A Survey on Security of Automatic Dependent Surveillance - Broadcast (ADS-B) Protocol : Challenges, Potential Solutions and Future Directions

Hammad Ahmed Khan*, Haibat Khan*†, Salman Ghafoor‡ and Mansoor Ahmed Khan*
*College of Aeronautical Engineering, National University of Sciences & Technology, Islamabad, Pakistan
‡SEECS, National University of Sciences and Technology (NUST), Pakistan

***Abstract*—This work delves into critical examination of the broadcast data safety of Automatic Dependent Surveillance-Broadcast (ADS-B) system, an essential protocol for aircraft identification and navigation. Globally mandated by civil aviation regulatory bodies, ADS-B plays a pivotal role in shaping the future of Air Traffic Management initiatives. This study thoroughly investigates the vulnerabilities inherent in the open and un-encrypted nature of ADS-B data transmission. Given the widespread availability of Software-Defined Radios (SDRs), these security threats pose significant risks to Air Traffic Services and passenger safety. In light of these challenges, the paper scrutinises existing research and industry documents to comprehensively understand ADS-B vulnerabilities and assess threat levels and potential attacks. We also review recent developments and analyze proposed countermeasures aimed at enhancing the security of ADS-B data, possibly through protocol modifications or infrastructure enhancements.**

***Index Terms*—ADS-B; Air Traffic Control; Authentication; Aviation; broadcast; data security; encryption; privacy; Private Key; transponders; wireless;**

I. Introduction

THE aviation industry has experienced unprecedented growth in recent decades, swiftly transitioning from basic flight training to achieving faster speeds, extended ranges, and efficiently airlifting heavy loads to support global economies. The International Civil Aviation Organization (ICAO), which serves as the core authority for regional aviation regulators and the global custodian of passenger and freight volume indicators, estimates an average of over 100,000 flights per day. This equates to approximately 400 departures per hour, transporting around 10 million passengers and billions worth of goods airborne [64]. Fig 1 illustrates the substantial volume managed by the Federal Aviation Administration in the year 2021 in the United States alone.

With the anticipated rise in unmanned airborne traffic, addressing airspace congestion has become critical. Traditional Air Traffic Management (ATM) approaches, that rely on procedural Air Traffic Control (ATC) and RADAR surveillance, are insufficient for growing demands. Regulatory bodies, like the US Federal Aviation Administration (FAA), are swiftly modernizing airspace control by transitioning to satellite-based systems, thereby enhancing capacity, safety, and navigation [1]. Global aviation authorities, including FAA and Eurocontrol, are integrating these solutions into Air Traffic Services (ATS) under ICAO. The Automatic Dependent Surveillance-Broadcast (ADS-B) system, a key enabler of this shift, provides comprehensive airspace coverage and a commercialized air traffic picture for both industry and the public.

Fig. 1: Air Traffic by the Numbers: FAA, USA April 2023

The evolution of ADS-B demands automation based on information technology and wireless communication, introducing significant information security challenges. Fig 2 depicts the Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of the ADS-B System, deduced from various sources, cited and discussed further in this paper. The open, un-encrypted broadcast nature of ADS-B makes it susceptible to confidentiality, availability, and integrity attacks. Low-cost software-defined radios and high-end processors facilitate data manipulation. Scholarly articles highlight security concerns, and ICAO urges research to mitigate threats. Current countermeasures rely on triangulation and data fusion with legacy systems, posing a paradox as ADS-B aims to replace them. Ensuring ADS-B security requires cryptographic means for authentication, prompting the need for global research on encryption and authentication techniques.

A. Motivation behind the Survey

Since its global mandate in 2020 by the FAA, ADS-B has significantly improved airport surveillance, providing

†Corresponding Author

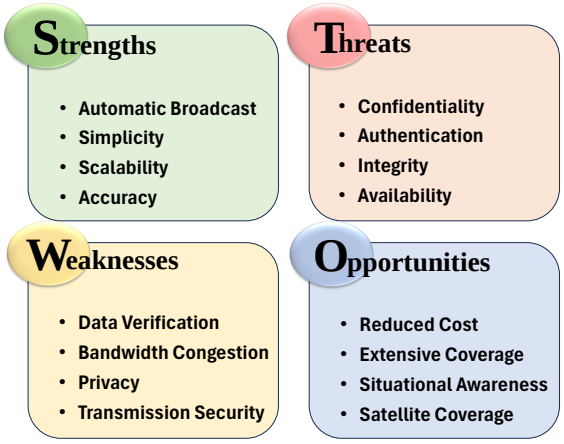


Fig. 2: ADS-B SWOT Analysis

comprehensive air traffic data on platforms like FlightRadar24 and OpenSky Networks. Live and historical data, accessible on PCs and mobile devices, enhance situational awareness. While ADS-B has become a standard retrofit for commercial aircraft, security concerns persist due to open communications. The ease of eavesdropping on ADS-B and other wireless protocols (e.g., ACARS, CPDLC) raises privacy and data confidentiality issues. Affordable Software-Defined Radios (SDRs) enable easy reception and positional tracking, challenging the security of ADS-B.

Signal triangulation and data fusion validate ADS-B data but increase operating costs, contrary to the cost-effective vision of future ATM systems. Full security and authentication of ADS-B require encryption, yet challenges in key distribution and protocol openness remain. Expedited exploration of encryption schemes is crucial for large-scale deployment assessments. This survey addresses post-mandate scenarios, real-world security issues, industrial opinions, limitations, research contributions, and analyses of implemented solutions in the context of ADS-B security.

B. Literary Contributions on ADS-B security surveys

The evolution of new security schemes, particularly those involving Machine Learning (ML) and Artificial Intelligence (AI), continues to offer improved mechanisms for validating positional information and enhancing broadcast security through encryption schemes. Review articles since the year 2011 have been summarily compared in Table I. Fig 4 illustrates various techniques discussed in previous reports and research articles. Despite this progress, the dynamic nature of ADS-B information security issues, especially in the post-mandate era, necessitates robust solutions against emerging challenges.

Extensive research has been conducted on the matters discussed above, reflecting the continuous advancements in Information Security and Machine Learning. Table II presents a comparison of previous ADS-B security surveys, including notable works by Strohmeier [86], Manesh [55], and Wu [98]. These studies delve into the implementation of ADS-B, its vulnerabilities, and proposed security solutions based on substantial research archives. It is essential to note that these articles predate the mandated implementation of the system and do not encompass insights from industrial / commercial-level documentations of regulatory authorities such as ICAO, FAA, Eurocontrol, etc. To the best of the authors' knowledge, no comprehensive article exists that compiles post-ADS-B mandate, industrial-level privacy and security issues, along with potential solutions to mitigate them. As a response to this gap, this research survey aims to compile state-of-the-art studies, literary work, and practical in-use systems and solutions deployed worldwide.

The paper is structured into several sections, each addressing specific aspects of ADS-B technology and its security implications. These sections include an overview of ADS-B (Section II), an exploration of its vulnerabilities (Section III), strategies for securing ADS-B information (Section IV), a discussion and reflection on the findings (Section V), future research directions (Section VI), and concluding remarks (Section VII).

II. ADS-B System Overview

The increasing diversity of aircraft roles, types, and capabilities requires more robust traffic control systems. While RADAR-based surveillance once served this purpose, limitations in ground-based systems and advancements in Satellite-based technologies prompted a shift. The FAA NextGen Air Traffic System (ATS) aims to replace land-based ATC systems with satellite-based technologies for enhanced situational awareness [1]. A key component of this transition is the Automatic Dependent Surveillance-Broadcast (ADS-B) system, transmitting aircraft identity, position/ speed, and operational status globally. ADS-B exists in two forms: "ADS-B Out" (transmitter) and "ADS-B In" (receiver) [7]. Fig. 3 illustrates an ADS-B integrated Traffic Collision Avoidance System (TCAS) display, available to aircrew, assisting in avoiding collision courses, often without ground controllers' intervention.

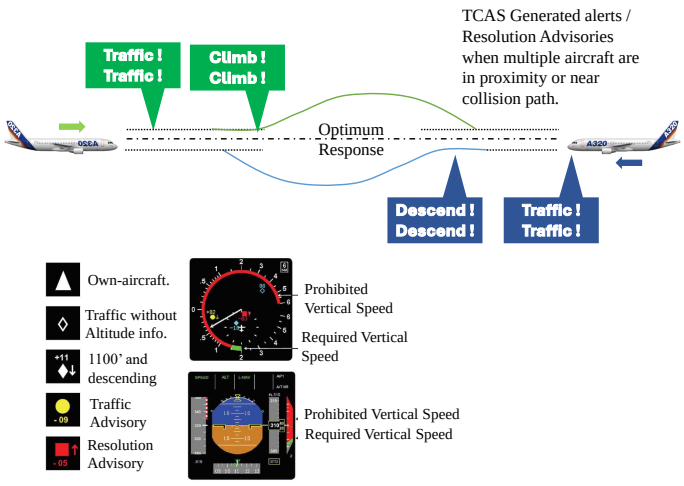


Fig. 3: Typical TCAS Display and Autopilot / Flight Director assisted collision avoidance concept

TABLE I: Comparison of existing ADS-B security survey articles

Author, Year	Title of Research	Aspect	Threat Perception	Security Solutions Compilation Work			Future Work Suggestion
				Position Verification	Broadcast Security	Attack Detection	
Sampigethaya et al, 2011 [75]	Security and privacy of future aircraft wireless communications with off-board systems	Aeronautical Wireless Data-Links & ISP Security	Data Corruption, Information Misuse, Delay and Repudiation	GBAS, MLAT, Data Fusion, Radio Nav, Group Certification, RSS	ICAO Pseudonym	X	Evaluation of threats related to ADS-B Jamming
McCallie et al., 2011 [58]	Security analysis of the ADS-B implementation in the next-generation air transportation system	ADS-B Attacks effects with the level of difficulty	Authentication, Integrity, Privacy, Jamming	General recommendations related to organizational de-classification of security certification procedures, holistic security analysis of complete NextGen program along with ADS-B implementation			Urge to devise solutions through research
Costin and Francillon, 2012 [20]	Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices	Inexpensive and highly successful attacks on ADS-B with COTS items	Authentication, Integrity, Privacy, Jamming, Replay	X	Lightweight PKI, Third-party certification	X	Security analysis of other ADS Data Formats (DF=19,22) and secure modes
Schaefer et al, 2013 [77]	Experimental Analysis of Attacks on Next-Generation Air Traffic Communication	Inexpensive and highly successful attacks on ADS-B with COTS items	Statistical profiling, message injection, modification and deletion	Kalman Filtering, MLAT	Symmetric Encryption (Pre-shared Key), Crypto Hash sums	X	
Strohmeier et al, 2013 [87]	Security of ADS-B State of the Art and Beyond	ADS-B Attack Detection and Prevention using other wireless communication security methods	Eavesdropping, Deletion, Jamming, Replay, Modification, Ghost Injection Attacks	Distance Bounding, Kalman Filtering with intent, MLAT, Group Verification, Data Fusion, Traffic Modeling, Spread Spectrum	Cryptographic Schemes (PKI, FPE, ECC, X509, TESLA, MAC). Spread Spectrum	Fingerprinting (Software, Hardware, Channel)	ADS-B Attack Reaction
Strohmeier et al, 2014 [88]	Realities and challenges of NEXTGEN air traffic management: the case of ADS-B	ADS-B channel behaviour and its security challenges in dense traffic	Message Collision, Antenna and Doughnut effects, Duplication due to Multipath, Weather Effects, Receiver Flooding, Ghost Data, Deletion, Modification, Spoofing	X	X	X	Future perspectives for ADS-B with exponentially growing airborne platforms, specifically UAVs
Strohmeier et al, 2015 [86]	On the Security of the Automatic Dependent Surveillance-Broadcast Protocol	Security Challenges of ADS-B, Attack detection and countermeasures	Risk Analysis and Effects of Interception, Deletion, Modification, Jamming and Injection Attacks	Distance Bounding, Kalman Filtering with intent, MLAT, Group Verification, Data Fusion, Traffic Modeling, Spread Spectrum	Cryptographic Schemes (PKI, FPE, ECC, X509, TESLA, MAC). Spread Spectrum	Fingerprinting (Software, Hardware, Channel)	Suggestion to implement position verification methods and future protocol development with security as a basic requirement
Viveros CAP, 2016 [94]	Analysis of the Cyber Attacks against ADS-B: Perspective of Aviation Experts	Obtaining user awareness on the impact of various types of ADS-B attacks and their consequences	Qualitative Analysis of ADS-B jamming, injection, deletion and modification attacks	X	X	X	Awareness program for pilots and controllers by training through simulated attacks and research on solutions to detect the attack
Manesh and Kaabouch, 2017 [55]	Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system	Security Challenges of ADS-B, Attack detection and countermeasures	Risk Analysis and Effects of Interception, Deletion, Modification, Jamming and Injection Attacks	Distance Bounding, Kalman Filtering, MLAT, Group Verification, Data Fusion, Traffic Modeling	Cryptographic Schemes (PKI, TESLA, MAC). Spread Spectrum	Fingerprinting (Software, Hardware, Channel)	Multi-layer security frameworks comprising a number of simple methods that can detect and mitigate different ADS-B attacks
Li and Wang, 2018 [52]	Sequential collaborative detection strategy on ADS-B data attack	Analysis of ADS-B Common Attack Patterns	Data Tampering, Ghost Data Injection, Data Replay, DoS Attack,	X	X	IMM Filter, MLAT, Distance bound, Statistical Methods, Flight Plan Validation, Air-Ground Collaboration,	Solutions for Replay and Ghost Data Injection Attacks
Mirzaei et al, 2019 [59]	Security of ADS-B: Attack Scenarios	Security Challenges of ADS-B, Attack detection and countermeasures	Eavesdropping, Deletion, Jamming, Replay, Modification, Ghost Injection Attacks	Kalman Filtering, Data Fusioning,	Cryptographic Schemes (PKI, TESLA). Spread Spectrum	X	Innovative multilayer solution with backward compatibility, cost-effectiveness and widespread acceptance
Zhijun Wu et al., 2020 [98]	Security Issues in Automatic Dependent Surveillance-Broadcast (ADS-B): A Survey	Security Challenges of ADS-B, Attack detection and countermeasures	Eavesdropping, Deletion, Jamming, Replay, Modification, Ghost Injection Attacks	MLAT, Kalman Filtering, Group Certification, Data Fusion, Distance Bounding, Traffic Modeling	Cryptographic Schemes (PKI, FPE, ECC, X509, TESLA, MAC). Spread Spectrum	Fingerprinting (Software, Hardware, Channel)	1090ES Channel Congestion Analysis, GNSS Accuracy Risk, Use of Blockchain Technology and Deep Learning for ADS-B Security, Satellite-based ADS-B
Kacem et al, 2021 [40]	ADS-B Attack Classification using Machine Learning Techniques	ADS-B Attacks classifiers using Machine Learning Technology	Eavesdropping, Jamming, Replay, Single and Multiple Aircraft Ghost Injection Attacks	X	HMAC in place of CRC in ADS-B	ML Multi-class Classifiers (SVM, Decision Tree, Random Forest)	Security patch with the consideration of backward compatibility, reducing costs of implementation, and widespread acceptance
Habler et al, 2023 [29]	Assessing Aircraft Security: A Comprehensive Survey and Methodology for Evaluation	Effects of cyber-attacks on avionics systems and their effect on aircraft essential capabilities	Eavesdropping, jamming, denial of service, spoofing and impersonation attacks	Integrity Frameworks proposed by Sampigethaya [75] (discussed above), MLAT Optimization, Data Fusion	Encryption Schemes discussed by Wu et al [98] (discussed above)	Machine and Deep Learning	Formulation of a unified platform to assess and evaluate all proposed security solutions

TABLE II: Comparison of this publication with existing ADS-B security survey articles

Domain	[86]	[55]	[98]	Our Survey
Understanding ADS-B and its impact on Air Traffic Management	✓	✓	✓	✓
Industrial guidelines and regulations in implementing ADS-B	Limited		Limited	Extensive
Industrially acknowledged security issues of ADS-B				✓
Probable scenarios consequent to ADS-B vulnerabilities	✓	✓	✓	✓
Commercially implemented ADS-B security solutions				✓
Theoretical and experimental work on countermeasures by research community	✓	✓	✓	✓
Additional hardware requirement for ADS-B data validation	✓	✓	✓	✓
Variation and deviation from standard ADS-B protocol in implementing security solutions	✓	✓	✓	✓
Analysis of implemented and proposed ADS-B security solutions	✓	✓	✓	✓

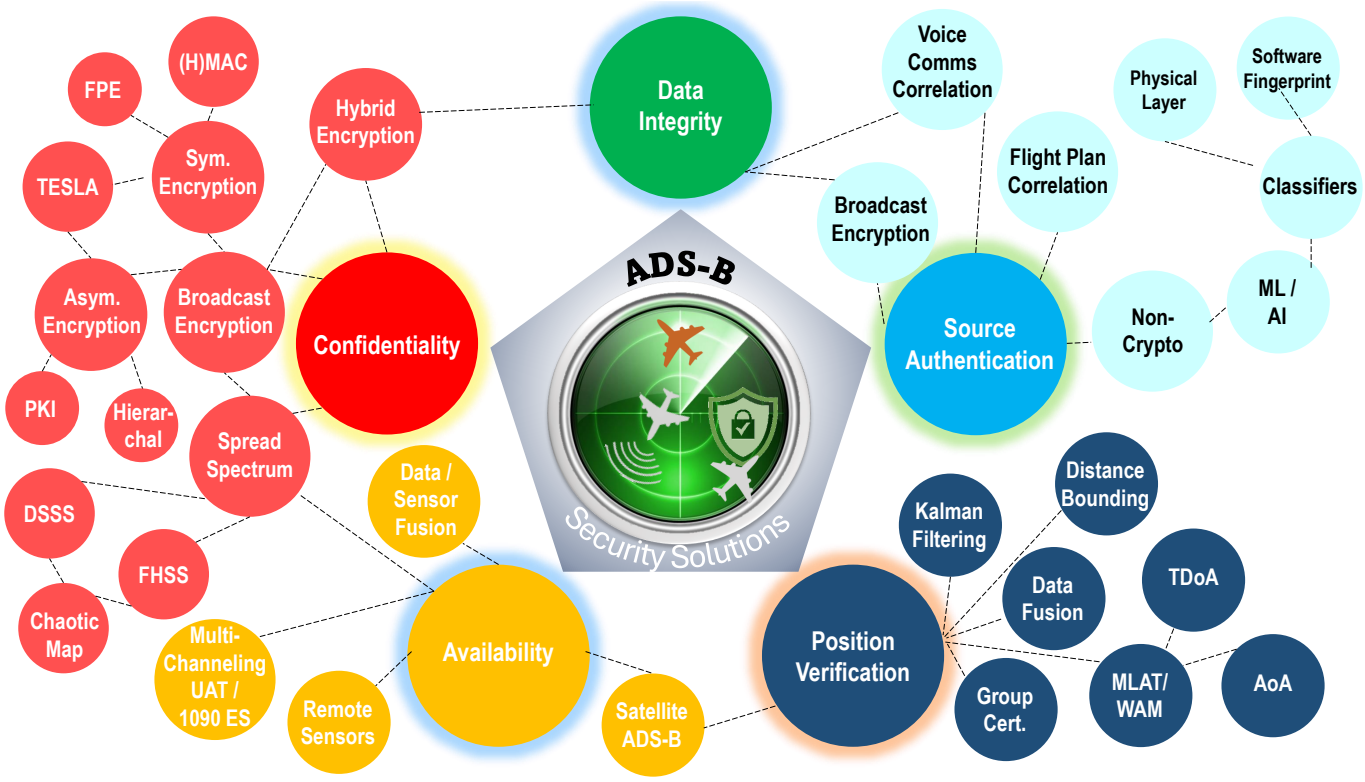


Fig. 4: Overview of the various techniques discussed in previous ADS-B security surveys

A. Legacy Airborne Surveillance and its Limitations

Electromagnetic reflection-based Primary Surveillance RADARs (PSRs) are the most common surveillance systems being used overtime. However, information provided by these, does not suffice in identification and classification of the identified entities. This gap brought-in the concept of Secondary Surveillance where the acquisition challenge from the interrogator is replied with requisite information by airborne transponder over standard 1030 MHz and 1090 MHz frequencies respectively. Fig 5 shows the principle of transponder operation [60]. Co-bore-sighted and usually mounted atop a PSR, Secondary Surveillance RADAR (SSR) initially used to identify aircraft through four octal digit squawk code (Mode A) and aircraft calculated barometric altitude (Mode C) in periodic challenges and replies. With time, growing air-traffic density led to the limitation of squawk codes (only 84 =4096 possible combinations) and problems such as synchronous garbling (due to reply signal overlap) and FRUIT (false replies un-synchronized in time) [89] in Mode A and C of SSR. To mitigate these, a new protocol Mode Select Beacon System or Mode-S was developed by MIT in the 1970s [89].

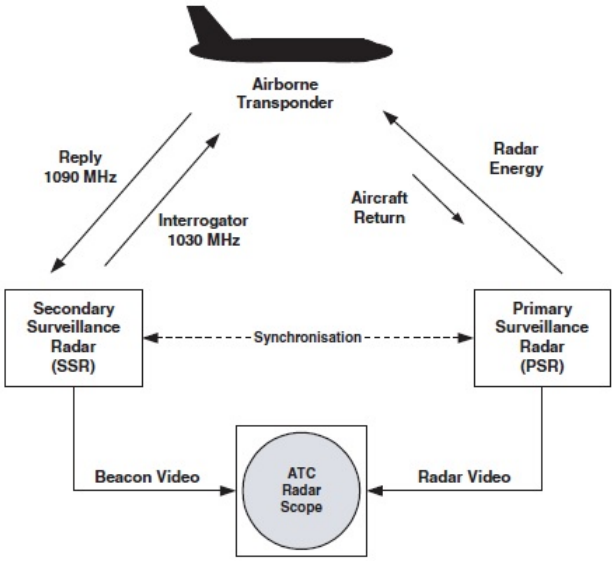


Fig. 5: Principle of transponder operation. *Source*[60]

B. Mode S

Evolving from the very basic identity (Mode A) and altitude (Mode C) information exchange, Mode-S functions on selective interrogations which allows it to gather different information from different aircraft conveniently. Because of its working principle, airborne transponder replies are only based on the type of information acquired by the interrogator, thereby effectively addressing the replies-interference problems. There are a total of 256 data registers in Mode-S transponder, containing different types of information regularly updated by the aircraft flight management systems and different on-board sensors [68]. Based on the information acquired by the interrogator, data contained within the appropriate register is transmitted over reply. Mode-S reply packet structure consists of 8 Preamble bits followed by either 56-bit (short) or 112-bit (extended) squitter message at 2Mbps rate (64 µs or 120 µs duration) as shown in Fig 6. Each bit is Pulse Position Modulated (PPM), which means every bit is distributed into 0.5 µs pulse which precedes to flat signal in case of 1 and reverse order for 0. Each message contains 5 format (up-link/down-link) bits, 24 address and parity bits each. Complete message length (short or extended squitter) and types of information, exchanged on Mode-S acquisition are identified with Up-link / Down-link Formats detailed in ICAO document 9871 [68] and summarized in Table III.

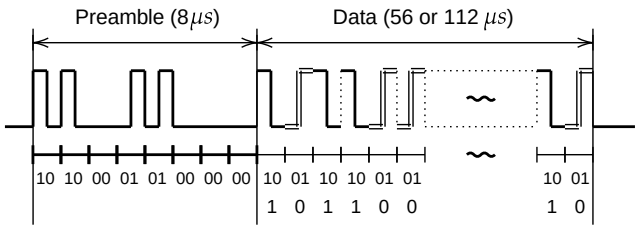


Fig. 6: An example of Mode S reply message. *Source*[89]

C. ADS-B Basics

Range of acquisition-based surveillance system is always limited by the geographical location of the interrogators. An aircraft cannot be detected on surveillance scope unless it is within the interrogator's coverage zone. To avoid this limitation, it is necessary that airborne transponder must not rely on the acquisitions only, and should also be able to announce its presence otherwise. This is where concept of ADS-B system comes in, where one of the Mode-S Downlink format (DF=17) has been reserved to broadcast information automatically, without the need of interrogations. This broadcast does not require operator / pilots' input (hence automatic) and delivers navigational information gathered by aircraft systems (dependent) through ADS-Out equipment

TABLE III: Mode S uplink and downlink formats

UF/DF	Bits	Uplink and Downlink type
0	56	Short air-air surveillance (ACAS)
4	56	Surveillance, altitude request and reply
5	56	Surveillance, identity request and reply
11	56	Mode S All-Call and reply
16	112	Long air-air surveillance (ACAS)
17	112	Extended squitter transmit
18	112	Extended squitter/non transponder transmit
19	112	Military extended squitter transmit
20	112	Comm-A/B, altitude request and reply
21	112	Comm-A/B, identity request and reply
24	112	Comm-C/D (ELM)

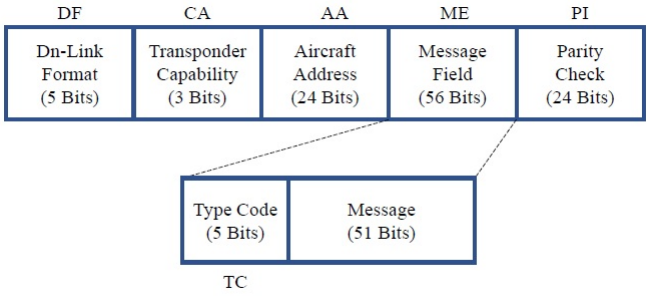


Fig. 7: ADS-B Message Format

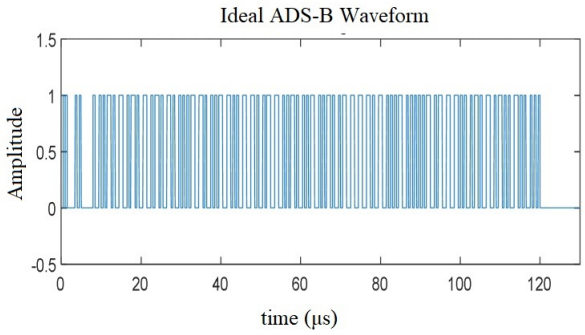


Fig. 8: Illustration of ADS-B Waveform

to surveillance nodes (ADS-In equipment), that can either be airborne or ground-based receivers. This information is shared around the globe on platforms such as Flightradar24 [26] for enhanced situational awareness and better air traffic management.

ADS-B Message is 28 hexadecimal-character long frame, coded into 112 bits (extended squitter) preceded by 8 standard Mode-S preamble bits. It contains Downlink Format (DF, 5 bits), Transponder Capability (CA, 3 bits), ICAO given Address (ICAO, 24 bits), Message Field (ME, 56 bits) and Parity Check (PI, 24 bits) as sub-frames shown in Fig 7. The initial five bits within a message (ME) subframe are Type Code (TC) and describe the type of information contained within the remaining 51 bits of the ME field (summarized in Table IV and detailed in ICAO 9871 document [68]). Following the same transmission mechanism of Pulse Position Modulation (PPM) as that of Mode-S reply, ADS-B message is broadcast over standard 1090 MHz, in the shape of Amplitude Modulated signals as illustrated in Fig 8.

TABLE IV: ADS-B Type Code and content

Type Code	Data frame content
1–4	Aircraft identification
5–8	Surface position
9–18	Airborne position (w/Baro Altitude)
19	Airborne velocities
20–22	Airborne position (w/GNSS Height)
23–27	Reserved
28	Aircraft status
29	Target state and status information
31	Aircraft operation status

'ADS-B In' equipped receivers listen, decode, present, and relay the information over Intranet / Internet protocols using third-party software. In addition to this, airborne ADS-B receivers can use this information to update their Traffic Collision Avoidance Systems (TCAS). The complete ADS-B concept is shown in Fig 9.

D. ADS-B Growth and Future

Presently, three ADS-B data link standards have been proposed including VHF digital link mode 4 and Secondary Surveillance Radar Mode S ultra-long message (1090ES). Among them, Universal Access Transceiver (UAT) and 1090 Extended Squitter (1090ES) are the two most popular models that compete with one another. For implementation, new hardware must be installed since the UAT mode, which operates at a frequency of 978MHz, specifically created for aviation services. Working at a frequency of 1090MHz is the 1090ES protocol. Only the aircraft's original S-mode transponder equipment has to be upgraded in order to use it. Fig 10 displays their relationship.

ADS-B broadcast operates in an open and clear format, with well-documented commercial encoding / decoding processes [68], [89], making it easily implementable. Widespread adoption of ADS-B has been accelerated by low-cost Software Defined Radios (SDRs) and straightforward decoding. Many aviation regulators globally mandate ADS-B Out on aircraft entering their airspace at specific altitudes. ICAO provides

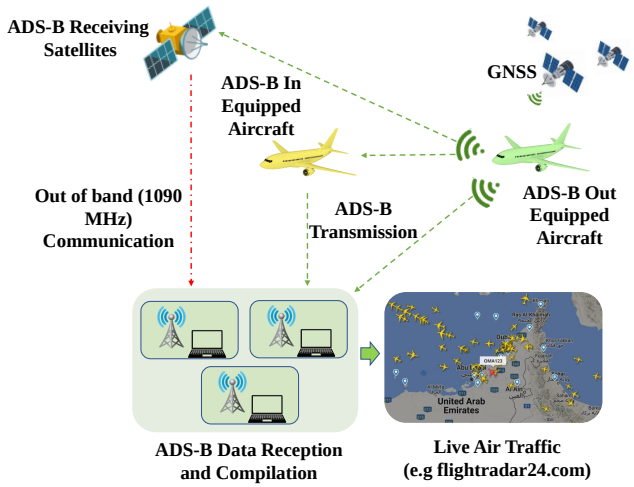


Fig. 9: ADS-B system concept. ADS-B signals are received both at ground and in air for a data-fused air picture. Moreover, satellite-based ADS-B receivers also relay the same information on system-specific frequencies other than 1090 MHz.

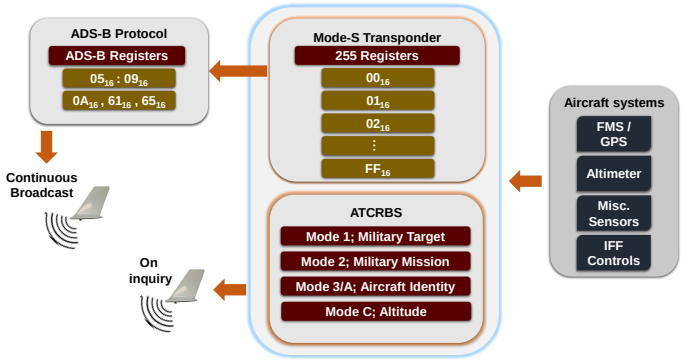


Fig. 10: ADS-B protocol hierarchy

precise Implementation and Operations Guidance for ADS-B worldwide, forming the backbone of projects like FAA's NextGen ATS. ATC automation systems using ADS-B enhance situational awareness for controllers, aiding in safer traffic routing. Coupled with ADS-Rebroadcast (ADS-R), Traffic Information System Broadcast (TIS-B), and Flight Information System Broadcast (FIS-B), ADS-B addresses range limitations and provides information on non-equipped aircraft [83]. However, substantial airspace remains uncovered globally due to geo-location constraints. To bridge this gap, Aireon extends ADS-B to satellite-based receivers [18]. Iridium-NEXT satellite system, hosting Aireon Systems, receives ADS-B data on standard 1090 MHz and relays it to ground stations for further dissemination to ATM nodes or Navigation Services Providers [15]. This extension reduces range constraints in remote areas, enabling Satellite-Based Air Traffic Management with comprehensive coverage at a lower cost, as illustrated in Fig 11.

In addition to ADS-B, European Union Aviation Safety Agency (EASA) has introduced Automatic Dependent Surveillance-Light (ADS-L) to cater for the exponential rise in UAV traffic [4]. They have doled out the concept of U-Space which is "a set of new services and specific procedures designed to support safe, efficient and secure access to airspace for large numbers of drones without airspace segregation for the sole use of drones". ADS-L is defined as the "minimum standard for making manned aircraft in U-space conspicuous (visible) to U-Space Service Providers (USSP)". It is a new standard, intended to operate on an 860 MHz short-range device band (860SRD), compatible with low-cost devices, GNSS enabled and based on simplified ADS-B for future use.

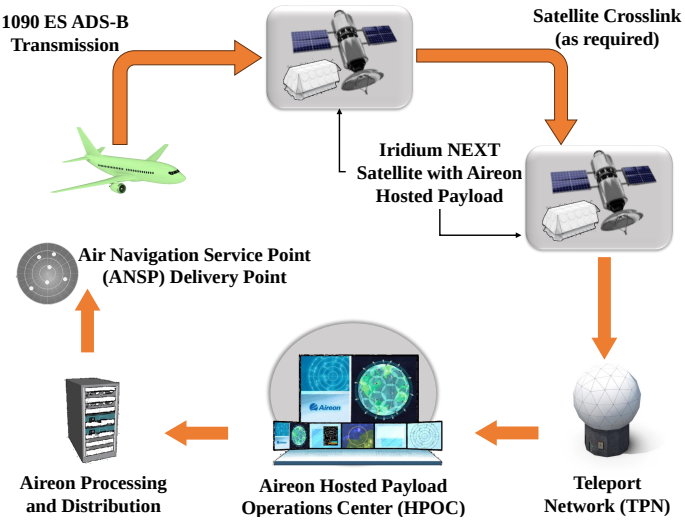


Fig. 11: The Aireon Space-based ADS-B System. ADS-B receivers are mounted over Iridium Satellites which receive and relay ADS-B information to ground and other satellites. The Operations Center combine the information for the consumption of ANSPs.

III. Literature Review on ADS-B Vulnerabilities and Countermeasures

Civil aviation communication channels, both voice and data, are usually kept open for clear and ambiguity-free message exchange essential to flight safety. However, the perils of data manipulation and denial are no stranger to ADS-B. Since the architecture is open, it becomes an attractive invitation for hackers, spoofers, and disrupters. The broadcast information remains available in the air, and can be easily downloaded using commercially available, low-cost Software Defined Radios (SDR). This information can be further used for eavesdropping, modification, deletion, playback and denial of service purpose. ICAO too understands the security risks involved and urges the stakeholders to assess the risks and propose mitigation in cognizance with national organizations [7], [66]. This section compiles ways and means researched over the years to protect ADS-B data and provide message authentication and integrity, core to securing digital communications, in line with the ICAO considerations.

A. Threat Perception by ICAO and FAA

Citing similarity with other civil Communication Navigation Surveillance (CNS) technologies, ICAO defines ADS-B as an 'open system', fully standardized and public. It also considers the simplicity of the technology and possibility of false traffic emission from airborne or ground locations, thereby resulting in affecting confidentiality (eavesdropping), integrity (spoofing and/ or modification) and availability of the transmitted ADS-B data [66]. Considerations have been proposed based on varying degree of threat that include EASA recommended switching off ADS-B transmissions over given scenarios, controlling information over the internet and use of encrypted ADS-B (DF=19) as potential measures among others to avert the confidentiality threat. It also suggests controllers to correlate ADS-B data with voice communication and other available ancillary information to identify false messages, false traffic information and false alarms from virtual (ghost) aircraft. Moreover, jamming scenarios based on disruption of GNSS services, transmission of high-powered noise on 1090 MHz and ADS-In saturation (due to excessive false message injections) have been discussed along with procedural remedial actions. Table V provides ICAO-identified security issues associated with

TABLE V: ICAO identified security risks associated with ADS-B

Security Requirement	Potential Vulnerability	Remedial Consideration (Procedural)
Confidentiality	Aircraft ID and positional data publicly known due to open broadcast	• Support masking off sensitive and military flights • Use of privacy modes (e.g FAA's PIA Program) • Use of DF=19 (encrypted ADS-B)
	Use of open ADS-B data to coordinate • Attacks against specific airborne targets (e.g VIP) • Flight surveillance for economic intelligence • ADS-B data relay over internet	• Variations in Flight ID • ADS-B switch off capability • Legislative Controls (likely ineffective)
Integrity	False Messages (from virtual aircraft) • Spoofing • False Short Term Collision Alert (STCA) • False traffic information • Spurious separation manoeuvres	• Correlate surveillance with comms, plans etc • Alert mechanism using data fusion • Multilateration • Automation to warn of suspicious activity
	Message Alteration / Deletion • between ground station and ATM system • loss of aircraft visualization for controller	• Appropriate schemes for network security • Management similar to avionics failure
Availability	Jamming • 1090 MHz; incapacitating ground station • GPS; denying positional data • False messages; saturating receiver and ATM services	• Management similar to ground station failure • Use of other navigational means like inertial • Data filtering, ground station disconnection

ADS-B.

The FAA portrays the ADS-B NextGen surveillance program as a game-changing initiative for the aviation industry [1]. It has real-time precise capabilities, shared situational awareness and enhanced applications for both controllers and pilots. Additionally, it decreases costs and lessens detrimental environmental consequences while increasing safety and effectiveness in the air and on runways. Having said so, the FAA also recognizes some operators' desire to restrict the amount of real-time ADS-B position and identification data that is available for a given aircraft. It started the Privacy ICAO aircraft Address (PIA) initiative over US registered, 1090 MHz ADS-B equipped aircraft, flying domestically in the US, and using third-party call-signs to address privacy concerns. With the help of the PIA program, interested aircraft owners can ask for a different, temporary ICAO aircraft address that won't be allocated to them in the Civil Aviation Registry (CAR).

B. Types of Attacks and Consequences

Numerous ongoing and past research works have identified and even practically demonstrated the types of attacks that could be carried out on ADS-B Systems. A simple code on MATLAB can generate, modulate, and transmit the ADS-B message of choice with the help of SDR. Fig 12 shows possible attack scenarios. Zhijun Wu et al [98] and Martin Strohmeier [86] has concisely explained in their surveys such attacks which are summarized in subsequent subsections.

1) Message Injection (Spoofing Attack): The standard message structure of ADS-B can be easily duplicated, modified (or spoofed) and re-transmitted as a ghost, over the air, only to be received by ADS-B ground receivers as a legitimate one. This ghost attack can be conveniently conceived with the help of commercially available SDRs and has been demonstrated by Pearce [69], Slimane [84], Shang [82] and Schäfer et al [77]. This attack can be carried out both from air or ground with varying options. An already recorded ADS-B data received earlier or a tactfully manufactured sequence of false ADS-B messages can be transmitted as a ghost data injection attack to distract the ground controller and pilots. Similarly, ghost aircraft data can disrupt traffic and confuse traffic collision avoidance systems (TCAS), as a result, jeopardizing flight

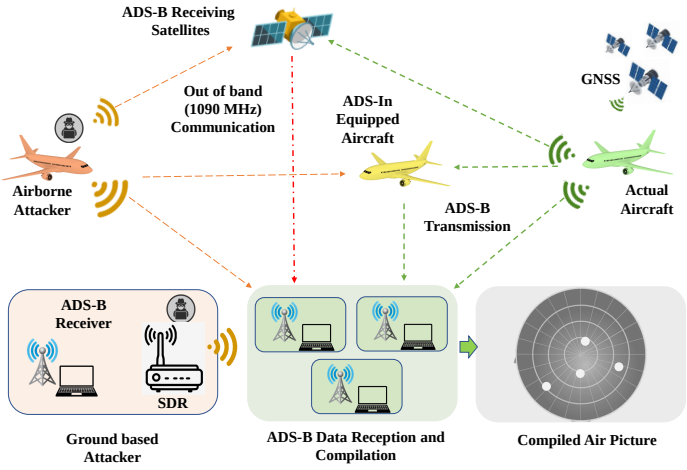


Fig. 12: ADS-B attack scenarios. Open communication remains susceptible to Spoofing and Denial Attacks over the air by either of ground or air-based attackers.

safety. The efficacy of such an attack lies in the proximity of the attacker to the receiver. An attacker can duplicate a legitimate ADS-B receiver, simply by tuning SDR to 1090 MHz and if close enough to the ground station, can assess signal strength information, time difference and angle of arrival information as well. This information can be used to synchronize the attack clock with the target system and a seamless intrusion can be made with false data while keeping in sync with all information passing nodes, consequently deceiving any triangulation-based counterattack setup. A controller can be deceived if false data is accompanied by an attacker's audio communication pretending to be a real pilot. In airborne attack setup, TCAS of target aircraft can be confused to generate false alarms or more dangerously saturating out, inhibiting its capacity to warn of impending collision.

2) Message Deletion (DoS Attack): There can be two ways to deny legitimate messages to the 'ADS-B In' receivers. One is to corrupt the message beyond parity correction and the other is to suppress it through synchronized opposite phase transmission. 24 bits of parity are used in ADS-B protocol messages that can rectify up to 5-bit errors. ADS-B message parity bits can correct errors up to 5 bits. Any message that has more than five incorrect bits is regarded as corrupted and is rejected. This type of attack, however, requires sophisticated equipment and strict time synchronization, which is extremely complex to attain. In this kind of attack, the perpetrator makes legal ADS-B messages disappear. An example of an attack that uses either constructive or destructive interference is an aircraft disappearance attack. In case of constructive interference, the attacker intentionally introduces enough bit errors into an ADS-B message for the receiver to mistakenly deduce that the message is corrupted and discard it. In the event of destructive interference, the ADS-B signal is obliterated while it is being transmitted. The attacker creates a time-synchronized signal that is the opposite of the ADS-B signal and reduces or entirely destroys the ADS-B message. Successful destructive interference depends on time synchronization; its complexity makes this kind of message deletion attack harder to carry out and less effective. A valid aircraft may become invisible to other aircraft and ground stations if a successful constructive interference or destructive interference attack is launched. This may result into air traffic disruptions and / or an elevated risk of aircraft crashes.

3) Message Modification (Integrity Attack): Extremely difficult to attain, such an attack focuses either on specific bit flipping of legitimate message by super-imposing fake information over the air or entire message deletion and retransmission of the modified message. Pöpper et al [72] and Wilhelm et al [97] have explained the difficulty level. It requires precise synchronization to target specific bit(s) and complex power calculations to cause bit flipping. The most challenging attack is one that involves altering a message transmitted by a valid ADS-B network node. The attacker would need to have access to the network hardware to successfully change a message, which is exceedingly difficult to acquire. To implement message modification attacks, however, three methods can be used:-

- *Overshadowing*. It is the act of an attacker sending powerful signals that completely or partially replace or alter a valid communication. In contrast to jamming, this technique focuses on the communications of a single node rather than the entire communications channel.
- *Bit flipping*. When an attacker overlays a fake signal that converts numerous 0 values to 1 values or vice versa.
- *Combined message deletion and insertion.* An attacker transmits a powerful signal to interrupt / deny an actual message while relaying ghost data simultaneously, effectively carrying out a modification attack.

4) Reconnaissance (Eavesdropping Attack): The absence of encryption in ADS-B messages makes these vulnerable to message interception, also known as eavesdropping or aerial reconnaissance. Every aircraft equipped with 'ADS-B Out' is visible to the public via commercial websites like [26], [25], [63], and [3]. While this information is valuable for legitimate purposes like tracking air traffic, it can also be exploited to monitor specific private jets or analyze air traffic patterns for malicious intent. Concerns about this potential for eavesdropping have existed since the inception of ADS-B. Although services mentioned earlier can legitimately trace air traffic, they can also be misused for highly sophisticated attacks. Examples include investigative journalists uncovering CIA rendition flights and business meetings leading to merger and acquisition reports [33]. The fundamental issue lies in the lack of encryption, rendering it technically impossible to prevent eavesdropping. Some nations, such as the United Kingdom, have enacted laws to prohibit unauthorized listening to ADS-B broadcast messages. However, the implementation of these rules is impractical due to inherent technical vulnerabilities. The absence of encryption allows easy interception, making it extremely challenging to effectively thwart eavesdropping and enforce compliance with these regulations.

5) Jamming: A message jamming attack involves the deliberate transmission of packets by a jammer to prevent authorized participants in a communications session from transmitting and/or receiving data, leading to a denial-of-service scenario. The jammer could hinder a genuine user from locating an open channel by persistently delivering data packets. Although jamming is a significant problem in wireless networks, its significance in aviation is heightened due to the importance of air traffic data and the large, prospectively uncontrolled operational environment. Ground station flood denial attacks and aircraft flood denial attacks are two types of ADS-B jamming techniques. By silencing communications, these attacks stop a monitoring network in its tracks. A ground station flood denial attack is simpler than an aircraft-based one since the attacker can approach the target more closely, using less power. Leonardi et al have presented in their work [50] vulnerabilities of ADS-B against low-cost jammers. They have concluded that considerable range degradation occurs in ADS-B coverage in relation to jammers' close location to ground stations. Their experiments showed effective range reduction from 220 NM to around 40 NM with a jammer within 1.10 km of the receiver. Evaluation of the arguments is based on three types of simulated jamming signals, which are as follows:-

1) *ADS-B message with random data block repeated with*

10 micro sec interval

2) *Stream of ICAO standard preambles*
3) *Random binary sequence with ppm mod*

ADS-B jamming can be of three types:-

- *Jamming / spoofing of GNSS data*. Since ADS-B positional information is derived from GNSS information, jamming same can adversely affect the performance. However, such an attack can be countered over the aircraft having backup inertial navigation or multi-constellation (GPS, GLONASS, BEIDOU etc) receivers.
- *Jamming of 1090 MHz band*. Such jamming incapacitates all sorts of surveillance communications occurring on 1090 MHz, which include SSR as well. A localized attack can be thwarted through data fusion, however, the risk remains higher in case jamming occurs near airports or dense traffic zones.
- *'ADS-B In' (receiver) saturation*. Heavy spoofing, which involves extensive transmission of false or malicious ADS-B messages, can overwhelm the processing capacity of receivers, potentially rendering them unable to function properly. In more severe cases where multiple receivers are subject to moderate spoofing attacks, there is a risk of overloading the central processing system responsible for providing air traffic information to controllers, leading to potential service disruptions.

Summarizing the possible attack types, it can be conveniently said that ADS-B's open broadcast can be easily corrupted. Moreover, with the advent of low-cost SDRs, implementation of most of such attacks is trivial. Malicious planning and ATM service disruptions are mostly the outcome of such attacks. Table VI shows ADS-B vulnerabilities, attack threat, cost / skill involved and possible consequences.

C. Industrial Impact and Deployed Security Mechanisms

EUROCONTROL opines Air Traffic Management as a cyber security challenge and appreciates its importance in the rapid pace of digitisation of ATM systems. Apart from history of ATM cyber-attacks and incidents, privacy exploitation of aviation users have been referred in [33]. As per their reports, of all attacks in 2019, 20% targeted ANSPs consequently leading to leakage of sensitive data to cyber criminals and state sponsored groups. A cyber incident reported at Boeing subsidiary 'Jeppesen' in 2022 caused flight planning disruptions [91]. The Airbus Group disclosed that, on average, twelve significant cyber attacks are launched against it annually [21]. Ukwandu et al have presented a comprehensive review of cyber-attack trends that occurred over the last 20 years [92]. Their findings indicate that the industry's primary cyber security concern arises from Advanced Persistent Threat (APT) groups, working in conjunction with state entities. Their objective is to obtain intellectual property and intelligence for the purpose of enhancing domestic aerospace capabilities, as well as to surveil, penetrate and undermine the capabilities of other nations. Such attacks can have a variety of effects, from minor pilot and ground controller distractions to major Denial-of-Service (DoS) attacks that can considerably increase the likelihood of aircraft crashes and negatively affect airspace security [55]. As per the law firm Stephenson Harwood's article [30], 61% of all cyber-attacks in 2020 targeted airlines. In face of such a degree of threat, open architecture of ADS-B is increasingly becoming a very soft target and with mandatory use in effect, the challenge grows even further.

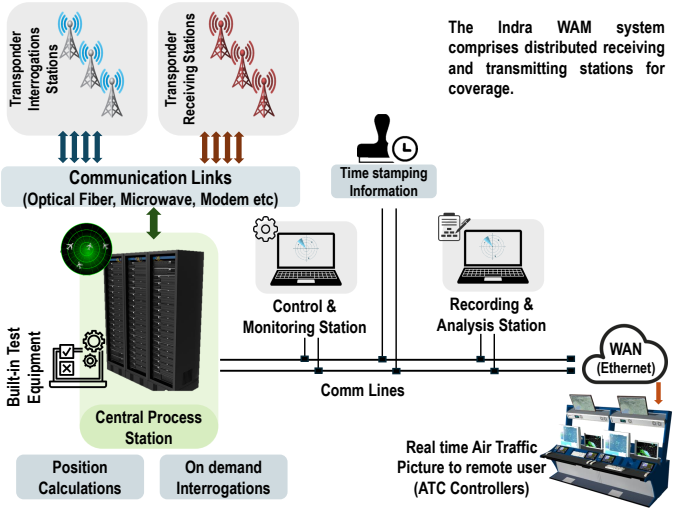


Fig. 13: Illustration of Indra WAM system[19]

Recent articles [23], [69], [90] and survey reports [86], [98] state that utilizing cheap and easily accessible off-the-shelf hardware and software, it is reasonably simple to exploit the un-encrypted ADS-B broadcast signals. Attackers can intercept and alter ADS-B communications using these techniques, as well as delete, falsify, and jam entire data exchange channels.

In response to the existential threat environment, major firms involved in aviation systems production have collaborated with ICAO and regional aviation regulators to come up with multi-dimensional systems to validate received ADS-B data and securely transport it to ATM nodes. Most of these systems are based on Multi-Lateration (MLAT; like signal triangulation but with more than 3 signals) and Data Fusion (independent sources), details of which are given in subsequent Sections IV-A. Some of the leading manufacturers of these equipment pitched their products during ICAO meetings in 2021. Fig 13 shows Indra Company's Wide Area Multi-Lateration (WAM) deployed in Spain, Switzerland, Geneva and Canada [19]. Thales Group presented Non-RADAR Surveillance products including a thorough report on ADS-B security issues and demonstrated spoofing and meaconing (change of identity) attacks. Fig 14 shows the excerpts from their presentations [61].

IV. Implemented and Academically Proposed Solutions for ADS-B Security

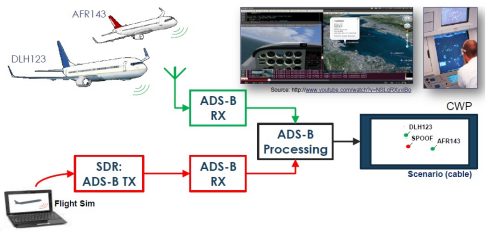
Vulnerabilities in ADS-B open broadcast and perceived threats are a reality. ICAO recommends studies to further assess security risks in coordination with state organizations and Air Navigation Service Providers (ANSPs) and appreciates devising mitigation steps to consider the operational

TABLE VI: ADS-B Attacks Analysis vis-à-vis required Skill and Cost

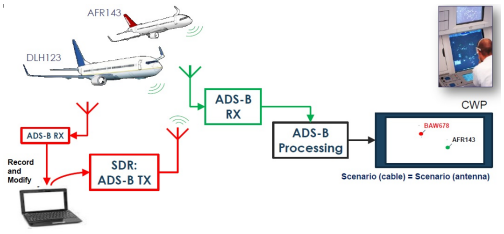
Security Requirement	Attack Threat	Required Skill	Cost Involved	Possible Consequence
Confidentiality	• Eavesdropping • Interception	• SDR operation • Relevant tracking software knowledge	• SDR • Internet Connection	• Personal / Entity Tracking • Harassment • Malicious Planning
Integrity	• Message Deletion • Message Modification	• SDR operation • RF Txr operation • ADS-B understanding • Aviation protocol understanding • Clock synchronization knowledge • Hacking skills	• Hi-power SDR • ADS-In Equipment (SDR) • Relevant Softwares	• Missing aircraft / information • Controller incapacity • Unreliable ATC Operations • Incorrect Traffic Management • TCAS Corruption • Flight Plan Deviation
Authentication	• Replay • Message Injection (Spoofing)	• SDR operation • ADS-B Out knowledge • Simulation parameters knowledge • Audio Communication conversant • Aviation protocols understanding • RF communication knowledge	• Hi-powered SDRs • ADS-In Equipment (SDR) • Relevant Softwares	• Traffic Saturation • Resource waste on ghost data • Controller confusion
Availability	• Jamming • Flooding	• RF knowledge • ADS-B working • Aviation protocols understanding • Hi-powered transmission handling • GNSS understanding • ADS-B Message injection capability	• Tactical Jammer • Hi-powered SDRs • Relevant Softwares	• Resource failure • Manual verification • Unreliable ATC operations

environment and air traffic management requirements [66]. An efficient security mechanism should neither be too naïve nor too overwhelming. Therefore, it becomes essential that vital areas be identified and protected in priority to those which do not pose a threat. ADS-B frame shown in Fig 7 has to be observed for the fields / sub-frames, manipulation of which can really make the dent. Based on data manipulation, sub-frames can be categorized into two types, those that can cause message rejection and others which can be spoofed and accepted by the receivers. Table VII summarizes the same.

There can be several ways an attacker can innovate means to exploit the lack of data security in ADS-B. The mind-diagram shown in Fig 15 entails a few of those along with the domain of security which gets affected due to open communications. In addition to information denial at the GNSS source via high-powered and long-ranged strategic jammers (typically state-sponsored and utilized in strategic scenarios), there are generally two overarching categories of attacks. The first involves variations that result in message rejection, typically producing a straightforward jamming effect. The second, and more concerning category, pertains to the spoofing of information that poses a substantial threat due to its potential to go undetected. Spoofed ADS-B data can result into falsified position and identity of the aircraft, which could be catastrophic in case of dense air traffic. Table VIII shows a review of Wu et al [98] on Vulnerability Risk Analysis based on various types of attacks on ADS-B.



(a) Spoofing Demo. In addition to actual ADS-B transmission from legitimate aircraft, a spoofer using SDR is able to inject false information into receiving nodes



(b) Meaconing (ID Changing) Demo. An attacker is using recorded ADS-B information from a legitimate flight, to modify its aircraft identity and re-transmit to look like an actual aircraft on the controllers' screen

Fig. 14: Thales Group ADS-B attack demonstrations. *Source* [61]

TABLE VII: ADS-B Sub-frames data variation effects

ADS-B Sub Frames		Data Variation	ADS-B In Response		Probable Effect Reason
			Likely Effect[a]	Probable Effect[b]	
Dn-Lnk Format (5 Bits)		Manipulation	Rejected		Only DF=17 is a valid ADS-B Message
		Jamming			
Capability (3 Bits)		Manipulation	Accepted		All possible 0-7 combination are ICAO defined
		Jamming	Accepted		Parity correctable (upto 5 bits error)
ICAO Address (24 Bits)		Manipulation	Accepted		Any combination can be taken as valid ICAO Address
		Jamming	Rejected	Accepted	Only if Parity correctable (upto 5 bits error)
Message Field (56 Bits)	**TC (5 Bits)**	Manipulation	Accepted	Rejected	In case TC is not defined by ICAO
		Jamming	Rejected	Accepted	Only if Parity correctable (upto 5 bits error)
	Message (51 Bits)	Manipulation	Accepted	Rejected	If message is not in cognizance with received TC
		Jamming	Rejected	Accepted	Only if Parity correctable (upto 5 bits error)
Parity Check (24 Bits)		Manipulation	Rejected		Failed parity
		Jamming	Rejected		Failed parity

[a]System's default response to incoming messages.
[b]System's response when it cannot differentiate between legitimate and spoofed incoming messages.

Over the years, a substantial amount of research and proposals has emerged focusing on identifying and mitigating spoofing attacks on ADS-B. Strohmeier [86] and Wu [98] have presented a taxonomy of ADS-B security, a framework that this paper also follows. This taxonomy broadly falls into two domains: Position Verification and Broadcast Security, both converging on concepts of Message Authentication, Confidentiality, and Integrity. Fig 16 illustrates the areas under these two domains. Our approach, depicted in Fig 17, slightly differs as it introduces additional techniques and involves a minor re-branching.

A. Position Verification

Air traffic controlling is all about guiding and directing the aircraft towards their destination while maintaining safe longitudinal, lateral, and vertical distances between them. This purpose cannot be achieved without precise position knowledge of the aircraft. Ground-based legacy surveillance systems are limited due to geographic/ terrain variations and might gradually be phased out once low-cost and high-coverage space-based ADS-B system comes into use. However, for that, it is necessary that positional information relayed through 'ADS-B Out' is accurate, authentic and beyond corruption when it is received for processing. While accuracy is already taken care of by GNSS constellations, however, it is the latter that matters now. ADS-B combines GNSS and Barometric data of the aircraft with its ICAO address to broadcast its airborne or surface position. However, an attacker can replicate and manipulate this broadcast information by means discussed in Section III-B of this paper. To verify the received position, techniques like Multi-Lateration, Kalman Filtering, Group Certification and Data Fusion have been proposed in past, which are worth the effort.

1) Multi-Lateration Surveillance (MLAT): Adopted by ICAO, this technique is part of future ATM services described in ICAO Global ATM Operational Concept (Doc 9854). It tracks all transponder equipped (Mode S, A/C and ADS-B) information and works on Signal Time Difference of Arrival

TABLE VIII: ADS-B Attacks ; vulnerability risk analysis [98]

Attack Classification	Level	Attack Method	Harmful	Difficulty	Affected Factor		
					Confidentiality	Integrity	Availability
Aircraft Reconnaissance	Phy + App	Eavesdropping	Low	Low	X		
Replay Attack	Phy + App	Message Injection	High	Low	X	X	
Aircraft Target Ghost Injection	App	Message Injection	Medium	Medium		X	
Ground Station Target Ghost Injection	App	Message Injection	High	Low		X	
Aircraft Flood Denial	Phy	Signal Jamming	Medium	Medium			X
Ground Station Flood Denial	Phy	Signal Jamming	Medium	Lower			X
Virtual Aircraft Hijacking	Phy + App	Message Modification	High	High	X	X	
Virtual Trajectory Modification	Phy + App	Message Modification	High	High	X	X	
Aircraft Disappearance	Phy	Message Deletion	High	Low	X	X	X
Aircraft Spoofing	Phy + App	Message Modification	High	Low	X	X	

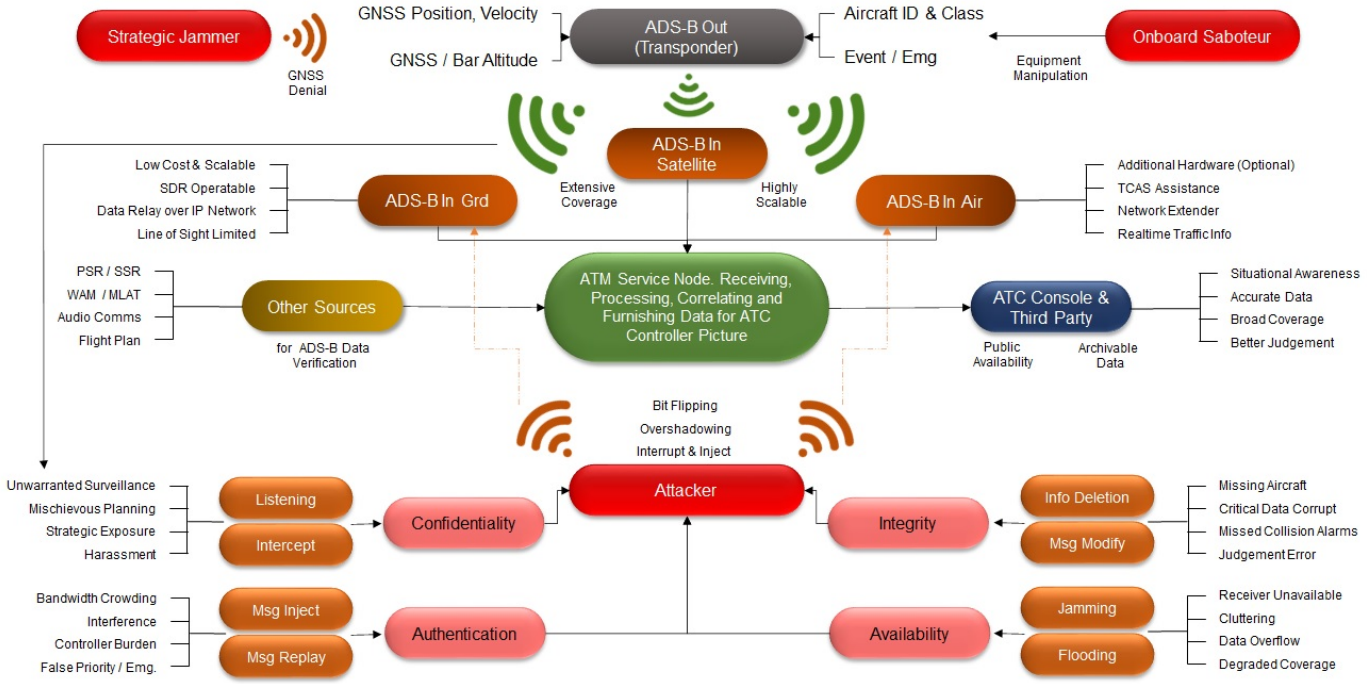


Fig. 15: Mind diagram on ADS-B working and threats

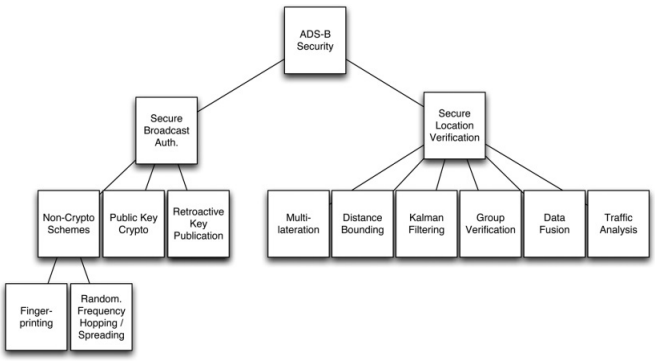


Fig. 16: Taxonomy of ADS-B security. *Source* [86]

(TDoA) between three or more distributed remote units (RU). It provides accurate position and identification information, benefiting from the triangulation of signals received at distant RUs, avoiding the line of sight and ground station failure issues. RUs receive, decode, timestamp, and send the data (over separate link) to Central Processor Stations (TP), which then perform position estimation and generate tracks to be used by Air Traffic Services Terminals through ASTERIX Cat 10/21 output [67]. Accuracy and low false tracks are achieved through Time Synchronization between all RUs and TP. ADS-B transponder performance validation is part of the MLAT scheme and with the fusion of information from other types of transponders, malicious attacks can be singled out and thwarted. Fig 18 shows the basic MLAT concept proposed in [35]. In case of ADS-B signals, the exact time the signal took to reach the receiver from the aircraft must be known to calculate the exact distance. This time information cannot be ascertained as received signals are interrogation-independent broadcasts from a moving platform. Therefore, the TDoA technique is used by utilizing a remotely distributing receiver antenna, which in this case is RU. Every RU has a hyperboloid coverage cone. TDoA information from specific aircraft received overall RUs gives an intersection point on constituent hyperboloids which gives accurate aircraft position. Fig 18 also shows the effect of geographically distributed RUs in positional estimation accuracy. In case of ADS-B positional information spoofing, this intersection point would either not exist or it might give multiple intersections as one from the original and the other from the attacker's side. It is pertinent that this position validation is as accurate as the number of RUs covering the transponder. This again brings in the issues

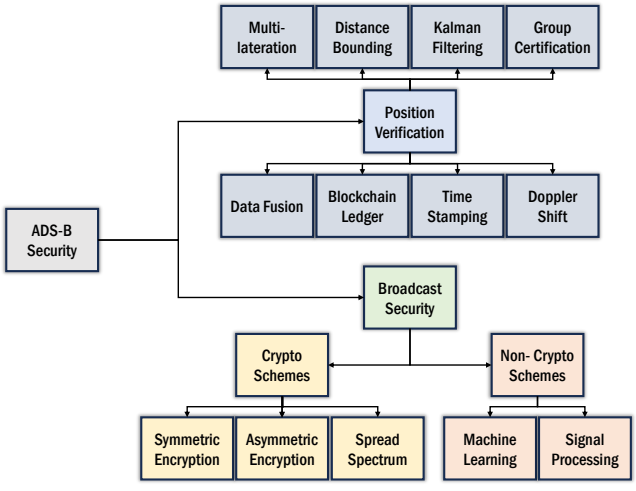


Fig. 17: Proposed taxonomy for ADS-B security

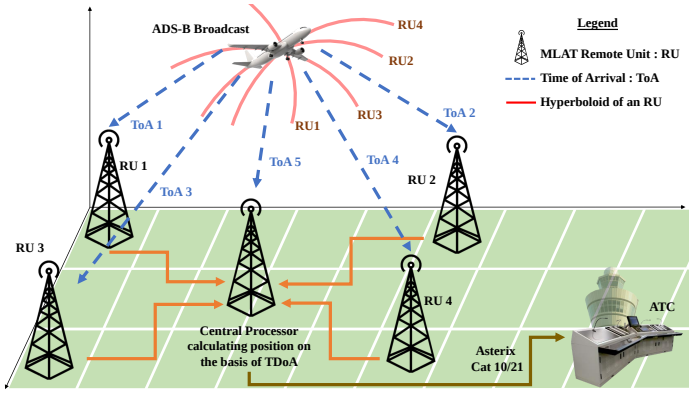


Fig. 18: Wide Area MLAT (WAM) conceptual architecture

of geo-location restrictions, installation and maintenance costs, automation setup, and equipment safety.

There are scenarios, in which MLAT can still be deceived. Some of them have been explained by Schuchman et al [79] in their secure ADS-S patent. In addition to those a few are annotated below:-

- Airborne spoofer can merely change its ICAO address over Mode-S only to be tracked as legitimate target.
- Another way to attack from a ground transmitter may be to use a unique ICAO address (in ADS-B broadcast) which is hitherto not present in MLAT coverage. This way a single intersection between limited hyperboloids can be observed as a legitimate target because of the absence of contradicting signals.

Many scholarly works exist regarding utilization of Multi-Lateration concept in aid to ADS-B location verification. Research works cited in [86] and [98] survey practical and experimental demonstrations and work studies. Apart from these, many state-of-the-art techniques have been lately proposed that can take the edge. Zhao et al [110] propose a hybrid TDoA and Angle of Arrival (AoA) technology with Extended Kalman Filtering (EKF), whereby en-route tracking accuracy of MLAT is enhanced by additional AoA measurements subsequently improving upon ADS-B position validation. The simulation and experimental findings illustrated that the inclusion of AOA measurements and the aircraft coordinated turn (CT) model can enhance positioning accuracy. Optimal positioning and alternative data processing schemes of MLAT RUs have been worked upon by Jheng [35], Ala' Darabseh [22], Bolelov [9] and Allmann et al [5]. Factors such as the inclusion of barometric altitude, signal time of arrival (ToA) localization techniques and received signal modelling can significantly improve the surveillance accuracy of WAM systems with errors as low as 150.87 m. Martone and Tucker [57] describe the evaluation of the Helicopter in-flight tracking system (HITS) project by the US Department of Transportation, which is about studying use of MLAT with ADS-B as an alternative to SSR in offshore areas with limited surveillance coverage. MLAT/ADS-B position validation uses a dynamic flight model only and establishes capability equivalence to the Air Traffic Control Beacon Interrogator Model 6 SSR system. El Marady [56] has proposed to fuse Flight Information System with same to improve upon the tracking accuracy by about a factor of 49%.

While the MLAT technique is currently in use and provides valuable functionality, it does increase the ongoing costs of ADS-B due to expenses associated with the installation, maintenance, and security of multiple RUs and TP.

2) Kalman Filtering: Kalman Filters find their extensive usage in numerous Guidance and Navigation-related technologies. These are particularly useful in determining the accuracy and integrity of the Navigation Sensors and related computations to determine the Actual Navigation Performance (ANP) of the system in real-time [60]. Basic theory pertains to the design of an estimator to predict un-measurable parameters from the measurable ones of the system based on its historical behaviour. State variables are given weightage based on their certainty levels and same are updated recursively on requirement [95]. This can be effectively used to smooth out data between instances with missing information, filter noise and elimination of bad data, which in this case could be false ADS-B messages. To understand the concept, we take the example of optimal position estimation from Inertial Navigation (prone to drifts with time) and GNSS sensors (susceptible to spoofing) readings. Kalman Filter combines inertial platform characteristics and their current errors, accuracy of GNSS signal and update of present position system estimate to compute and systematically decrease Circular Error Probability (CEP), thus providing the best possible Position Estimate. Analogous to the same, ADS-B receivers can use Kalman Filtering to estimate aircraft position based on its historical position broadcast and other known parameters to filter out malicious messages. Information in between missing ADS-B messages (disrupted for any reason) can be coasted and an inaccurate jitter or jump from a normal trajectory can be identified by using this technique.

One of the NASA-funded studies by Krozel et al [46] proposes a "system to provide continuous real-time state estimates of the aircraft being tracked and a verification that the aircraft is following the ADS-B broadcast intent". In their preposition, a correlation has been depicted between actual aircraft manoeuvres and ADS-B intent messages followed by geometrical computation to validate the conformance in horizontal, vertical and velocity dimensions. By using a suite of Kalman Filters on a fixed-size moving window over one of the data dimensions, ADS-B data is smoothed-out from erroneous, jittery, and noisy signals while ADS-B intent is analyzed to be within Required Navigational Parameters (RNP).

Leonardi et al have derived mathematical models of different attack types possible on ADS-B [51]. They propose a crowd sensor network and Extended Kalman Filtering to derive an aircraft kinematic model and continually predict its track to compare it with the emitter position to detect the false position reporting attacks. The aircraft kinematic model and emitter position are evaluated for consistency to detect false tracks that show deviation from the aircraft's estimated position forecasted from Kalman Filtering. They have modelled four types of threats given in Table IX.

Like MLAT, this scheme also makes use of signal TDoA

TABLE IX: Leonardi's modeled attacks and their consequences. [51]

Attack Type	Consequences
1. GNSS Jamming	Adverse effect on ADS-B Position reporting
2. GNSS Spoofing	
3. Fake ADS-B Message	Compromised Message Integrity
4. On-board Equipment Tampering	

in its attack detection algorithms. However, unlike MLAT, where this information is directly used for triangulation, it is used to verify consistency between model forecast and actual emission without solving the MLAT problem. This scheme has been extensively tested by the authors on OpenSky Network's public data [78] with promising results. Yang et al have identified limitations in the Kalman Filtering technique to correctly predict aircraft trajectory during fast maneuvering. They have analyzed the performance of the fading-memory filter, augmented process noise and particle filter techniques to be used along Kalman Filtering with tuned parameters to overcome the limitation in fast manoeuvring trajectory detection [105]. Weicai et al have designed an extended Kalman Filtering (EKF) algorithm to assess the ADS-B signal source in combination with the Low Earth Orbiting (LEO) satellite's location characteristics to verify the correctness in the reported and actual position of the ADS-B source [104]. They have verified the feasibility of their model with the help of software simulations.

Kalman Filtering techniques can be easily implemented and do not require any change in existing ADS-B system since they are working out of the network for verifying real-time location claim. They use historical data to predict trajectories and assess deviation from the same to identify an attack. The seemingly favourable solution to ADS-B security issues, Kalman Filters, however, would require parallel processing for every aircraft. Hence, in areas with dense air traffic, its implementation would remain ever-challenging with an increasing number of airborne platforms. Moreover, attacks such as those explored by Hopper [16] can deceive Kalman Filtering where the actual signal is jammed while continuously transmitting a spoofed signal with slight variations. This way, the spoofed signal would be considered as an actual signal and trajectory predictions would give in to the intent of the attack.

3) Distance Bounding: Based on the idea of determining the upper bound on physical distance between the communicating parties, Stefan et al proposed the "distance bounding" technique by timing the delay between challenge and response signals [13]. Initially implemented for the RFID checks, this concept has been scaled and enhanced for the ADS-B system. The basic idea revolves around time measurement between challenge and replies signals traveling at the speed of light to determine the max distance or upper bound of responder, which in this case is ADS-B transponder. Fig 19 shows the concept of distance bounding protocol. Distance bounding has been mostly used in limited space areas like security entrances or close distance Vehicular Adhoc Networks (VANETs). Languell et al have proposed a multi-point distance bounding technique for UAV Collision Avoidance. They use the 'Prover' and 'Verifier' concepts of distance bounding and introduce multiple points in the prover i.e. UAV's flight path and enable the verifier (either of another UAV or ground station) to measure the distance from the prover in noisy settings. The verifier chooses random time points and predicts the position of the prover over these points. This way, the lack of two-way communication in ADS-B is addressed [47].

Like MLAT, distance bounding works on the triangulation principle with various sensors sensing the same signal to estimate the accurate position of the emitter. Application of distance bounding in ADS-B security does not remain a very viable option since it works on challenge and reply concept, which is not the case for ADS-B. While Mode S replies based on acquisitions or interrogations can aptly apply distance bounding, it would require a major protocol shift for ADS-B to incorporate the same and would virtually reduce it back to the Mode S mechanism.

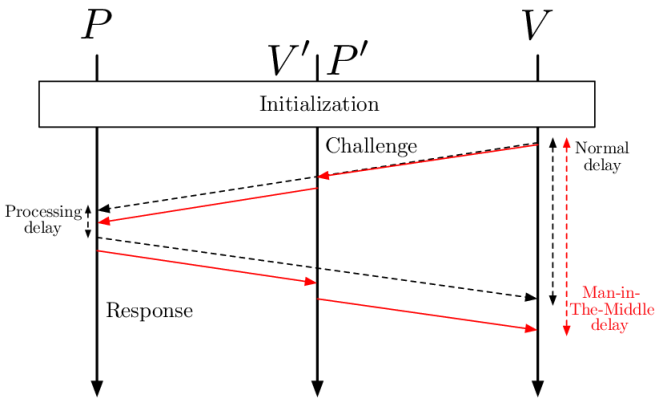


Fig. 19: Principle of distance bounding protocols. The verifier V sends a challenge to the prover P, who, after processing, sends his response (black dashed arrows). A man in the middle (V /P) can only increase the distance by adding further processing delays, but not decrease it (red arrows). *Source* [86]

4) Group / Batch Certification: Scholarly work on security and privacy of aircraft wireless communication by Sampigethaya extensively elaborates the working and future of e-enabled aircraft i.e. the ones which have the capability to reprogram flight critical avionics components wirelessly and via various data transfer mechanisms [75]. Vulnerabilities of open ADS-B system remain critical to the performance of same. This research not only presents the working mechanism but also the type of threats along with proposed various mitigation solutions. Author has observed that multiple aircraft in given distance can navigate as a group in geographical proximity, while they can maintain a fully connected IP network with insignificant signal degradation. This way, every member of the group will be able to share a communication link with every other member for intra-net communication and broadcast messages coming out of any constituent member, a scenario analogous to military formation flying. Like the concept of

MLAT, and with receivers being airborne group members, ADS-B signal from one aircraft can use the TDoA technique to estimate the actual position of the emitter once received by four or more aircraft of the group. Figure 20 shows the ADS-B group concept with details in [75]. This idea seemingly alleviates the geo-location limitations of MLAT, however, it is essential that all aircraft of the group are equipped with ADS-In equipment to listen to the transmissions. The mandate of ADS-In has not yet been established and not all commercial aircraft are fitted with the same. Moreover, criterion for joining group and building a trust within a network remains challenging aspect. Furthermore, identifying and countering an attacker within constituent members also presents a tricky situation.

5) Data Fusion: Data fusion is defined as "Joint analysis of multiple inter-related datasets that provide complementary views on the same phenomenon" [17]. In the case of ADS-B validation, data from multiple other Navigational Aids (including primary RADARs) can be fused for more accurate and reliable aircraft position estimation as compared to a single source. Considerable research work exists in devising techniques that can combine the available resources in an efficient and resilient way. The primary focus remains on the comparison of ADS-B reported data with information reported from other independent systems like RADAR, MLAT or Flight Plan for validity. The foremost benefit of Data Fusion remains in its compatibility with existing systems. Since the data verification is outside the ADS-B system, it can be implemented as a parallel process to the existing setup. Various data fusion techniques have been discussed by Manesh et al in their research. These can be Probabilistic Modeling and Analysis, Machine Learning and Fuzzy Logic [55]. The application of these techniques is based on data types and situation requirements.

With extensive development in field of Machine Learning and Artificial Intelligence (AI), several other data fusion techniques have been discovered that take into account satellite-based data Mode S as well. Jiushun Ni et al have analyzed the application of Space-borne Mode S and ADS-B Data fusion to estimate the coverage of secondary RADAR signal which is around 90% of the flight path area[62]. Luo et al have cited data fusion of PSR, SSR and WAM with Interacting Multiple Model (IMM) filters to ADS-B and Probability Hypothesis Density (PHD) filter to fuse SSR and ADS-B data in their work to detect ADS-B anomalies using support vectors [54]. Their proposal provides good detection with low false positives and false negatives. Moreover, it is compatible with existing ADS-B protocol.

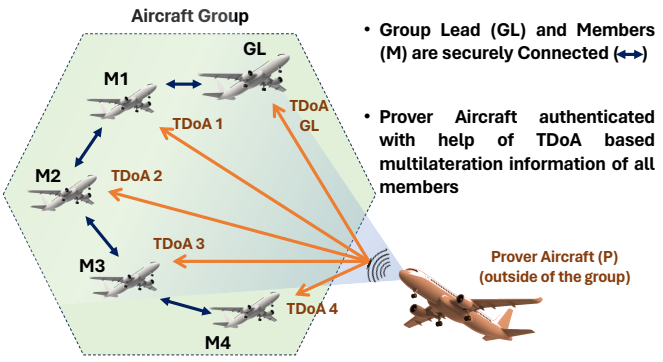


Fig. 20: Group certification concept.[75]

In the purview of increasing traffic of unmanned aerial vehicles (UAVs), data fusion becomes all the more important in their dynamic tracking and guidance, usually based on ADS-B data. Raz and Sabatini have presented a use case for UAV Traffic Management (UTM) that utilizes data fusion from ADS-B, PSR, LiDAR and visual data to provide effective positioning in response to various cyber attacks on the ADS-B data [73]. They successfully use this information for UTM autonomy, command and control as well as surveillance.

Since data fusion takes place between independent systems with different protocols, it is mostly challenged due to time synchronization between the players who are operating at different sampling frequency, message type and structure and varying degree of accuracy. Yong et al have identified the problematic area in ADS-B and RADAR data fusion mainly based on the difference in the Coordinates system of both i.e. ADS-B location reporting is in LAT/LON whereas that of RADAR is based on Azimuth and Elevation with respect to the RADAR itself [108]. They have proposed the use of a unified Cartesian Coordinates system to address this issue with promising results showing improvement in track accuracy, updating rate and overall surveillance coverage. Koh Che Hun has developed an algorithm for correlation of aircraft positioning data from RADAR and ADS-B sensors [45]. In this research, integration of ADS-B data with widely used Multi-RADAR Tracking System (MRTS) has been proposed to augment a Single Integrated Air Picture (SIAP), which is a multiple PSR and SSR data fusion product. Author has identified the correlation problem for the purpose and has suggested an algorithm which aims to resolve ambiguities and conflicting information to provide an operationally useful synthesis of the surveillance data. The algorithm's validation involves the utilization of real-time radar and ADS-B data obtained from the Department of Civil Aviation Malaysia (CAAM) and results show successful transformation and correlation between radar and ADS-B measurements.

Apart from academic research, ICAO itself has issued guidance material on ATM data fusion at the airports [65]. The document appreciates the use and benefits of multi-sensor data fusion in providing quality surveillance track data to air traffic controllers. Various concern areas have been identified along with real problems and related suggestions in using multiple attributes of different sensors to provide a coherent picture. Data fusion is an implemented technology with varying options in development by multiple firms around the globe, as they make full use of every sensor's potential and verify positional reporting by every other constituent system of which, ADS-B is a critical part. In principle, various techniques like MLAT are also data fusion nodes which are considering SSR data as well. It is yet to be seen that if legacy surveillance systems are de-commissioned in future, what would be other options to incorporate into data fusion.

6) Blockchain Encryption: One of the emerging techniques to allow information access to all designated nodes or members who can record, share, and view encrypted transnational data on their network through a decentralized ledger system is Blockchain. Originally intended to support Bitcoin, Blockchain, as defined by IBM, is a comprehensive risk management system for a Blockchain network, using cyber security frameworks, assurance services and best practices to reduce risks against attacks and fraud [34]. Due to its soaring popularity in world of cyber security, Blockchain Ledger System security is finding its way into many other applications, of which ADS-B security can be a potential beneficiary. Pennapareddy et al [70] have presented a study based on scholarly works related to the application of the Blockchain concept in resolving many problems related to the aviation industry. In specificity to its use in securing ADS-B information, they have argued for its use as a temper-resistant Ledger System to securely contain Flight Information to be used as a validating tool of position and other information of the aircraft parameters being received over the open broadcast. In addition to a comprehensive review, they have also proposed a novel solution whereby continuously securing the ADS-B data transmissions, based upon the filed flight plans in real-time, can provide a mechanism to identify spoofed aircraft messages and communicate the same to ground stations for authentication of the existence of such a malicious aircraft. Zhijun Wu et al [99] have designed a blockchain model for ADS-B which records messages and uses immutable and traceable features of the blockchain to ensure the authenticity and reliability of data. Their proposed idea serves security purposes by preventing internal, counterfeiting, replay, and DoS attacks while catering for anonymity as well at a relatively faster processing rate. However, implementation of such a system is expected to result in a major overhaul of the ATM services and related information technology and cyber security programs. Moreover, Blockchain security does not provide broadcast security and strictly follows the authentic flight plan information contained within the ledger. Any flight that is not part of the ledger, though being legitimate, would still be considered a threat.

7) Time Stamping: Kim et al have proposed a practical method for FAA's NextGen program that can reject virtually all spoofed ADS-B messages by monitoring the radio propagation time between senders and receivers [44]. Their method involves time-stamping ADS-B information and thus term it ADS-B with Timestamp (ADS-BT). ADS-BT monitors the discrepancy between the time of flight based on the timestamp values and the time of flight based on the location data. In spoofed ADS-B messages, the discrepancy between them diverges over time, which allows to identification of spoofed ADS-B messages accurately. A frame can be rejected as an attack frame if the time difference is beyond a specific threshold. ADS-BT does not require any special hardware or third-party stations to collaborate, nor does it require synchronized clocks or cryptographic processing. Their method is based on the premise that an attacker can spoof the GPS coordinates in the ADS-B messages but not the time-of-flight correctly in multiple frames. Since, the time at the sender is currently not available in ADS-B, Automatic Dependent Surveillance-Broadcast with Timestamp (ADS-BT) introduces a new timestamp field to record the time of transmission while using GPS data for a low-cost solution.

8) Doppler Shift Measurements: Doppler spread estimation has been extensively used in wireless communications for improving functions at the PHY layer (adaptive coding, modulation, antenna diversity, power control, hand-off etc). Ghose et al have used the Doppler shift concept for their proposed solution in verifying Navigation information of ADS-B transmissions [27]. It is based on a physical layer verification method that exploits RF attributes of ADS-B transmission to verify velocity and position. Authors have argued that the solution provides security equivalent to the hardness of under-defied quadratic equation systems using Private Key cryptography. Doppler spread phenomenon is utilized for measuring the relative radial velocity between the *Verifie* (legit aircraft) and the *Prover* (rogue ground station). Their work shows the difficulty for *Prover* to manipulate the maximum Doppler spread measurements performed by the *Verifie*. Using the relative radial velocity, an *Verifie* aircraft can check both the velocity and position claims of a *Prover* which are connected through well-defined kinematic equations. The present work considers a verification process that occurs at cruising altitude and cruising speed only. Verification of ADS-B signals during other flight phases, such as takeoff and landing, requires further investigation.

B. Broadcast Security

Simplicity in implementation of ADS-B coding allows replication using low-cost SDRs [23] [20]. Similar to other Civil Aviation communication protocols like Pilot – Ground Audio Communication and data links, ADS-B is kept open for clarity in message exchange. However, the mandated implementation of ADS-B has rendered an open system vulnerable to threats outlined in Section III-B. These threats aim to manipulate or spoof the information within ADS-B messages, posing risks to message integrity and confidentiality, and potentially compromising passenger and flight safety. Securing this open transmission is a key solution to mitigate attack probability. Yet, implementing an encryption scheme requires a comprehensive key management and exchange mechanism, a major overhaul of the ADS-B system, and a change in its inherent broadcast nature. Numerous research works have assessed threats and proposed solutions since the onset of ADS-B deployment, categorized into Non-Cryptographic and Cryptographic Schemes as depicted in our taxonomy (Fig 17).

1) Non-cryptographic ; Machine Learning Techniques: Such proposals are based on making use of advancements in Machine Learning / Artificial Intelligence to classify malicious transmission from the original ones through Hardware /

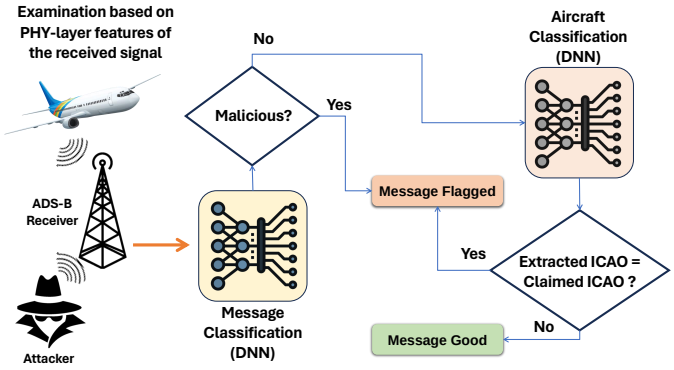


Fig. 21: Algorithm using Deep Neural Networks to detect ground-based spoofing attacks. *Source* [107]

Software fingerprinting. Like position verification techniques, these too are implemented in parallel to ADS-B, whereby all transmissions are sensed and analyzed to identify the attack. Since all-passive processing is used in modelling the references, the system keeps evolving with continuous input of information and results are refined with more data, which is a major benefit of using Machine Learning (ML) techniques. The biggest advantage is its compatibility of use with existing ADS-B setups as it does not interfere with the system, while collecting a comprehensive database for its processing.

Suleman Khan et al have worked on dataset generation and classifier training for false name, information, heading and squawk attacks. They have proceeded to evaluate Logistic Regression, Naïve Bayes, and k-NN classifiers for intrusion detection [43]. This elementary research, despite being focused on limited attack areas, shows promising results depicting kNN outperforming (99% accuracy) Naive Bayes and Logistic Regression algorithms. Authors were able to achieve 0% and 0.1% FAR for anomaly and normal ADS-B messages respectively.

Xuhang Ying et al have used deep neural networks to examine each incoming message based on physical layer features such as In-phase and Quadrature (I/Q) samples and phases to flag suspicious activity [107]. Verifiable ADS-B data and emulated threats generated from commercial SDRs have been used to train the classifiers over raw I/Q samples as features. Figure 21 shows an illustration of the proposed architecture. Their proposed model detects spoofing attacks with a probability of 99.34%, while having a minimal false alarm rate of 0.43%, outperforming legacy machine learning techniques such as XGBoost, Logistic Regression and Support Vector Machine.

Nikita et al have developed a spoofer detection and aircraft identification system using raw ADS-B data and termed it FlightSense [37]. They make use of Generative Adversarial Networks (GAN) and Neural Networks (NN) with a focus on radio device's inherent I/Q imbalances features as classifying parameters. Within GAN, Adversarial Learning between NN-trained threat generator (near realistic to actual) and detector (actual – fake discriminator) continuously evolve the classifier subsequently refining both threat perception as well as the ability to counter the same. Figure 22 shows GAN architecture.

Jin Lei et al [48] have presented a study that focuses on vulnerabilities in the machine learning-based ADS-B abnormal data detection model, introducing a method for constructing broadly applicable poisoning data and establishing an attack model. The injection of malicious data, generated by a GAN, degrades the trained model's performance, showcasing the effectiveness of the proposed method. These findings lay the groundwork for enhancing system defence technology and ensuring the security of ADS-B.

2) Non-cryptographic ; Signal Processing Techniques: ADS-B services can be denied either directly or indirectly through tactical jammers employed either over GNSS or ADS-B signals bandwidth. Leonardi et al, while evaluating low-cost jammers effect on ADS-B, have suggested the following proposals in their work [49], [50], using digital filters and RF signal tracking techniques using multi-channel receivers to thwart DoS / Jamming attacks:

- *Digital Processing block for pulse extraction*. Algorithm to filter out ADS-B messages from the extensive Noise floor
- *Preamble Detector*. To keep a check on flooding attacks, as preambles without messages can usurp the receiver's processing capacity
- *Projection Algorithm for Single and Multiple Antenna*. Makes use of Signal Angle of Arrival (AoA) to separate the sources

Authors have concluded that while any type of ADS-B jamming can significantly reduce its intended range. However, if the receiver is not saturated, ADS-B signal can be separated from the noise floor and significant improvement from 0% to at least 63.3% can be observed in decoding replies without errors.

Rudys et al have recently proposed a solution based on physical layer signal analysis i.e. estimation of signal source range and direction of arrival (DoA) [74]. The article a method and a system architecture for the authentication of

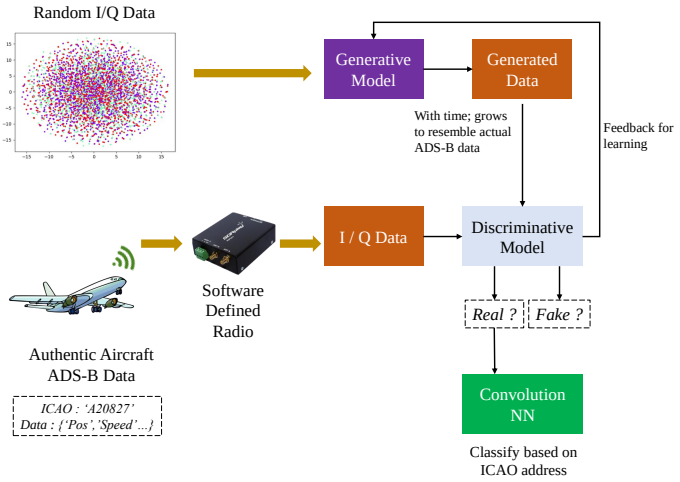


Fig. 22: Proposed FlightSense GAN architecture

signal genuineness for ADS-B enabled aircraft, based on secure location verification. The proposed system architecture includes a directional slotted antenna system and multi-channel receiver on ADS-B Inside but requires no change to the existing ADS-B protocol. The proposed techniques provide security against message injection attacks such as spoofing and partial security against jamming. For enabling the DoA estimation, use of either a multi-channel receiver connected to directional antennas or antenna array elements integrated with the aircraft body has been proposed. The signal direction of arrival is estimated in this case by sensing the difference in the amplitudes of the signal after individual antennas. The second option is to use a set of antenna elements, together with corresponding number of phase-synchronized receiver channels, allowing for the phased array type of signal processing such as digital beam-forming. These two options represent a trade-off between DoA estimation accuracy and system complexity. Nevertheless, RSS measurements can serve as mitigation of spoofing attacks or as an additional parameter for estimating the distance between aircraft in a doomsday scenario when the Global Navigation Satellite System (GNSS) is unavailable and does not allow more accurate position determination. In this case, RSS measurements are helpful in maintaining ADS-B functionality with reduced accuracy. In comparison with a regular ADS-B receiver, the proposed system concept requires more complex antennas, receivers and additional signal processing and verification algorithms. More importantly, it does not require any change to ADS-B protocol or ADS-B Out systems. The structure of improved ADS-B receiver system is presented in Fig 23. Location is estimated via the use of ranging and signal direction-of-arrival measurements. The performance of the proposed method is evaluated by establishing an estimation of error bounds and analyzing a spoofing scenario.

3) Crypto Scheme ; Spread Spectrum: One of the ways to secure a broadcast is to spread a narrow-band message signal to a wide-band signal using SS techniques. This way transmitted signal can be hidden from unauthorised listeners who are not aware of the spread sequence. Spread Spectrum can be broadly of two types i.e. Direct Sequence Spread Spectrum (DSSS) and Frequency Hop Spread Spectrum (FHSS). In FHSS, data is split into pieces and each piece is transmitted over different frequencies in a spectrum as per the defined sequence. In DSSS, instead of frequency hops, the split data pieces are transmitted over a complete spectrum at once, with each piece valued by an algorithm-based spreading sequence. Analogous to encryption, in both SS techniques, the receiver and sender should be knowledgeable of the spreading sequence and hopping frequencies, which logically becomes a shared Key between communicating parties.

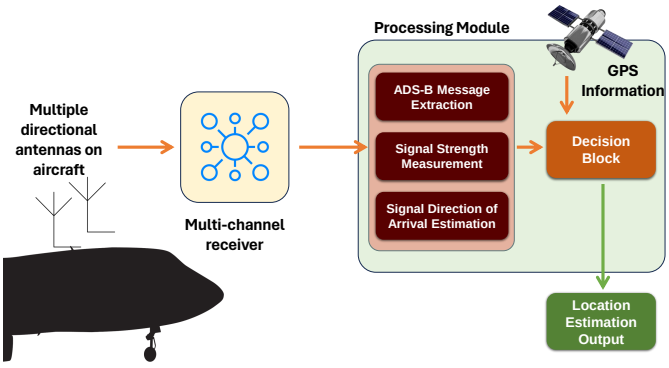


Fig. 23: Improved ADS-B receiver system. *Source* [74]

Sharing of sequence or the Key which governs the spread and hop sequence remains a challenge. Surveys conducted by Strohmeier [86] and Zhijun Wu [98] collectively inform of works conducted by Strasser et al [85], Pöpper et al [71], and Liu et al [53] to circumvent the problem of pre-shared spreading codes/ modes. They have proposed to use random jumps to frequencies or random spread codes instead of pre-defined ones. They statistically model the probability of both sender and receiver being on the same channels.

The concept has been furthered by Gopalakrishnan through the use of hopping channels based on a Chaotic Map which is aperiodic and sensitive to initial conditions, thus providing a high level of security [28].

Vázquez has proposed a birthday problem using Entropy measures, which allows us to obtain the optimal spreading code set sizes that guarantee asymptotically zero collision probability [93].

Hasjuks et al have forwarded a study on the performance of chaos-based DSSS and FHSS multi-user communications systems. They have conclusively shown the configurations in multi-user scenarios, which can perform better than pseudo-noise (pseudo-random) sequences in FHSS and DSSS [31].

While considering valuable research output, the problem however remains in deviation from the standard 1090 MHz of ADS-B system. Any spread spectrum technique with or without a pre-shared sequence will consume more bandwidth. Moreover, complexity and time consumption in processing transmission and reception of the same along with its scalability issues still prevents this technique from being employed over worldwide civil aviation systems like ADS-B.

4) Crypto Scheme; Symmetric Encryption: Symmetric key cryptography uses a common key for encrypting and decrypting plain text, primarily aiming for confidentiality but also serving authentication and message integrity purposes. Its simplicity and robustness make it fast and strong. Symmetric encryption, coupled with Message Authentication Codes (MACs), ensures data origin authenticity and integrity by appending the MAC to the clear text. Pre-sharing the common key poses challenges, particularly in scenarios with numerous communicating entities, requiring 'out of band' relations and introducing non-repudiation problems. Trusted Third Parties can address some of these challenges by establishing keys and secret channels with all communicating nodes. Another technique involves using Hash (or Message Digest), reducing plain text to a fixed-size fingerprint for message integrity. The combination of Hash and MAC, known as HMAC (or secured-Hash technique), combines benefits for both sender

authenticity and message integrity. This research section explores scholarly works applying these techniques to the ADS-B network.

In previous surveys [86] , [98] works of Samuelson [76], Jochum [36], Finke [24] and Yang [103] are prominently mentioned. The proposed schemes revolve around the following:-

- Appending Message Authentication Code (MAC) to original ADS-B message to keep its openness as well as to ensure the authenticity for those with key to MAC
- Format preservation encryption to keep the format of ciphertext the same as that of ADS-B message
- Use of selective field encryption instead of the complete ADS-B message

In all cases, a certain level of deviation from the existing ADS-B setup exists. While **appending MAC keeps** the openness, the resulting message size crosses over the standard size of the protocol and would remain illegible unless ADS-B In protocol is changed to accept additional MAC bits. **Selective field and Format preservation encryption** technique converts the complete or partial message to a meaningless transmission for open nodes, thus violating the clear message exchange protocol in the existing setup. Moreover, it would require a major shift worldwide to accept a complete or partial encrypted broadcast.

Even in the face of all, if ADS-B encryption gets actively deployed, key generation, distribution and management worldwide presents another domain altogether. Haomiao Yang et al have comprehensively compiled various systems and research proposals for securing ADS-B transmissions [102]. Apart from discussing the benefits and limitations of existing systems based on Symmetric and Asymmetric encryption, they provide insight into emergent technologies such as Format Preserving Encryption, Vector Homomorphic Encryption, Time Efficient Stream Loss Tolerant Authentication (TESLA) and Location Privacy Management.

Addressing the lack of authentication and shared-key problem in symmetric encryption, Baek et al have proposed a confidentiality framework based on staged identity-based encryption [8]. They have adopted the Identity Based Encryption (IBE) introduced by Boneh and Franklin [10] which uses receiving parties' identities as Private Keys for encryption. This way, it will greatly simplify the key management in Private Key encryption compared with traditional PKI-based key management which mandates digital certificates be used for authenticating every Private Key. In order to reduce involved computational cost problem associated with IBE based key encryption, a hybrid approach has been used by the authors [11] whereby data is encrypted by a symmetric encryption scheme using a chosen random key, like a block cipher, while the key is encrypted by IBE. Their scheme offsets from standard IBE during the key sharing mechanism. Authors have considered ICAO (or any other TTP) in granting ground controllers with unique Private Keys. When an aircraft enters an airspace managed by one ground controller, the aircraft encrypts a securely generated random symmetric key with the identity of the ground controller (Private Key). It then encrypts subsequent messages using a secure symmetric encryption scheme under the random key it had selected

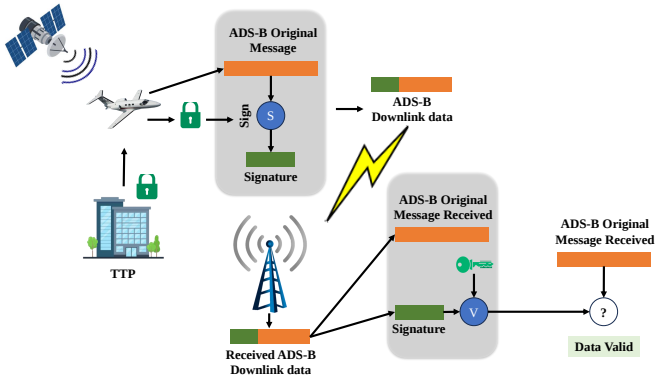
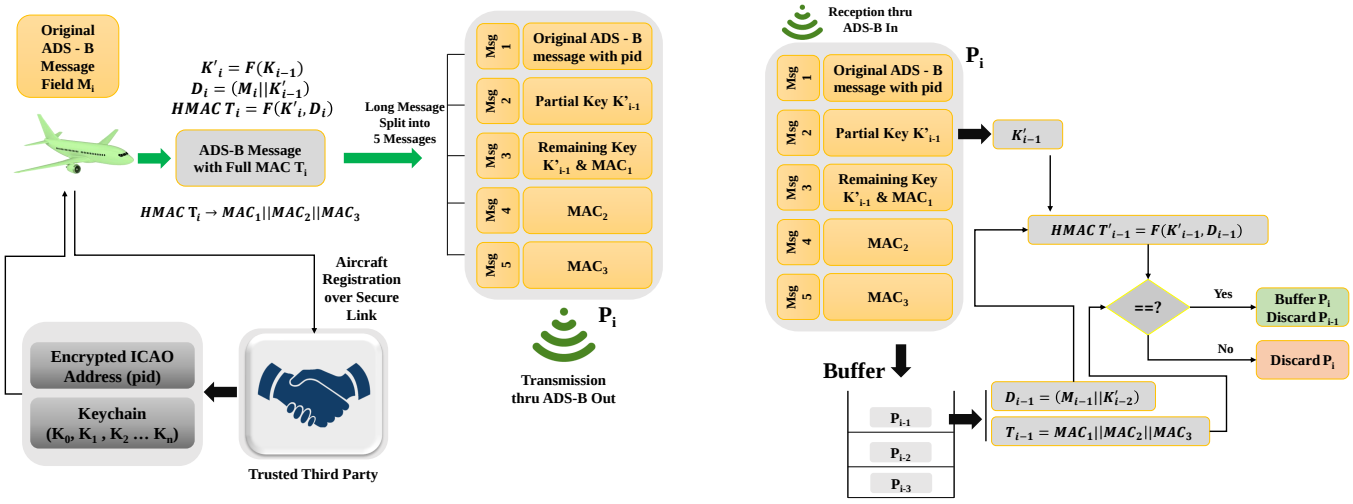


Fig. 24: Proposed certificate-less message authentication method, Before takeoff, the aircraft shares identity info, obtains a partial Private Key and computes its complete Private Key and corresponding Private Key. It publishes its Private Keys and during flight, it uses Private Keys to sign and broadcast ADS-B messages. Receivers verify messages with the published Private Key for data integrity.

before. On entering a new area, a new Private Key, pertaining to the area-specific controller will be used and so forth. Improving upon the same, Zhijun Wu et al make use of certificate-less short signatures crypto-system to ADS-B to provide integrity and authenticity in ADS-B messages [100]. Figure 24 shows the following approach. Aircraft obtains a partial Private Key from the airport based on its identity and generates a pair of private/Private Keys. Keeping the Private Key to itself, the aircraft publishes the Private Key. It further utilizes Private Keys to sign ADS-B messages and broadcasts message-signature pairs. All ADS-B equipped receivers can verify the messages with a published Private Key. Since the signature is appended to the original ADS-B message, which can still be seen by all participants without having the requisite Private Key, the openness condition remains available. This method very closely resembles Samuelson [76] work, however, the difference is a small signature size which is further split into segments. These segments are then packaged into several ADS-B messages for broadcast, unlike the previous technique which transmits the signature at once. This way communication cost is reduced, however, a delay is induced between the original message and its authentication causing a processing latency.

Haomiao Yang et al have developed a so-called Lightweight and Highly-Compatible Solution for ADS-B Security (LHCSAS). They have exploited the reserved fields in ADS-B messages along with the relation between aircraft ICAO address (AA) and the rest of the ADS-B message sub-fields [103]. It is argued that the AA field is the one which links the information field with the rest of the message to make meaningful data. By encrypting the AA field only, an attacker can be prevented from establishing the relation between identification and its corresponding position information. Due to resource-constrained onboard avionics, it is suggested to use a Trusted Third Party (TTP) which may be ATCO or any other legal institution. TTP is used to initialize the whole process,



(a) Transmission Side (b) Reception Side

Fig. 25: LHCSAS scheme

generate, and distribute various parameters and keys. This also includes the generation of an encrypted ICAO Address termed as 'pid' and sending it to the concerned aircraft. In response, the aircraft changes its AA field to received 'pid' in its ADS-B messages. Format-preserving encryption is used in TTP to keep the 'pid' format the same as that of the AA field. Moreover, TTP also generates a keychain (split pieces of a single key) for MAC calculation and sends it over to the aircraft over a secure channel. On the aircraft side, the received keychain is compiled to get the key, which is used to generate MAC from the ADS-B message field. Finally, the aircraft transmits a modified ADS-B message with a type code set to 25 (reserved), carrying an encrypted ICAO address, MAC and Keychain element for receivers to compile the key from the keychain, verify MAC and authenticate the message. Figure 25 shows the process flow and packet construction. The benefits achieved from this method are compatibility with the existing setup by virtue of using reserved type code to transmit encrypted data following acceptable time overheads. It is pertinent to note that authors have effectively used the TESLA protocol for their solution to achieve integrity, tolerating the package loss common in ADS-B transmission [80].

TESLA protocol works around keychain usage which is continuously derived from a single key using a hash process. It works on loose time synchronization where the sender attaches a key computed MAC to every packet only for the receiver to keep on saving incoming messages in a buffer. Later, the sender releases the key, enabling the receiver to authenticate the buffered messages [2]. Though TESLA works purely on symmetric encryption-based MAC, however, it achieves properties of asymmetric encryption with the Keychain process.

Building on to handling of encrypted ADS-B data, Zeng has argued that despite encryption, an attacker still has the chance to destroy ADS-B protection by modifying the ciphertext [109]. Fig 26 shows the conceptualized network model. A dynamic order-preserving encryption (DOPE) has been proposed in his work to achieve data confidentiality and sequential search of desired data in the ciphertext. Unique verification labels are calculated to ensure the integrity of ciphertext for auditing purposes. This technique is useful for targeted ciphertext searching in chronologically arranged ADS-B data that is widely used for queries by ATC controllers. It enables one to directly point to a required ciphertext instead of deciphering the whole database to find the requisite information.

Kacem et al have proposed a secure ADS-B framework that could enhance the security of the original protocol by using Key Hashed (HMAC) sums in place of CRC (Parity) bits of the ADS-B message as later is a commercial standard algorithm [39] [42]. This arrangement also keeps the format within the specified standard and avoids scalability issues. Their technique is achieved by assembling as many ADS-B messages as needed to split the HMAC digest among the different CRCs of these messages. A number of these messages are dependent upon the size of the HMAC being used. Required ADS-B messages are in fact even and odd pairs of positional information. Given 24 bits of CRC fields, it would require 6 messages to transmit 128-bit HMAC. Therefore, these 6 messages are first buffered,

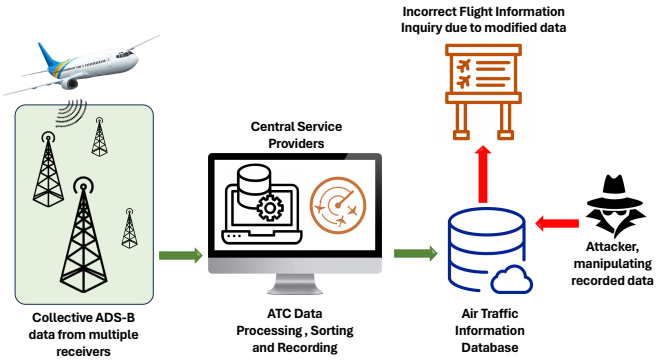


Fig. 26: Conceptual network model susceptible to attack. *Source* [109]

concatenated and fed to the HMAC generator for 128-bit digest output. Further, this digest is broken and serialized into 6 components, each to be inserted into previously buffered 6 original ADS-B messages' CRC field. These messages are then sequentially transmitted as per the standard defined for their Type Code. The serializing mechanism is to recognize the order of portions of the digest. This ensures that the whole HMAC can be reconstructed at the receiver for integrity verification. However, as identified by the authors, buffering messages fed in the HMAC algorithm induces a delay in the transmission process. These delays are then evaluated through Monte-Carlo Simulations. The results show that increasing the ADS-B message sending rate would reduce the incurred processing delays. Since the HMAC algorithm would essentially require a Key distribution mechanism between the aircraft and ground station, this arrangement has been left with a trusted third party (which could be concerned ATC Tower) that provides region base Keys to the aircraft while authorizing them to enter their airspace as per flight plan. Moving on from their initial work, authors increased the number of buffered ADS-B messages from 6 to 8 to gain better resistance against loss / scrambled messages [38]. Improving further, the number of messages required to generate HMAC where finally reduced to two [41]. The bit correction capability of CRC is however lost after using HMAC in its place. Moreover, this protocol needs an SNR of at least 8 dB to correctly reassemble the HMAC at the receiver.

5) Crypto Sceheme ; Asymmetric Encryption: Asymmetric or Private Key Cryptography is an algorithm-based process which uses a pair of dissimilar keys (public and private) for encryption purposes. The data encrypted with one key (public) can only be decrypted with a matching Private Key. Best suited for short messages, these algorithms are used to achieve authentication, integrity and non-repudiation, and support confidentiality through Key management. Asymmetric Encryption usually finds its utility in three types of operations that can be:

- **Digital Signature.** Plain text can be digitally stamped with the use of a Private Key to authenticate the sender as it is only decipherable by its paired Private Key.
- **Key Transportation.** Due to their relatively slower performance, Private Key Cryptographers are never used for long messages, instead, they are used to secure short messages like Symmetric Keys for transportation.
- **Key Agreement**. Asymmetric algorithms can be used to generate the same secret value between trusted parties. This value is then utilized as a secret Key for encryption purposes.

Over the years, considerable work has been carried out to explore Asymmetric Encryption utility in securing ADS-B communications, since it suits best in situations where message length is short and pre-sharing of Keys is improbable due to unidirectional transmission.

Peng Yi et al and Asari et al [6] have developed hierarchical signature scheme with a batch verification function suitable for ADS-B [106]. Their works very closely resemble and provide efficient use of the Certificate-Less Signature Scheme (CLS) used with aggregate Signatures (CLAS) to reduce processing time in comparison to Yang [101] and He et al's [32] work. They use the Key agreement setup of Diffie-Hellman to prove the security of their proposal. In their scheme, multiple out-of-band communications are occurring between servers which are additional to the existing setup. Three Key generating algorithms namely '*Setup*', '$Extract^A$' and '$Extract^F$', Signing algorithm '*Sign*', single signature and Batch signature validity check '*Verify*' are introduced as programs. Additional hardware has been used to contain aforementioned algorithms in the form of Private Key Generator (PKG) for *Setup* and, $Extract^A$, Airline Server (ALS_i) for $Extract^F$, airborne equipment for *Sign* and other ground equipment for *Verify*. The following hierarchical functions (with inputs in brackets on the left side of the equation) are involved in the process:

1) *Setup* (security parameter) = Public Parameters (*par*) and Master System Key (*msk*)
2) $Extract^A$ (*msk*, Airline ID (ID_{A_i}), *par*) = Airline secret Key (sk_{AL_i})
3) $Extract^F$ (Aircraft Identity $ID_{F_{ij}}$, sk_{AL_i}) = Aircraft secret Key ($sk_{AC_{ij}}$)
4) *Sign* ($ID_{F_{ij}}$, $sk_{AC_{ij}}$, par, message(m_{ij})) = Signature (σ_{ij})
5) *Verify* (ID_{A_i}, $ID_{F_{ij}}$, m_{ij},σ_{ij}, *par*) = 1 (for valid σ_{ij}) or 0 (for invalid σ_{ij})
6) *BVerify* (Batch of data as in *Verify*) = 1 (for a valid batch group of signatures) or 0 (Invalid batch)

Burfeind et al have devised a so-called lightweight and inter-operable confidential sub-protocol for Mode S Extended Squitter (ADS-B) using Format Preserving Encryption (FPE) in unidirectional asymmetric cryptography [14]. Authors argue that the stateless and broadcast nature of ADS-B makes it suitable for asymmetrical encryption. However, it is also acknowledged that a significant protocol shift is in the offing if a PKI solution to ADS-B is used, a situation which seems likely to be rejected. Therefore, a mix of symmetric and public crypto-techniques has been used in this research. ATC or CAA has been chosen as a TTP to generate and publish a Public-Private Key pair with a 28-day flight information cycle. Aircraft is to generate a session key (SK) and session unique ICAO address (SUIA) for a single session from a random set of ICAO addresses. Moreover, the aircraft encrypts ADS-B data ME fields using FF1 (Format Preserving Fiestel-based Encryption) technique using the already generated SK and uses SUIA instead of the original ICAO address to obfuscate the transmission. To communicate ADS-B securely, the aircraft uses TTP generated Private Key to encrypt SK and SUIA and transmit them to TTP (ATC in this case) under different Mode S Downlink Formats for deciphering the received secure ADS-B packets.

Several ADS-B security surveys have cited Wesson et al research [96] while considering the use of various cryptography techniques that can be applied. Most have agreed to the conclusion that owing to standard constraints related to ADS-B, asymmetric encryption best suites the requirement and Elliptic Curve Digital Signature Algorithm (ECDSA) is the best solution owing to its relatively smallest signature

length [98] [86] [55] [81]. Out-of-band transmissions have been recommended for signed ADS=B data broadcast as its size flows out of existing standards.

Braeken has proposed a system, termed as Holistic Air Protection (HAP) which provides different levels of ADS-B data security with potential encryption of identifier and /or payload of the message [12]. The author has argued that most of the previous research work is focused on singleton field encryption and lacks holistic flexibility to provide multiple options in a single framework. Holistically approaching the problem can provide a solution which can be used both in civil and military usage to secure the privacy and confidentiality of the intended aircraft. Use of the Elliptic Curve Qu-Vanstone (ECQV) Implicit Certificate Scheme and generalized Elliptic curve-based Signcryption scheme (signing and encryption in a single logical step) has been suggested to avoid secure channel requirement and provide options of either authentication, confidentiality or doing both on the ADS-B data. Standard 1090ES format is used for maintaining the compatibility and security evaluation of the proposal has been done against Packet Injection, Selective Jamming and Spoofing, and Packet Modification. Comparison has been drawn relative to TESLA using techniques for communication and computational analysis and found to be performing better, however at the cost of additional data bits. Three phases are defined in the proposed scheme which works in following ways:

1) ***Set-up***. ECQV algorithm provides aircraft long-term Private Key (to be stored within aircraft) and associated Private Key (to be published) based on the security certificate and aircraft ID. Aircraft, before takeoff, through a Private Key signed message requests TTP a short-term private-Private Key pair for in-flight use. TTP on verification provides ECQV algorithm calculated, short-term Private Key for publishing and Private Key for aircraft along with its applicable duration. An emergency parameter is also shared between aircraft and TTP to be used selectively against spoofing and jamming. This step uses a secure channel for key communication.
2) ***Online Phase***. There are four security levels defined in this step (Table X which are used as per the situation
3) ***Verification Phase***. Published Keys (public) are searched against ICAO IDs and message types given in Table X are verified and decrypted at the receiver's end.

TABLE X: Security levels defined in Braeken's work [12]

Security Levels of Online Phase		
Security Level	**ICAO**	**Payload**
Level 1	Plain	Signed
Level 2	Encrypted, Signed	Signed
Level 3	Encrypted	Encrypted
Level 4	Encrypted, Signed	Encrypted, Signed

Limitations of Cryptography Methods in ADS-B

Encrypting the ADS-B content can provide requisite security against varying degrees of attacks. However, it also violates the ICAO standard openness requirement. Besides, Key management and distribution remain the greatest of the challenges. Yang et al have described limitations in Cryptography Methods for securing ADS-B broadcast [102]. They have elaborated their arguments based on the fragile trust-base between communicating parties for symmetric encryption and the increase in maintenance and running costs for PKI in asymmetric encryption with relatively low performance. Table XI shows salient features of their research.

V. Discussion and Reflections

The air transport industry is rapidly growing and so is the demand for robust systems to manage its traffic. ICAO estimates over 10 million passengers and around USD 18 billion worth of goods being transported every day through millions of flights [64]. Fig 27 shows a quick glance over the FlightRadar24 aviation map showing the extent of densely populated airspace worldwide. Achieving this massive growth and sustaining it responsibly requires automation and efficient systems that could ease out burden of human intervention. ADS-B is one of the realities shaping up future of ATM automation. With almost worldwide mandated deployment today, ADS-B is finding its way to replace legacy surveillance systems. However, its usage as a solitary source is hindered in the face of associated security vulnerabilities owing to its open communication protocol that is susceptible to attacks like eavesdropping, spoofing, false data injections and jamming etc. With commercial markets filling in on cheap SDRs, the attack probability keeps rising. Moreover, with the burst growth of unregistered, non-recognizable unmanned vehicular traffic, the threat has grown even stronger as the attacker base has risen from ground to air. In cognizance of the realities above, this work is an effort to understand the ADS-B system and its employment needs, associated vulnerabilities

TABLE XI: Limitations of securing ADS-B with cryptography methods argued in [102]

Limitations of Cryptography Methods	
Symmetric	**Asymmetric**
Violation of ADS-B standard openness	Scalability, management and recurring cost on PKI
Symmetric Key security cannot be ensured when globally distributed	Relatively low performance as compared to Symmetric Encryption
Short life-cycle of Key due to dispersal in potentially untrustworthy groups	Aviation Asset Distribution Systems (AADS) availability and management for Certificate distribution
Equipment temper resistance quality if Keys are hardwired onto aircraft	All aircraft carry a list of all other aircraft Private Keys for signature verification
Presumed resistance from ICAO and FAA due to flight safety requirements of open communications	Private Key protection during transmission and usage

Fig. 27: FlightRadar24 website map screenshot

and attacks exploiting those as well as analyze the already proposed or deployed preventive measures to address these.

Innovative means of cyber-attacks are pacing with the availability of commercially available high-end processing machines and SDRs. With the involvement of both state and non-state actors, a paradigm shift is probable which could scale these attacks globally and can be utilized to dent the economies and peace of the affected. Most vulnerable to such attacks are open and unprotected air traffic communication and automation channels that are purposefully kept clear for aviation safety needs. However, it is no surprise that the same safety need has become the source of catastrophe in the hands of purposeful and deceiving attacks such as those on ADS-B. Fig 28 shows the hierarchical flow of ADS-B vulnerabilities and possible consequences to follow.

Realizing the threat, the academic community has been researching for better and more efficient ways to enhance air traffic management by securing ADS-B communication. Since ADS-B is already deployed and mandated in most parts of the world, any applicable solution would require some level of changes to the existing setup. This is a big ask and only possible if the degree of offered protection is attractive and efficient enough. Therefore, before analyzing applicability, we must first review the kind of protection offered as well as unaddressed areas before devising any proposed solution. Table XII presents the said comparative analysis. The threat perception is divided into *Position Verification, Confidentiality, Integrity, Availability* and *Authentication* as additionally described in Fig 28. As observable, none of the techniques addresses the full set of security requirements.

TABLE XII: ADS-B security requirements met by various proposed solutions

Proposed Solution	Position Verification	Confidentiality	Integrity	Availability	Authentication
Multilateration	✓			✓	
Kalman Filtering	✓		✓		✓
Distance Bounding	✓				
Group Certification	✓				
Data Fusion	✓			✓	✓
ML Techniques					✓
Spread Spectrum		✓		✓	
Symmetric Encryption		✓			✓
Private Key Encryption		✓	✓		✓

Since ADS-B is a global standard, any technique securing it must be applicable globally. This is only possible if the proposal is applicable in terms of scalability, cost, sustenance, and minimum protocol variations acceptable to ICAO. Going through the considerable research work done in thwarting the threats which are exploiting ADS-B security vulnerabilities, it can be said for sure that none of the proposals come in as a fully compatible all-in-one solution. A varying degree of change in protocol or requirement of additional infrastructure is essential for any of the discussed techniques. Table XIII draws a comparison between the applicability effect of various proposed solutions. While it remains a fact that to ensure ADS-B security, some investments and deviations are essential from the existing setup. However, their side effects on already crowded 1090 MHz frequency and loss of ADS-B packets due to inherent interference in crowded airspace are yet to be examined if any of them are to be scaled and deployed globally. Hence, there is still a need for a holistic solution that can cover all security requirements with no/ minimal changes

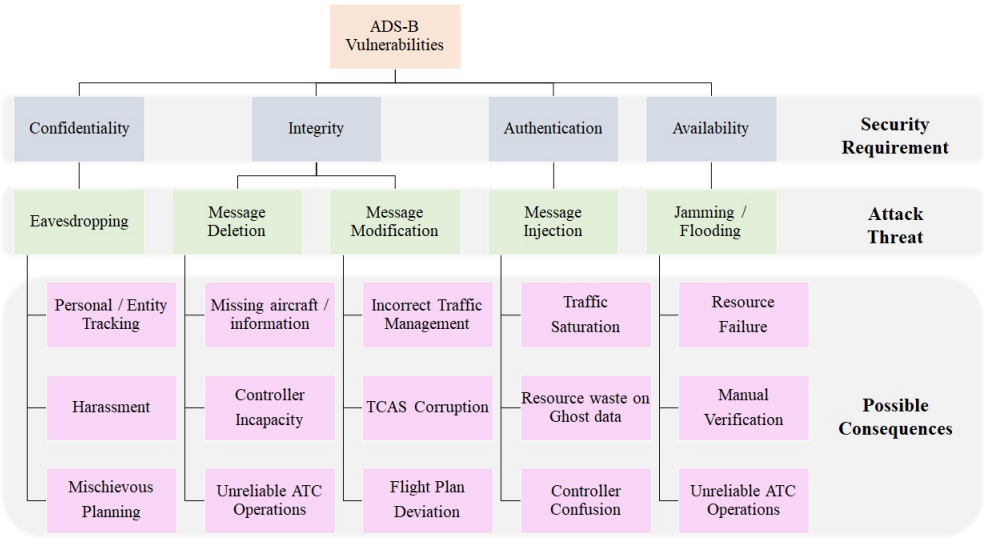


Fig. 28: Hierarchical flow of ADS-B vulnerabilities and possible consequences

TABLE XIII: Applicability effect of various proposed solutions

Technique	Area Coverage	Dependencies	Additional Hardware	Out of band communication	Protocol change	Cost to scalability	Deployment Challenge
Multilateration	Limited	Remote Units	Required	Essential		High	Infrastructure
Distance Bounding	Localized	Remote Units	Required	Not ascertained	Required	High	Protocol change, Infrastructure
Kalman Filtering	Localized	Parallel Processing	Required			Low	Sustenance in dense traffic
Group Verification	Localized	ADS-In	Required	Minimal	Not ascertained	High	no ADS-In mandate
Data Fusion	Extensive	Multiple surveillance sensors	Required	Essential		High	Infrastructure
Anomaly Detection using ML / AI	Localized	Training datasets	Required			Low	Reliability in dense traffic
Spread Spectrum	Extensive	SS capable transmitter	Embeddable	Essential		High	Deviation from 1090 MHz
Symmetric Encryption	Extensive	Pre-shared Key security	Embeddable		Required for MAC	Low	Untrustworthy groups
Asymmetric Encryption	Extensive	PKI, TTP, CA	Embeddable	Key exchange	Multiple Options	High	PKI, TTP, CA Management

for implementation and adaptation.

Upon comparison, position verification techniques, excluding *distance bounding*, operate independently of the ADS-B protocol due to parallel processing. These methods rely on received signal strength, behaviour analysis, and triangulation principles to detect suspicious activity within ADS-B data, necessitating additional hardware and data from legacy surveillance systems for verification. This creates an ironic situation, as ADS-B was designed to replace these legacy systems, yet their vulnerabilities mandate their retention for verifying ADS-B data accuracy. Similarly, Machine Learning techniques, also parallel processes independent of the ADS-B protocol, do not require data from external sources. Classifiers are trained on extensive datasets to differentiate legitimate from malicious data based on software, hardware, and channel usage properties. However, training these algorithms globally poses challenges due to diverse transponder manufacturers, and varying hardware, and software techniques on aircraft equipment. While *multilateration (MLAT)* and *Data Fusion* are utilized, their recurring maintenance and security costs accumulate, with coverage limited to geographical constraints unless supplemented by satellite-based ADS-B systems.

Securing broadcast either by *Spread Spectrum* or Encryption schemes not only minimizes the dependencies on legacy systems but also provides better security to positional as well as other data fields in ADS-B protocol. Symmetric encryption is the easiest way to achieve the goal, however, keeping a pre-shared *Key* secret globally amongst millions of users is a naive idea. This problem can be very well addressed with the use of Private Key Encryption. This technique has been effectively used in wireless broadcasts where trust issues limit the use of common *Key*. Security levels achieved with asymmetric encryption edge out all other techniques, however, their inherent slow processing due to embedded complex mathematical algorithms and *Public-Private Key* management make them less of a choice in ADS-B security. Therefore more recent proposals make use of a hybrid approach where data is encrypted using *Symmetric* encryption and *Key* exchange is done over *Public Encryption* governed either by PKI, Certification Authority (CA) or TTP. Though seemingly favourable, management and cost effects associated with PKI setups (TTP, CA etc) again bring them in line with those in need of additional infrastructure. Moreover, encrypted ADS-B comes at the cost of foregoing openness in the architecture and broadcast nature (in encryption) and/or deviation from standard 1090 MHz (spread spectrum), thereby violating the standard. ICAO and other regulators' interest is yet to be assessed in the employment of such techniques and it would require much more than a theoretical and simulation approach to assess the applicability in the real world. Announcing and handling the emergencies over an encrypted channel would remain a hurdle in any organizational approval.

VI. Future Research Directions

Future research directions should focus on making ADS-B information exchange secure from spoofing and modification. This may include developing robust encryption methods and authentication protocols to ensure that transmitted data cannot be tampered with or falsified. Additionally, advanced intrusion detection systems are necessary to promptly identify and mitigate any unauthorized access or interference. These measures are essential not only for the aviation sector but also for the broader integration of unmanned systems and automated technologies. In the present scenario, ADS-B is an open system susceptible to security attacks due to the non-availability of an encryption mechanism. Various research programs over the years have presented their solutions, some of which, like Multi-Lateration (MLAT) and Data Fusion, are widely in use. However, given the susceptibility, solutions offered by researchers and academia may be considered as well. These solutions can be broadly categorized as encryption-based and non-encryption-based solutions.

A. Encryption-Based Solutions

Implementing encryption schemes, no matter how simple or complex, may require retiring the current ADS-B protocol and developing an entirely new system, potentially introducing new vulnerabilities and problems. Despite this, to remove current shortcomings and vulnerabilities, a more robust solution involving encryption might be necessary. This would

ensure secure data channels, preventing unauthorized access and maintaining data integrity.

B. Non-Encryption-Based Solutions

Non-encryption-based solutions are more likely to be deployed as they do not affect existing operations and would require only supporting infrastructures and / or parallel processing to identify false data from authentic data. This approach includes using Artificial Intelligence for ADS-B spoofing detection. However, while AI can help identify unauthorized data, it cannot restrict access to unauthorized intruders, a limitation that secure channels would address. Further research should focus on enhancing non-encrypted techniques with more robust Access Control mechanisms. Incorporating more data, RF/equipment fingerprints and sensor fusion could improve the accuracy of these techniques, giving ATC controllers the confidence to de-clutter their screens of ghost data without the risk of missing actual aircraft.

C. Hybrid Solutions

A more comprehensive and holistic solution is required, one that can be compatible and flexible with future iterations of the ADS-B system. This might include hybrid solutions utilizing reserved ADS-B type codes, different DF fields in the 1090ES format, and the possibility of shifting ground operations to satellite-based ADS-B with directly embedded GNSS information. Such hybrid approaches can provide a viable path forward, ensuring both low-cost and high-coverage benefits while addressing current vulnerabilities.

D. Era of Unmanned Traffic and Aviation Industry

As the integration of advanced technologies progresses, particularly in the aviation sector, ensuring the safety and efficiency of operations becomes increasingly important. Automatic Dependent Surveillance-Broadcast (ADS-B) technology plays a critical role in enhancing situational awareness and conspicuity, particularly for initiatives like ADS-Light in U-space for drone integration. However, the inherent lack of security features in ADS-B, such as vulnerabilities to spoofing and data modification, poses significant risks. Addressing these security concerns is crucial for the safe integration of drones with manned aircraft and the effective management of shared airspace. Collaborative efforts between regulatory bodies like the European Union Aviation Safety Agency (EASA), the Federal Aviation Administration (FAA), and the International Civil Aviation Organization (ICAO), along with technology developers and cyber security experts, are essential to address these challenges. Ensuring reliable and secure ADS-B communication will enhance situational awareness, improve collision avoidance, and support the safe and efficient operation of U-space services. Identifying research gaps in encryption technology, real-time authentication mechanisms, and intrusion detection systems will be crucial steps toward achieving these objectives and ensuring the long-term safety and viability of integrating ADS-B into shared airspace globally.

E. Use of Phase Modulation to assist in managing Band Congestion

A promising direction for future research in alleviating ADS-B transmission band congestion due to encryption overheads involves exploring the application of ”Phase modulation (PM)” techniques. By utilizing advanced PM schemes, such as ”Quadrature Phase Shift Keying (QPSK)” or ”16-PSK”, more data can be transmitted per symbol, significantly increasing spectral efficiency without expanding bandwidth usage. This approach could reduce transmission time for each aircraft, lowering the likelihood of signal collisions and improving overall airspace communication efficiency. Additionally, PM’s resilience to noise and interference would decrease the need for re-transmissions, further alleviating congestion. Integrating PM with ”error correction techniques” and implementing it in hybrid systems described above can optimize performance under varying conditions. While the increased complexity of phase-modulated systems and the requirement for synchronization pose challenges, advancements in transponder and receiver technology could make this approach viable. Thus, investigating the use of ”Phase Modulation” in ADS-B systems offers a promising path toward addressing bandwidth congestion, especially as airspace becomes increasingly saturated with UAVs and small airborne platforms.

VII. Conclusion

To ensure the safe and efficient integration of drones and other unmanned systems into shared airspace, addressing the security vulnerabilities of ADS-B is crucial. Current solutions, both encryption and non-encryption based, offer different advantages and challenges. Non-encryption-based methods can enhance existing systems without major overhauls, while encryption-based methods promise more secure data channels but require significant changes to current protocols.

The necessity to prevent potential safety hazards caused by false data and maintain the reliability of collision avoidance systems underscores the importance of this research. Collaborative efforts between regulatory bodies like EASA, FAA, and ICAO, technology developers, and cyber security experts are essential to develop robust solutions. Ensuring reliable and secure ADS-B communication will enhance situational awareness, improve collision avoidance, and support the safe and efficient operation of U-space services.

Identifying research gaps in encryption technology, real-time authentication mechanisms, and intrusion detection systems will be crucial steps toward achieving these objectives. ICAO should lean towards accommodating research, especially in the emerging deployment of ADS-B in the UAT (978 MHz) band and ADS-Light. Addressing these gaps with innovative hybrid solutions that incorporate both existing and new technologies will ensure the long-term safety and viability of integrating ADS-B into shared airspace globally.

References

[1] Federal Aviation Administration. *NextGen Annual Report, Fiscal Year 2020*. URL: https://www.faa.gov/sites/faa.gov/files/2022-06/NextGenAnnualReport-FiscalYear2020.pdf. (accessed: 20.12.2022).

[2] Perrig Adrian, Canetti Ran, and JD Tygar. "The TESLA broadcast authentication protocol". In: *RSA CryptoBytes* 5 (2002), p. 2002.

[3] *ADS-B Exchange*. URL: https://globe.adsbexchange.com/. accessed: 28.10.2023.

[4] Europeand Union Aviation Safety Agency. *iConspicuity & ADS-L*. URL: https://www.easa.europa.eu/en/downloads/138140/en. (accessed: 25.11.2023).

[5] Clemens Allmann, Stefan Stanzel, and Christian Steffes. "TDOA-based Position Verification of ADS-B Information Using a Sensor Network". In: *2022 Sensor Data Fusion: Trends, Solutions, Applications (SDF)*. IEEE. 2022, pp. 1–6.

[6] Amirhossein Asari et al. "A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems". In: *Computer Networks* 185 (2021), p. 107599.

[7] International Civil Aviation Organization Asia and Pacific Office. *ADS-B IMPLEMENTATION AND OPERATIONS GUIDANCE DOCUMENT*. URL: https://www.icao.int/APAC/Documents/edocs/cns/AIGD%20Edition%2015.0.pdf. (accessed: 21.12.2022).

[8] Joonsang Baek et al. "How to protect ADS-B: Confidentiality framework and efficient realization based on staged identity-based encryption". In: *IEEE Transactions on Intelligent Transportation Systems* 18.3 (2016), pp. 690–700.

[9] Eduard A Bolelov et al. "A Study of Aircraft Positioning Precision in a MLAT Surveillance System with Different Flight Paths and Ground Station Layouts". In: *2022 XIX Technical Scientific Conference on Aviation Dedicated to the Memory of NE Zhukovsky (TSCZh)*. IEEE. 2022, pp. 71–75.

[10] Dan Boneh and Matt Franklin. "Identity-based encryption from the Weil pairing". In: *Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings*. Springer. 2001, pp. 213–229.

[11] Xavier Boyen. "A tapestry of identity-based encryption: practical frameworks compared". In: *International Journal of Applied Cryptography* 1.1 (2008), pp. 3–21.

[12] An Braeken. "Holistic air protection scheme of ADS-B communication". In: *IEEE Access* 7 (2019), pp. 65251–65262.

[13] Stefan Brands and David Chaum. "Distance-bounding protocols". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1994, pp. 344–359.

[14] Brandon Burfeind et al. "Confidential ADS-B". In: *2019 IEEE Aerospace Conference*. IEEE. 2019, pp. 1–11.

[15] Vincent Capezzuto and Greg Dunstone. *Aireon Space-Based ADS-B Implementation and Operation*. URL: https://www.icao.int/APAC/Meetings/2018%20WASS/3 - 1_Aireon % 20Status % 20Briefing_up_REV2 . pdf. (accessed: 10.01.2023).

[16] Eric Chan-Tin et al. "The frog-boiling attack: Limitations of anomaly detection for secure network coordinate systems". In: *International Conference on Security and Privacy in Communication Systems*. Springer. 2009, pp. 448–458.

[17] Christos Chatzichristos et al. "Coupled tensor decompositions for data fusion". In: *Tensors for Data Processing*. Elsevier, 2022, pp. 341–370.

[18] Aireon Company. *THE EXECUTIVE REFERENCE GUIDE TO SPACE-BASED ADS-B*. URL: https://aireon.com/media-kit-assets/Aireon-ExecRefGuide.pdf. (accessed: 02.01.2023).

[19] Indra Company. *ADSB, WAM, MLAT ATM International & Airports implementations. ADSB/WAM integration with Indra's ATC Systems*. URL: https://www.icao.int/NACC/Documents/Meetings/2021/ADSB2/06-IndraWAMMLATInformation.pdf. (accessed: 20.01.2023).

[20] Andrei Costin and Aurélien Francillon. "Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices". In: *black hat USA* 1 (2012), pp. 1–12.

[21] Allie Coyne. *How Airbus defends against 12 big cyber attacks each year*. URL: https://www.itnews.com.au/news/how-airbus-defends-against-12-big-cyber-attacks-each-year-418131. (accessed: 20.01.2023).

[22] Ala' Darabseh et al. "On ads-b sensor placement for secure wide-area multilateration". In: *Multidisciplinary Digital Publishing Institute Proceedings* 59.1 (2020), p. 3.

[23] Sofie Eskilsson et al. "Demonstrating ADS-B AND CPDLC attacks with software-defined radio". In: *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*. IEEE. 2020, 1B2–1.

[24] Cindy Finke et al. "Enhancing the security of aircraft surveillance in the next generation air traffic control system". In: *International Journal of Critical Infrastructure Protection* 6.1 (2013), pp. 3–11.

[25] *FlightAware*. URL: https://flightaware.com/live/. accessed: 28.10.2023.

[26] *Flightradar24.com*. URL: https://www.flightradar24.com. accessed: 28.10.2023.

[27] Nirnimesh Ghose and Loukas Lazos. "Verifying ADS-B navigation information through Doppler shift measurements". In: *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*. IEEE. 2015, 4A2–1.

[28] Balamurugan Gopalakrishnan et al. "Comparative Analysis of FH and CFH Spread Spectrum Under Different Jammers". In: *2020 International Conference on Communication and Signal Processing (ICCSP)*. IEEE. 2020, pp. 1361–1365.

[29] Edan Habler, Ron Bitton, and Asaf Shabtai. "Assessing Aircraft Security: A Comprehensive Survey and Methodology for Evaluation". In: *ACM Computing Surveys* 56.4 (2023), pp. 1–40.

[30] Stephenson Harwood. *Aviation is facing a rising wave of cyber-attacks in the wake of COVID*. URL: https://www.shlegal.com/insights/aviation-is-facing-a-

rising-wave-of-cyber-attacks-in-the-wake-of-covid#. (accessed: 20.01.2023).

[31] Nikolajs Hasjuks, Horst Hellbruck, and Arturs Aboltins. "Performance study of chaos-based DSSS and FHSS multi-user communication systems". In: *2022 Workshop on Microwave Theory and Techniques in Wireless Communications (MTTW)*. IEEE. 2022, pp. 23–28.

[32] Debiao He et al. "Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system". In: *IEEE Transactions on Information Forensics and Security* 12.2 (2016), pp. 454–464.

[33] John Hird. *Air Traffic Management A Cybersecurity Challenge*. URL: https://www.eurocontrol.int/sites/default/files/2021-12/eurocontrol-atm-cybersecurity-report.pdf. (accessed: 20.01.2023).

[34] USA IBM. *What is Blockchain Security?* URL: https://www.ibm.com/topics/blockchain-security. (accessed: 25.01.2023).

[35] Siang-Lin Jheng et al. "1090 MHz ADS-B-based wide area multilateration system for alternative positioning navigation and timing". In: *IEEE Sensors Journal* 20.16 (2020), pp. 9490–9501.

[36] John Richard Jochum. *Encrypted mode select ADS-B tactical military situational awareness*. 2001. URL: https://dspace.mit.edu/bitstream/handle/1721.1/86721/49223652-MIT.pdf;sequence=2. (accessed: 20.12.2023).

[37] Nikita Susan Joseph et al. "FlightSense: A spoofer detection and aircraft identification system using raw ADS-B data". In: *2020 IEEE International Conference on Big Data (Big Data)*. IEEE. 2020, pp. 3885–3894.

[38] T Kacem et al. "Risk-adaptive engine for secure ADS-B broadcasts". In: *Commercial Aviation Cyber Security: Current State and Essential Reading*. SAE International, 2016, pp. 47–55.

[39] Thabet Kacem, Duminda Wijesekera, and Paulo Costa. "Integrity and authenticity of ADS-B broadcasts". In: *2015 IEEE Aerospace Conference*. IEEE. 2015, pp. 1–8.

[40] Thabet Kacem et al. "ADS-B Attack Classification using Machine Learning Techniques". In: *2021 IEEE Intelligent Vehicles Symposium Workshops (IV Workshops)*. IEEE. 2021, pp. 7–12.

[41] Thabet Kacem et al. "Secure ADS-B design & evaluation". In: *2015 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*. IEEE. 2015, pp. 213–218.

[42] Thabet Kacem et al. "Secure ADS-B framework "ADS-Bsec"". In: *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*. IEEE. 2016, pp. 2681–2686.

[43] Suleman Khan et al. "Intrusion Detection in Automatic Dependent Surveillance-Broadcast (ADS-B) with Machine Learning". In: *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*. IEEE. 2021, pp. 1–10.

[44] Yoohwan Kim, Ju-Yeon Jo, and Sungchul Lee. "A secure location verification method for ADS-B". In: *2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*. IEEE. 2016, pp. 1–10.

[45] Che Hun Koh. "Development of an algorithm for correlation of aircraft positioning data from radar and ADS-B sensors/Koh Che Hun". PhD thesis. University of Malaya, 2019. URL: http://studentsrepo.um.edu.my/12008/2/Koh_Che_Hun.pdf. (accessed: 10.01.2023).

[46] Jimmy Krozel et al. "Aircraft ADS-B data integrity check". In: *AIAA 4th aviation technology, integration and operations (ATIO) Forum*. 2004, p. 6263.

[47] Zachary P Languell and Qijun Gu. "Securing ads-b with multi-point distance-bounding for uav collision avoidance". In: *2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE. 2019, pp. 145–153.

[48] Jin Lei, Ruifang Jiang, and Zhijun Wu. "Malicious ADS-B data Generation Based on Improved GAN". In: *2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. IEEE. 2023, pp. 72–77.

[49] Mauro Leonardi, Emilio Piracci, and Gaspare Galati. "ADS-B jamming mitigation: a solution based on a multichannel receiver". In: *IEEE Aerospace and Electronic Systems Magazine* 32.11 (2017), pp. 44–51.

[50] Mauro Leonardi, Emilio Piracci, and Gaspare Galati. "ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions". In: *2014 Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)*. IEEE. 2014, pp. 41–46.

[51] Mauro Leonardi and Gheorghe Sirbu. "Ads-b crowdsensor network and two-step kalman filter for gnss and ads-b cyber-attack detection". In: *Sensors* 21.15 (2021), p. 4992.

[52] Tengyao Li and Buhong Wang. "Sequential collaborative detection strategy on ADS-B data attack". In: *International Journal of Critical Infrastructure Protection* 24 (2019), pp. 78–99.

[53] Yao Liu et al. "Randomized differential DSSS: Jamming-resistant wireless broadcast communication". In: *2010 Proceedings IEEE INFOCOM*. IEEE. 2010, pp. 1–9.

[54] Peng Luo et al. "ADS-B anomaly data detection model based on VAE-SVDD". In: *Computers & Security* 104 (2021), p. 102213.

[55] Mohsen Riahi Manesh and Naima Kaabouch. "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system". In: *International Journal of Critical Infrastructure Protection* 19 (2017), pp. 16–31.

[56] Ahmed Abdel Wahab El Marady. "Enhancing accuracy and security of ADS-B via MLAT assisted-flight information system". In: *2017 12th International*

Conference on Computer Engineering and Systems (ICCES). 2017, pp. 182–187. DOI: 10.1109/ICCES.2017.8275300.

[57] P.J. Martone and G.E. Tucker. "Candidate requirements for multilateration and ADS-B systems to serve as alternatives to secondary radar". In: *20th DASC. 20th Digital Avionics Systems Conference (Cat. No.01CH37219)*. Vol. 2. 2001, 7C2/1–7C2/12 vol.2. DOI: 10.1109/DASC.2001.964193.

[58] Donald McCallie, Jonathan Butts, and Robert Mills. "Security analysis of the ADS-B implementation in the next generation air transportation system". In: *International Journal of Critical Infrastructure Protection* 4.2 (2011), pp. 78–87.

[59] Kayvan Faghih Mirzaei, Bruno Pessanha De Carvalho, and Patrick Pschorn. "Security of ADS-B: Attack scenarios". In: *EasyChair, Tech. Rep* (2019).

[60] Ian Moir. *Military avionics systems*. 1st ed. John Wiley & Sons, 2006.

[61] HOLGER NEUFELDT. *Non-Radar Surveillance ADS-B/MLAT/WAM Products*. URL: https://www.icao.int/NACC/Documents/Meetings/2021/ADSB1/P02-ThalesExpertise.pdf. (accessed: 20.01.2023).

[62] Jiushun Ni et al. "Analysis and Application of Spaceborne Mode S and ADS-B Data Fusion". In: *2021 International Conference on Big Data Engineering and Education (BDEE)*. IEEE. 2021, pp. 51–55.

[63] *Opensky Network*. URL: https://opensky-network.org/. accessed: 28.10.2023.

[64] International Civil Aviation Organization. *Future of Aviation*. URL: https://www.icao.int/Meetings/FutureOfAviation/Pages/default.aspx. (accessed: 20.01.2023).

[65] International Civil Aviation Organization. *GUIDANCE MATERIAL ON ISSUES TO BE CONSIDERED IN ATC MULTI-SENSOR FUSION PROCESSING INCLUDING THE INTEGRATION OF ADS-B DATA*. URL: https://www.icao.int/APAC/Documents/edocs/cns/grpt_atcmulti_adsbdata.pdf. (accessed: 10.01.2023).

[66] International Civil Aviation Organization. *GUIDANCE MATERIAL: SECURITY ISSUES ASSOCIATED WITH ADS-B*. URL: https://www.atlascorporation.ro/upl/documents/01gd_security_adsb.pdf?time=1669851787. (accessed: 12.01.2023).

[67] International Civil Aviation Organization. *Multilateration (MLAT) Concept of use*. URL: https://www.icao.int/APAC/Documents/edocs/mlat_concept.pdf. (accessed: 06.01.2023).

[68] International Civil Aviation Organization. *Technical Provisions for Mode S Services and Extended Squitter (Doc 9871)*. 2nd ed. ICAO, 2012. ISBN: 978-92-9249-042-3.

[69] Nolan Pearce, Kate J Duncan, and Bryan Jonas. "Signal discrimination and exploitation of ads-b transmission". In: *SoutheastCon 2021*. IEEE. 2021, pp. 1–4.

[70] Swathi Pennapareddy and K Natarajan. "Securing ADS-B data transmissions using blockchain: a comprehensive survey and analysis". In: *Aircraft Engineering and Aerospace Technology* ahead-of-print (2022).

[71] Christina Pöpper, Mario Strasser, and Srdjan Capkun. "Jamming-resistant broadcast communication without shared keys." In: *USENIX security Symposium*. 2009, pp. 231–248.

[72] Christina Pöpper et al. "Investigation of signal and message manipulations on the wireless channel". In: *European Symposium on Research in Computer Security*. Springer. 2011, pp. 40–59.

[73] Ali K Raz and Roberto Sabatini. "Information fusion as an autonomy enabler for uav traffic management". In: *AIAA Scitech 2021 Forum*. 2021, p. 0658.

[74] Saulius Rudys et al. "Physical layer protection for ADS-B against spoofing and jamming". In: *International Journal of Critical Infrastructure Protection* 38 (2022), p. 100555.

[75] Krishna Sampigethaya et al. "Future e-enabled aircraft communications and security: The next 20 years and beyond". In: *Proceedings of the IEEE* 99.11 (2011), pp. 2040–2055.

[76] Ken Samuelson, Ed Valovage, and Dana Hall. "Enhanced ads-b research". In: *2006 IEEE Aerospace Conference*. IEEE. 2006, 7–pp.

[77] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. "Experimental analysis of attacks on next generation air traffic communication". In: *International Conference on Applied Cryptography and Network Security*. Springer. 2013, pp. 253–271.

[78] Matthias Schäfer et al. "Bringing Up OpenSky: A Large-scale ADS-B Sensor Network for Research". In: *Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*. IPSN '14. Berlin, Germany, Apr. 2014, pp. 83–94.

[79] Leonard Schuchman. *Automatic dependent surveillance system secure ads-s*. US Patent 7,876,259. Jan. 2011.

[80] Savio Sciancalepore, Saeif Alhazbi, and Roberto Di Pietro. "Reliability of ADS-B communications: Novel insights based on an experimental assessment". In: *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*. 2019, pp. 2414–2421.

[81] Arslan Shafique, Abid Mehmood, and Mourad Elhadef. "Survey of security protocols and vulnerabilities in unmanned aerial vehicles". In: *IEEE Access* 9 (2021), pp. 46927–46948.

[82] Fute Shang et al. "Multidevice false data injection attack models of ADS-B multilateration systems". In: *Security and Communication Networks* 2019 (2019).

[83] Sathya S Silva, Luke Jensen, and R John Hansman. "Pilot Perception and Use of ADS-B In Traffic and Weather Services (TIS-B and FIS-B)". In: *15th AIAA Aviation Technology, Integration, and Operations Conference*. 2015, p. 2849.

[84] Hadjar Ould Slimane et al. "ADS-B Message Injection Attack on UAVs: Assessment of SVM-based Detection Techniques". In: *2022 IEEE International Conference*

on Electro Information Technology (eIT). IEEE. 2022, pp. 405–410.

[85] Mario Strasser et al. "Jamming-resistant key establishment using uncoordinated frequency hopping". In: *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE. 2008, pp. 64–78.

[86] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. "On the security of the automatic dependent surveillance-broadcast protocol". In: *IEEE Communications Surveys & Tutorials* 17.2 (2014), pp. 1066–1087.

[87] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. "Security of ADS- B: State of the Art and Beyond". In: DCS, University of Oxford, UK. 2013.

[88] Martin Strohmeier et al. "Realities and challenges of nextgen air traffic management: the case of ADS-B". In: *IEEE Communications Magazine* 52.5 (2014), pp. 111–118.

[89] Junzi Sun. *The 1090 Megahertz Riddle: A Guide to Decoding Mode S and ADS-B Signals*. 2nd ed. TU Delft OPEN Publishing, 2021. ISBN: 978-94-6366-402-8. DOI: 10.34641/mg.11.

[90] Mahyar TajDini, Volodymyr Sokolov, and Pavlo Skladannyi. "Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio". In: *2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*. IEEE. 2021, pp. 1–5.

[91] Garrett Thompson. *Boeing Subsidiary Jeppesen Suffers Cyberattack*. URL: https://www.binarydefense.com/threat_watch/boeing-subsidiary-jeppesen-suffers-cyberattack/. (accessed: 20.01.2023).

[92] Elochukwu Ukwandu et al. "Cyber-security challenges in aviation industry: A review of current and future trends". In: *Information* 13.3 (2022), p. 146.

[93] Ángeles Vázquez-Castro. "Asymptotically Guaranteed Anti-Jamming Spread Spectrum Random Access Without Pre-Shared Secret". In: *IEEE Transactions on Information Forensics and Security* 17 (2022), pp. 332–343.

[94] Camilo Andres Pantoja Viveros. "Analysis of the cyber attacks against ADS-B perspective of aviation experts". PhD thesis. University of Tartu Tartu, Estonia, 2016.

[95] Gref Welch and Gary Bishop. "An introduction to the Kalman Filter, Department of computer science". In: *University of North Carolina* (2006).

[96] Kyle D Wesson, Todd E Humphreys, and Brian L Evans. "Can cryptography secure next generation air traffic surveillance?" In: *IEEE Security and Privacy Magazine* (2014).

[97] Matthias Wilhelm, Jens B Schmitt, and Vincent Lenders. "Practical message manipulation attacks in IEEE 802.15. 4 wireless networks". In: *MMB & DFT 2012 Workshop Proceedings*. 2012, pp. 29–31.

[98] Zhijun Wu, Tong Shang, and Anxin Guo. "Security issues in automatic dependent surveillance-broadcast (ads-B): a survey". In: *IEEE Access* 8 (2020), pp. 122147–122167.

[99] Zhijun Wu et al. "ADS-Bchain: A Blockchain-based Trusted Service Scheme for Automatic Dependent Surveillance-Broadcast". In: *IEEE Transactions on Aerospace and Electronic Systems* (2023).

[100] Zhijun Wu et al. "An ADS-B message authentication method based on certificateless short signature". In: *IEEE Transactions on Aerospace and Electronic Systems* 56.3 (2019), pp. 1742–1753.

[101] Anjia Yang et al. "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification". In: *IEEE Transactions on Services Computing* 10.2 (2015), pp. 165–175.

[102] Haomiao Yang, Hongwei Li, and Xuemin Sherman Shen. *Secure Automatic Dependent Surveillance-Broadcast Systems*. Springer, 2022.

[103] Haomiao Yang et al. "LHCSAS: A lightweight and highly-compatible solution for ADS-B security". In: *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE. 2017, pp. 1–7.

[104] Weicai Yang et al. "Location Awareness Method for ADS-B Signal Source Based on Satellite". In: *2022 15th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*. IEEE. 2022, pp. 1–5.

[105] Xuzhou Yang, Junzi Sun, and Raj Thilak Rajan. "Aircraft Trajectory Prediction using ADS-B Data". In: *42nd WIC Symposium on Information Theory and Signal Processing in the Benelux (SITB 2022)*. 2022.

[106] Peng Yi et al. "Efficient Hierarchical Signature Scheme with Batch Verification Function Suitable for ADS-B System". In: *IEEE Transactions on Aerospace and Electronic Systems* (2022).

[107] Xuhang Ying et al. "Detecting ADS-B spoofing attacks using deep neural networks". In: *2019 IEEE conference on communications and network security (CNS)*. IEEE. 2019, pp. 187–195.

[108] Tang Yong et al. "ADS-B and SSR data fusion and application". In: *2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*. Vol. 2. IEEE. 2012, pp. 255–258.

[109] Feng Zeng. "Secure ADS-B protection scheme supporting query". In: *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*. IEEE. 2021, pp. 513–518.

[110] Dongxu Zhao, Jinlong Sun, and Guan Gui. "En-route multilateration system based on ADS-B and TDOA/AOA for flight surveillance systems". In: *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. IEEE. 2020, pp. 1–6.