Review

Advancements in ADS-B Security: A Comprehensive Survey of Vulnerabilities, Mitigation Strategies, System Requirements, and Emerging Research Trends

Waqas Ahmed *

Posted Date: 10 May 2024

doi: 10.20944/preprints202405.0586.v1

Keywords: ADS-B security; vulnerability analysis; threat assessment; mitigation strategies; security solutions; system requirements; research trends; aviation technology

Review

Advancements in ADS-B Security: A Comprehensive Survey of Vulnerabilities, Mitigation Strategies, System Requirements, and Emerging Research Trends

Waqas Ahmed

Department of Cyber Security Air University Islamabad, Pakistan
* Correspondence: waqaskhattak99@gmail.com

Abstract: The Automatic Dependent Surveillance-Broadcast (ADS-B) protocol stands as a cornerstone in modern aviation surveillance and Aircraft Traffic Control systems, integral to the NextGen project initiated by the US Department of Federal Aviation Administration (FAA) in 2005. ADS-B utilizes data links to autonomously broadcast Aircraft navigational and identification information to augment air transportation system capacity and safety. However, concerns regarding the protocol's security persist, particularly as its adoption expands. The unencrypted nature of transmitted aircraft data and the absence of robust authentication mechanisms render the protocol susceptible to exploitation by malicious actors. In this study, we comprehensively reviewed existing research in the field, identifying a crucial gap necessitating a holistic survey. Prior surveys have predominantly focused on specific aspects, such as vulnerabilities, attacks, or critiques of existing solutions. Our survey addresses this gap by thoroughly exploring the aviation system, providing readers with a nuanced understanding of ADS-B security. Utilizing a detailed SWOT analysis diagram, our paper delves into the vulnerabilities inherent in the ADS-B protocol outlines potential threats and scrutinizes various attack scenarios. We systematically categorize and analyze existing security solutions, considering cost-effectiveness, scalability, implementation complexity, and coverage against diverse attack vectors. Furthermore, we critically evaluate these solutions, elucidate ADS-B security requirements, discuss current challenges, and propose future research directions. This survey serves as a comprehensive resource for researchers and practitioners alike, shedding light on the multifaceted landscape of ADS-B security and paving the way for enhanced aviation system resilience in the face of evolving cybersecurity threats.

Keywords: ADS-B security; vulnerability analysis; threat assessment; mitigation strategies; security solutions; system requirements; research trends; aviation technology

1. Introduction

Since the 1920s, the prevalence of air traffic has steadily increased, leading to a growing number of Aircraft navigating the airspace [1]. The continuous expansion of air transport necessitates the enhancement of air surveillance systems to effectively manage the escalating volume of flights. Over the years, air transport has experienced consistent growth, a trend projected to persist. According to the International Air Transport Association, passenger numbers are anticipated to surpass 8 billion by 2037 [1]. With this sustained growth, it becomes imperative for ATC to adapt and accommodate the consistent increase in flight numbers. Meeting this challenge requires a simultaneous boost in the volume of surveillance techniques while maintaining robust safety standards. The ICAO introduced the GANP (Global Air Navigation Plan) to address this magnificent goal in the early 2000s [2]. Since its initiation, the GANP has experienced continuous development, serving as a universal standard to transform the air navigation system in a developing approach. The fundamental aim for ICAO is to determine a worldwide interoperable air navigation system, satisfying all users throughout every point of flight. This projected system meets agreed-upon safety standards, ensures environmental sustainability, and facilitates optimal economic operations. The GANP serves as a comprehensive framework to guide the evolution of air navigation, aligning with the dynamic landscape of the aviation industry [1].

High reliance on computer systems can be found in normal operations in aviation. Close connections are formed between aviation systems as information technology goes through developments that create a welcoming environment for new possibilities for attackers accessing the system. ICT (Information and Communications Technology) dependent disruptions and numerous cyber-attacks are among these possibilities. With the economic growth, the number of consumers in the aviation industry is growing, marking the significance of securing aviation systems [3]. As per the FAA, the unprecedented growth of passengers is anticipated to be around 1.15 billion by 2033 [1]. Hence, an increase in space traffic is expected for the foreseeable future, requiring highly secure communication protocols to avoid unwanted incidents.

In 2004, the FAA of the US initiated a project called NextGen Air Transportation System to cater to future navigation demands, flight security, and airspace capacity [2,3]. The gradual transformation of land-based Air Traffic Control (ATC) systems sought in this project showed heavy dependency on radar and satellite-based navigation systems. ADS-B is the most important component of the NextGen project. In contrast to conventional radar-based systems, ADS-B can provide accurate information on aircraft positioning in real-time. Also, low maintenance costs and longer service life are promised by this system. In particular, the maintenance and construction costs were reduced by one-tenth of their predecessor [3,4]. Since 2020, the American Federal Regulations 14 CFR 91.225 and 91.227 have mandated that Aircraft installed with an ADS-B OUT device be out in the most controlled and secure air space [4]. However, the comprehensiveness, internet connectivity, and systems' interoperability that come with it have introduced new weaknesses to the systems that are worth confronting. The proposed research highlights and confronts system weaknesses to improve security [5].

During the 1990s, implementing RF (Radio Frequency) communication technology was laborious and expensive. It was intended to function as a secure means of communication. Nevertheless, preserving ADS-B communications' confidentiality was not a primary concern. The official standard [6] established by the Radio Technical Committee (RTC) does not address this matter, nor do any of the pertinent demand files [7,8] of security discussions address it. A significant technological advancement, namely the Software Defined Radio (SDR), has enabled hackers to execute radio frequency (RF) signal transmission and signal reception at a minimal expense. ADS-B is vulnerable to a multitude of assaults on account of its deficient security measures and the employment of an exposed, unencrypted protocol for information dissemination. Following substantial attention from the general public and numerous security conferences [9,10], it garnered considerable coverage in the mainstream media [11–13].

Researchers have identified and verified the vulnerability of ADS-B protocol to security breaches by utilizing pre-existing hardware and software [14]. The ICAO incorporated civil aviation safety into the agenda of the 12th Air Navigation Conference in light of the considerable attention it received from the media. Considering cyber security as a significant implementation impediment, the group established a working committee to facilitate stakeholder collaboration [15]. ADS-B lacks a contingency plan to verify the position in the case of a transmitter failure, notwithstanding the absence of an attack. Numerous perilous circumstances have arisen due to deficiencies in avionics equipment, most notably those concerning the Automatic Collision Avoidance System (ACAS) [16]. The aviation industry is progressively expressing apprehension regarding the viability of executing the NextGen deployment strategy in light of the security vulnerabilities present in ADS-B as 2024 approaches. As per the Ministry of Communication Attorney General, NextGen has expressed its intention to prolong the deployment beyond the initial projections [17]. The ADS-B security vulnerability must, therefore, be remedied promptly.

The aviation industry has three main components: communication, Navigation, and Surveillance, as shown in Figure 1 [18]. Communication is the exchange of data between Aircraft and ATC; navigation is the process of extracting, processing, broadcasting, and controlling the Aircraft's seamless, accurate, and reliable position; and ATC uses Surveillance systems to calculate the Aircraft's accurate position in the airspace.

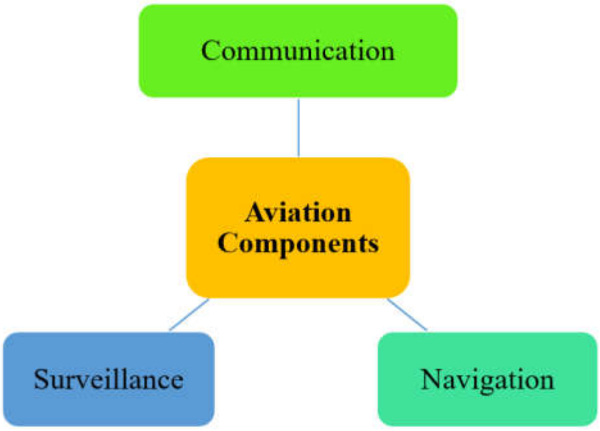


Figure 1. Aviation industry components.

1.1. Research Motivation

Since 2020, the FAA has mandated the ADS-B system for all commercial Aircraft globally. Several researchers published survey papers, as mentioned in Table 1, and research papers on ADS-B security and vulnerabilities, as mentioned in Tables 4 and 5. However, to the best of our knowledge, the existing survey papers didn't cover the ADS-B comprehensively as per Table 1 attributes. The research motivations for writing this survey paper on ADS-B security are as follows:

- To comprehensively identify and discuss the vulnerabilities of the ADS-B system and explore potential exploitation scenarios.
- To assess and acknowledge the limitations of existing security solutions, emphasizing their inability to offer complete defense to the ADS-B system and their lack of practical implementation in real-world scenarios (experimental phase).
- To evaluate existing security solutions from multiple perspectives, including cost-effectiveness, implementation difficulty, scalability, and coverage against potential attacks.
- To highlight the challenges and obstacles researchers face in developing holistic security solutions tailored to the unique complexities of the ADS-B system.

Table 1. Comparison of the Proposed Survey with Existing Surveys.

Ref. & Year	Aviation Security	Security Analysis	Security Analysis Diagram	Security Solution Analysis			Security Requirements	Research Direction
				Cryptography	Non-Cryptography	ML/DL		
[1] 2023	×	✓	✓	✓	✓	✓	×	×
[2] 2022	✓	✓	×	✓	×	×	✓	×
[3] 2020	×	✓	×	✓	✓	×	✓	✓
[4] 2017	✓	✓	×	✓	✓	×	×	✓
[5] 2015	×	✓	×	✓	✓	×	✓	✓
[6] 2014	✓	✓	×	×	×	×	×	✓
[7]	×	✓	×	✓	✓	×	×	×

2013								
[8] 2011	✓	✓	×	×	×	×	✓	×
Proposed Survey	✓	✓	✓	✓	✓	✓	✓	✓

1.2. Research Objectives

The proposed research survey discussed ADS-B vulnerabilities, possible attacks, and the drawbacks of existing solutions. The research survey conducted a detailed security analysis of the ADS-B system with the help of a diagram and analyzed existing security solutions and security requirements. The objectives of the proposed research survey included: -

- Offer a detailed overview of the aviation system to enhance readers' understanding of ADS-B technology and its security implications.
- Provide an in-depth analysis of ADS-B vulnerabilities, potential threats, and attack vectors supported by illustrative diagrams.
- Evaluate existing security solutions based on cost-effectiveness, scalability, implementation complexity, and coverage against various attack scenarios.
- Identify the security requirements and challenges in ADS-B systems and propose future research directions to address emerging threats and enhance system resilience.

In addition to the above, the proposed research survey is compared with the existing research survey published by well-known researchers based on selected attributes mentioned in Table 1. In this research survey, we discussed aviation security to familiarize readers with general aviation infrastructure and security protocols; presented a detailed security analysis of ADS-B from the perspective of threats, vulnerabilities, and attacks; and drew a SWOT analysis diagram of the ADS-B. The survey categorized existing solutions into cryptography, non-cryptography, and ML/DL techniques. It also presented the security requirements for proposing a valuable framework for the security of ADS-B with future research directions.

1.3. Paper Structure

ADS-B is a wireless communication protocol. Commercial Aircraft use ADS-B protocol to broadcast their identity and navigation information for Surveillance. The rest of the survey paper is structured as follows: Section 2 provides a comprehensive overview of the aviation system to familiarize readers with the topic. Section 3 presents the summary of the ADS-B protocol, including protocol working, components, and message format, whereas section 4 analyzes ADS-B vulnerabilities, possible threats, and attacks. Section 5 critically examines the existing security solutions and presents valuable insights with drawbacks, whereas section 6 presents the requirements of the ADS-B security solution. Section 7 presents the future research directions for the researchers, whereas section 8 concludes the research survey. Table 2 presents the notation used in the proposed research survey.

Table 2. List of Notations.

Abbreviation	Description	Abbreviation	Description
ADS-B	Automatic Dependent Surveillance-Broadcast	ICT	Information and Communications Technology
NextGen	Next Generation	ATC	Air Traffic Control
FAA	Federal Aviation Administration	RF	Radio Frequency
ACAS	Automatic Collision Avoidance System	RTC	Radio Technical Committee
CPDLC	Controlled Pilot Data-Link Communication	VHF	Very High-Frequency
HF	High-Frequency	DL	Deep Learning
ILS	Instrument Landing System	ICAO	International Civil Aviation Organization
PSR	Primary Surveillance Radar	SSR	Secondary Surveillance Radar
ATM	Air Traffic Management	DSCN	Digital Satellite Communication Networks
NIST	National Institute of Standards and Technology	MPLS	Multiprotocol Labeled Switching
CA	Certification Authority	MAC	Message Authentication Code
ECDSA	Elliptic Curve Digital Signature Algorithm	IBE	Identity-Based Encryption
HAP	Holistic Air Protection	LSTM	Short-Term Long Memory
CNN	Conventional Neural Network	P2P	Peer-to-Peer

2. Overview of Aviation System

Before advancing toward ADS-B security, it is essential to understand the complexities of the aviation system's workings. Three main tasks are carried out by the wireless technologies and subsystems of the aviation system: communication, navigation, and surveillance [27]. In addition, the national security agency is mostly in charge of aviation safety. Figure 2 shows a comprehensive aviation system architecture [28]. The airplane must land at the airfield to complete a circuit. Satellites, ground stations, and peer aircraft all assist it in achieving this goal [29]. Send and receive audio and message communications, and the pilot uses communication protocols [30,31] including CPDLC, VHF, and HF between the satellite and ground station. It travels and lands reliably using navigational techniques (such as the ILS, VHF Omni-directional Range (VOR), and DME). PSR, SSR, and ADS-B technologies are among the surveillance protocols used by the ground station to track aircraft movement and identify airspace incursions [30]. These systems continue to function during an aircraft's flight and descent.

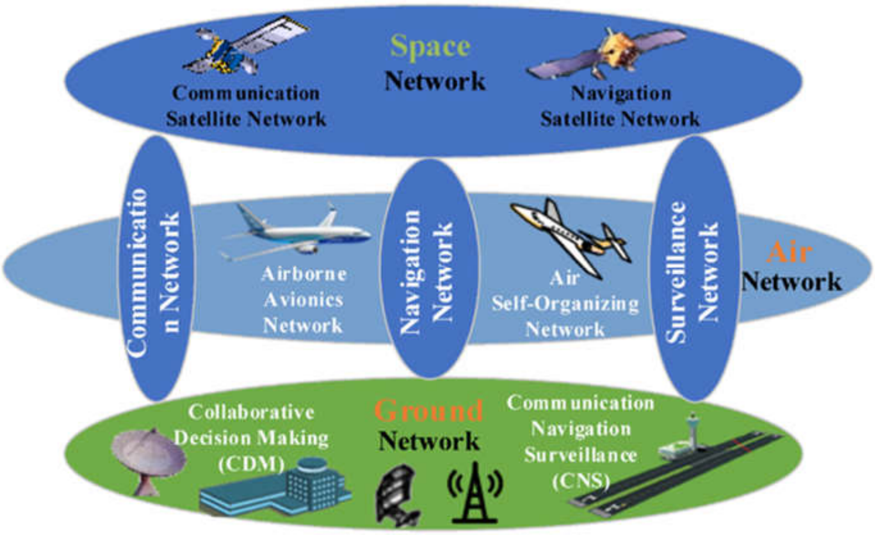


Figure 2. Overview of the Aviation System Architectural [28].

Aviation system connection is the monitoring of the ATM system. Consequently, the primary component of the ATM system is air traffic control [32], which is also utilized to connect satellites and Aircraft. Data centers are connected to the internet, and ATC links them to ground networks. Satellite and aircraft networks are managed by ground networks, among other things. The connection between the ground station and the Aircraft is essential to the operation of the aviation system. Usually, the task of initiating communication with an incoming aircraft falls to the ground station. According to [33], an ATC is part of a ground station that ensures connection with auxiliary ground units such as antennas, data centers, and ground radars.

ATC and aircraft voice communication must be maintained, and this is the duty of VHF and CPDLC [34]. CPDLC uses VHF data-link for message-based communication, whereas VHF is used for voice-based communication. Digital Satellite Communication Networks (DSCN) facilitate and enable satellite network operations. The protocol used for navigation and communication is called DSCN [30,34]. ILS, DME, and VOR are used to help in landing and navigation. The distance between the airplane and the station is computed via DME. A short-range VOR device assists in aircraft position determination and course maintenance. The ILS is in charge of directing the landing procedure. For surveillance purposes, PSR and SSR are used to identify airborne craft. ADS-B has recently been introduced to provide effective Surveillance between planes or in combination with a ground station [35]. With the stated essential protocols, the aviation system aids air traffic operations.

3. Overview of Automatic Dependent Surveillance-Broadcast (ADS-B)

ADS-B is a technology used in aviation for aircraft surveillance and tracking. In ADS-B, A stands for Automatic, which means the message transmission process is done automatically without human intervention; D stands for Dependent, which means the protocol is dependent on the aircraft navigation system and GPS; S stands for Surveillance, which means providing Surveillance to nearby Aircraft and ground stations; and B stands for Broadcast, which implies the information is shared with receivers without reception capability.

ADS-B technology allows Aircraft to transmit their precise location, including longitude, latitude, altitude, speed, and other data, to nearby Aircraft and the ground stations in the vicinity, as shown in Figure 3. This information is broadcast twice a second from the Aircraft's transponder and can be received from nearby Aircraft with the capability of ADS-B receivers and ATC [36]. ADS-B technology has several benefits over traditional radar systems, including improved accuracy, coverage, and reliability. It reduces the risk of mid-air collisions and makes ATC more efficient. Furthermore, ADS-B technology is becoming increasingly important as more countries are transitioning to ADS-B as the primary means of air traffic surveillance and management.

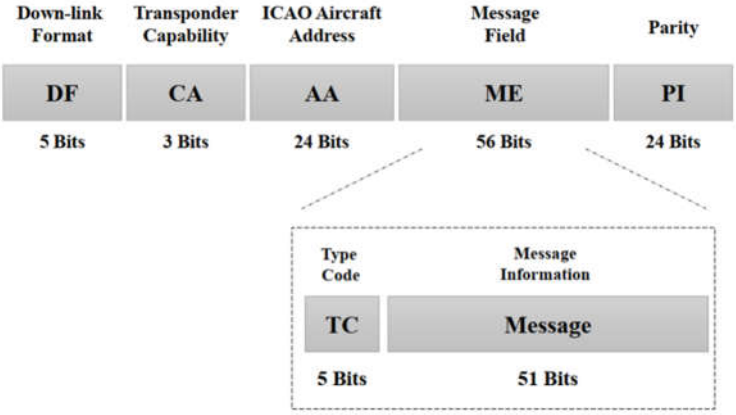


Figure 3. ADS-B Message Format.

ADS-B has two main functionalities: ADS-B Out and ADS-B In, as shown in Figure 4. ADS-B Out is carried out by Aircraft for automatic message broadcasting. It consistently transmits aircraft-related information, such as altitude, velocity, latitude, longitude, etc. The Aircraft carries ADS-B In to receive data from ATC and nearby Aircraft. It can also allow the pilots to view altitude, velocity, lateral position, aircraft category, flight numbers, and distance from nearby Aircraft in the airspace.

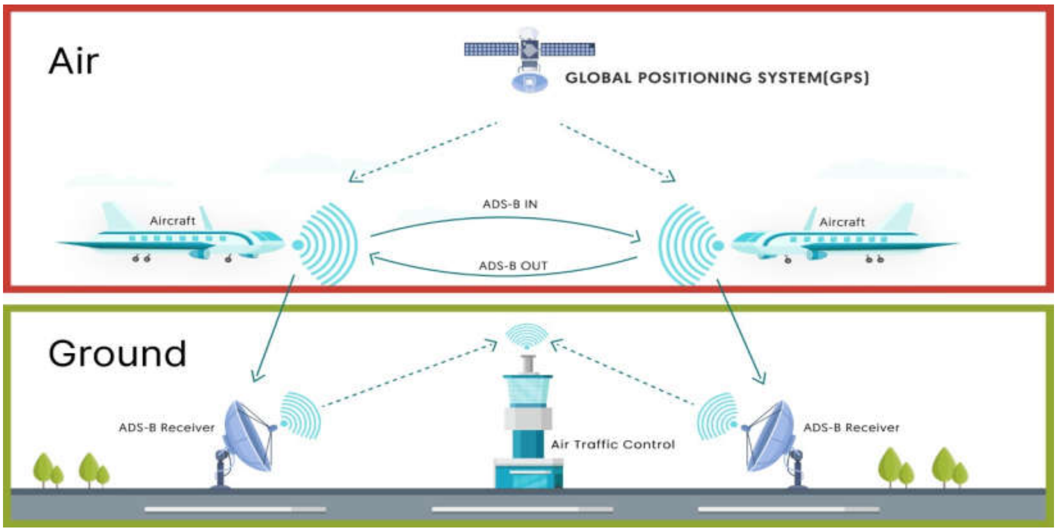


Figure 4. ADS-B Working.

Within the ICAO Aviation System Block Upgrades (ASBU) framework, Automatic Dependent Surveillance Broadcast (ADS-B) stands out as a promising technology for ATC surveillance. It serves as both a complement and an alternative to the long-standing PSR and SSR systems that have been in use since the 1970s. Two primary advantages underscore the efficacy of ADS-B in ATC surveillance. Its accuracy is notable, relying on GPS coordinates provided directly by the Aircraft through nearby satellites. Secondly, ADS-B offers a more straightforward and cost-effective alternative to traditional radar stations, making it an appealing choice for modernizing air navigation technologies. However, despite these advantages, ADS-B is not without its challenges. One significant drawback is its vulnerability to various cyber-attacks due to the protocol's inherent broadcasting of open clear-text messages on the 1090 MHz band. This susceptibility poses potential risks to the integrity and security of ADS-B data, necessitating careful consideration of cybersecurity measures to safeguard the system against possible threats.

4. Security Analysis of ADS-B

In this section, security concerns regarding the implementation of the ADSB are examined. The primary source of the vulnerabilities of the implementation is the tension between security objectives and the promotion of open information sharing.

4.1. ADS-B Vulnerabilities

Surveillance technology in aviation evolved to give rise to ADS-B. Although regulations in America and Europe have mandated that Aircraft be equipped with ADS-B, a collection of security problems remains inherited from adopting this system. The problem begins when the navigation and positioning information from the satellite is acquired by the Aircraft through its airborne equipment and GPS to perform real-time positioning for accurate determination of the Aircraft's current speed and current position, along with other information. Another issue emerges as the required parameters are obtained by sending equipment ADS-B from related airborne equipment for broadcasting through a digital data link [37].

ADS-B technology faces some serious security vulnerabilities. The transmission of aircraft data over the airwaves can be intercepted, spoofed, or otherwise manipulated, potentially compromising the safety and security of the aviation system. Therefore, there is a need to develop effective security measures to protect ADS-B technology and ensure its continued safe and reliable operation. The results of security certification and accreditation processes were disclosed to the public by the FAA in October 2009 [38]. The report expressed concerns from various entities, including the Department of Defence, concerning the possibility that malicious actors could intercept transmissions, exploit broadcasts to damage and target aircraft, and interfere with position and timing signals. Particular entities proposed the implementation of licensing and supervision protocols for ground receivers.

As per the report, the FAA undertook multiple evaluations of the security dimensions of ADS-B. Compliance with regulations set forth by the NIST on security objectives such as availability, integrity, and confidentiality necessitated the system's accreditation and certification. The report [22] asserts:

"the FAA assessed the vulnerability risk associated with using ADSB broadcast messages to target air carrier aircraft in particular." The current assessment includes Sensitive Security Information, subject to the regulations outlined in 49 CFR Parts 1 and 1520. Apart from that, the data it comprises is protected from being disclosed to the public. While the agency refrains from offering commentary on the study's data, it can affirm, in response to the remarks expressed throughout this rulemaking procedure, that the application of ADS-B data does not augment the existing level of risk to an aircraft".

The FAA has concluded from its investigation that there is no more risk associated with the intentional insertion of bogus targets into ADS-B transmissions than with the current SSR transmissions. Furthermore, the FAA declares that because the ADS-B surveillance information is integrated with main radar information before transmission for ATM (Air Traffic Management), the probability of deceit and interference is extremely low. Furthermore, encryption would unnecessarily complicate the worldwide deployment of ADS-B [39,40].

There are serious security issues with the FAA report. The main objective is to compare ADS-B's security concepts with modern operating systems [22]. Current secondary surveillance radar signals cooperate and reply to ground station probes (e.g., Modes A, C, and S). ADS-B, on the other hand, uses a continuous data broadcast technique. While the systems could have certain security features in common, it would be incorrect to assume they are equally open to attack. The risk of burglary for a home watched over by a dog cannot be compared to the risk for a home secured by an alarm system; each has unique weaknesses that may be targeted differently.

Verification of the data is also a challenge [38]. According to the FAA study, data and automation integration will reveal any discrepancies between the target provided by a radar system and the spoof or obstructed ADSB target. Given the prevalence of location mistakes in radar signals from artificial and natural objects, the system must come up with a way to determine the precise target. Regarding ADS-B message traffic error probability calculation, can ADS-B data be considered more accurate than radar data? Is there a plan to use operational testing to confirm that the system correctly identifies the intended target even in the event of malicious traffic injections? [22].

It is essential to acknowledge that the precise functional properties are still unknown. When ADS-B is fully operational, the main radar systems will likely be eliminated. The FAA Final Ruling [38] also addresses the security concerns of data fusion. Furthermore, the NextGen deployment strategy names ADS-B as the primary surveillance technology [41]. Ultimately, it is clear from past events that an adversary with the right kind of motivation may take advantage of data linkages that are not secured. In 2009, the US forces captured a Shite insurgent, and his laptop was discovered to have video files from Predator broadcasts [42]. There is no encryption on the communication channel between a predator and a local ground force. It was determined that the terrorists used the $26 piece of software SkyGrabber to intercept the unencrypted Predator footage. The same vulnerability is associated with the 1997 mission in Lebanon, where Hezbollah ambushed Israeli operators and killed them in the process. Hezbollah used surveillance film that they had obtained from Israeli uncrewed planes to carry out their attack [43].

4.2. ADS-B Vulnerabilities Exploits

Preliminary apprehensions emerged in 2006 regarding the capacity of malicious actors to populate air traffic controller radar displays with up to fifty fictitious targets [44]. Former chairman of the Civil Aviation Administration of Australia, Dick Smith, stated that this could be accomplished with a $5 antenna, a laptop computer, and a general aviation transponder. Smith further cautioned that adversaries could trace military flights and monitor law enforcement agents' movements through real-time positioning broadcasts [44]. Plane Finder AR, an app for Android and iOS devices that allows for accurate airplane monitoring using ADS-B signals, was released in 2010 [45]. A user may identify a nearby aircraft by pointing their mobile device into the sky, and the app will tell them the plane's name, position, altitude, takeoff, destination, and likely course. According to the creators, over two thousand apps were downloaded in the first month after their release.

For instance, the system will transmit data from a ground station to the ATC using AT&T's multiprotocol labeled switching (MPLS) network [46]. Although data connection is the primary emphasis of this research, it acknowledges that network backbone security is critical for ADS-B adoption. Concerns about the security of MPLS networks are discussed in greater depth in [47]. Security assessments often look at availability, confidentiality, and integrity. Refuting apparent flaws without actual proof is challenging. These principles were evaluated according to the FAA's security accreditation and certification criteria [26]. Secrecy does not exist in the absence of unfettered broadcasting or encryption. Without authentication or verification procedures, data integrity is at risk. The capability to jam signals might impact the system's availability. To carry out any surveillance activity, ADS-B requires an open and, by extension, risky way. Using ADS-B raises the stakes for bad actors looking to exploit these flaws [22]. Figure 5 presents a detailed security analysis of the ADS-B system. The security analysis divided the ADS-B system into 4 parts: threats, strengths, opportunities, and system weaknesses.

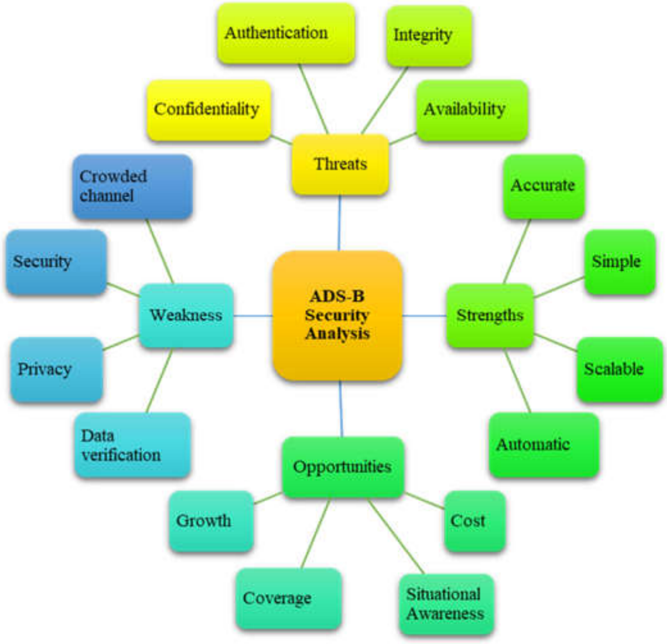
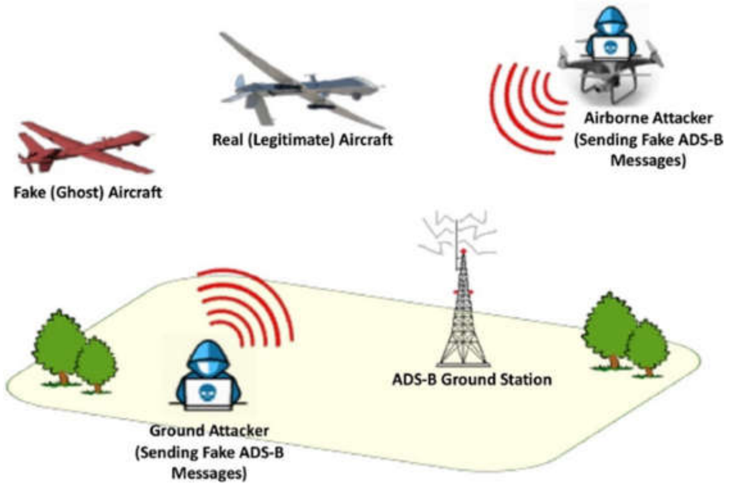


Figure 5. ADS-B Security Analysis.

4.3. ADS-B Attacks

The lack of a built-in security mechanism and its open communication makes ADS-B vulnerable to several attacks, including message deletion, injection and modification attacks, jamming, eavesdropping, spoofing, etc.) [48]. Figure 6 illustrates a message injection attack on the ADS-B system [40].



Real (Legitimate) Aircraft
Airborne Attacker (Sending Fake ADS-B Messages)
Fake (Ghost) Aircraft
ADS-B Ground Station
Ground Attacker (Sending Fake ADS-B Messages)

Figure 6. Message Injection Attack.

- *Message Injection Attack*: This is a type of attack in which an attacker sends nonlegitimate ADS-B messages to nearby Aircraft and ATC. These nonlegitimate messages deceive the system into believing that an aircraft is flying at a different altitude or location or on a different course than its original location. This attack can create a dangerous situation and confuse ATC and the pilots. Message injection attacks violate the authentication of the ADS-B protocol. In [49], the authors investigate the impact of message injection and spoofing attacks on ADS-B.
- *Message Deletion Attack*: An attack in which an attacker intercepts and deletes legitimate messages broadcast by other Aircraft in the surroundings. From an ATC and aircraft point of view, ADS-B messages are critical because they provide real-time information about Aircraft, such as current altitude, speed, and other important information. An attacker can cause accidents or confusion

by deleting ADS-B messages and hiding the Aircraft's status and location from ATC. Message deletion attacks violate the Integrity of ADS-B protocol. In [50], the authors discuss two strategies for deleting a legitimate ADS-B message.

- *Message Modification Attack*: In a message modification attack, the attacker intercepts a legitimate broadcast message by violating ADS-B confidentiality and modifying different message values, such as altitude, speed, etc. The modified message is transferred to ATC, making it difficult for ATC to track the Aircraft's updated location and status. Message modification attacks violate the Integrity of the ADS-B protocol. In [51], authors proposed a mechanism for injecting and verifying a modified message in the ATC system.
- *Eavesdropping Attack*: An attack in which an attacker intercepts and listens to legitimate messages broadcast by Aircraft. These messages contain critical data related to Aircraft, such as altitude, position, etc. The intercept messages also provide sensitive information to the attacker, such as flight status and path. In [52], the authors discuss and implement multiple methods of passive attacks, such as eavesdropping. Eavesdropping violates the confidentiality of ADS-B protocol.
- *Jamming Attack*: Transmitting similar high-power radio signals on a frequency similar to that used by aircraft for communication can prevent air traffic controllers from receiving legitimate ADS-B messages. This attack will disrupt communication between air traffic control and air, creating difficulties for pilots in receiving instructions from air traffic controllers. Message jamming attacks violate the availability of ADS-B protocol. In [52], the authors discuss and implement multiple methods of active attacks, such as eavesdropping. Table 3 presents a summary of ADS-B Attacks.

Table 3. Possible Attacks Summary.

Sr#	Attack	Sub-Attacks	Attack Purpose	Attack Method
1.	Eavesdropping	Reconnaissance attack	Getting aircraft information is also called aircraft reconnaissance.	Using an ADS-B receiver, obtain the corresponding airspace data.
2.	Jamming	Denial of service, flooding attack	Jam ADS-B communicates for a certain amount of time in a specific airspace.	Transmit high-frequency signal on the targeted frequency band (1090ES)
3.	Message Injection	Ghost injection	To mislead ATC in the targeted airspace, inject fake aircraft.	Using a power transmitting device generates and injects fake messages using relevant frequency.
4.	Message deletion	Aircraft disappearance	Deleted target field or complete message	At physical layers, flip the bits in the ADS-B message.
5.	Message modification	Virtual trajectory modification	Modify the content of the message	Implemented by combining message injection and deletion attack.

It is very important to raise awareness among air traffic controllers, pilots, and stakeholders about attacks on such a critical system. Management should train their employees involved in these activities to identify and respond to such attacks, such as the absence of ADS-B messages or disruptions in communication. The aviation industry can improve against these attacks by taking proactive measures and ensuring efficient air travel. Table 4 presents possible threats and their impact on the ADS-B system.

Table 4. Threats and its Impact on ADS-B System.

Threat	Impact on System
Interception	Protocol-insignificant but perhaps useful for malicious tracking
Data Manipulation	Message Integrity is compromised, leading to misleading or omitted collision avoidance alerts, confusion, and incorrect controller actions; Safety Hazard.
Identity Spoofing	The integrity of the message is undermined by fraudulent tracks utilized for deceiving air traffic control; Risk to Safety
Ghost Flights	False flight information is transmitted with the intention of perplexing controllers or overloading receiver processing capacity, compromising its dependability. Prudence for Safety
Disappearance of Original Flight	This is accomplished by replaying the Aircraft's previous flight data before its presence in the coverage area, thus preventing the dissemination of the most recent flight information.

5. Analysis of Existing Solutions

This section summarizes the merits and demerits of the existing solution in terms of ADS-B feasibility and security. As discussed earlier, the existing solutions are not optimal from the perspective of impact on the system. To secure the ADS-B system, the existing security solutions required modifications in the ADS-B infrastructure. The feasibility of existing solutions is greatly reduced by not considering ADS-B system problems such as software and hardware compatibility and the burden on the 1090MHz channel.

Over the past few years, numerous researchers and industrial developers have introduced several security frameworks, some of which have enhanced existing ones to bolster the security of ADS-B. The proposed research survey categorized current security solutions into two primary domains: Cryptography and Non-Cryptography. Figure 7 visually represents this categorization. In the following subsections, a detailed explanation of each category will be drawn upon relevant literature to elucidate the concepts and approaches within each domain.

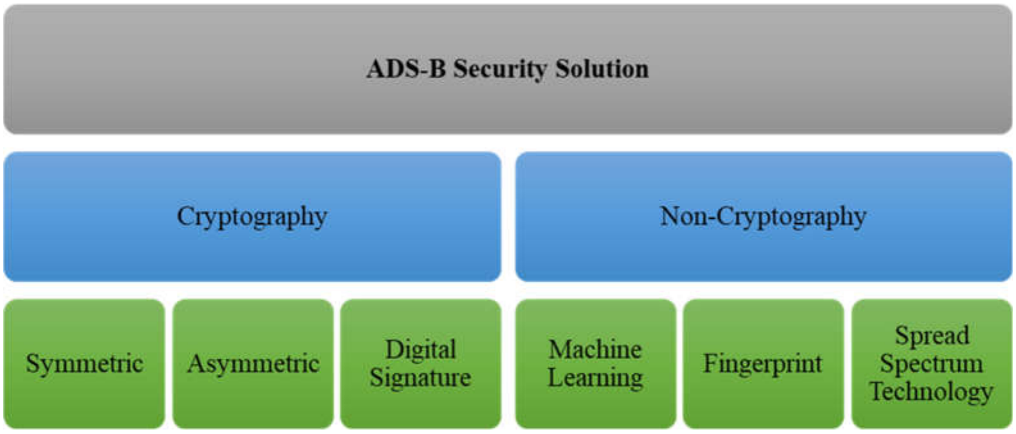


Figure 7. ADS-B Security Solution Classification.

5.1. Cryptography Schemes

Data encryption, encompassing both symmetric and asymmetric cryptography, stands as two pivotal techniques employed in fortifying the security of the ADS-B protocol. In this cryptographic paradigm, successful communication between parties, namely the sender and receiver, necessitates the utilization of a pre-shared secret key, commonly referred to as the secret key. However, the real-time exchange of this secret key presents formidable challenges, rendering this technique less than ideal for deployment in the ADS-B environment [53]. The inherent complexity and vulnerability associated with securely sharing secret keys underscore the potentially catastrophic consequences of a key leak during this process, jeopardizing the entire system's integrity.

Conversely, the encryption of ADS-B messages introduces a noteworthy dilemma, as it conflicts with the system's fundamentally open nature. Balancing operational requirements and flight safety, the Federal Aviation Administration (FAA) advocates for the transmission of unencrypted ADS-B data [11], emphasizing the delicate equilibrium that must be struck between security and the seamless functionality of this critical aviation protocol.

5.1.1. Symmetric Cryptography

It, also known as conventional or secret-key cryptography, is a technique where both parties use the same key for encryption and decryption. In this cryptography, both sender and receiver select a secret key. The selected secret key is used for both encryption on the sender side and for decryption on the receiving side [54]. To protect ADS-B messages in [35], authors proposed a framework based on encryption and MAC (Message Authentication Code). All active entities transfer ADS-B messages in plaintext in the proposed authentication framework. A MAC is attached to every broadcast ADS-B message to prove the entity authentication. To retain the protocol openness, all entities see the broadcast messages, whether the authentication process passed or failed. The proposed certification framework [35] is shown in Figure 8.

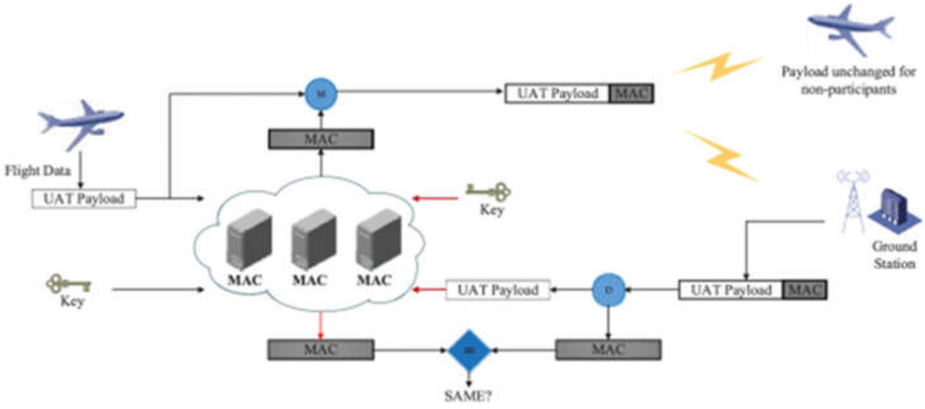


Figure 8. Message Authentication Code for Entity Identification Verification.

A similar framework based on encryption technology proposed by [55], both frameworks provides rough encryption as the authors didn't mention any encryption algorithms. The encryption framework of [35] is shown in Figure 9.

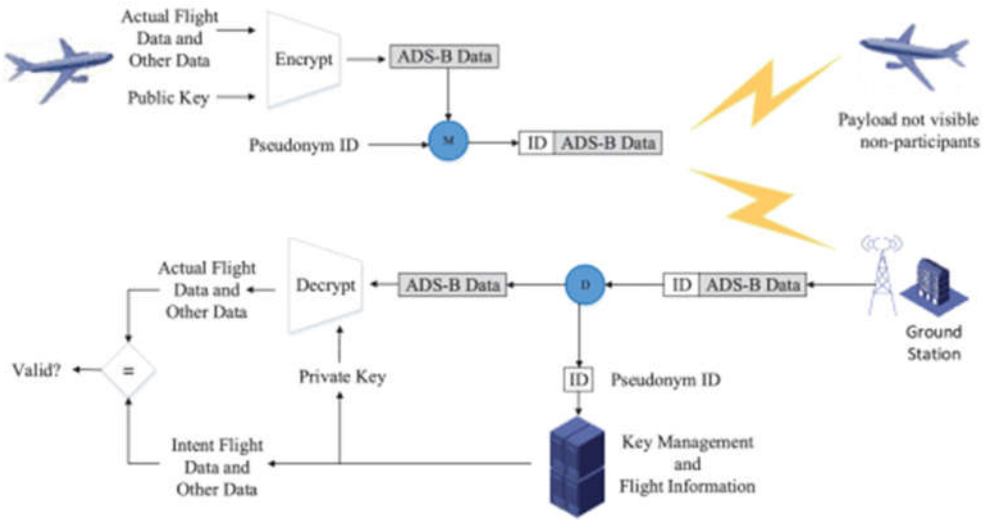

Actual Flight Data and Other Data
Public Key
Encrypt
ADS-B Data
Pseudonym ID
M
ID ADS-B Data
Payload not visible by non-participants
Actual Flight Data and Other Data
Decrypt
ADS-B Data
D
ID ADS-B Data
Ground Station
Valid?
=
Private Key
ID Pseudonym ID
Key Management and Flight Information
Intent Flight Data and Other Data

Figure 9. Encryption Framework.

Authors in [27] proposed a technique based on format-preserving encryption to protect ADS-B message integrity. The technique didn't confirm the standard block size of the ADS-B message. [38] also, assess the limitations of the traditional system presently used in the ATC and analyze reserved format encryption feasibility for the ADS-B protocol. Unlike [38] to preserve ADS-B protocol openness property for completed message encryption, authors in [56] also used reserved format encryption techniques. However, they only encrypt the AA of the message in place of complete encryption. From the applicability, security, and performance points of view of ADS-B messages, authors in [57] evaluated different reserved format algorithms. Authors in [58] discussed whether ADS-B broadcast messages could be secure using cryptography and also studied the flaws raised in the ADS-B system after incorporating symmetric encryption. The authors recommended public-key encryption for the ADS-B message integrity.

Authors in [59,60] presented different methods based on symmetric cryptography to ensure the Aircraft's identity and privacy by encrypting the whole ADS-B message. In this case, the participants who didn't have the keys will not have access to the ADS-B encrypted positional information, affecting the aircraft and flight safety. Traditional block cipher algorithms such as AES required extra padding to complete block size, increasing the ADS-B message length and burden on the 1090ES channel.

Researchers must develop a highly compatible and practically applicable solution based on symmetric cryptography to enhance and protect the security of the ADS-B messages' confidentiality and integrity.

5.1.2. Asymmetric Cryptography

Due to the open nature of ADS-B, it lacks security techniques for message integrity and authenticity, making it vulnerable to many attacks. In 2010, authors [61] proposed a data authentication scheme for ADS-B protocol based on asymmetric cryptography. The main idea of the paper [61] was to store, manage, and distribute the cryptography keys using public key infrastructure, which required a lot of space for storage. The proposed scheme cannot apply due to the massive increase in inbound and outbound flights. In [62] and [63] the authors proposed a technique requiring a pair of keys for every use, which must be authenticated quickly. The authentication process of keys increases the calculation cost of the techniques.

In [64], the authors presented an authentication scheme for ADS-B messages. The proposed scheme used public key infrastructure to validate that all ADS-B messages are from registered Aircraft. To share symmetric keys, authors used asymmetric cryptography. The shared symmetric key verifies the message's integrity and authenticity [64]. To ensure the integrity and authenticity of the ADS-B transmitted data, the authors in [65] proposed a novel framework based on symmetric and asymmetric cryptography approaches. As per the author's results, the proposed framework minimized the computation overhead and increased message security. Figure 10 presents the proposed framework of [65].

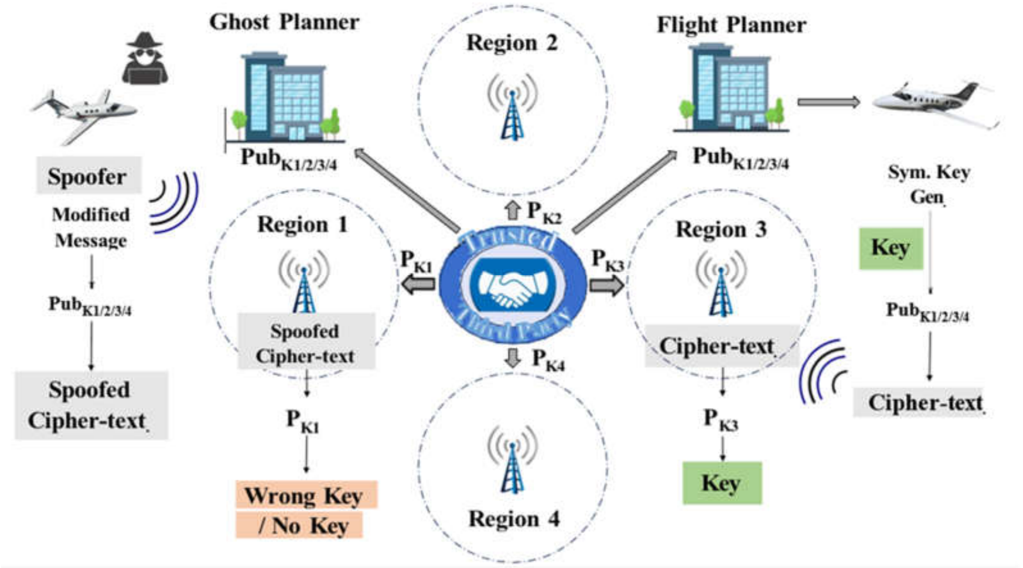


Figure 10. ADS-B Security Framework.

Authors in [66] proposed an ADS-B message authentication technique based on X.509 and an elliptic curve. The technique required a centralized CA (Certification Authority) to manage the aircraft certificate. The involvement of CA increased the ADS-B operation cost, including communication and computation costs. In asymmetric cryptography, to improve the signature efficiency based on ID-based online signatures, authors [67] proposed an authentication framework. Due to the ADS-B low-bandwidth data link, based on ID-based signature, authors in [68] proposed an authentication scheme with message recovery. The ADS-B message length is reduced in this scheme as the broadcast message can be retrieved from the ID-based signature, reducing ADS-B communication costs.

5.1.3. Digital Signature

Digital Signature is a cryptography approach used to verify message integrity and authenticity in a tamper-proof and secure manner. Digital signatures involve secret keys and mathematical algorithms to generate a unique signature for a message. Digital signatures preserve the ADS-B system openness property by not modifying the ADS-B message content. A digital signature guarantees the ADS-B message authentication and integrity with the help of signatures appended to every message [69].

An IBV signature technique proposed by [70] for ADS-B protocol is considered insecure as it can't pass the single message signature verification. The proposed techniques pass the batch/group verification. Authors in [71] proposed two YTBW1 and YTBW2 identity-based signatures and three levels of the ADS-B system. In [72], authors identified three weaknesses in the two identity-based signatures proposed by [71].

Asymmetric encryption schemes require a Centralized Authority (CA) in the ADS-B System to manage certificates. The involvement of CA increases the ADS-B system operating costs and complexity. In the existing signature-based ADS-B security solution, the signature length is large, which requires a high computation cost for the system. Such security solutions are not applicable in low-bandwidth data link systems like ADS-B. Table 5 presents a summary of cryptographic solutions.

Table 5. Summary of Cryptographic Solutions.

Ref. Year	Cryptographic Technique	Research Contribution	Strengths	Challenges
[9] 2006	Symmetric Cryptography	The authors proposed research surveys on the ADS-B potential solutions and security concerns.	Symmetric cryptography-based solutions are suitable for bulk data, with less overhead, speed and efficiency.	Challenges included data integrity, message authentication, key management, and exchange.
[5] 2014				
[10] 2020				
[11] 2013		The authors proposed an encryption algorithm based on FFX-A2 (Format Preserving)		
[12] 2017		Using Vector Homomorphic and FFX encryption, the authors proposed solutions for ADS-B message integrity and privacy.		
[13] 2022				
[14] 2012		Using IBE (Identity-Based Encryption) for key encryption and sharing and hybrid technique with symmetric cryptography for data.		
[15] 2017		Proposed a technique to address the problems of key sharing and authentication.		
[16] 2023	Asymmetric Cryptography	The authors proposed a solution based on a hierarchical signature technique based on a certificate-less signature technique utilizing aggregate signatures to reduce the processing time using key validation and setup processes through various communication components.	Asymmetric cryptography-based solutions are suitable for ADS-B message integrity, privacy, cryptography key distribution, message confidentiality and authentication.	Challenges included message overhead, increase in computational cost, performance, and key management.
[17] 2021				
[18] 2017				
[19] 2019		The authors proposed a lightweight protocol based on symmetric and asymmetric encryption for ADS-B message confidentiality. ATC plays the role of TTP in the proposed protocol to manage the session data and the encryption keys.		

[20] 2014		From the ADS-B security point of view, the authors discussed the suitability of ECDSA (Elliptic Curve Digital Signature Algorithm) from the perspectives of signature length and standard constraints.		
[21] 2019		To protect ADS-B message confidentiality and authentication, the author proposed a technique based on HAP (Holistic Air Protection) using an elliptic curve and certificates-based encryption.		
[22] 2019	Digital Signature	Based on the certificated less signature, the authors presented the ADS-B message authentication technique. The proposed technique is performance efficient and does not need any certificate management authority.	Digital signatures provide integrity, authentication, and non-repudiation to ADS-B message data.	Challenges included complexity, interoperability, algorithm performance and key management in a large space.

5.2. Non-Cryptography Schemes

As discussed, cryptography solutions are incompatible with the ADS-B system due to key generation, management, and distribution issues. On the other hand, non-cryptography techniques did not require key generation, management and distribution. Non-cryptography techniques included machine learning, spread spectrum and fingerprinting technology.

In recent years, Artificial Intelligence (AI) methodologies, including Machine Learning (ML) and Deep Learning, have experienced a surge in popularity. These approaches offer a diverse range of algorithms applicable across various domains, facilitating tasks such as prediction, regression, and classification. This versatility enables their application to a wide array of problem domains. Within the realm of cybersecurity, Machine Learning has become a prominent tool, being utilized for purposes such as anomaly detection, intrusion detection, and attack classification. The adaptability of ML algorithms makes them well-suited to address the dynamic and evolving nature of cybersecurity challenges, providing effective solutions in the identification and mitigation of cyber threats.

5.2.1. Machine Learning-Based Security Solutions

The classification of ADS-B attacks assumes a paramount significance, as it holds the potential to not only empower Air Traffic Control (ATC) controllers and security experts in augmenting existing security solutions but also aids in pinpointing the origin of the attacks. Numerous researchers have devised various machine-learning solutions to detect anomalies within ADS-B messages. Regrettably, the literature concerning machine learning-based automatic ADS-B attack classification remains limited. The available literature primarily dichotomizes ADS-B messages into two fundamental categories: malicious and non-malicious. This limitation underscores the need for further research and development in this critical area of aviation security.

In [83], the authors presented a machine-learning-based approach for classifying and detecting jamming attacks and highlighted the importance of machine learning in this research area. Different supervised learning models, including decision tree, support vector machine, artificial neural network and k-nearest neighbor, are implemented on a simulated dataset, and the accuracy is compared with the highest accuracy of artificial neural network (81%). In this research, authors selected energy statistics, bad packet ratio, and bit error rate as features to train the model on the simulated dataset and differentiate between legitimate and jamming signals. In this research paper, the authors only work on the jamming attack with a small dataset. In [83], the authors create a dataset using an ADS-B transmitter, as presented in Figure 11. The authors did not share the dataset for future research work.

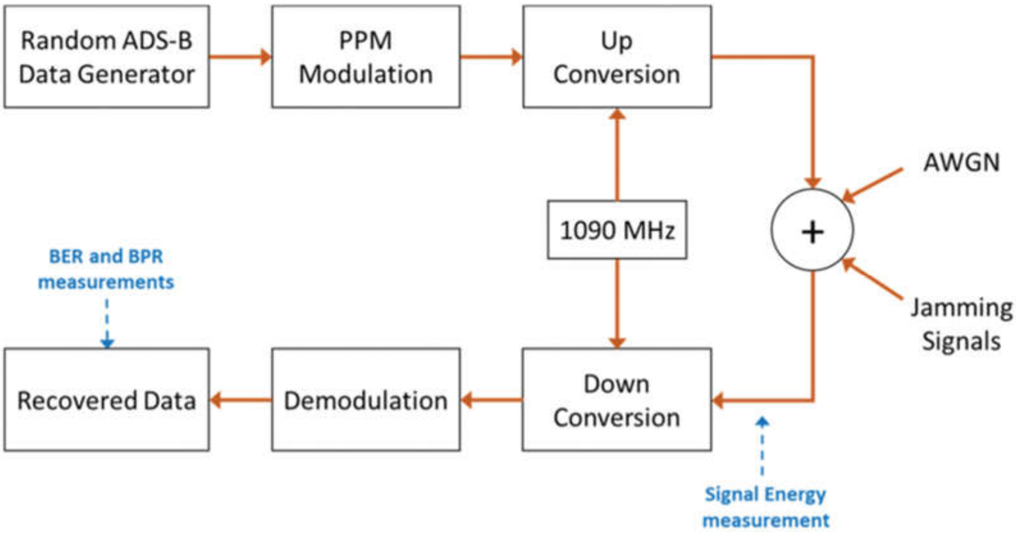


Figure 11. Block of Jamming Attack.

In [84], authors proposed a machine learning-based multi-class classification framework to improve the security of ADS-B by implementing random forest, support vector machines, and decision tree models to classify ghost aircraft and replay attacks. The authors performed several experiments on a dataset from fightRadar24 between Paris and Lisbon to evaluate and illustrate the research ideas. The author trained the model on a simulated dataset with 96.66% accuracy. The authors find that decision tree performance is best with 92% accuracy among the implemented models. The dataset size and accuracy are small, which is unacceptable in such a critical infrastructure environment. In [85], authors proposed a spoofing attack detection based on a two-step DNN for aircraft and message classification. Based on the PHY layer features used in this research work, the proposed framework allows ATC to examine every message and identify malicious messages.

In [86], the authors proposed a classification framework, shown in Figure 12, based on K-Nearest Neighbor, Logistic regression, and Naïve Bayes models. The authors generated a dataset using OpenSky API with different attacks: false squawk, false information, name jumping, and false heading attack. The authors used false alarm rate, precision, F1-Score, and recall to evaluate the performance of the proposed technique. The k-nearest Neighbor model outperforms other models with an accuracy of 99.57%. A real-time intrusion detection system for ADS-B is proposed by [87] using a Support Vector Machine model with 80% accuracy. The authors train the model on a dataset generated with the help of OpenSky.

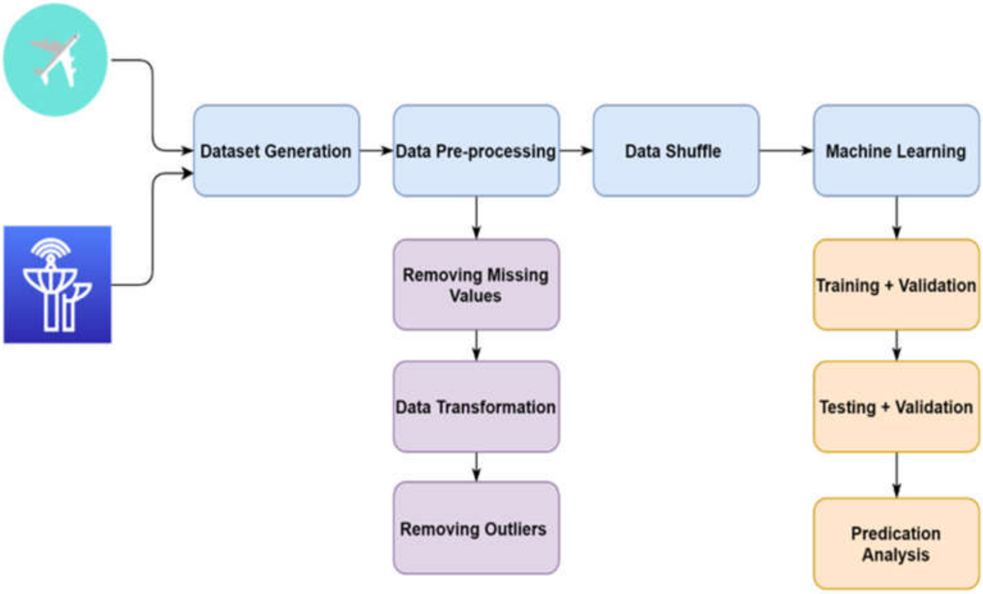


Figure 12. Machine Learning-Based Classification Framework.

A Short-Term Long Memory (LSTM) model based on deep learning architecture is proposed for detecting malicious ADS-B messages [88]. The model is trained on a dataset generated with the help of FlightRadar24, which contains data from 10 different aircraft. The model is trained on the OpenSky dataset with 91.59% testing accuracy. Based on the ADS-B messages sequence [86] designed, a message spoofing attack detection framework based on the LSTM model with 95.50% accuracy on the testing dataset.

From the perspective of ADS-B messages, a spoofing attack detection technique based on LSTM is proposed [89]. In this research paper, the author focused on three different ADS-B attacks: injection, jamming, and modification. The flowchart of the proposed technique is shown in Figure 13 [89]. Based on the sliding window, the ADS-B messages sequence is pre-processed and implemented in the LSTM network model with 93% accuracy [89]. To detect ADS-B spoofed data, [25] used adversarial learning techniques with 98.87% accuracy. The authors also used the Conventional Neural Network (CNN) technique for aircraft classification based on the ADS-B signals and I/Q samples with 99% accuracy.

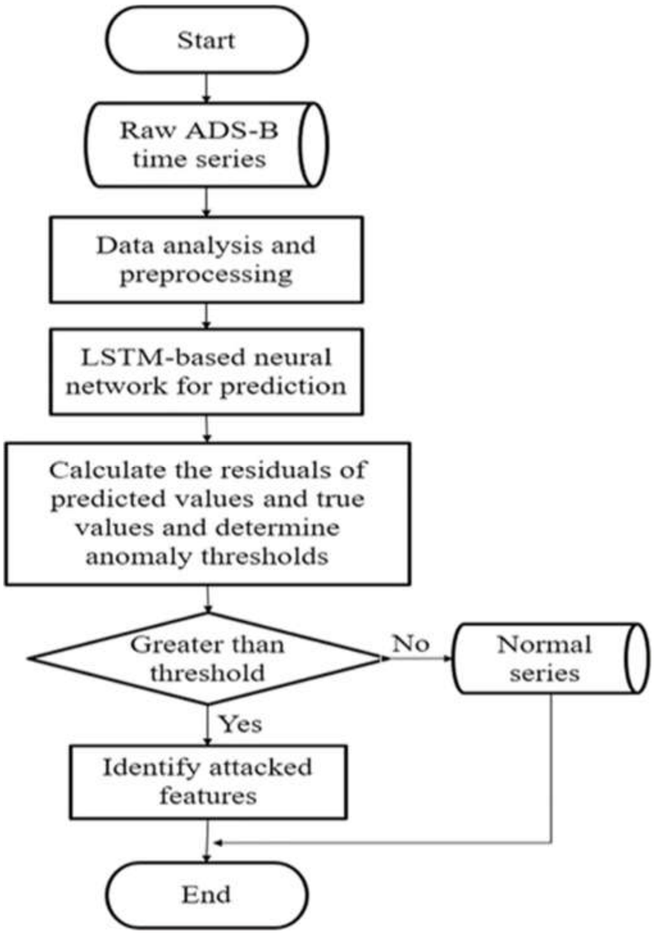

Start
Raw ADS-B time series
Data analysis and preprocessing
LSTM-based neural network for prediction
Calculate the residuals of predicted values and true values and determine anomaly thresholds
Greater than threshold
No
Normal series
Yes
Identify attacked features
End

Figure 13. LSTM-Based Spoofing Attack Detection.

To detect ADS-B message modification attacks, [90] proposed an LSTM Network based on a deep learning technique with 98% accuracy. The authors generated a small, simulated dataset containing malicious and non-malicious messages with the help of a false data generator tool. Based on an improved version of the LSTM model (Generative Adversarial Network) authors in [91], the proposed anomaly detection model for ADS-B data has 97% accuracy. The dataset is generated from FlightRadar24 API. Table 6 presents a comprehensive overview of the machine learning-based literature review.

Table 6. Summary of Machine Learning Approaches.

Year & Ref.	Dataset Description	ML Models	Accuracy
2022 [23]	Opensky (20 randomly chosen flights are downloaded from the OpenSky Network)	LSTM	98%
2021 [24]	FlightRadar24 (authors used a dataset containing messages of 1 flight from Lisbon to Paris)	SVM DT RF	91% 92% 90%
2021 [25]	OpenSky (the dataset containing 26000)	LR NB K-NN	52.10% 82.10% 99.57%

doi:10.20944/preprints202405.0586.v1

Year & Ref.	Dataset Description	ML Models	Accuracy
2021 [26]	Flightradar24 (authors didn't mention the details of the dataset)	LSTM with GAN	97%
2021 [27]	OpenSky (dataset with 20,000 messages, 10,000 legitimate and 10,000 nonlegitimate)	SVM	80%
2020 [28]	Simulated (authors didn't mention the details of the dataset)	LSTM	93%
2020 [29]	Simulated (18675 messages are collected for experiments)	GAN CNN	98.87 % 99%
2020 [30]	OpenSky (the author didn't mention the number of legitimate and nonlegitimate messages)	LSTM	91.59%
2019 [31]	Simulated (authors didn't mention the details of the dataset and number of messages used in the experiments)	LR SVM KNN ANN DT	65.6% 67.3% 74.6% 81% 74.2%
2019 [32]	Simulated (the dataset contains only 18675 messages, and the author didn't mention the number of legitimate and nonlegitimate messages)	DNN	96.66%
2018 [33]	Simulated (authors didn't mention the details of the dataset)	LSTM	95.50%

5.2.2. Fingerprint

A non-cryptography technique based on unique characteristics to identify devices such as radio circuits, operating systems, clocks, and drivers [95]. Location/channel-based, hardware-based, and software-based are three possible fingerprinting techniques used in the ADS-B system [96]. Location/channel-based fingerprinting based on channel impulse response, received signal strength, or carrier phase. Identify devices based on unique hardware characteristics such as clock skew, radio modulation signal, and turn-on/off transient called hardware-based fingerprinting. In contrast, software-based fingerprinting uses unique characteristics of software installed on hardware, such as behavior, patterns, etc. Fingerprinting techniques require a nonzero positive ratio, higher manufacturing cost, and sophisticated devices because of these techniques' statistical approach.

5.2.3. Spread Spectrum Technology

In wireless communication networks, a spread spectrum technology minimizes or stops eavesdropping and jamming, including frequency-hopping and direct sequence spread spectrum. The network entities (sender and receiver) must pre-share frequency hopping mode or spreading code while using this technology. This technology has issues similar to cryptography, including key generation, distribution, and management issues.

Authors in [97–99] discard the pre-shared spreading modes and codes problem. Unlike the previously shared spreading code, uncoordinated spread spectrum communication involves the sender and receiver not requiring prior sharing of the spreading code. Instead, they randomly switch between channels or employ spreading codes, making it difficult for attackers to effectively jam or eavesdrop on the channel. The drawback is the inefficient use of bandwidth resources, as communication parties (sender and receiver) are often not on a similar channel. Despite the spread spectrum technology's effectiveness in countering diverse attacks, its inherent limitations, such as extended time requirements and low performance, pose challenges for its application in ADS-B systems [98,99].

Table 7 compares existing ADS-B security solutions categorized in the proposed research survey based on compatibility, scalability, difficulty, and cost.

Table 7. Comparison of Security Solutions on Selected Attributes.

Category	Compatibility	Scalability	Difficulty	Cost
Symmetric Cryptography	Key management and sharing	Medium	High	High
Asymmetric Cryptography	Key generation, sharing, and storing	Medium	High	High
Message Authentication Code (MAC)	Key management and change message format	Medium	Low	Low
Machine Learning	Need to add software	High	Low	Low
Spread Spectrum	Change the system and add hardware	Medium	High	High
Fingerprinting	We need to add hardware, but there is no need to modify the system	Medium	Medium	High

6. Security Requirements

To design an effective and applicable security solution for securing ADS-B protocol from different attacks should fulfill the following security requirements:

- *Standard Compliance:* Security solutions must align with the updated version of the ADS-B protocol to ensure compliance with message format and communication logic.
- *Backward compatibility:* New security solutions should seamlessly integrate with existing systems, allowing aircraft that have yet to update their systems to continue operating.
- *No Modifications in Hardware*: The proposed security solution should require a simple software update without requiring hardware modifications in terms of maintenance and cost.
- *Limited Message Overhead*: Security techniques must introduce minimal additional message overhead to avoid congestion on the 1090ES frequency band.
- *Cryptography Elements:* Despite the limited message size in standard ADS-B packets, the solution's security level should not be compromised.
- *Packet Loss Events*: Given the prevalent packet loss phenomena in the 1090ES frequency band, effective security solutions should demonstrate resilience against incomplete packet reception caused by obstacles and other factors.

7. Challenges and Future Research Directions

ADS-B stands out as a leading protocol within ATC. Its principal strengths stem from leveraging GPS as a location provider, resulting in heightened location accuracy. Furthermore, it presents a cost-effective alternative with significant operational expenses and lower deployment compared to traditional radar technologies. ADS-B augments radar coverage and functions independently in areas missing radar support. Although these notable benefits, the broader adoption of ADS-B faces constraints due to associated security vulnerabilities, primarily linked to the protocol's open broadcast of clear-text messages. This side has raised alarms about the potential exploitation of security loopholes. Despite the gravity of the abovementioned concerns, only a few researchers have endeavored to propose effective strategies for moderating such vulnerabilities.

The ADS-B protocol is a valuable complement to radar-based ATC and a feasible replacement in regions where radar implementation is impractical. However, a notable concern arises because ADS-B messages lack inherent integrity or authenticity, making them susceptible to manipulation using affordable hardware and open-source software. This vulnerability stems from the absence of mechanisms ensuring the credibility and security of transmitted data. Addressing this issue is complex, primarily due to the impracticality of modifying the ADS-B message format. Such modifications would render the already extensively implemented base obsolete, posing a significant challenge in enhancing the protocol's security without disrupting existing systems. This underscores the need for innovative solutions that balance maintaining compatibility with current infrastructure and fortifying the security of ADS-B transmissions against potential tampering.

In the future landscape of aviation, the anticipated growth in the number of Aircraft in the airspace poses a challenge, potentially leading to congestion and a surge in ADS-B messages. Addressing the need for swift and accurate reception and processing of these messages while expanding the transmission range on the ADS-B 1090ES frequency to mitigate message loss and congestion is a key focal point for further investigation.

- *Blockchain Integration:* Blockchain, a composite system incorporating P2P (peer-to-peer) networks, smart contracts, consensus mechanisms, and cryptography, emerges as a promising solution for secure data sharing in an untrusted network. Blockchain is an exceptional public trust technique that applies to ADS-B protocol, using group certification techniques for ADS-B message integrity and authentication. The researchers should focus on the blockchain's usability in forthcoming research endeavors in ADS-B security. Pioneering work by authors in [21] introduced blockchain technology for identity recognition employing P2P technology for distributed data storage and authentication. This technique showcases high security, reliability, and scalability, offering identity authentication across different infrastructures [104]. Articles such as "Aviation Blockchain Infrastructure" (ABI) propose leveraging blockchain for effective, secure, and private communication between Aircraft and authorized individuals [100].
- *Machine Learning Applications*: Given the importance of abnormal data detection, particularly in a non-encrypted and open protocol like ADS-B, machine learning (ML) provides a compelling solution. In recent years, a surge in anomaly detection techniques based on ML has been witnessed, with deep learning gaining prominence in various domains. Deep learning and machine learning applications will play vital roles in anomaly detection in the ADS-B system. The time series algorithm can enhance detection efficacy by augmenting feature dimensions by leveraging the qualities of rapid ADS-B message updates with accurate time correlation and utilizing deep learning and machine learning models for detecting malicious ADS-B messages. This approach ensures compatibility with existing ADS-B protocols without additional sensors. Numerous articles, including works by [101]–[103], illustrate using deep learning techniques or LSTM networks to enhance ADS-B system security.
- *Multi-layered Security Framework*: The existing security solutions proposed by researchers failed to protect ADS-B from attack as they only provide a certain level of security. Researchers must design and test a security framework based on multi-layered security that can detect and defend ADS-B systems from different attacks.
- *High Attack Detection with Low False Alarm*: Researchers face challenges in developing an attack detection method with low false alarms and high attack detection probabilities. The existing security solutions published by researchers have fundamental implementation limitations. To implement existing methods, researchers have to modify the infrastructure of the ADS-B system or the ADS-B message format. Most importantly, the developed solutions are not tested in a real-

time environment, which will affect the method's efficiency. ADS-B system requires a security solution that overcomes the mentioned limitations.

8. Conclusions

To enhance air transportation safety, the NextGen project launched by the FAA's US Department in 2005 represents a significant stride. However, as NextGen, particularly its core element, the ADS-B protocol, continues to be implemented, researchers have encountered potential security vulnerabilities. The examination of ADS-B security has illuminated the inherent risks accompanying its deployment. Over recent years, numerous research papers have tackled solutions for the ADS-B protocol, categorizing them into cryptography and non-cryptography-based solutions. In this context, our survey delves into machine learning and deep learning-based solutions within the non-cryptography realm, providing valuable insights into aviation security, ADS-B vulnerabilities, existing security solution analyses, and pertinent future research directions. Our survey aims to comprehensively identify ADS-B security vulnerabilities and associated attack vectors, raising awareness within the research community. The existing body of research strongly advocates upgrading security measures to mitigate these vulnerabilities effectively. This necessitates a strategic approach encompassing meticulous planning, thorough testing, a robust operational life cycle, and seamless implementation to enhance the system's resilience.

It is crucial to note that the perspectives presented in our survey are gleaned from existing research papers and do not replicate official policies or reports. Nonetheless, our survey serves as a valuable resource, contributing to ongoing efforts to fortify ADS-B security and ensure the continued safety and reliability of the aviation system.

References

1. Z. Wu, T. Shang, and A. Guo, "Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey," IEEE Access, vol. 8, pp. 122147–122167, 2020.
2. P. Jacob, R. P. Sirigina, A. S. Madhukumar, and V. A. Prasad, "Cognitive radio for aeronautical communications: A survey," IEEE Access, vol. 4, pp. 3417–3443, 2016.
3. S. Sciancalepore and R. Di Pietro, "SOS: Standard-compliant and packet loss tolerant security framework for ADS-B communications," IEEE Trans Dependable Secure Comput, vol. 18, no. 4, pp. 1681–1698, 2019.
4. C. Yang, J. Mott, and D. M. Bullock, "Leveraging aircraft transponder signals for measuring aircraft fleet mix at non-towered airports," International Journal of Aviation, Aeronautics, and Aerospace, vol. 8, no. 2, p. 1, 2021.
5. J. Baek, E. Hableel, Y. J. Byon, D. S. Wong, K. Jang, and H. Yeo, "How to Protect ADS-B: Confidentiality Framework and Efficient Realization Based on Staged Identity-Based Encryption," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 690–700, Mar. 2017, doi: 10.1109/TITS.2016.2586301.
6. R. (Firm). SC-186, Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance Broadcast (ADS-B). RTCA, 2004.
7. P. J. Martone and G. E. Tucker, "Candidate requirements for multilateration and ADS-B systems to serve as alternatives to secondary radar," in 20th DASC. 20th Digital Avionics Systems Conference (Cat. No. 01CH37219), IEEE, 2001, pp. 7C2-1.
8. C. Rekkas and M. Rees, "Towards ADS-B implementation in Europe," in 2008 Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles, IEEE, 2008, pp. 1–4.
9. A. Costin and A. Francillon, "Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," black hat USA, vol. 1, pp. 1–12, 2012.
10. B. Haines, "Hackers+ airplanes," No good can come of this. Defcon, vol. 20, pp. 26–29, 2012.
11. H. Kelly, "Researcher: New air traffic control system is hackable. CNN." 2012.
12. P. Marks, "Air traffic system vulnerable to cyber attack." Elsevier, 2011.
13. A. Greenberg, "Next-gen air traffic control vulnerable to hackers spoofing planes out of thin air," Forbes Magazine. Retrieved September, vol. 10, p. 2014, 2012.
14. M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28, 2013. Proceedings 11, Springer, 2013, pp. 253–271.
15. G. Dave, G. Choudhary, V. Sihag, I. You, and K.-K. R. Choo, "Cyber security challenges in aviation communication, navigation, and surveillance," Comput Secur, vol. 112, p. 102516, 2022.

16. T. L. Kraus, "Celebrating a history of excellence: the Federal Aviation Administration and Space Education Outreach Program.," 2011.
17. D. I. N. U. EQUIPAGE, “Audit Report,” 2014.
18. G. Dave, G. Choudhary, V. Sihag, I. You, and K.-K. R. Choo, "Cyber security challenges in aviation communication, navigation, and surveillance," Comput Secur, vol. 112, p. 102516, 2022.
19. H. Ahmed, H. Khan, and M. A. Khan, "A survey on security and privacy of automatic dependent surveillance-broadcast (ads-b) protocol: Challenges, potential solutions and future directions," Authorea Preprints, 2023.
20. S. Pennapareddy and K. Natarajan, "Securing ADS-B data transmissions using blockchain: a comprehensive survey and analysis," Aircraft Engineering and Aerospace Technology, vol. 95, no. 3, pp. 452–463, Jan. 2023, doi: 10.1108/AEAT-02-2022-0058/FULL/PDF.
21. Z. Wu, T. Shang, and A. Guo, "Security Issues in Automatic Dependent Surveillance-Broadcast (ADS-B): A Survey," IEEE Access, vol. 8, pp. 122147–122167, 2020, doi: 10.1109/ACCESS.2020.3007182.
22. M. Riahi Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system," International Journal of Critical Infrastructure Protection, vol. 19, pp. 16–31, Dec. 2017, doi: 10.1016/J.IJCIP.2017.10.002.
23. M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," IEEE Communications Surveys and Tutorials, vol. 17, no. 2, pp. 1066–1087, Apr. 2015, doi: 10.1109/COMST.2014.2365951.
24. M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, "Realities and challenges of nextgen air traffic management: the case of ADS-B," IEEE Communications Magazine, vol. 52, no. 5, pp. 111–118, 2014.
25. M. Strohmeier, V. Lenders, and I. Martinovic, "Security of ADS− B: State of the Art and Beyond," DCS, 2013.
26. D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," International Journal of Critical Infrastructure Protection, vol. 4, no. 2, pp. 78–87, Aug. 2011, doi: 10.1016/J.IJCIP.2011.06.001.
27. L. Chongrui et al., "Protecting aviation safety against cybersecurity threats," IOP Conf Ser Mater Sci Eng, vol. 1226, no. 1, p. 012025, Feb. 2022, doi: 10.1088/1757-899X/1226/1/012025.
28. X. Lu, R. Dong, Q. Wang, and L. Zhang, "Information Security Architecture Design for Cyber-Physical Integration System of Air Traffic Management," Electronics 2023, Vol. 12, Page 1665, vol. 12, no. 7, p. 1665, Mar. 2023, doi: 10.3390/ELECTRONICS12071665.
29. E. P. Paraschi, A. Georgopoulos, and M. Papanikou, "Safety and security implications of crisis-driven austerity HRM practices in commercial aviation: A structural equation modelling approach," Saf Sci, vol. 147, p. 105570, Mar. 2022, doi: 10.1016/J.SSCI.2021.105570.
30. G. Dave, G. Choudhary, V. Sihag, I. You, and K. K. R. Choo, "Cyber security challenges in aviation communication, navigation, and surveillance," Comput Secur, vol. 112, p. 102516, Jan. 2022, doi: 10.1016/J.COSE.2021.102516.
31. E. Ukwandu et al., "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," Information 2022, Vol. 13, Page 146, vol. 13, no. 3, p. 146, Mar. 2022, doi: 10.3390/INFO13030146.
32. J. Tang, G. Liu, and Q. Pan, "Review on artificial intelligence techniques for improving representative air traffic management capability," Journal of Systems Engineering and Electronics, vol. 33, no. 5, pp. 1123–1134, Oct. 2022, doi: 10.23919/JSEE.2022.000109.
33. Z. Rezo, S. Steiner, T. Mihetec, and O. Čokorilo, "Strategic planning and development of Air Traffic Management system in Europe: A capacity-based review," Transportation Research Procedia, vol. 69, pp. 5–12, Jan. 2023, doi: 10.1016/J.TRPRO.2023.02.138.
34. N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and S. Grundner-Culemann, "Security in Digital Aeronautical Communications A Comprehensive Gap Analysis," International Journal of Critical Infrastructure Protection, vol. 38, p. 100549, Sep. 2022, doi: 10.1016/J.IJCIP.2022.100549.
35. E. Valovage, "Enhanced ADS-B research," AIAA/IEEE Digital Avionics Systems Conference - Proceedings, 2006, doi: 10.1109/DASC.2006.313672.
36. X. Boyen, "A tapestry of identity-based encryption: practical frameworks compared," International Journal of Applied Cryptography, vol. 1, no. 1, pp. 3–21, 2008.
37. E. Chan-Tin, D. Feldman, N. Hopper, and Y. Kim, "The frog-boiling attack: Limitations of anomaly detection for secure network coordinate systems," in Security and Privacy in Communication Networks: 5th International ICST Conference, SecureComm 2009, Athens, Greece, September 14-18, 2009, Revised Selected Papers 5, Springer, 2009, pp. 448–458.
38. C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system," International Journal of Critical Infrastructure Protection, vol. 6, no. 1, pp. 3–11, Mar. 2013, doi: 10.1016/J.IJCIP.2013.02.001.
39. N. S. Joseph, C. Banerjee, E. Pasiliao, and T. Mukherjee, "FlightSense: A Spoofer Detection and Aircraft Identification System using Raw ADS-B Data," Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020, pp. 3885–3894, Dec. 2020, doi: 10.1109/BIGDATA50022.2020.9377975.

40. M. Riahi Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," Comput Secur, vol. 85, pp. 386–401, Aug. 2019, doi: 10.1016/J.COSE.2019.05.003.
41. "FAA Reauthorization Act: Progress and Challenges Implementing Various Provisions of the 2012 Act." Accessed: Dec. 23, 2023. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1102097
42. S. Gorman, Y. J. Dreazen, and A. Cole, "Insurgents hack US drones. The Wall Street Journal." Upd. Dec, 2009.
43. Y. Katz, "IDF encrypting drones after Hezbollah accessed footage," Jerusalem Post, 2010.
44. A. Wood, "After ADS-B launch, security concerns raised," Aviation International News, vol. 38, no. 16, Jul. 2006.
45. "INDIA'S NATIONAL SECURITY: ISSUES AND CHALLENGES - Dr. NASIR AHMAD GANAIE - Google Books." Accessed: Dec. 23, 2023. [Online]. Available: https://books.google.com.pk/books?hl=en&lr=&id=adWmEAAAQBAJ&oi=fnd&pg=PA59&dq=NDTV,+A+phone+application+that+threatens+security,+Press+Trust+of+India,+New+Delhi,+India,+October+4,+2010.&ots=F5jZB7KOW6&sig=heSBl1Bmq6nbxSXXql1snctwwQc&redir_esc=y#v=onepage&q&f=false
46. M. Unnikrishnan, "ITT Calls on AT&T for ADS-B infrastructure," Aviation Week, 2007.
47. M. Spainhower, J. Butts, D. Guernsey, and S. Shenoi, "Security analysis of RSVP-TE signaling in MPLS networks," International Journal of Critical Infrastructure Protection, vol. 1, pp. 68–74, Dec. 2008, doi: 10.1016/J.IJCIP.2008.08.005.
48. Z. Wu, A. Guo, M. Yue, and L. Liu, "An ADS-B message authentication method based on certificateless short signature," IEEE Trans Aerosp Electron Syst, vol. 56, no. 3, pp. 1742–1753, 2019.
49. M. R. Manesh, M. Mullins, K. Foerster, and N. Kaabouch, "A preliminary effort toward investigating the impacts of ADS-B message injection attack," in 2018 IEEE Aerospace Conference, IEEE, 2018, pp. 1–6.
50. K. F. Mirzaei, B. P. De Carvalho, and P. Pschorn, "Security of ADS-B: Attack scenarios," EasyChair, Tech. Rep, 2019.
51. F. Shang, B. Wang, F. Yan, and T. Li, "Multidevice false data injection attack models of ADS-B multilateration systems," Security and Communication Networks, vol. 2019, 2019.
52. A. Costin and A. Francillon, "Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," black hat USA, vol. 1, pp. 1–12, 2012.
53. H. Yang, H. Li, and X. S. Shen, "Modern Cryptography for ADS-B Systems," in Secure Automatic Dependent Surveillance-Broadcast Systems, Springer, 2022, pp. 19–59.
54. R. Bavdekar, E. J. Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations," International Conference on Information Networking, vol. 2023-January, pp. 146–151, 2023, doi: 10.1109/ICOIN56518.2023.10048976.
55. L. R. John Jochum, "Encripted mode select ADS-B for tactical military situational awareness," 2001, Accessed: Dec. 25, 2023. [Online]. Available: https://dspace.mit.edu/bitstream/handle/1721.1/86721/49223652-MIT.pdf;sequence=2
56. H. Yang, M. Yao, Z. Xu, and B. Liu, "LHCSAS: A Lightweight and Highly-Compatible Solution for ADS-B Security," 2017 IEEE Global Communications Conference, GLOBECOM 2017 - Proceedings, vol. 2018-January, pp. 1–7, Jul. 2017, doi: 10.1109/GLOCOM.2017.8254500.
57. R. Agbeyibor, "Secure ADS-B: Towards Airborne Communications Security in the Federal Aviation Administration's Next Generation Air Transportation System," Theses and Dissertations, Mar. 2014, Accessed: Dec. 25, 2023. [Online]. Available: https://scholar.afit.edu/etd/584
58. K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Can cryptography secure next generation air traffic surveillance?," IEEE Security and Privacy Magazine, 2014.
59. S. Zhang, H. Li, Y. Dai, J. Li, M. He, and R. Lu, "Verifiable Outsourcing Computation for Matrix Multiplication with Improved Efficiency and Applicability," IEEE Internet Things J, vol. 5, no. 6, pp. 5076–5088, Dec. 2018, doi: 10.1109/JIOT.2018.2867113.
60. H. Li, Y. Yang, Y. Dai, S. Yu, and Y. Xiang, "Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data," IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484–494, Apr. 2020, doi: 10.1109/TCC.2017.2769645.
61. Z. Feng, W. Pan, and Y. Wang, "A data authentication solution of ADS-B system based on X. 509 certificate," in 27th International Congress of the Aeronautical Sciences, ICAS, 2010, pp. 1–6.
62. C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 2501, pp. 548–566, 2002, doi: 10.1007/3-540-36178-2_34/COVER.
63. S. S. M. Chow, L. C. K. Hui, S. M. Yiu, and K. P. Chow, "Secure hierarchical identity based signature and its application," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 3269, pp. 480–494, 2004, doi: 10.1007/978-3-540-30191-2_37/COVER.

64. E. Cook, "ADS-B, friend or foe: ADS-B message authentication for NextGen aircraft," in 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, IEEE, 2015, pp. 1256–1261.
65. H. Khan, H. Khan, and S. Ghafoor, "Securing ADS-B Communications through a Novel Authentication Framework," 2023.
66. W. Pan, Z. Feng, Y. W.-J. of E. S. and, and undefined 2012, "ADS-B data authentication based on ECC and X. 509 certificate," journal.uestc.edu.cnWJ Pan, ZL Feng, Y WangJournal of Electronic Science and Technology, 2012•journal.uestc.edu.cn, doi: 10.3969/j.issn.1674-862X.2012.01.009.
67. J. Baek, Y. J. Byon, E. Hableel, and M. Al-Qutayri, "An authentication framework for Automatic Dependent Surveillance-Broadcast based on online/offline identity-based signature," Proceedings - 2013 8th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2013, pp. 358–363, 2013, doi: 10.1109/3PGCIC.2013.61.
68. H. Yang, R. Huang, X. Wang, J. Deng, and R. Chen, "EBAA: An efficient broadcast authentication scheme for ADS-B communication based on IBS-MR," Chinese Journal of Aeronautics, vol. 27, no. 3, pp. 688–696, Jun. 2014, doi: 10.1016/J.CJA.2014.04.028.
69. J. Habibi Markani, A. Amrhar, J.-M. Gagné, and R. J. Landry, "Security establishment in ADS-B by format-preserving encryption and blockchain schemes," Applied Sciences, vol. 13, no. 5, p. 3105, 2023.
70. "EBSCOhost | 100818950 | An Efficient Broadcast Authentication Scheme with Batch Verification for ADS-B Messages." Accessed: Dec. 26, 2023. [Online]. Available: https://web.s.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=19767277&AN=100818950&h=TvZ4Ne1ukku%2fhD0aeo%2b%2f09%2fGkYyBFZcpHy%2bND%2bDGPvpWm%2fD1kjjgBLTouRjqDOR1%2fC04tSdBXQ07dlSl6WYGjA%3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d19767277%26AN%3d100818950
71. A. Yang, X. Tan, J. Baek, and D. S. Wong, "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification," IEEE Trans Serv Comput, vol. 10, no. 2, pp. 165–175, 2015.
72. D. He, N. Kumar, K. K. R. Choo, and W. Wu, "Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system," IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 454–464, Feb. 2017, doi: 10.1109/TIFS.2016.2622682.
73. Z. Wu, T. Shang, and A. Guo, "Security Issues in Automatic Dependent Surveillance-Broadcast (ADS-B): A Survey," IEEE Access, vol. 8, pp. 122147–122167, 2020, doi: 10.1109/ACCESS.2020.3007182.
74. C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system," International Journal of Critical Infrastructure Protection, vol. 6, no. 1, pp. 3–11, Mar. 2013, doi: 10.1016/J.IJCIP.2013.02.001.
75. H. Yang, M. Yao, Z. Xu, and B. Liu, "LHCSAS: A Lightweight and Highly-Compatible Solution for ADS-B Security," 2017 IEEE Global Communications Conference, GLOBECOM 2017 - Proceedings, vol. 2018-January, pp. 1–7, Jul. 2017, doi: 10.1109/GLOCOM.2017.8254500.
76. H. Yang, H. Li, and X. S. Shen, "Secure Automatic Dependent Surveillance-Broadcast Systems," 2023, doi: 10.1007/978-3-031-07021-1.
77. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," https://doi.org/10.1137/S0097539701398521, vol. 32, no. 3, pp. 586–615, Feb. 2012, doi: 10.1137/S0097539701398521.
78. P. Yi, J. Li, Y. Zhang, and Y. Chen, "Efficient Hierarchical Signature Scheme With Batch Verification Function Suitable for ADS-B System," IEEE Trans Aerosp Electron Syst, vol. 59, no. 2, pp. 1292–1299, Apr. 2023, doi: 10.1109/TAES.2022.3197684.
79. A. Asari, M. R. Alagheband, M. Bayat, and M. R. Asaar, "A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems," Computer Networks, vol. 185, p. 107599, Feb. 2021, doi: 10.1016/J.COMNET.2020.107599.
80. D. He, N. Kumar, K. K. R. Choo, and W. Wu, "Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system," IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 454–464, Feb. 2017, doi: 10.1109/TIFS.2016.2622682.
81. B. Burfeind, R. Mills, S. Nykl, J. A. Betances, and C. Sielski, "Confidential ADS-B," IEEE Aerospace Conference Proceedings, vol. 2019-March, Mar. 2019, doi: 10.1109/AERO.2019.8742166.
82. A. Braeken, "Holistic Air Protection Scheme of ADS-B Communication," IEEE Access, vol. 7, pp. 65251–65262, 2019, doi: 10.1109/ACCESS.2019.2917793.
83. M. R. Manesh, M. S. Velashani, E. Ghribi, and N. Kaabouch, "Performance comparison of machine learning algorithms in detecting jamming attacks on ADS-B devices," in 2019 IEEE International Conference on Electro Information Technology (EIT), IEEE, 2019, pp. 200–206.

84. T. Kacem, A. Kaya, A. S. Keceli, C. Catal, D. Wijsekera, and P. Costa, "ADS-B Attack Classification using Machine Learning Techniques," in 2021 IEEE Intelligent Vehicles Symposium Workshops (IV Workshops), IEEE, 2021, pp. 7–12.
85. H. Yang, H. Li, and X. S. Shen, "Complete ADS-B Security Solution," in Secure Automatic Dependent Surveillance-Broadcast Systems, Springer, 2022, pp. 117–141.
86. S. Khan, J. Thorn, A. Wahlgren, and A. Gurtov, "Intrusion detection in automatic dependent surveillance-broadcast (ADS-B) with machine learning," in 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), IEEE, 2021, pp. 1–10.
87. D. M. Mink et al., "Near-Real-Time IDS for the US FAA's NextGen ADS-B," Big Data and Cognitive Computing, vol. 5, no. 2, p. 27, 2021.
88. R. Karam, M. Salomon, and R. Couturier, "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, pp. 241–246.
89. J. Wang, Y. Zou, and J. Ding, "ADS-B spoofing attack detection method based on LSTM," EURASIP J Wirel Commun Netw, vol. 2020, no. 1, pp. 1–12, 2020.
90. R. Karam, M. Salomon, and R. Couturier, "Supervised ADS-B Anomaly Detection Using a False Data Generator," in 2022 2nd International Conference on Computer, Control and Robotics (ICCCR), IEEE, 2022, pp. 218–223.
91. X. Guo, C. Zhu, J. Yang, and Y. Xiao, "An Anomaly Detection Model for ADS-B Systems Based on Improved GAN and LSTM Networks," in 2021 IEEE 21st International Conference on Communication Technology (ICCT), IEEE, 2021, pp. 802–809.
92. N. S. Joseph, C. Banerjee, E. Pasiliao, and T. Mukherjee, "FlightSense: A spoofer detection and aircraft identification system using raw ADS-B data," in 2020 IEEE International Conference on Big Data (Big Data), IEEE, 2020, pp. 3885–3894.
93. X. Ying, J. Mazer, G. Bernieri, M. Conti, L. Bushnell, and R. Poovendran, "Detecting ADS-B spoofing attacks using deep neural networks," in 2019 IEEE conference on communications and network security (CNS), IEEE, 2019, pp. 187–195.
94. E. Habler and A. Shabtai, "Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages," Comput Secur, vol. 78, pp. 155–173, 2018.
95. B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," ACM Computing Surveys (CSUR), vol. 45, no. 1, pp. 1–29, 2012.
96. K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," IEEE Wirel Commun, vol. 17, no. 5, pp. 56–62, 2010.
97. Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in 2010 Proceedings IEEE INFOCOM, IEEE, 2010, pp. 1–9.
98. C. Pöpper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys.," in USENIX security Symposium, 2009, pp. 231–248.
99. M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in 2008 IEEE Symposium on Security and Privacy (sp 2008), IEEE, 2008, pp. 64–78.
100. R. J. Reisman, "Air traffic management blockchain infrastructure for security, authentication, and privacy," AIAA Scitech 2019 Forum, 2019, doi: 10.2514/6.2019-2203.
101. E. Habler and A. Shabtai, "Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages," Comput Secur, vol. 78, pp. 155–173, Sep. 2018, doi: 10.1016/J.COSE.2018.07.004.
102. S. Akerman, E. Habler, and A. Shabtai, "VizADS-B: Analyzing Sequences of ADS-B Images Using Explainable Convolutional LSTM Encoder-Decoder to Detect Cyber Attacks," Jun. 2019, Accessed: Dec. 24, 2023. [Online]. Available: https://arxiv.org/abs/1906.07921v1
103. S. Chen, S. Zheng, L. Yang, and X. Yang, "Deep Learning for Large-Scale Real-World ACARS and ADS-B Radio Signal Classification," IEEE Access, vol. 7, pp. 89256–89264, 2019, doi: 10.1109/ACCESS.2019.2925569.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.