Review

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

Waqas Ahmed *

Posted Date: 15 July 2024

doi: 10.20944/preprints202405.0586.v2

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, Zip code 4400, Islamabad, Pakistan
* Correspondence: waqaskhattak99@gmail.com

Abstract: The Automatic Dependent Surveillance–Broadcast (ADS-B) protocol is a cornerstone of modern aviation surveillance and aircraft traffic control systems, pivotal 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, enhancing air transportation system capacity and safety. However, concerns regarding the protocol's security persist, especially as its adoption expands. The unencrypted transmission of aircraft data and the lack of robust authentication mechanisms expose the protocol to exploitation by malicious actors. In this study, we conducted a comprehensive review of existing research in the field, identifying a critical gap necessitating a holistic survey. Prior surveys have primarily 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 security vulnerability analysis diagram, our paper delves into the vulnerabilities inherent in the ADS-B protocol, outlines potential threats, and scrutinizes various attack scenarios. We systematically categorized and analyzed existing security solutions, considering factors such as 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 airspace [1]. The continuous expansion of air transport necessitates enhancing air surveillance systems to manage the escalating volume of flights effectively. Over the years, air transport has experienced consistent growth, which is 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 air traffic control (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 International Civil Administration Organization (ICAO) introduced the Global Air Navigation Plan (GANP) 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 using a developing approach. The fundamental aim of the ICAO is to determine a worldwide interoperable air navigation system that will satisfy 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. Information and Communications Technology (ICT)--dependent disruptions and numerous cyberattacks are among these possibilities. With 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 2005, the US FAA initiated a NextGen Air Transportation System project to cater to future navigation demand, flight security, and airspace capacity [2,3]. The gradual transformation of land-based ATC systems sought in this project showed a heavy dependency on radar and satellite-based navigation systems. ADS-B is the most critical 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, this system promises low maintenance costs and a longer service life. In particular, 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 in the most controlled and secure airspace [4]. However, the comprehensiveness, internet connectivity, and systems' interoperability that come with it have introduced new weaknesses to these systems worth confronting. The proposed research highlights and confronts these system weaknesses to improve security [5].

During the 1990s, implementing radio frequency (RF) 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) did not address this matter, nor did any of the pertinent demand files [7,8] of security discussions. A significant technological advancement, namely software-defined radio (SDR), has enabled hackers to execute RF signal transmission and 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 12th Air Navigation Conference agenda in light of the considerable attention it received from the media. Considering cybersecurity 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's Attorney General, NextGen intends to prolong 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 the 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 precise position in the airspace.

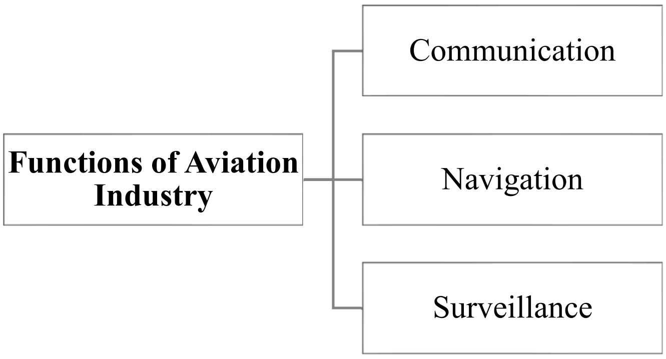

Figure 1. Functions of Aviation Industry Infrastructure.

1.1. Research Motivation/Problem

Since 2020, the FAA has mandated the ADS-B system for all commercial aircraft globally. Several researchers have published survey papers, as mentioned in Table 1, and research papers on ADS-B security and vulnerabilities. However, to the best of our knowledge, the existing survey papers did not comprehensively cover ADS-B as per Table 1's attributes. The research motivations for writing this survey paper on ADS-B security are the following:

- 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 a 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.

1.2. Research Objectives/Contributions

The proposed research survey aims to address key aspects of ADS-B security, including its vulnerabilities, potential attacks, and the limitations of existing solutions. The objectives of this research are the following:

- To offer a comprehensive overview of the aviation system to enhance readers' understanding of ADS-B technology and its security implications.
- To provide an in-depth analysis of ADS-B vulnerabilities, potential threats, and attack vectors, supported by illustrative diagrams, to facilitate a deeper understanding of security risks.
- To evaluate existing security solutions published till 2024 based on cost-effectiveness, scalability, implementation complexity, and coverage against diverse attack scenarios to inform decision making for security implementations.
- To identify 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 was compared with the papers published by well-known researchers based on the selected attributes mentioned in Table 1. We selected multiple papers as base paper for the proposed research survey. The base paper comprehensively studied recent advancements in ADS-B using deep learning and machine learning, covers various attacks, techniques, and applications, and has been highly cited. In this research survey, we discussed aviation security to familiarize readers with general aviation infrastructure and security protocols; we presented a detailed security analysis of ADS-B from the perspective of threats, vulnerabilities, and attacks. The survey categorized existing solutions into cryptography, and non-cryptography techniques. It also presented the security requirements for proposing a valuable framework for the security of ADS-B with future research directions.

Table 1. Comparison of Survey Features: Proposed vs. Existing (✓ Included, × Not Included).

Ref. and Year	Aviation System	Security Analysis	Existing Security Solution			Security Requirements	Future 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	✓	✓	✓	✓	✓	✓	✓

1.3. Research Methodology

In this survey paper, the keyword search criteria include “ADS-B security”, “Machine Learning for ADS-B”, and “Vulnerabilities in ADS-B”. We found several research papers where the keywords were not in the paper title or abstract. In such situations, we used a manual process to find the appropriate papers. The key challenges in various applications include their application privacy and security, so the search string “privacy and security issues” showed irrelevant papers. We used relevant and recent (2018–2024) research papers to make the paper impactful and attractive. We also used tutorial papers, books, survey articles, technical reports, technical patents, and other resources for broader coverage. The search filter depended on multiple layers based on the paper title, investigation, title, and abstract. Finally, we found some focused and relevant research papers covering the criteria.

1.4. 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 this 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 how the protocol works, its components, and its message format, whereas Section 4 analyzes ADS-B’s vulnerabilities, possible threats, and attacks. Section 5 critically examines the existing security solutions and presents valuable insights with drawbacks, while Section 6 presents the requirements of the ADS-B security solution. Section 7 presents the future research directions for researchers, and Section 8 concludes the 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	Controller–Pilot Data Link Communications	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 [19–22]. In addition, a national security agency is mainly responsible for aviation safety. Figure 2 shows a comprehensive aviation system architecture [23–25]. The airplane must land at the airfield to complete a circuit. Satellites, ground stations, and peer aircraft all assist it in achieving this goal [26,27]. Audio and message communications are sent and received, and the pilot uses communication protocols [28–31], including CPDLC, VHF, and HF, between the satellite and ground station. They travel and land reliably using navigational techniques (such as the ILS, VHF omnidirectional range (VOR), and DME). The PSR, SSR, and ADS-B technologies are among the surveillance protocols a ground station uses to track aircraft movement and identify airspace incursions [15]. These systems continue to function during an aircraft's flight and descent.

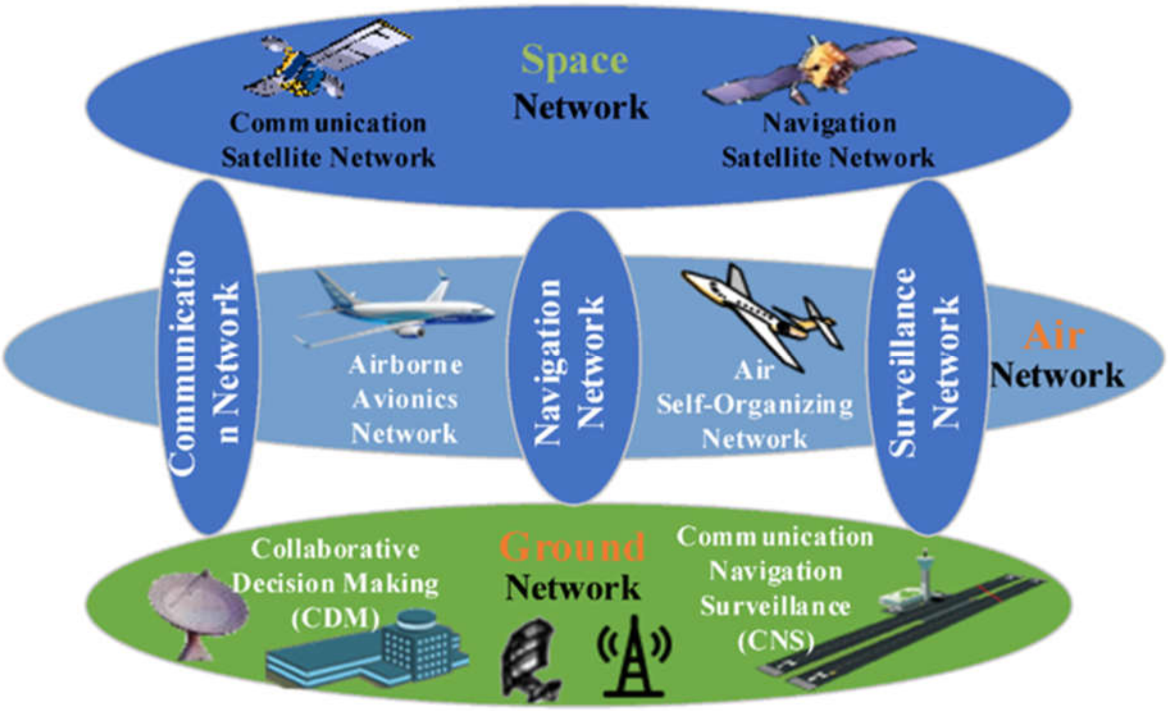

Figure 2. Schematic Overview of the Aviation System Architecture.

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, initiating communication with aircraft causes an incoming plane to fall 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, which is the duty of VHF and CPDLC [34]. CPDLC uses VHF data link for message-based communication, whereas VHF is for voice-based communication. Digital Satellite Communication Networks (DSCNs) 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 completed 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 their 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.

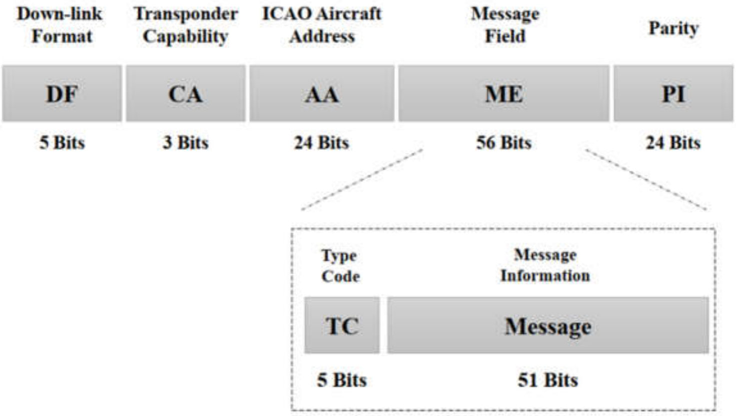

Figure 3. ADS-B Message Format.

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 the altitude, velocity, latitude, longitude, etc. The aircraft carries ADS-B In to receive data from ATC and nearby aircraft. It can also allow pilots to view the altitude, velocity, lateral position, aircraft category, flight numbers, and distance from nearby aircraft in the airspace.

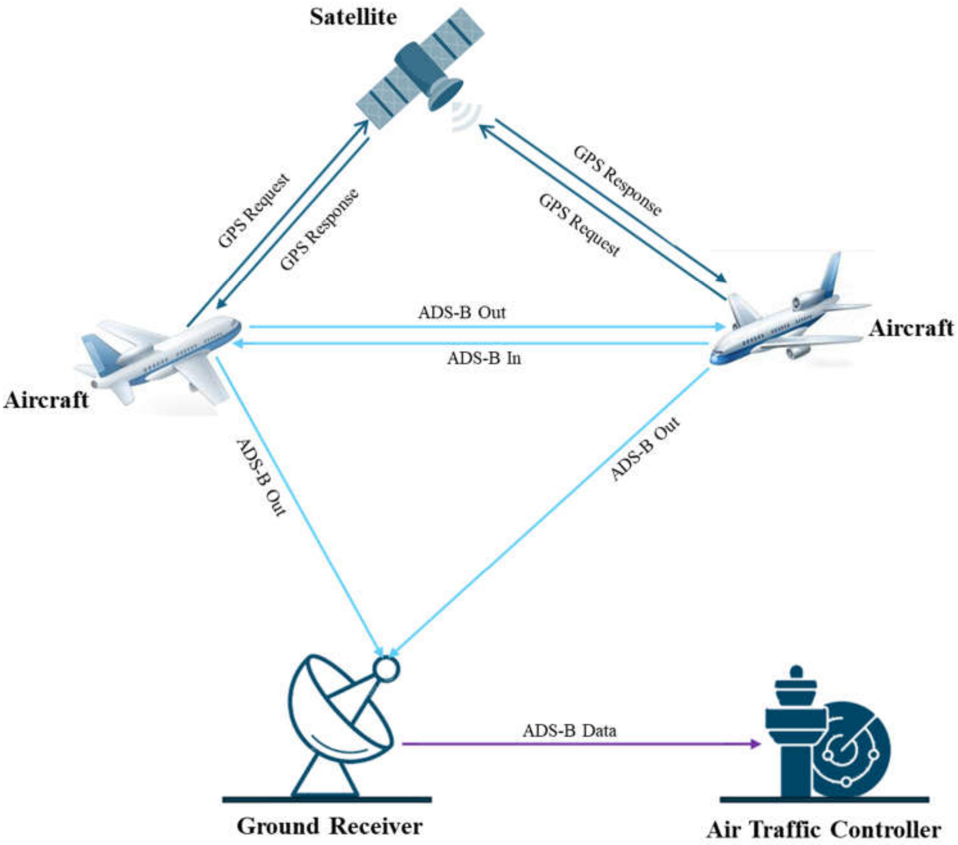

Figure 4. Functional Diagram of ADS-B.

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 cyberattacks 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

This section examines security concerns regarding the implementation of the ADSB. The primary source of the implementation's vulnerabilities is the tension between security objectives and promoting 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 a satellite is acquired by 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] asserted the following:

> "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 concluded from its investigation that there was no more risk associated with the intentional insertion of bogus targets into ADS-B transmissions than with the current SSR transmissions. Furthermore, the FAA declared that because the ADS-B surveillance information is integrated with main radar information before transmission for air traffic management (ATM), the probability of deceit and interference was 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 was 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 specific 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 would 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 central radar systems will likely be eliminated. The FAA Final Ruling also addressed the security concerns of data fusion. Furthermore, the NextGen deployment strategy named 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 Shiite insurgent, and his laptop was discovered to have had 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 USD 26 piece of software SkyGrabber to intercept the unencrypted Predator footage. The same vulnerability was 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 Vulnerability 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 USD 5 antenna, a laptop computer, and a general aviation transponder. Smith 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. This capability to jam signals might impact a system's availability. To carry out any surveillance activity, ADS-B requires an open and, by extension, risky method. Using ADS-B raises the stakes for bad actors looking to exploit these flaws [22]. The security analysis section divided the ADS-B system into four parts: threats, strengths, opportunities, and system weaknesses.

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 5 illustrates a cyber-attack on ADS-B system [40].

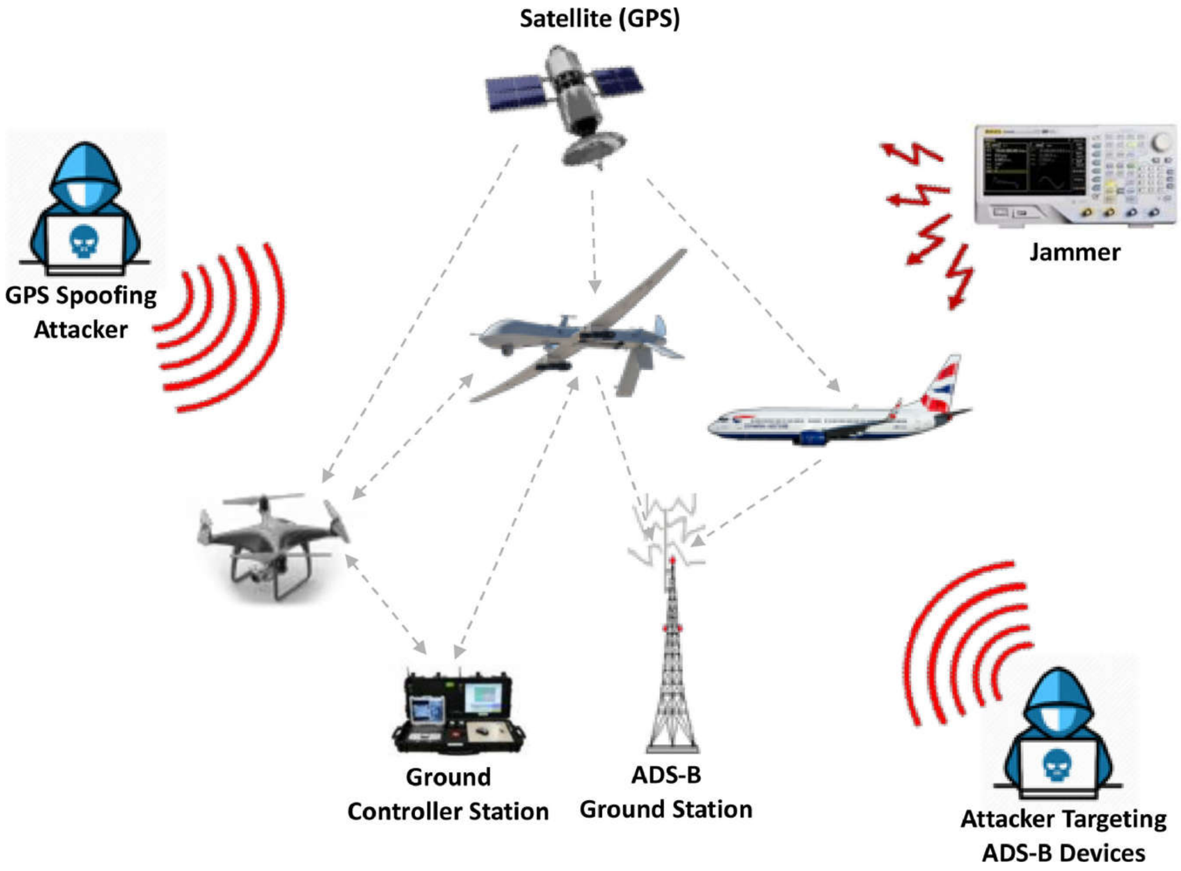

Figure 5. Illustration of Cyber-Attacks.

- Message Injection Attack: This is an 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: This is 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 the 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 the 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], the authors proposed a mechanism for injecting and verifying a modified message in the ATC system.
- Eavesdropping Attack: This is 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 the altitude, position, etc. The intercept messages also provide sensitive information to the

attacker, such as the 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 identical 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. Summary of Potential Security Attacks.

Sr#	Attack	Sub-Attack	Attack Purpose	Attack Method
1.	Eavesdropping	Reconnaissance attack	Obtaining aircraft information is also called aircraft reconnaissance.	Using an ADS-B receiver, the corresponding airspace data are obtained.
2.	Jamming	Denial of service, flooding attack	Jam ADS-B communicates for a certain amount of time in a specific airspace.	A high-frequency signal is transmitted on the targeted frequency band (1090ES).
3.	Message injection	Ghost injection	To mislead ATC in the targeted airspace, fake aircraft is injected.	Using a power-transmitting device generates and injects fake messages using relevant frequency.
4.	Message deletion	Aircraft disappearance	A target field or complete message is deleted.	At physical layers, bits are flipped in the ADS-B message.
5.	Message modification	Virtual trajectory modification	The content of the message is modified.	Message injection and deletion attack are combined.

It is essential 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 impacts on the ADS-B system.

Table 4. Threats and Their Impacts on the 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 disseminating the most recent flight information.

5. Security Analysis of Existing Solutions

This section summarizes the merits and demerits of the existing solution regarding 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 significantly reduced by not considering ADS-B system problems such as software and hardware compatibility and the burden on the 1090 MHz 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 6 visually represents this categorization. In the following subsections, a detailed explanation of each category will have drawn upon the relevant literature to elucidate the concepts and approaches within each domain.

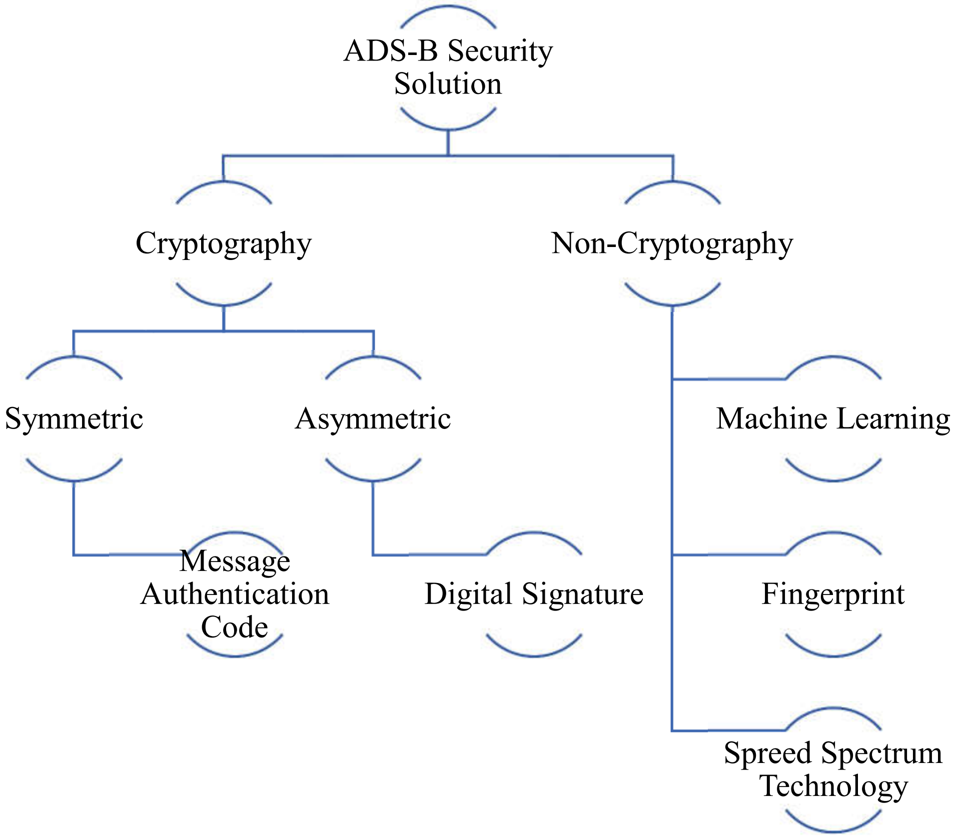

Figure 6. Overview of ADS-B Security Solution Classifications.

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 critical 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 the security and seamless functionality of this critical aviation protocol.

5.1.1. Symmetric Cryptography

Symmetric cryptography, 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 the 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]. Similar to a framework based on encryption technology proposed by [55], both frameworks provide rough encryption as the authors did not mention any encryption algorithms. The encryption framework of [35] is shown in Figure 7.

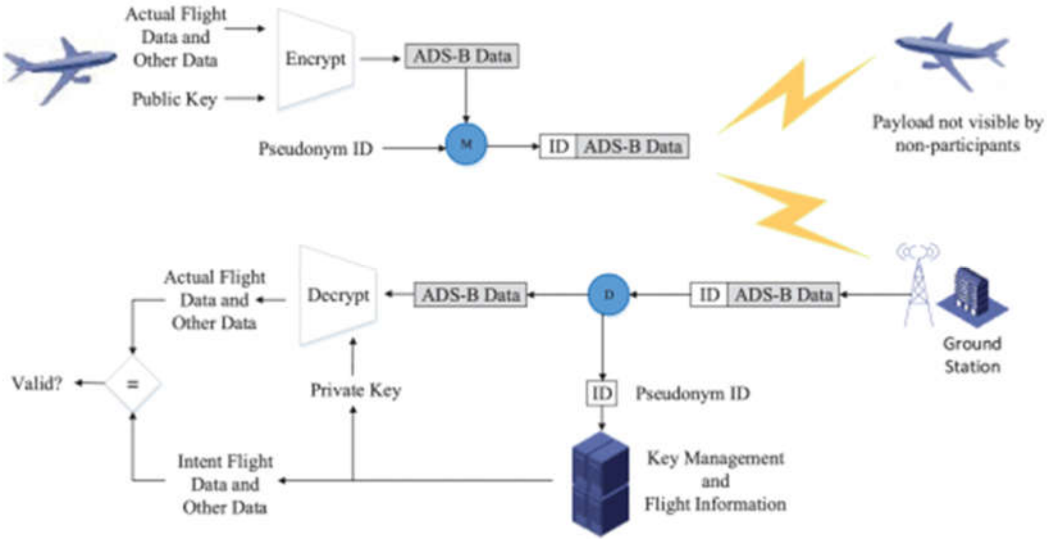
Actual Flight Data and Other Data
Public Key
Encrypt
ADS-B Data
Pseudonym ID
M
ID ADS-B Data
Payload not visible by non-participants
Actual Flight Data and Other Data
Decrypt
ADS-B Data
D
ID ADS-B Data
Ground Station
Valid?
=
Private Key
ID Pseudonym ID
Intent Flight Data and Other Data
Key Management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

Figure 7. Encryption Framework.

The authors in [27] proposed a technique based on format-preserving encryption to protect ADS-B message integrity. The technique did not confirm the standard block size of the ADS-B message. Also, the authors assessed the limitations of the traditional ATC system and analyzed the feasibility of reserved format encryption for the ADS-B protocol. However, unlike in [38], to preserve the ADS-B protocol's openness property for completed message encryption. From the applicability, security, and performance points of view of ADS-B messages, the authors in [56,57] evaluated different reserved format algorithms. The 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.

The 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 did not have the keys would 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.

5.1.1.1. Message Authentication Code (MAC)

To protect ADS-B messages in [35], the authors proposed a framework based on encryption and message authentication code (MAC). In the proposed authentication framework, all active entities transfer ADS-B messages in plain text. A MAC is attached to every broadcast ADS-B message to prove the entity's authentication. To retain the protocol's openness, all entities see the broadcast messages, whether the authentication process passed or failed. The proposed certification framework [35] is shown in Figure 8.

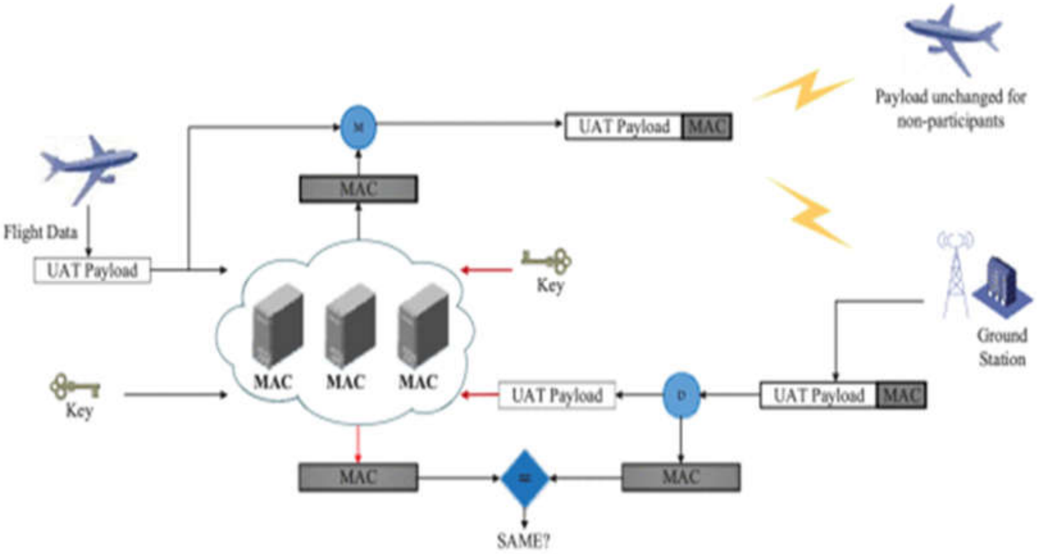

Figure 8. Message Authentication Code for Entity Identification Verification.

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, the authors in [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 cryptography keys using public key infrastructure, which required a lot of space for storage. The proposed scheme could not be applied due to the massive increase in inbound and outbound flights. In [62,63], the authors proposed a technique requiring a pair of keys for every use, which had to 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 were from registered aircraft. To share symmetric keys, the authors used asymmetric cryptography. The shared symmetric key verified 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 authors’ results, the proposed framework minimized the computation overhead and increased message security. Figure 9 presents the proposed framework in [65].

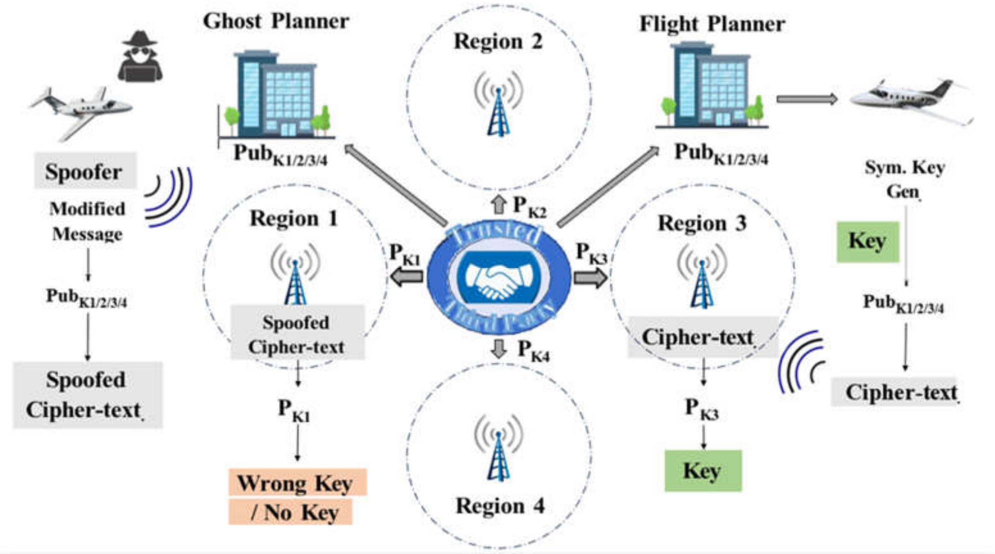

Figure 9. ADS-B Security Framework.

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

5.1.2.1. Digital Signature

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

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

Asymmetric encryption schemes require a centralized authority (CA) in the ADS-B system to manage certificates [74]. The involvement of a CA increases the ADS-B system's operating costs and complexity. In the existing, signature-based ADS-B security solution, the signature length is considerable, which requires a high computational 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.	Cryptographic Technique	Research Contribution	Strengths	Challenges
[73]	Symmetric Cryptography	The authors proposed a lightweight, highly compatible, and resource-constrained framework for ADS-B security.	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.
[74]		Based on the modified AES algorithm, the authors proposed a framework to increase ADS-B message integrity and secure ADS-B messages.		
[75]		Using vector-homomorphic and FFX encryption, the authors proposed solutions for ADS-B message integrity and privacy.		
[76]		The authors proposed using identity-based encryption (IBE) for key encryption and sharing and a hybrid technique with symmetric cryptography for data.		
[77]		The authors proposed a technique to address the problems of key sharing and authentication.		
[78]	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.
[79]		The authors proposed a lightweight protocol based on symmetric and asymmetric encryption for ADS-B message confidentiality. In the proposed protocol, ATC manages the session data and the encryption keys, acting as TTP.		
[80]		From the ADS-B security's point of view, the authors discussed the suitability of the Elliptic Curve Digital Signature Algorithm (ECDSA) from the perspectives of signature length and standard constraints.		
[81]		To protect ADS-B message confidentiality and authentication, the author proposed a holistic air protection (HAP) technique using an elliptical curve and certificate-based encryption.		
[82]	Digital Signature	The authors presented an ADS-B message authentication technique based on a certificate-less signature. The proposed method is performance-efficient and does not need a 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 an ample space.

5.2. Non-Cryptography Schemes

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

In recent years, artificial intelligence (AI) methodologies, including machine learning (ML) and deep learning, have experienced a surge in popularity. These approaches offer various algorithms applicable across domains, facilitating tasks such as prediction, regression, and classification. This versatility enables their application to a wide array of problem domains. Within cybersecurity, ML has become a prominent tool, utilized for 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 practical solutions in identifying and mitigating 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) and security experts in augmenting existing security solutions but also aid 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 the decision tree, support vector machine, artificial neural network, and k-nearest neighbor, are implemented on a simulated dataset, and their accuracy is compared with the highest accuracy of an artificial neural network (81%). In this research, the authors selected energy statistics, a bad packet ratio, and a 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 worked on the jamming attack with a small dataset. In [83], the authors created a dataset using an ADS-B transmitter. The authors did not share the dataset for future research work.

In [84], the authors proposed a machine learning-based multi-class classification framework to improve the security of ADS-B by implementing random forests, support vector machines, and decision tree models to classify ghost aircraft and replay attacks. The authors performed several experiments on a dataset from Filghtradar24 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 found that decision tree performance was best with 92% accuracy among the implemented models. The dataset size and accuracy were small, which is unacceptable in such a critical infrastructure environment. In [85], the authors proposed a spoofing attack detection method 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 the ATC to examine every message and identify malicious messages.

In [86], the authors proposed a classification framework, based on the 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 the false alarm rate, precision, F1 core, and recall to evaluate the performance of the proposed technique. The k-nearest neighbor model outperformed other models with an accuracy of 99.57%. A real-time intrusion detection system for ADS-B was proposed in [87] using a support vector machine model with 80% accuracy. The authors trained the model on a dataset generated with the help of OpenSky.

A Short-Term Long Memory (LSTM) model based on deep learning architecture was also proposed for detecting malicious ADS-B messages [88]. The model was trained on a dataset generated with the help of Flightradar24, which contained data from 10 different aircraft. The model was trained on the OpenSky dataset with 91.59% testing accuracy. Based on the ADS-B message sequence [86] designed, a message-spoofing attack detection framework based on the LSTM model was proposed with 95.50% accuracy on the testing dataset.

From the perspective of ADS-B messages, a spoofing attack detection technique based on LSTM was proposed [89]. In this research paper, the author focused on three different ADS-B attacks: injection, jamming, and modification. Based on the sliding window, the ADS-B message sequence was pre-processed and implemented in the LSTM network model with 93% accuracy [89]. To detect ADS-B spoofed data, the authors in [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.

To detect ADS-B message modification attacks, the authors in [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) by the authors in [91], the proposed anomaly detection model for ADS-B data had 97% accuracy. The dataset was 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 and Ref.	Dataset Description	ML Models	Accuracy
2019 [83]	Simulated (the authors did not mention the details of the dataset and number of messages used in the experiments)	LR	65.6%
		SVM	67.3%
		KNN	74.6%
		ANN	81%
		DT	74.2%
2021 [84]	Flightradar24 (the authors used a dataset containing messages of 1 flight from Lisbon to Paris)	SVM	91%
		DT	92%
		RF	90%
2019 [85]	Simulated (the author did not mention the number of legitimate and nonlegitimate messages)	DNN	96.66%
2021 [86]	OpenSky (the dataset containing 26,000)	LR	52.10%
		NB	82.10%
		K-NN	99.57%
2021 [87]	OpenSky (dataset with 20,000 messages, 10,000 legitimate and 10,000 nonlegitimate)	SVM	80%
2020 [88]	OpenSky (the author did not mention the number of legitimate and nonlegitimate messages)	LSTM	91.59%
2020 [89]	Simulated (detecting spoofing attack, authors did not mention the details of the dataset)	LSTM	93%
2022 [90]	OpenSky (20 randomly chosen flights were downloaded from the OpenSky Network)	LSTM	98%
2021 [91]	Flightradar24 (the authors did not mention the details of the dataset)	LSTM with GAN	97%
2020 [92]	Simulated (18,675 messages were collected for experiments)	GAN	98.87%
		CNN	99%

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 July 2024 doi:10.20944/preprints202405.0586.v2

5.2.2. Fingerprint

A non-cryptographic technique based on unique characteristics to identify devices such as radio circuits, operating systems, clocks, and drivers was proposed [93–95]. Location-/channel-based, hardware-based, and software-based are three possible fingerprinting techniques used in the ADS-B system [96]. Location-/channel-based fingerprinting is based on a channel impulse response, received signal strength, or carrier phase. Devices based on unique hardware characteristics such as a clock skew, radio modulation signal, and turn-on/off transient are identified, which is 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 a direct sequence spread spectrum. The network entities (sender and receiver) must pre-share a frequency hopping mode or spreading code while using this technology. This technology has issues similar to cryptography, including key generation, distribution, and management issues.

The 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 jam or eavesdrop on the channel effectively. 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].

6. Security Requirements

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

- Cryptography Elements—Despite the limited message size in standard ADS-B packets, the solution's security level should not be compromised.
- No Modifications in Hardware—The proposed security solution should require a simple software update without requiring hardware modifications in terms of maintenance and cost.
- 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.
- Backward Compatibility—New security solutions should seamlessly integrate with existing systems, allowing aircraft that have yet to update their systems to continue operating.
- Standard Compliance—Security solutions must align with the ADS-B protocol's updated version to ensure message format and communication logic compliance.
- Limited Message Overhead—Security techniques must introduce a minimal additional message overhead to avoid congestion on the 1090ES frequency band.

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 changing message format	Medium	Low	Low
Machine Learning	Need to add software	High	Low	Low
Spread Spectrum	Changing the system and adding hardware	Medium	High	High
Fingerprinting	Adding hardware, but there is no need to modify the system	Medium	Medium	High

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 than traditional radar technologies. ADS-B augments radar coverage and functions independently in areas missing radar support. Although these notable benefits exist, 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 practical 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 [102].

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 critical focal point for further investigation.

- Blockchain Integration*:* Blockchain, a composite system incorporating peer-to-peer (P2P) 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. Researchers should focus on blockchain's usability in forthcoming research endeavors in ADS-B security. Pioneering work by the authors in [21] introduced blockchain technology for identity recognition by employing P2P technology for distributed data storage and authentication. This technique showcases high security, reliability, and scalability, offering identity authentication across different infrastructures [103]. 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. A 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 the works of [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. The ADS-B system requires a security solution that overcomes the mentioned limitations.

8. Conclusions

The NextGen project initiated by the FAA’s US Department in 2005 significantly enhances air transportation safety. However, researchers have uncovered potential security vulnerabilities as NextGen, particularly its core component, the ADS-B protocol, sees widespread implementation. The examination of ADS-B security has shed light on the inherent risks accompanying its deployment. In recent years, numerous research papers have proposed solutions for securing the ADS-B protocol, categorizing them into cryptography- and non-cryptography-based approaches. Our survey explicitly explored machine learning- and deep learning-based solutions within the non-cryptography domain, providing valuable insights into aviation security, ADS-B vulnerabilities, analysis of existing security solutions, and relevant future research directions. Our survey aimed to comprehensively identify ADS-B security vulnerabilities and associated attack vectors, thereby raising awareness within the research community. The existing body of research strongly advocates for 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. This survey paper focused on the security of the ADS-B from a SWOT analysis perspective. The proposed paper is a review paper to guide future researchers. We did not propose any security solution to overcome the ADS-B vulnerabilities. Our future work will present machine learning- and deep learning-based intrusion detection systems for ADS-B.

Author Contributions: Research planning, outline, and writing, Waqas Ahmed; Research planning, outline, and proofreading Naveed Anwar Bhatti; Research supervising, and planning, Ammar Masood; Proofreading, supervising and planning, Abeer A. K. Alharbi and Salihah Alotaibi.

Funding: This research received no external funding.

Institutional Review Board Statement: N/A.

Informed Consent Statement: N/A.

Data Availability Statement: N/A.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wu, Z.; Shang, T.; Guo, A. Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey. *IEEE Access* **2020**, *8*, 122147–122167. https://doi.org/10.1109/ACCESS.2020.3007182.
2. Jacob, P.; Sirigina, R.P.; Madhukumar, A.S.; Prasad, V.A. Cognitive radio for aeronautical communications: A survey. *IEEE Access* **2016**, *4*, 3417–3443. https://doi.org/10.1109/access.2016.2570802.
3. Sciancalepore, S.; Di Pietro, R. SOS: Standard-compliant and packet loss tolerant security framework for ADS-B communications. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 1681–1698.
4. Yang, C.; Mott, J.; Bullock, D.M. Leveraging aircraft transponder signals for measuring aircraft fleet mix at non-towered airports. *Int. J. Aviat. Aeronaut. Aerosp*. **2021**, *8*, 1.
5. Baek, J.; Hableel, E.; Byon, Y.-J.; Wong, D.S.; Jang, K.; Yeo, H. How to Protect ADS-B: Confidentiality Framework and Efficient Realization Based on Staged Identity-Based Encryption. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 690–700. https://doi.org/10.1109/tits.2016.2586301.
6. *RTCA DO-282*; Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance Broadcast (ADS-B). RTCA: Washington, DC, USA, 2004.
7. Martone, P.J.; Tucker, G.E. Candidate requirements for multilateration and ADS-B systems to serve as alternatives to secondary radar. In Proceedings of the 20th DASC. 20th Digital Avionics Systems Conference (Cat. No. 01CH37219), Daytona Beach, FL, USA, 14–18 October 2001; IEEE: New York, NY, USA; pp. 7C2-1.
8. Rekkas, C.; Rees, M. Towards ADS-B implementation in Europe. In Proceedings of the 2008 Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles, Capri, Italy, 3–5 September 2008; IEEE: New York, NY, USA, ; pp. 1–4.
9. Costin, A.; Francillon, A. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *Black Hat USA* **2012**, *1*, 1–12.
10. Haines, B. “Hackers+ airplanes,” No good can come of this. *Defcon* **2012**, *20*, 26–29.
11. Kelly, H. Researcher: New air traffic control system is hackable. *CNN blog*, July 26, 2012.
12. Marks, P. *Air Traffic System Vulnerable to Cyber Attack*; Elsevier: Amsterdam, The Netherlands, 2011.
13. Greenberg, A. Next-gen air traffic control vulnerable to hackers spoofing planes out of thin air. *Forbes Mag.* **2012**, *10*, 2014.
14. Schäfer, M.; Lenders, V.; Martinovic, I. Experimental analysis of attacks on next generation air traffic communication. In Proceedings of theApplied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, 25–28 June 2013; Proceedings 11; Springer: Berlin/Heidelberg, Germany, 2013; pp. 253–271.
15. Dave, G.; Choudhary, G.; Sihag, V.; You, I.; Choo, K.-K.R. Cyber security challenges in aviation communication, navigation, and surveillance. *Comput. Secur.* **2022**, *112*, 102516.
16. Kraus, T.L. *Celebrating a History of Excellence: The Federal Aviation Administration and Space Education Outreach Program*; U.S. Department of Transportation, Federal Aviation Administration: Washington, DC, USA, 2011.
17. Williams, G. (2009). GPS for the sky: A survey of automatic dependent surveillance-broadcast (ADS-B) and its implementation in the United States. J. Air L. & Com., 74, 473.
18. Petrović, G. (2024). View on Regulations Concerning Communication, Navigation and Surveillance (CNS) Service in Civil Aviation. Air and Space Law, 49(2).
19. Kumari, A., Kumar, D., Sati, P., Kumar, S., Yadav, A. K., & Verma, A. S. (2024). Overview of Aviation Sector, Feedstock, and Supply Chain. In Biojet Fuel: Current Technology and Future Prospect (pp. 17-35). Singapore: Springer Nature Singapore.
20. Pennapareddy, S.; Natarajan, K. Securing ADS-B data transmissions using blockchain: A comprehensive survey and analysis. *Aircr. Eng. Aerosp. Technol.* **2023**, *95*, 452–463. https://doi.org/10.1108/aeat-02-2022-0058.
21. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, 14(11), 341.
22. Manesh, M.R.; Kaabouch, N. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. *Int. J. Crit. Infrastruct. Prot.* **2017**, *19*, 16–31. https://doi.org/10.1016/j.ijcip.2017.10.002.
23. Strohmeier, M.; Lenders, V.; Martinovic, I. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1066–1087. https://doi.org/10.1109/comst.2014.2365951.
24. Strohmeier, M.; Schafer, M.; Lenders, V.; Martinovic, I. Realities and challenges of nextgen air traffic management: The case of ADS-B. *IEEE Commun. Mag.* **2014**, *52*, 111–118. https://doi.org/10.1109/mcom.2014.6815901.
25. Strohmeier, M.; Lenders, V.; Martinovic, I. *Security of ADS−B: State of the Art and Beyond*; Department of Computer Science, University of Oxford: Oxford, UK, 2013.

26. McCallie, D.; Butts, J.; Mills, R. Security analysis of the ADS-B implementation in the next generation air transportation system. *Int. J. Crit. Infrastruct. Prot.* **2011**, *4*, 78–87. https://doi.org/10.1016/j.ijcip.2011.06.001.
27. Stastny, P.; Stoica, A.-M. Protecting aviation safety against cybersecurity threats. *IOP Conf. Series Mater. Sci. Eng.* **2022**, *1226*, 012025. https://doi.org/10.1088/1757-899x/1226/1/012025.
28. Lu, X.; Dong, R.; Wang, Q.; Zhang, L. Information Security Architecture Design for Cyber-Physical Integration System of Air Traffic Management. *Electronics* **2023**, *12*, 1665. https://doi.org/10.3390/electronics12071665.
29. Paraschi, E.P.; Georgopoulos, A.; Papanikou, M. Safety and security implications of crisis-driven austerity HRM practices in commercial aviation: A structural equation modelling approach. *Saf. Sci.* **2022**, *147*, 105570. https://doi.org/10.1016/j.ssci.2021.105570.
30. Imran, M. A., Zennaro, M., Popoola, O. R., Chiaraviglio, L., Zhang, H., Manzoni, P., ... & Pietrosemoli, E. (2024). Exploring the Boundaries of Connected Systems: Communications for Hard-to-Reach Areas and Extreme Conditions. Proceedings of the IEEE.
31. Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information* **2022**, *13*, 146. https://doi.org/10.3390/info13030146.
32. Tang, J.; Liu, G.; Pan, Q. Review on artificial intelligence techniques for improving representative air traffic management capability. *J. Syst. Eng. Electron.* **2022**, *33*, 1123–1134. https://doi.org/10.23919/JSEE.2022.000109.
33. Rezo, Z.; Steiner, S.; Mihetec, T.; Čokorilo, O. Strategic planning and development of Air Traffic Management system in Europe: A capacity-based review. *Transp. Res. Procedia* **2023**, *69*, 5–12. https://doi.org/10.1016/j.trpro.2023.02.138.
34. Mäurer, N.; Guggemos, T.; Ewert, T.; Gräupl, T.; Schmitt, C.; Grundner-Culemann, S. Security in Digital Aeronautical Communications A Comprehensive Gap Analysis. *Int. J. Crit. Infrastruct. Prot.* **2022**, *38*, 100549. https://doi.org/10.1016/j.ijcip.2022.100549.
35. Valovage, E. Enhanced ADS-B Research. In Proceedings of the 2006 IEEE/AIAA 25TH Digital Avionics Systems Conference, Portland, OR, USA, 15–19 October 2006; pp. 1–7. https://doi.org/10.1109/DASC.2006.313672.
36. Boyen, X. A tapestry of identity-based encryption: Practical frameworks compared. *Int. J. Appl. Cryptogr.* **2008**, *1*, 3. https://doi.org/10.1504/ijact.2008.017047.
37. Chan-Tin, E.; Feldman, D.; Hopper, N.; Kim, Y. The frog-boiling attack: Limitations of anomaly detection for secure network coordinate systems. In Proceedings of the Security and Privacy in Communication Networks: 5th International ICST Conference, SecureComm 2009, Athens, Greece, 14–18 September 2009; Revised Selected Papers 5; Springer: Berlin/Heidelberg, Germany, 2009; pp. 448–458.
38. Finke, C.; Butts, J.; Mills, R.; Grimaila, M. Enhancing the security of aircraft surveillance in the next generation air traffic control system. *Int. J. Crit. Infrastruct. Prot.* **2013**, *6*, 3–11. https://doi.org/10.1016/j.ijcip.2013.02.001.
39. Phelps, B., Klinger-Neviska, Z., Mourning, C., & Braasch, M. (2024, April). Quantum in Aviation Security: ADS-B Protection with QKD. In 2024 Integrated Communications, Navigation and Surveillance Conference (ICNS) (pp. 1-8). IEEE.
40. Manesh, M.R.; Kaabouch, N. Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Comput. Secur.* **2019**, *85*, 386–401. https://doi.org/10.1016/j.cose.2019.05.003.
41. FAA Reauthorization Act: Progress and Challenges Implementing Various Provisions of the 2012 Act. Available online: https://apps.dtic.mil/sti/citations/AD1102097 (accessed on 23 December 2023).
42. Gorman, S.; Dreazen, Y.J.; Cole, A. Insurgents hack US drones. *The Wall Street Journal*, *Dec. 17*, December 2009. https:/*/www.wsj.com/articles/SB126102247889095011*..
43. Katz, Y. IDF encrypting drones after Hezbollah accessed footage. *Jerusalem Post*, 2010. https:/*/www.jpost.com/israel/idf-encrypting-drones-after-hizbullah-accessed-footage*.
44. Wood, A. (2024). After ADS-B launch, security concerns raised: AIN., September 14, 2006, Retrieved from https://www.ainonline.com/aviation-news/air-transport/2006-09-14/after-ads-b-launch-security-concerns-raised
45. Ganaie, N.A. India's National Security: Issues and Challenges. Available online: 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 (accessed on 23 December 2023).
46. Unnikrishnan, M., ITT Calls On AT&T For ADS-B Infrastructure, Network Centers. (2007). September 04, 2007, Retrieved from https://aviationweek.com/itt-calls-att-ads-b-infrastructure-network-centers
47. Spainhower, M.; Butts, J.; Guernsey, D.; Shenoi, S. Security analysis of RSVP-TE signaling in MPLS networks. *Int. J. Crit. Infrastruct. Prot.* **2008**, *1*, 68–74. https://doi.org/10.1016/j.ijcip.2008.08.005.

48. Fried, A., & Last, M. (2021). Facing airborne attacks on ADS-B data with autoencoders. Computers & Security, 109, 102405.
49. Manesh, M.R.; Mullins, M.; Foerster, K.; Kaabouch, N. A preliminary effort toward investigating the impacts of ADS-B message injection attack. In Proceedings of the in 2018 IEEE Aerospace Conference, Big Sky, MT, USA, 3–10 March 2018; IEEE: New York, NY, USA; 2018, pp. 1–6.
50. Mirzaei, K. F., Carvalho, B. P. de, & Pschorn, P. (2019). March 23, 2019, EasyChair Preprint no. 851, Security of ADS-B: Attack Scenarios. Retrieved from https://easychair.org/publications/preprint/DpM4
51. Shang, F.; Wang, B.; Yan, F.; Li, T. Multidevice false data injection attack models of ADS-B multilateration systems. *Secur. Commun. Netw.* **2019**, *2019*, 8936784. https://doi.org/10.1155/2019/8936784.
52. Lubbe, H., Serfontein, R., & Coetzee, M. (2024, March). Assessing the Effectiveness of ADS-B Mitigations. In International Conference on Cyber Warfare and Security (Vol. 19, No. 1, pp. 535-544).
53. Yang, H.; Li, H.; Shen, X.S. Modern Cryptography for ADS-B Systems. In *Secure Automatic Dependent Surveillance-Broadcast Systems*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 19–59.
54. Bavdekar, R.; Chopde, E.J.; Agrawal, A.; Bhatia, A.; Tiwari, K. Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations. In Proceedings of the International Conference on Information Networking, Bangkok, Thailand, 11–14 January 2023; pp. 146–151. https://doi.org/10.1109/ICOIN56518.2023.10048976.
55. Jochum, L.R.J. Encripted Mode Select ADS-B for Tactical Military Situational Awareness. 2001. Available online: https://dspace.mit.edu/bitstream/handle/1721.1/86721/49223652-MIT.pdf;sequence=2 (accessed on 25 December 2023).
56. Kožović, D. V., Đurđević, D. Ž., Dinulović, M. R., Milić, S., & Rašuo, B. P. (2023). Air traffic modernization and control: ADS-B system implementation update 2022: A review. FME Transactions, 51(1), 117-130.
57. Agbeyibor, R. Secure ADS-B: Towards Airborne Communications Security in the Federal Aviation Administration's Next Generation Air Transportation System. Theses and Dissertations. 2014. Available online: https://scholar.afit.edu/etd/584 (accessed on 25 December 2023).
58. Wesson, K.D.; Humphreys, T.E.; Evans, B.L. Can cryptography secure next generation air traffic surveillance? *IEEE Security and Privacy Magazine*, 20-Mar-2014., p. 1-8
59. Zhang, S.; Li, H.; Dai, Y.; Li, J.; He, M.; Lu, R. Verifiable Outsourcing Computation for Matrix Multiplication With Improved Efficiency and Applicability. *IEEE Internet Things J.* **2018**, *5*, 5076–5088. https://doi.org/10.1109/jiot.2018.2867113.
60. Li, H.; Yang, Y.; Dai, Y.; Yu, S.; Xiang, Y.; Bai, J. Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data. *IEEE Trans. Cloud Comput.* **2020**, *8*, 484–494. https://doi.org/10.1109/TCC.2017.2769645.
61. Feng, Z.; Pan, W.; Wang, Y. A data authentication solution of ADS-B system based on X. 509 certificate. In Proceedings of the 27th International Congress of the Aeronautical Sciences, ICAS, Nice, France, 19–24 September 2010; pp. 1–6.
62. Gentry, C.; Silverberg, A. Hierarchical ID-based cryptography. In Proceedings of the Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, New Zealand, 1–5 December 2002; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2501, pp. 548–566. https://doi.org/10.1007/3-540-36178-2_34/COVER.
63. Chow, S.S.M.; Hui, L.C.K.; Yiu, S.M.; Chow, K.P. Secure hierarchical identity based signature and its application. In Proceedings of the Information and Communications Security: 6th International Conference, ICICS 2004, Malaga, Spain, 27–29 October 2004; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3269, pp. 480–494. https://doi.org/10.1007/978-3-540-30191-2_37/COVER.
64. Cook, E. ADS-B, friend or foe: ADS-B message authentication for NextGen aircraft. In Proceedings of the 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, New York, NY, USA, 24–26 August 2015; IEEE: New York, NY, USA, 2015; pp. 1256–1261.
65. Sher, B., Ahmad, M., Mansoor, K., Bangash, Y. A., Iqbal, W., & Mussiraliyeva, S. (2024). Lightweight secure authentication protocol for automatic dependent surveillance broadcast system. Cluster Computing, 1-16.
66. Pan, W.J.; Feng, Z.L.; Wang, Y. ADS-B data authentication based on ECC and X. 509 certificate. *J. Electron. Sci. Technol.* **2012**, *10*, 51–55. https://doi.org/10.3969/j.issn.1674-862X.2012.01.009.
67. Baek, J.; Byon, Y.J.; Hableel, E.; Al-Qutayri, M. An authentication framework for Automatic Dependent Surveillance-Broadcast based on online/offline identity-based signature. In Proceedings of the 2013 8th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2013, Compiegne, France, 28–30 October 2013; pp. 358–363. https://doi.org/10.1109/3PGCIC.2013.61.
68. Yang, H.; Huang, R.; Wang, X.; Deng, J.; Chen, R. EBAA: An efficient broadcast authentication scheme for ADS-B communication based on IBS-MR. *Chin. J. Aeronaut.* **2014**, *27*, 688–696. https://doi.org/10.1016/j.cja.2014.04.028.

69. Markani, J.H.; Amrhar, A.; Gagné, J.-M.; Landry, R.J. Security establishment in ADS-B by format-preserving encryption and blockchain schemes. *Appl. Sci.* **2023**, *13*, 3105.
70. EBSCOhost∣100818950∣ An Efficient Broadcast Authentication Scheme with Batch Verification for ADS-B Messages. Available online: 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 (accessed on 26 December 2023).
71. Yang, A.; Tan, X.; Baek, J.; Wong, D.S. A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification. *IEEE Trans. Serv. Comput.* **2015**, *10*, 165–175.
72. Chen, X., He, D., Peng, C., Luo, M., & Huang, X. (2024). A Secure and Effective Hierarchical Identity-based Signature Scheme for ADS-B Systems. IEEE Transactions on Aerospace and Electronic Systems.
73. Yang, H., Zhou, Q., Yao, M., Lu, R., Li, H., & Zhang, X. (2018). A practical and compatible cryptographic solution to ADS-B security. IEEE Internet of Things Journal, 6(2), 3322-3334.
74. Pennapareddy, S., Srinivasan, R., & K, N. (2024). A method to mitigate cyber exploits on automatic dependent surveillance-broadcast (ADS-B) data transmissions. Aircraft Engineering and Aerospace Technology, 7 May 2024.
75. Yang, H.; Yao, M.; Xu, Z.; Liu, B. LHCSAS: A Lightweight and Highly-Compatible Solution for ADS-B Security. In Proceedings of the 2017 IEEE Global Communications Conference, GLOBECOM 2017—Proceedings, Singapore, 4–8 December 2017; Volume 2018; pp. 1–7. https://doi.org/10.1109/GLOCOM.2017.8254500.
76. Yang, H.; Li, H.; Shen, X.S. *Secure Automatic Dependent Surveillance-Broadcast Systems*; Springer: Berlin/Heidelberg, Germany, 2022. https://doi.org/10.1007/978-3-031-07021-1.
77. Boneh, D.; Franklin, M. Identity-Based Encryption from the Weil Pairing. *SIAM J. Comput.* **2003**, *32*, 586–615. https://doi.org/10.1137/S0097539701398521.
78. Yi, P.; Li, J.; Zhang, Y.; Chen, Y. Efficient Hierarchical Signature Scheme with Batch Verification Function Suitable for ADS-B System. *IEEE Trans. Aerosp. Electron. Syst.* **2023**, *59*, 1292–1299. https://doi.org/10.1109/taes.2022.3197684.
79. Asari, A.; Alagheband, M.R.; Bayat, M.; Asaar, M.R. A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems. *Comput. Networks* **2021**, *185*, 107599. https://doi.org/10.1016/j.comnet.2020.107599.
80. He, D.; Kumar, N.; Choo, K.-K.R.; Wu, W. Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 454–464. https://doi.org/10.1109/tifs.2016.2622682.
81. Burfeind, B.; Mills, R.; Nykl, S.; Betances, J.A.; Sielski, C. Confidential ADS-B. In Proceedings of the IEEE Aerospace Conference Proceedings, Big Sky, MT, USA, 2–9 March 2019; Volume 2019. https://doi.org/10.1109/AERO.2019.8742166.
82. Braeken, A. Holistic Air Protection Scheme of ADS-B Communication. *IEEE Access* **2019**, *7*, 65251–65262. https://doi.org/10.1109/access.2019.2917793.
83. Manesh, M.R.; Velashani, M.S.; Ghribi, E.; Kaabouch, N. Performance comparison of machine learning algorithms in detecting jamming attacks on ADS-B devices. In Proceedings of the 2019 IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 20–22 May 2019; IEEE: New York, NY, USA, 2019; pp. 200–206.
84. Kacem, T.; Kaya, A.; Keceli, A.S.; Catal, C.; Wijsekera, D.; Costa, P. ADS-B Attack Classification using Machine Learning Techniques. In Proceedings of the 2021 IEEE Intelligent Vehicles Symposium Workshops (IV Workshops), Nagoya, Japan, 11–17 July 2021; IEEE: New York, NY, USA, 2021; pp. 7–12.
85. Yang, H.; Li, H.; Shen, X.S. Complete ADS-B Security Solution. In *Secure Automatic Dependent Surveillance-Broadcast Systems*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 117–141.
86. Khan, S.; Thorn, J.; Wahlgren, A.; Gurtov, A. Intrusion detection in automatic dependent surveillance-broadcast (ADS-B) with machine learning. In Proceedings of the 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, 3–7 October 2021; IEEE: New York, NY, USA, 2021; pp. 1–10.
87. Mink, D.M.; McDonald, J.; Bagui, S.; Glisson, W.B.; Shropshire, J.; Benton, R.; Russ, S. Near-Real-Time IDS for the U.S. FAA's NextGen ADS-B. *Big Data Cogn. Comput.* **2021**, *5*, 27. https://doi.org/10.3390/bdcc5020027.
88. Karam, R.; Salomon, M.; Couturier, R. A comparative study of deep learning architectures for detection of anomalous ADS-B messages. In Proceedings of the 2020 7th International Conference on Control, Decision and Information Technologies (CoDIT), Prague, Czech Republic, 29 June 2020–2 July 2020; IEEE: New York, NY, USA, 2020; pp. 241–246.
89. Wang, J.; Zou, Y.; Ding, J. ADS-B spoofing attack detection method based on LSTM. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 1–12. https://doi.org/10.1186/s13638-020-01756-8.

90. Karam, R.; Salomon, M.; Couturier, R. Supervised ADS-B Anomaly Detection Using a False Data Generator. In Proceedings of the 2022 2nd International Conference on Computer, Control and Robotics (ICCCR), Shanghai, China, 18–20 March 2022; IEEE: New York, NY, USA, 2022; pp. 218–223.
91. Guo, X.; Zhu, C.; Yang, J.; Xiao, Y. An Anomaly Detection Model for ADS-B Systems Based on Improved GAN and LSTM Networks. In Proceedings of the 2021 IEEE 21st International Conference on Communication Technology (ICCT), Tianjin, China, 13–16 October 2021; IEEE: New York, NY, USA, 2021; pp. 802–809.
92. Joseph, N.S.; Banerjee, C.; Pasiliao, E.; Mukherjee, T. FlightSense: A spoofer detection and aircraft identification system using raw ADS-B data. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020; IEEE: New York, NY, USA, 2020; pp. 3885–3894.
93. Ying, X.; Mazer, J.; Bernieri, G.; Conti, M.; Bushnell, L.; Poovendran, R. Detecting ADS-B spoofing attacks using deep neural networks. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; IEEE: New York, NY, USA, 2019; pp. 187–195.
94. Habler, E.; Shabtai, A. Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages. *Comput. Secur.* **2018**, *78*, 155–173. https://doi.org/10.1016/j.cose.2018.07.004.
95. Danev, B.; Zanetti, D.; Capkun, S. On physical-layer identification of wireless devices. *ACM Comput. Surv.* **2012**, *45*, 1–29. https://doi.org/10.1145/2379776.2379782.
96. Zeng, K.; Govindan, K.; Mohapatra, P. Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]. *IEEE Wirel. Commun.* **2010**, *17*, 56–62. https://doi.org/10.1109/mwc.2010.5601959.
97. Liu, Y.; Ning, P.; Dai, H.; Liu, A. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In Proceedings of the 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; IEEE: New York, NY, USA, 2010; pp. 1–9.
98. Pöpper, C.; Strasser, M.; Capkun, S. Jamming-resistant broadcast communication without shared keys. In Proceedings of theUSENIX Security Symposium, Montreal, QC, Canada, 10–14 August 2009; pp. 231–248.
99. Strasser, M.; Popper, C.; Capkun, S.; Cagalj, M. Jamming-resistant key establishment using uncoordinated frequency hopping. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 18–22 May 2008; IEEE: New York, NY, USA, 2008, pp. 64–78.
100. Reisman, R.J., “Air traffic management blockchain infrastructure for security, authentication, and privacy. In Proceedings of the AIAA Scitech 2019 Forum, San Diego, CA, USA, 7–11 January 2019. https://doi.org/10.2514/6.2019-2203.
101. Kakimoto, K., Immaru, T., Ikeda, M., & Barolli, L. (2024, April). A Filtering Method for Machine Learning Utilization of ADS-B Data. In International Conference on Advanced Information Networking and Applications (pp. 251-260). Cham: Springer Nature Switzerland.
102. Akerman, S.; Habler, E.; Shabtai, A. VizADS-B: Analyzing Sequences of ADS-B Images Using Explainable Convolutional LSTM Encoder-Decoder to Detect Cyber Attacks. *arXiv* **2019**, arXiv:1906.07921. https://arxiv.org/abs/1906.07921v1.
103. Chen, S.; Zheng, S.; Yang, L.; Yang, X. Deep Learning for Large-Scale Real-World ACARS and ADS-B Radio Signal Classification. *IEEE Access* **2019**, *7*, 89256–89264. https://doi.org/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.