The Role of Machine Learning in Enhancing ADS-B Communication Security: A Comprehensive Review

Waqas Ahmed

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. The Role of Machine Learning in Enhancing ADS-B Communication Security: A Comprehensive Review. Premier Journal of Computer Science 2024;1:100008

DOI: https://doi.org/10.70389/PJCS.100008

Received: 7 December 2024

Revised: 21 December 2024

Accepted: 21 December 2024

Published: 3 January 2025

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 in air traffic management (ATM) is among the significant technologies developed to improve airspace proficiency. However, it is linked with some vulnerabilities, such as jamming, spoofing, and data injection attacks, which pose a significant risk to aviation safety. The aim of the current study is to focus on security issues and potential solutions through machine learning (ML) to increase the communication security of ADS-B. The main ML types are supervised, unsupervised, and deep learning models that assist in identifying abnormal behavior of in-flight data, predicting evolving threats, and detecting spoofing attempts. ML techniques assess the historical data and indicate potential system failure and vulnerabilities. A proactive response is possible through real-time deep learning methods to ensure the operational efficiency of the ATM following ADS-B. ML models have scalability issues and computational complexities that indicate the use of mixed methods to increase the identification of security issues, as there can be a larger dataset, and every ML technique cannot process such a larger dataset for real-time threat mitigation. ADS-B security is increased due to collaborative efforts and innovations that can resolve the complicated evolving risks in ATM.

Keywords: ADS-B communication security, Machine learning models, Jamming and spoofing detection, Anomaly detection, Air traffic management

Introduction

Importance of ADS-B in Air Traffic Management

ADS-B is one of the significant innovations in air traffic management (ATM) that impacts efficiency, safety, and capacity in the global airspace.[1] It is a satellite-based surveillance technology that aids aircraft in broadcasting their position, altitude, speed, and other data to air traffic controllers and adjacent aircraft in real time. Improved safety is associated with ADS-B due to its situational awareness for controllers and pilots and its capacity to provide real-time and accurate data.[2] Precise location assessment reduces the risks of mid-air collisions, and it also improves the detection of conflicts to resolve these timely.[3] Furthermore, precise tracking through ADS-B also supports minimizing the separation between aircraft and allows efficient usage of airspace.[4] This is specifically useful within high-traffic regions and in remote areas with limited radar systems. The system eliminates the need for expensive radar infrastructures that are usually ground-based and supports optimal routes of flights by minimizing fuel consumption and carbon emissions.[5] Unlike radars, ADS-B provides coverage in oceanic and remote areas, ensuring seamless control of air traffic.[3]

Overview of Vulnerabilities and Security Challenges

Due to increased digital applications, security and vulnerability challenges pose a significant risk in aviation. ADS-B has transformed ATM with the help of increased situational awareness and efficiency; however, it is also linked with various vulnerabilities. The unencrypted data transmission makes ADS-B susceptible to jamming attacks and spoofing that can happen due to disruptions and false signals impacting the reliability of the system.[2,6] Furthermore, a lack of authentication leads to malicious actors that can imitate ground stations and legitimate aircraft.[7] On the other hand, security channels also include the mitigation of the risks from cyberattacks that are exploited by the vulnerabilities and also guarantee flexibility against signal interference.[3] The dependence on publicly accessible broadcast data intensifies the unauthorized monitoring exposure that can lead to privacy breaches and national security risks.[8]

The Potential of Machine Learning to Address Challenges

Advanced machine learning methods are useful to detect anomalies related to ADS-B ins ATM as analyzed by.[9] Anomalies are detected by ML and deep learning models as these models are able to analyze huge amounts of ADS-B data to find spoofed signals and irregular patterns, and they alert controllers regarding further potential attacks like jamming or spoofing.[10] This is due to the ability of these systems to learn historical data to improve threat detection over time. ML models can make a difference in the authentication of ADS-B signals from any malicious interference.[11] It increases reliability in contested and complicated environments. Furthermore, predictive maintenance to manage resilience ensures proactive measures that are implemented to establish operational integrality.[12] The study by[13] elaborated that ML algorithms are able to validate ADS-B as it does not directly encrypt data. It applies cross-referencing with auxiliary and historical data that ensure consistency and authenticity.

Objectives and Scope of the Review

The research objectives are:

a) Examine ADS-B systems' inherent weaknesses and potential risks that can compromise aviation safety and privacy.
b) Review machine learning techniques for anomaly detection, message authentication, and threat mitigation, including supervised, unsupervised, and deep learning models.
c) Assess the effectiveness of these models in addressing specific threats like spoofing,

jamming, and injection attacks based on accuracy, scalability, and computational feasibility.

d) Highlight limitations in existing machine learning applications for ADS-B security and propose areas requiring further exploration.

e) Suggest innovative approaches, including hybrid techniques, explainable AI (XAI), and federated learning, to enhance the security and resilience of ADS-B communication systems.

ADS-B Communication and Security Overview

ADS-B is the foundation of the modern ATM system that assists in providing real-time aircraft tracking with the help of satellite-based communication.[2] The functionality is based on the principles of automatic, surveillance, dependent, and broadcast. In terms of automatic, ADS-B is operating in an autonomous environment without controller or pilot inputs. The dependence functions are based on the onboard systems that include the GPS for finding aircraft velocity and position. Surveillance indicates that the system consistently monitors the movements of aircraft. Furthermore, broadcast presents the data is shared to nearby aircrafts and ground stations through unencrypted frequencies (Figure 1).

Functional Architecture and Working Principles

The ADS-B architecture is based on the three main components of ADS-B Out, ADS-B In, and Ground Infrastructure.[14] ADS-B Out includes the aircraft's broadcast position, altitude, speed, and identification of data at regular intervals through onboard transponders.[2] ADS-B In includes ground stations and aircraft and received ADS-B broadcast that increases the situational awareness for air traffic controllers and pilots.[15] Ground infrastructure is based on the receiver processes where ADS-B data is used to manage traditional radar systems.[13]

The working principle shows that the aircraft uses GPS to find the exact location. The information is combined with the data of other flights, and then it is encoded and transmitted through transponders over 1090 MHz radio frequency for international use and 978 MHz in the US.[16] Ground stations and related aircraft in the range receive and decode the signals for real-time tracking. The security concerns can be related to the authentication and encryption in the ADS-B broadcasts that leave the system vulnerable to eavesdropping, spoofing, and jamming attacks. Interference of signals and unauthorized monitoring can increase challenges to advanced security measures and integrity. ADS-B increases safety and efficiency, increases the risks, and makes it vital for global ATM and its components (Figure 2).

Identified Vulnerabilities and Threats

According to the study by,[1,4] the absence of encryption allows unauthorized parties to intercept ADS-B signals, compromising operational confidentiality. Malicious actors can introduce false data like incorrect positions and fictitious aircraft within the system.[18,19] The outcomes overwhelm the traffic control system through phantom aircraft and generate an illusion of collision paths and, thereby, severely disrupting operations. Furthermore, ADS-B signals transmitted at 1090 MHz are also vulnerable to jamming, which can render critical communication channels inoperable.[20]

The attack can include low-cost equipment that makes it accessible to potential attackers. Such threats are intercepted with valid messages about retransmission that can cause confusion in the monitoring system of airspace.[21] In this case, the main threat is that the ADS-B messages that can be transmitted without verification of senders can enable the legitimate takeoff of aircraft.[1] The ultimate

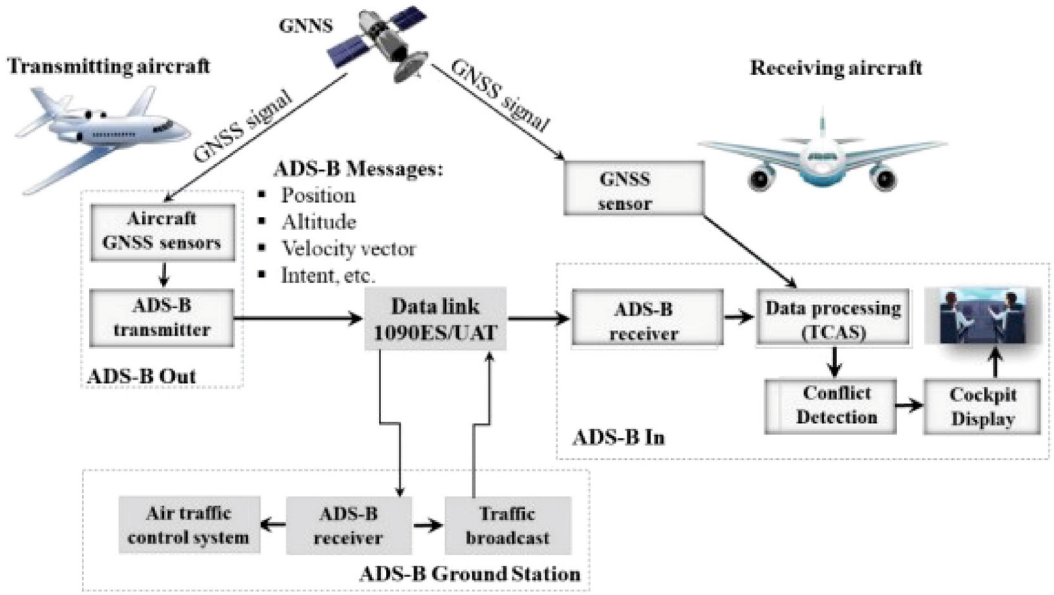

Fig 1 | ADS-B architecture[2]

DOI: https://doi.org/10.70389/PJCS.100008 | Premier Journal of Computer Science 2024;1:100008

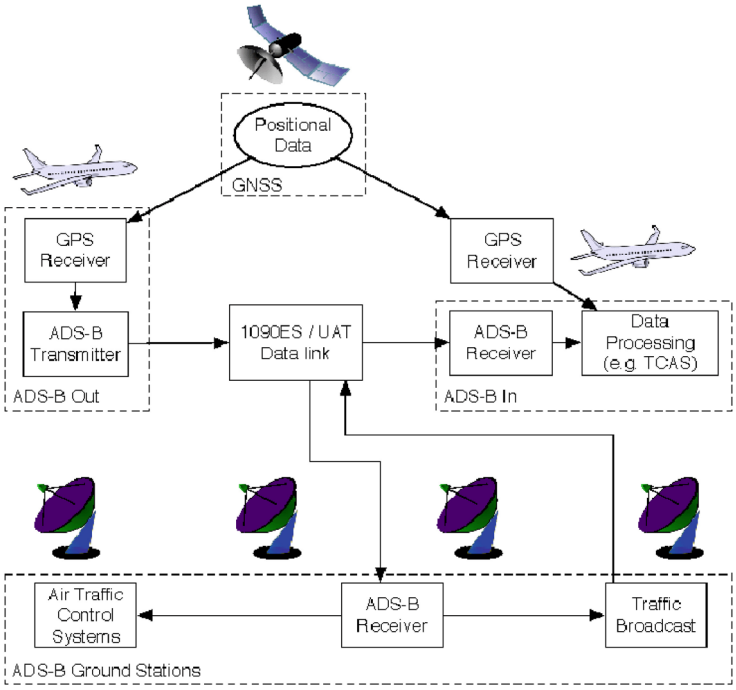

Fig 2 | ADS-B system architecture overview[17]

outcome is the manipulation of flight data that leads to cyberattacks. ADS-B also depends on the global navigation satellite system to position data that is vulnerable to signal disruption and spoofing.[22] Encryption of ADS-B messages and the addition of the sender identification can reduce spoofing and eavesdropping by implementing the potential system latency and implementation costs that have notable challenges.[23] Furthermore, multilateration (MLAT) and time difference of arrival methods can assist in detecting and preventing positional spoofing attacks and data injections.[24] Anti-jamming methods with signal processing can synchronize the receiver network and minimize the susceptibility to jamming.

The Current State of Security Measures

The security landscape of ADS-B is observed to show progress, but it is a challenge because of inherently unencrypted and unauthenticated communication protocols.[6] Current measures focus on mitigation, detection, and increased resilience as compared to the fully renovated system and its basic vulnerabilities.[25] Air navigation service providers enhance the use of MLAT for validation of the ADS-B data.[24,26] The technique is based on the comparison of signal times from various receivers for the detection of anomalies like spoofed positions. However, encryption is not adopted widely because of compatibility with legacy systems and because of latency risks.[7] Such services offer a future-proof solution for eavesdropping and spoofing threats, help reduce jamming and frequency hopping, and utilize signal processing methods as anti-jamming strategies.[4] These methods are helpful in improving the robustness of signals against interference.

Global Implementation Challenges

Advanced ML and algorithm systems assess the ADS-B data streams for the detection of discrepancies and unusual patterns.[27] Such systems can also flag potential malicious activities and increase situational awareness. EUROCONTROL and the International Civil Aviation Organization (ICAO) are driving collaborative efforts for establishing the global security standards for ADS-B.[2] Implementation is inconsistent globally in various regions, which shows that a proactive design of ADS-B integration and authentication is required for long-term security. The differences in the aviation regulations of various regions and standards of ATM bring more challenges to the European Union Aviation Safety Agency, Federal Aviation Administration, and ICAO, which have different operational and security requirements globally.[28] For this, ML adoption in the ADS-B system needs compliance with such standards, which makes the cross-border system integration complicated. Regional certifications and compliance requirements include as those laid out by ISO/IEC 27001 and DO-178C.[29] Collaborative efforts are required to meet the challenges and to be in compliance with global air transportation standards in various regions.

Overview of Machine Learning Techniques for Security

Types of Machine Learning

The study by[30] indicates that supervised learning is one of the most powerful tools for detecting anomalies and classifying threats to security systems. Supervised learning is an approach that helps detect anomalies and classify threats to security systems. Furthermore, it applies labeled training data for creating models that can find unusual patterns and behaviors indicating security threats like system malfunctions and cyberattacks. Support vector machines (SVMs) are

neural networks that analyze known data patterns for the detection of deviations.[31] Such models improve the accuracy of the identification of spoofing threats in communication systems like ADS-B over time after learning from historical incidents.[1] The supervised learning models in classification are categorized with the security events in predefined types, like differentiating between insider threats and external attacks. It directly improves the response prioritization and allocation of these resources. However, effective supervised learning needs high-quality labeled datasets that make its success important for robust data collection and preprocessing exertions.

Another type of machine learning method is unsupervised learning, which plays a critical role in identifying and clustering novel threats within dynamic security environments.[32] Unsupervised learning without labeled data uncovers the hidden structures and dataset patterns. For example, clustering algorithms like DBSCAN and K-means group similar amounts of data points on the basis of features.[33] In network security, clustering assists in finding unusual traffic patterns that can also signify attacks.[34] For novel threat identification, anomaly detection finds the data points that are significantly different from the majority. Gaussian mixture models and autoencoders are applied to flag the outliers like spoofed ADS-B signals or unexpected behavior of the system.[35]

Deep learning leverages neural networks to find intricate patterns in data with the help of the hierarchal extraction of features.[36] Convolutional neural networks (CNNs) recognize the anomalies and objects in image form; however, recurrent neural networks (RNNs) assist in processing sequential data like time-series signals and text. Deep learning in aviation security detects jamming and spoofing by assessing complex signal patterns.[37] The capability of the unstructured data process, like speech and images, makes it ideal for diverse applications like natural language understanding, and unstructured data processing or speech makes it ideal for a diverse population. In aviation security, deep learning perceives jamming or spoofing by assessing the complex signal patterns.[38] The ability of the method for unstructured data like speech and images makes it ideal for various types of applications like natural language system facial recognition and advanced anomaly detection.

Advantages of Machine Learning in Aviation Security

ML algorithms are important for vast datasets to find patterns and anomalies in real time.[39] In the ADS-B systems, ML is able to detect spoofed signals, unusual aircraft behavior and jamming by associating the transmitted data against predictive models and historical patterns.[40] In aviation, a huge amount of data is generated from the radar signals for passenger information. Furthermore, ML assists the rapid data analysis that allows security teams to respond to threats immediately.[41] The agility increases safety and reduces operational disruptions. The analysis of historical data performance through ML can predict potential system failures and vulnerabilities to enable preemptive maintenance.[42] This minimizes downtime and leads to increased robustness of the critical aviation systems, including the communication and surveillance infrastructure. ML-powered automation minimizes the human errors and increases operational efficiency.[33] Automated systems are able to monitor multiple inputs, recommend actions, free security personnel, and prioritize alerts for highly sensitive tasks. ML continuously improves the new data that makes the aspects well-suited for the emerging security challenges.

Applications of Machine Learning in ADS-B Security

Anomaly Detection

ML increases ADS-B security by automating the anomaly detection and abnormal behavior of flights, which is important to maintain air traffic system integrity.[1] SVMs and neural networks find threats like spoofing and injected signals in historical dataset training.[43] In the meantime, unsupervised models, including autoencoders and clustering algorithms, detect novel threats by assessing the deviation from typical data patterns from in-flight data. ML flags the ADS-B signal discrepancies like improbable speed and changes in the altitude that show the manipulated or spoofed data.[38] Real-time anomaly detection through deep learning assists proactive responses to security breaches by ensuring operational efficiency.

Attack Classification

ML increases attack classifications, like jamming, spoofing, and injection in the ADS-B systems. Spoofing attacks are found by assessing anomalies in the aircraft velocity, position, and consistency of signals using deep learning and decision tree networks.[44] Jamming is assessed through disruption patterns of signals that are supervised models to assess the abnormal noise in the communication channels.[40] Injection attacks assess the falsified data and categorize it to use the algorithms that identify the deviations.[45] Such classifications assist in the precise detection of threats and facilitate tailored control strategies by ensuring traffic integrity during adaptation to evolve the attack vectors.

Real-Time Threat Mitigation

Predictive models in machine learning are essential in the real-time mitigation of threats by analyzing live and historical data to encounter and anticipate evolving threats.[46] These models utilize methods like anomaly detection, trend forecasting, and pattern recognition to find risks before materialization. The predictive algorithm monitors ADS-B data streams to indicate the irregular flight paths, mismatches, and signal disruptions that are expected in aircraft behavior.[47] The learning from previous patterns of historical attacks by ML assists in assessing the potential injection attempts, spoofing, and jamming, and it can trigger automatic responses in the form of alters.[44] Real-time updates also enable the system to recalibrate the predictions, and it ensures the adaptability towards novel threats.

DOI: https://doi.org/10.70389/PJCS.100008 | Premier Journal of Computer Science 2024;1:100008

Comparative Analysis

Comparative Analysis of Non-ML Methods and ML-Based Methods

Various non-ML-based approaches, including authentication techniques, cryptographic checks, redundancy checks, and physical-layer security, create a primary defense against threats, including jamming, spoofing, and injection attacks.[47,48] Furthermore, cryptographic methods are dependent on encryption for securing the ADS-B signals, and this confirms the legitimate parties that can interpret data.[49] On the other hand, an open broadcast system of ADS-B and encryption has limited feasibility because of interoperability and computational challenges with legacy systems. Another solution is message authentication codes that verify the origin and integrity of the broadcast messages, and they also struggle to establish real-time performance for crowded and large air spaces.[50]

Redundancy-based methods cross-verify the flight data through multiple sensor inputs like ground-based sensors and radar to detect spoofed signals. The approach is effective but increases the cost and system complexity.[51] The signal strength monitoring can assist in finding jamming strength and detect unusual signal fluctuations, but it needs specialized hardware that is at risk for false positives. However, physical-layer security methods like fingerprinting detect the unique characteristics of transmission for authenticating the aircraft. These can be bypassed with sophisticated attacks that imitate the transmission signatures.

On the other hand, ML-based methods suggest data-driven and proactive detection and threat classification. Supervised learning models like random forest (RF) and SVMs are more effective in detecting anomalies to assess deviation from historical data of flights.[52] Deep learning models, including RNNs and CNNs, assess the multi-denomination relations and complex patterns from real-time flight data. The large volume of ADS-B data can be processed through deep learning, which increases the accuracy of threat detection.[53]

Comparative Analysis of Machine Learning Approaches

Performance Metrics

The study by[54] evaluated the performance of ML approaches, which showed that gradient boosting and adaptive boosting were highly accurate (91.34%). The true positive prediction of adaptive boosting was highly precise for adaptive boosting. The recall score of KNN was highest, at 95%, and the F1 score was highest for the gradient boosting. The study by[55] identified mixed machine learning to predict diseases and evaluated the accuracy of 98.56% by focusing on overall reliability. The measure of precision was 97.81%, which shows the effectiveness of the model to provide the true results of positive cases. The sensitivity or recall was 98.92%, which shows the ability of the model to find actual cases. The F1 score was 98.36%, highlighting the robustness of mixed ML to handle reliability and data complexity. The study by[56] identified RF among high performers. Another study[57] has explored the various ML techniques, including CNN, SVM, KNN, RF, and XGBoost. The CNN accuracy was outperforming at 98.6% for the air traffic control system.

Computational Complexity and Scalability

The scalability and computational complexity of ML approaches are based on the data size and algorithm.[12] The linear model has a lower complexity level that assists the approach to scale the larger datasets. RF and decision tree scalability can be increased with deep tress; however, deep tress can increase complexity.[53] On the other hand, SVM is inefficient with larger datasets because of cubic or quadratic complexity.[58] Neural networks need computational power as they face scalability challenges. On the other hand, advancements in approximation methods and distributed computing, like mini-batch gradient, are helpful in increasing scalability in the case of large datasets.[59]

Strengths and Limitations of Different Models

SVM is effective in classifying the problems, specifically with medium and small-size datasets. The main strength is in the high-dimensional spaces; however, they struggle with very large datasets because of quadratic complexity that needs careful hyperparameter tuning.[58] Furthermore, SVM might not perform effectively with noisy data, including overlapping classes. Long and short-term memory (LSTM) networks are based on the sequence of data that makes it perfect for time-series forecasting.[60] LSTM also captures long-range dependencies, but they are prone to overfitting if not regularized properly.[61] New data samples can be generated with images for generative adversarial networks.[62] They are useful for unsupervised learning tasks, but the main issues are related to training these models, and they are prone to collapse.

Conclusion

ADS-B indicates that security risks like spoofing, injection attacks, and jamming can compromise ATM system.[63] Such threats can lead to severe consequences like aircraft misidentification and air traffic control disruption.[64] The solutions to control these risks are the ML method for effective anomaly detection and real-time monitoring to increase the identification of abnormal behavior. Consistent innovations are vital to maintaining robust ADS-B security.

Future Research Directions

Future research is intended to be conducted using explainable and robust AI models. It will also integrate federated learning to enhance privacy in ADS-B communication. Furthermore, it will use machine learning solutions and hybrid cryptography. It will also standardize machine learning practices in ADS-B security. Future research will explore the combined ML and non-ML model-like hybrid approaches for anomaly detection. The approach can be useful by adding a multi-layered defense system that can work against a broader range of attacks. ML scalability is also possible through hybrid models. Deep learning is assessed

to be managing an exceptional accuracy, but these are operated like "black boxes," which makes it challenging to interpret logic. Future research through XAI can increase the transparency of the models. This will help air traffic controllers in understanding the specific anomalies and reasons why these were flagged as a threat.

References

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

2 Kožović DV, Đurđević DŽ, Dinulović MR, Milić S, Rašuo BP. Air traffic modernization and control: ADS-B system implementation update 2022–A review. FME Trans. 2023;51(1):117–30.

3 Abu Al-Haija Q, Al-Tamimi A. Secure aviation control through a streamlined ADS-B perception system. Appl Syst Innov. 2024;7(2):27.

4 Ferrara A. ADS-B in context: A Comprehensive Threat Analysis. POLITesi – digital archive of degree and doctoral theses. 2023.

5 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.

6 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.

7 Wu Z, Shang T, Guo A. Security issues in automatic dependent surveillance-broadcast (ADS-B): a survey. IEEE Access. 2020;8:122147–67.

8 Habler E, Bitton R and Shabtai A. Evaluating the security of aircraft systems. arXiv preprint arXiv:2209.04028, 2022.

9 Çevik N, Akleylek S. SoK of machine learning and deep learning based anomaly detection methods for automatic dependent surveillance-broadcast. IEEE Access. 2024;12:35643–62.

10 Karam R, Salomon M, Couturier R. A comparative study of deep learning architectures for detection of anomalous ADS-B messages. In 2020 7th International Conference on Control, Decision and Information Technologies (CoDIT). IEEE; 2020. Vol. 1, pp. 241–6.

11 Luo P, Wang B, Li T, Tian J. ADS-B anomaly data detection model based on VAE-SVDD. Comput Secur. 2021;104:102213,

12 Wang E, Song Y, Xu S, Guo J, Qu P, Pang T. A detection model for anomaly on ADS-B data. In 2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA). IEEE; 2020. pp. 990–4.

13 Çevik N, Akleylek S. Comparison of machine learning based anomaly detection methods for ADS-B system. In International Conference on Information Technologies and Their Applications. Cham: Springer Nature Switzerland; 2024. pp. 275–86.

14 Lin YH, Lin CE, Chen HC. Ads-b like UTM surveillance using APRS infrastructure. Aerospace. 2020:7(7):100.

15 Ajhari AA, Ibrahim R, Pramodana A, Pramudito JS, Tasyam JR, Hilmy W. ADS-B mobile ground station receiver flight surveillance architecture. In 2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST). IEEE; 2021. pp. 174–8.

16 Avula P. Automatic dependent surveillance broadcast (ADS-B) ground station. Eurocontrol. 2022.

17 Strohmeier M. Security in next generation air traffic communication networks [Doctoral dissertation]. University of Oxford; 2016.

18 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.

19 Ray G, Ray J. Detecting ADS-B replay cyberattacks in the national airspace system. Issues Inf Syst. 2023;24(1):170–85.

20 Burfeind BC. Interoperable ADS-B confidentiality [thesis]. Airforce Institute of Technology; 2020.

21 Strohmeier M, Lenders V, Martinovic I. Security of ADS– B: State of the art and beyond. DCS. 2013;17(2). doi:10.1109/COMST.2014.2365951

22 Leonardi M, Sirbu G. ADS-B crowd-sensor network and two-step Kalman filter for GNSS and ADS-B cyber-attack detection. Sensors. 2021;21(15):4992.

23 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(2):3322–34.

24 Stefanski J, Sadowski J. TDOA versus ATDOA for wide area multilateration system. EURASIP J Wirel Commun Netw. 2018;2018:1–13.

25 Abbass K, Qasim MZ, Song H, Murshed M, Mahmood H, Younis I. A review of the global climate change impacts, adaptation, and sustainable mitigation measures. Environ Sci Pollut Res. 2022;29(28):42539–59.

26 ODonnell KJ. Exploring strategies human-computer interaction specialists need to improve ADS-B Console Functionality for ATC controllers in the United States [Doctoral dissertation]. Colorado Technical University; 2020.

27 Karam R. Automatic detection of business data anomalies with deep learning and application to the ADS-B protocol [Doctoral dissertation]. Université Bourgogne Franche-Comté; 2022.

28 Batuwangala E, Kistan T, Gardi A, Sabatini R. Certification challenges for next-generation avionics and air traffic management systems. IEEE Aerosp Electron Syst Mag. 2018;33(9):44–53.

29 Ponsard C, Grandclaudon J, Massonet P. A goal-driven approach for the joint deployment of safety and security standards for operators of essential services. J Softw Evol Process. 2021;33(9):e2338.

30 Abhale AB, Manivannan SS. Supervised machine learning classification algorithmic approach for finding anomaly type of intrusion detection in wireless sensor network. Opt Memory Neural Netw. 2020;29(3):244–56.

31 Xu P, Wei G, Song K, Chen Y. High-accuracy health prediction of sensor systems using improved relevant vector-machine ensemble regression. Knowl.-Based Syst. 2021;212:106555.

32 Balantrapu SS. Current trends and future directions exploring machine learning techniques for cyber threat detection. Int J Sustain Dev Through AI, ML IoT. 2024;3(2):1–15.

33 Paramita AS, Hariguna T. Comparison of K-means and DBSCAN algorithms for customer segmentation in e-commerce. J Digit Mark Digit Curr. 2024;1(1):43–62.

34 Rajendran A, Balakrishnan N, Ajay P. Deep embedded median clustering for routing misbehaviour and attacks detection in ad-hoc networks. Ad Hoc Netw. 2022;126:102757.

35 Zhang J, Pan L, Han QL, Chen C, Wen S, Xiang Y. Deep learning based attack detection for cyber-physical system cybersecurity: a survey. IEEE/CAA J Automat Sin. 2021;9(3):377–91.

36 Patil D, Rane NL, Desai P, Rane J. Machine learning and deep learning: Methods, techniques, applications, challenges, and future research opportunities. Trustworthy Artificial Intelligence in Industry and Society. 2024; pp. 28–81.

37 Squatrito A. Quatrit learning-based GPS jamming and spoofing detection [dissertation]. Embry-Riddle Aeronautical Univesity; 2024.

38 Swinney CJ. Winney classification at discrete frequencies using machine learning [doctoral dissertation]. University of Essex; 2023.

39 Ukwandu E, Ben-Farah MA, Hindy H, Bures M, Atkinson R, Tachtatzis C, et al. Cyber-security challenges in aviation industry: A review of current and future trends. Information. 2022;13(3):146.

40 Dave G, Choudhary G, Sihag V, You I, Choo KKR. Cyber security challenges in aviation communication, navigation, and surveillance. Comput Secur. 2022;112:102516.

41 Sarker IH. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Ann Data Sci. 2023;10(6):1473–98.

42 Lee J, Ni J, Singh J, Jiang B, Azamfar M, Feng J. Intelligent maintenance systems and predictive manufacturing. J Manuf Sci Eng. 2020;142(11):110805.

43 Shafique A, Mehmood A, Elhadef M. Detecting signal spoofing attack in UAVs using machine learning models. IEEE Access. 2021;9:93803–15.

44 Wei S, Fan Z, Chen G, Blasch E, Chen Y, Pham K. TADAD: Trust AI-based decentralized anomaly detection for urban air mobility networks at tactical edges. In 2024 Integrated Communications, Navigation and Surveillance Conference (ICNS); 2024. pp. 1–10.

45 Musleh AS, Chen G, Dong ZY. o survey on the detection algorithms for false data injection attacks in smart grids. IEEE Trans Smart Grid. 2019;11(3):2218–34.

46 Shah V. Machine learning algorithms for cybersecurity: detecting and preventing threats. Revista Espanola de Documentacion Cientifica. 2021;15(4):42–66.
47 Kenaudekar J. Anomalous Behavior Detection in Aircraft based Automatic Dependent Surveillance–Broadcast (ADS-B) system using Deep Graph Convolution and Generative model (GA-GAN) (independent thesis). 2022.
48 Liu J, Nogueira M, Fernandes J, Kantarci B. Adversarial machine learning: a multilayer review of the state-of-the-art and challenges for wireless and mobile systems. IEEE Commun Surv Tutor. 2021;24(1):123–59.
49 Khan H, Khan H, Ghafoor S, Khan MA. A survey on security of automatic dependent surveillance-broadcast (ADS-B) protocol: Challenges, potential solutions and future directions. IEEE Commun Surv Tutorials. 2024. doi:10.36227/techrxiv.23535726.v1
50 Sleem L. Noura HN, Couturier R. Towards a secure ITS: overview, challenges and solutions. J Inf Secur Appl. 2020;55:102637.
51 Chiocchio S, Persia A, Santucci F, Graziosi F, Pratesi M, Faccio M. Modeling and evaluation of enhanced reception techniques for ADS-B signals in high interference environments. Phys Commun. 2020;42:101171.
52 Rodriguez-Galiano VF, Castillo MS, Chica M, Chica-Rivas M. Machine learning predictive models for mineral prospectivity: an evaluation of neural networks, random forest, regression trees and support vector machines. 2015. doi:10.1016/j.oregeorev.2015.01.001
53 Rahmati O, Falah F, Naghibi SA, Biggs T, Soltani M, Deo RC, et al. Land subsidence modelling using tree-based machine learning algorithms. Sci Total Environ. 2019;672:239–52.
54 Afuwape AA, Xu Y, Anajemba JH, Srivastava G. Performance evaluation of secured network traffic classification using a machine learning approach. Comput Standards Interfaces. 2021;78:103545.
55 Ahmad G, Fatima NH, Abbas M, Rahman O, Alqahtani MS. Mixed machine learning approach for efficient prediction of human heart disease by identifying the numerical and categorical features. Appl Sci. 2022;12(15):7449.
56 Xu S, Song Y, Hao X. A comparative study of shallow machine learning models and deep learning models for landslide susceptibility assessment based on imbalanced data. Forests. 2022;13(11):1908.
57 Saini N. Multi-label Image classification to detect air traffic controllers' drowsiness using facial features (doctoral dissertation, Dublin, National College of Ireland). 2019.
58 Cervantes J, Garcia-Lamont F, Rodríguez-Mazahua L, Lopez A. A comprehensive survey on support vector machine classification: Applications, challenges and trends. Neurocomputing. 2020;408:189–215.
59 Yang Z, Wang C, Zhang Z, Li J. Mini-batch algorithms with online step size. Knowl-Based Syst. 2019;165:228–40.
60 Song X, Liu Y, Xue L, Wang J, Zhang J, Wang J, et al. Time-series well performance prediction based on long short-term memory (LSTM) neural network model. J Petrol Sci Eng. 2020;186:106682.
61 Siami-Namini S, Tavakoli N, Namin AS. The performance of LSTM and BiLSTM in forecasting time series. In 2019 IEEE International Conference on Big Data (Big Data). IEEE; 2019. pp. 3285–92.
62 Alqahtani H, Kumar G. Machine learning for enhancing transportation security: a comprehensive analysis of electric and flying vehicle systems. Eng Appl Artif Intell. 2024;129:107667.
63 Wang M, Fu W, He X, Hao S, Wu X. A survey on large-scale machine learning. IEEE Trans Knowl Data Eng. 2020;34(6):2574–94.
64 Khandker S, Turtiainen H, Costin A, Hämäläinen T. Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures. IEEE Trans Aerosp Electron Syst. 2021;58(4):2702–19.