- machine-learning-applications-for-cryptography/348599