IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 16, 2020, accepted June 29, 2020, date of publication July 6, 2020, date of current version July 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007182

Security Issues in Automatic Dependent Surveillance - Broadcast (ADS-B): A Survey

ZHIJUN WU, TONG SHANG, AND ANXIN GUO
School of Electronics & Information & Automation, Civil Aviation University of China, Tianjin 300300, China

Corresponding author: Zhijun Wu (zjwu@cauc.edu.cn)

This work was supported in part by the Joint Foundation of National Natural Science Committee of China and Civil Aviation Administration of China under Grant U1933108, in part by the Scientific Research Project of Tianjin Municipal Education Commission under Grant 2019KJ117, and in part by the Fundamental Research Funds for the Central Universities of China under Grant 3122019051.

ABSTRACT As a new generation of air transportation surveillance technology, the automatic dependent surveillance - broadcast (ADS-B) system mainly completes the extraction and processing of the position information and other additional information of the aviation aircraft to form a clear and intuitive background map and trajectory. However, ADS-B broadcasts information via open and unencrypted protocols, it is vulnerable to deliberate intrusions and attacks, which poses a great security risk. This paper studies the security issues of the ADS-B system in information leakage and tampering. Starting from the vulnerability of the ADS-B system, it is divided into vulnerability based on attack intention and vulnerability based on security requirements. Various solutions for solving vulnerabilities from two aspects, secure location authentication, and secure broadcast authentication are proposed, and the solutions are compared in terms of security and feasibility. The research results show that a single solution does not fully protect the security of the ADS-B system. For example, the PKI (Public Key Infrastructure) technology and the SS (Spread Spectrum) technology can resist most attacks, but there are still deficiencies. Therefore, this paper proposes to propose a multi-layered security framework in future research work, which includes detecting and preventing different attacks in the ADS-B system.

INDEX TERMS Automatic dependent surveillance - broadcast (ADS-B), security, vulnerability, authentication, protection.

I. INTRODUCTION

The normal operation of aviation relies heavily on computer systems. With the development of information technology, the links between aviation systems connect more closely, which also increases the possibility of attackers entering the system. In recent years, information security incidents in the global aviation industry have gradually increased, such as cyber-attacks and ICT (Information and Communications Technology) dependent disruptions [1]. Table 1 shows the cyberattacks against ATC (Air Traffic Control) systems in recent years. Within 2008, a total of 800 network alarm incidents were discovered, and more than 150 incidents have not been resolved yet. Besides, Airbus Group revealed in a report, the company suffers about 12 major cyber-attacks every year [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

More and more people prefer to travel by airplane nowadays because of the economic growth and development. Federal Aviation Administration (FAA) predicts, as of 2033, the number of passengers in commercial aviation will increase to an unprecedented 1.15 billion [3]. As a result, the number of aircraft in the airspace will continue to increase for the foreseeable future, and the airspace will be more crowded. In order to enlarge current airspace capacity, improve flight safety and meet future navigation needs, Federal Aviation Administration (FAA) was formulated NextGen (Next Generation Air Transportation System) project in 2004, the project aims to gradually transform a land-based ATC system which relies on radar networks into the satellite-based navigation system, ultimately realizing the modernization of the National Airspace System. As a pivotal part of the NextGen project, ADS-B can greatly improve the operational efficiency of air traffic control and reduce the maintenance cost of air traffic control infrastructure. Compared to

TABLE 1. List of aviation network security incidents in recent years.

Years	Event Description
2006	Air traffic control system of Federal Aviation Administration (FAA) infected with the virus, leading to partial ATC system closed in Alaska [3]
2007	Avionics electronic flight bag of Thailand was infected with the virus, causing the electronic flight bag to fail [3]
2008	800 cyber-attacks against air traffic control facilities were detected, more than 150 incidents have not been resolved yet [3]
2009	FAA server was attacked, 48,000 employee names and social security numbers were stolen [3]
2009	Truck drivers carrying Global Positioning System (GPS) jammers inadvertently disrupted the ground enhancement system at Newark Liberty International Airport [4],[5]
2011	The airport code was maliciously broken by software engineers, causing 50 flight delays [6]
2014	European 13 aircraft disappeared from the air traffic control radar for 25 minutes, suspected air traffic control system was hacked [7]
2015	Federal Aviation Administration network encounters hacker attacks [8]
2016	The aviation industry has suffered more than 1,000 attacks per month [9]
2017	750GB of internal sensitive data at the Stewart International Airport in New York was leaked, including various device passwords and employee social security numbers.
2018	The Bristol Airport in the United Kingdom was attacked by extortion. The airport's flight information showed that the system was disrupted, causing airport personnel to work with whiteboards and markers.
2019	Malaysia airlines, millions of details of passengers' passports, addresses and phone numbers were leaked and uploaded to data interchange forums

traditional radar-based surveillance systems, ADS-B can provide not only real-time and accurate aircraft positioning information, but also has a lower maintenance cost and longer service life. Specifically, the construction and maintenance costs of which are only one-tenth of the former [10], [11]. Federal Aviation Administration (FAA) claims, as of January 2020, all commercial aircraft must be retrofitted ADS-B OUT device [12]. However, as a result of the internet connection, comprehensiveness, and interoperability between systems, the implementation of these new technologies to the aviation industry has brought new network weakness [13].

In the 1990s, RF communication technology was relatively complex and costly to implement. It was considered a secure communication method. Therefore, the priority of ensuring ADS-B communication security was not very high. Neither the Radio Technical Committee (RTCA) official standard [14]–[16] nor other concerned demand files [17], [18] security mentioned in this aspect. While the development of technology, especially the appearance of the SDR (Software Defined Radio), enables potential attackers to achieve RF transmission and reception at a low cost. Because ADS-B broadcasts information using an open unencrypted protocol, it lacks relevant security measures, making it vulnerable to various attacks. Widely reported that in the mainstream media [19]–[23] and under the impetus of various security conferences [24], [25], gradually attracted people's attention. Researchers have also demonstrated that the security of ADS-B systems can be easily compromised using existing hardware and software [26]. Extensive news exposure prompted ICAO (International Civil Aviation Organization) to include the safety of civil aviation on the agenda of its 12th Air Navigation Conference, viewed ''cyber safety as a high-level barrier to implementation'' and created a working group to help coordinate stakeholder work [27].

Even if it is not attacked, ADS-B does not have an auxiliary mechanism to confirm the position when the transmitter fails. There have been many incidents of dangerous situations caused by ACAS (Automatic Collision Avoidance System) or other avionics equipment failures [28], [29]. As 2020 approaches, ADS-B's security deficiencies have also raised some concerns in the aviation community about following the NextGen deployment plan. The Attorney General of the Ministry of Communications mentioned in a report that NextGen plans to complete the deployment longer than expected [30]. Therefore, there is an urgent need to solve the security problem of ADS-B.

A. MOTIVATION

There have been many published research reports on attacks and security protection schemes suffered by the ADS-B system. However, as far as we know, existing research has not dealt well with certain attacks and defense mechanisms against ADS-B systems. The motivation for writing this article is as follows.

1) Existing solutions can only solve one or several kinds of attacks, but cannot achieve complete defense. There is no comprehensive defense system.
2) Most of the solutions that have been proposed are only in the experimental stage, under the designed experimental environment, and have not been put into practice.
3) There is less contrast between various ADS-B system attack and defense mechanisms.
4) Summarize the latest relevant research of ADS-B system security protection.

TABLE 2. Comparison with existing surveys considering the discussion of ADS-B system security.

Work	Compare with prior surveys	ADS-B working principle diagram	Attack model diagram	Attacker classification	TESLA principle diagram	Attack layer	Defensive security level	Defensive scalability	Blockchain and Deep learning
[37]	×	×	×	√	×	×	√	×	×
[44]	×	√	×	×	√	√	×	√	×
Our survey	√	√	√	√	√	√	√	√	√

Therefore, it is necessary to classify, compare, and summarize the published solutions, analyze the advantages and disadvantages, and propose a comprehensive plan as the future research direction.

B. CONTRIBUTIONS

This article introduces the development status of the ADS-B system, the existing loopholes and the proposed solutions. This article has conducted a detailed study of the attacks and solutions received by the ADS-B system. It is hoped that the research and summary of this article will help relevant personnel develop effective defense solutions and protect the security of the ADS-B system. The new contributions of this article are as follows.

1) The working principle of the ADS-B system is analyzed, and the attack scenarios suffered by the ADS-B system are given in conjunction with the chart.
2) The published solutions have been evaluated from the perspectives of system requirements, costs, attack coverage, and implementation difficulty, and their advantages and disadvantages were analyzed.
3) In view of the existing defects and risks, combined with the new technology blockchain, a solution to use the blockchain to protect the security of the ADS-B system is proposed, and it will be the main direction of future research.
4) Compared with the previous review articles, we have updated the current solutions, summarized more new methods, and combined with some existing solutions, put forward our ideas for the future development of this field.

In addition, this article is compared with two well-known review articles in this field. See Table 2 for details.

The remainder of the survey is organized as follows. Section 2 introduces some related work about how to secure the ADS-B. Classifies and analyzes ADS-B system vulnerabilities in Section 3. In section 4 we analyze current ADS-B security solutions. Section 5 compares the advantages and disadvantages of different solutions. Section 6 briefly describes the current challenges and puts forward the direction of future development and finally, we draw a conclusion of this paper in section 7.

II. THREAT TO ADS-B SYSTEM

Figure 1 shows the basic framework of the working principle of ADS-B.

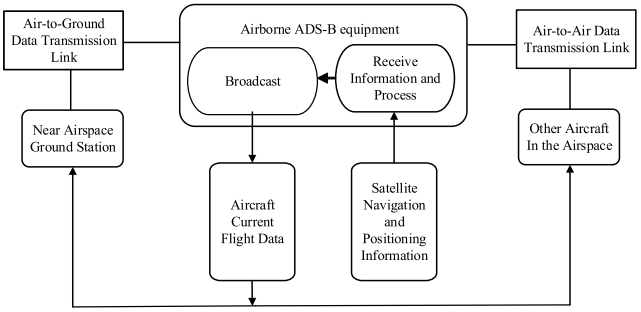

FIGURE 1. Working principle of the ADS-B system.

First, the aircraft obtains the navigation and positioning information transmitted by the satellite through its own equipped GPS and airborne equipment, and performs real-time positioning to accurately determine the current position and speed of the aircraft and other information. Secondly, the ADS-B sending equipment obtains the required parameters from the relevant airborne equipment and broadcasts the information through the digital data link through broadcast. For different types of messages, the sending equipment broadcasts at different frequencies. At this time, other aircraft and adjacent ground receiving devices in the adjacent airspace can receive broadcast messages. The flight data of the broadcast aircraft can be obtained by receiving and processing all the signals that need to be received. At the same time, the aircraft can also receive broadcast messages sent by other aircraft. The data transmission between the aircraft and the aircraft, and between the aircraft and the ground, form an air-air, air-ground data transmission link.

There are currently three ADS-B data link standards that have been proposed, namely the secondary surveillance radar mode S ultra-long message (1090ES), VHF digital link mode 4, Universal Access Transceiver (UAT) mode. Among them, UAT and 1090ES are the two most used models at present, and they have a competitive relationship with each other. The UAT mode is specifically designed for aviation services, with a frequency of 978MHz, and new hardware needs to be installed when it is applied. The 1090ES works at

a frequency of 1090MHz. When it is used, it can be used by simply upgrading the aircraft's original S-mode transponder system. The relationship is shown in Figure 2.

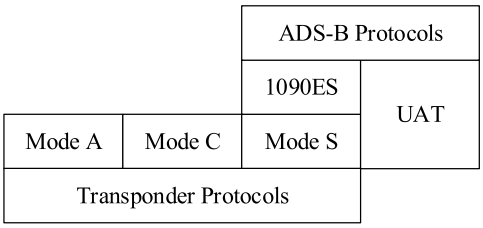

FIGURE 2. ADS-B protocol hierarchy.

According to the working principle of the ADS-B system, Figure 3 shows the common attack methods in the actual situation.

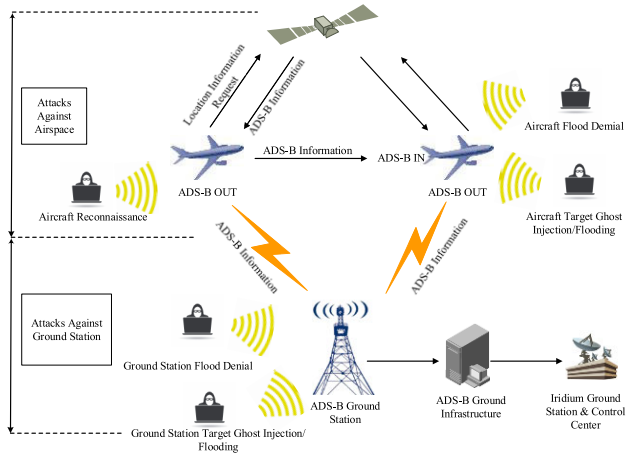

FIGURE 3. Attacks in the real environment.

Current attacks are mainly divided into attacks against aircraft and attacks against ground stations. Mainly by eavesdropping on the message packet, interfering with the signal propagation, and intercepting the message to modify or delete. So that the receiver receives the wrong information or cannot receive the message. Use this to cause damage and achieve the purpose of the attack.

III. ADS-B SYSTEM VULNERABILITY

ADS-B messages send by radio channels open unencrypted and do not take any security measures to protect the transmission of data. Therefore, an attacker can easily launch attacks such as eavesdropping, jamming, and message modification, which brings great security risks to large-scale applications in the latter stage. This section mainly uses two methods to classify ADS-B system vulnerabilities. Based on attack intentions and based on security requirements, and risk analysis of different vulnerabilities.

A. ATTACK INTENTION

European Union Agency for Network and Information Security [31] classifies attackers into three types of insider attackers, malicious airport/aircraft passengers, and remote attackers. With traditional wired networks and computer systems of different, the ''internal'' concept of wireless communication is not clear. Since both the wireless communication network does not require a physical connection and without particular physical isolation, they have the same internal and external access, namely data reception and data transmission. Referring to the survey by Zargar [32] *et al.*, this article is classified according to the attacker's intention. The target of the attacker is not only the ADS-B system but also the entire ATC system. We can attack divided into four categories according to the intention of the attack. Table 3 gives a detailed classification.

1) INFORMATION COLLECTION/PERSONAL INTEREST

This kind of attack is a passive attack, and its harm is the lowest, the attacker is mainly amateurs. They can use the public website [33] or the mobile app [34] to display real-time ADS-B information. Due to the natural openness of the ADS-B system, the aircraft periodically broadcasts plaintext information at a fixed frequency using ADS-B technology. Similarly, they can use inexpensive SDR receivers to collect and store ADS-B messages from nearby airspace. Although such attacks will not interfere with normal air traffic, the collection of sensitive information is the basis for launching other active attacks.

2) ECONOMIC BENEFIT

Attackers in this category usually have a clear purpose, most have basic hardware and RF communication knowledge, and are familiar with the various communication protocols in modern ATC systems. The main purpose of such an attacker is to generate ghost aircraft or false collision warning signals, distracting pilots and ground controllers, and disrupting flights. We can imagine a typical attack scenario, an attacker uses an SDR transceiver to listen, collect ADS-B messages, and then change the speed, altitude, etc. of the aircraft in the message, and then launch it. They usually presuppose a wide range of failures in the ATC system, using methods such as extortion to gain substantial economic benefits.

3) TERRORISM

Attackers in this category are the worst and more harmful. The aviation industry is an important part of the national infrastructure and the key to sustaining economic development. As a source of power for national infrastructure, aviation networks naturally become targets of terrorists or attackers for political purposes. Traditionally, terrorist organizations need to use force to hijack or destroy aircraft to achieve the purpose of the attack. Nowadays, exploiting the loopholes in wireless air communication can attack the aircraft from the ground within a safe distance, which will pose a great threat to national security.

4) CYBER WARFARE

Such attackers usually belong to the military sector of a country and have sufficient knowledge and near-infinite resources

TABLE 3. Classification of attack intentions.

Attack Intention	Attacker Category	Ability	Attack Cost
Information Collection / Personal Interest	Amateurs	Eavesdropping	SDR receiver, Network connection
Economic Benefit	Hacker	Eavesdropping within a certain range, message modification, deletion, playback attack	SDR launcher, Certain RF communication and aviation protocol knowledge
Terrorism	Terrorist Organization	Wide range of eavesdropping, message modification, deletion, playback attack	SDR launcher, Rich RF communication and aviation protocol knowledge
Cyber Warfare	National Military Organization	Any physical or network attack	Military radio, ability to launch electronic warfare

to attack the critical infrastructure of another country for political or military purposes. Such attacks can smash a country and have a serious economic impact.

Reducing the attacker's interest in a target is a basic defense. Therefore, studying the attack intention of the attacker helps to formulate effective strategies to defend against possible attacks. These strategies will make the attacker lose interest in the target, such as making the attack target technically impossible, otherwise the attacker will be severely punished (economic loss, life imprisonment, etc.).

B. SECURITY REQUIREMENTS

According to different attack targets, attacks can be classified into two types, one is attacking navigation information, and another is attacking ADS-B information. The current ADS-B mainly relies on GPS navigation signals as the main data source. When an attacker interferes or modifies the navigation signal, the aircraft may not be able to receive navigation signals [35], [36]. This article focuses on attacks targeting ADS-B information.

In line with the security requirements for the ADS-B information attack, it will be classified as authentication, integrity, confidentiality, and availability of four categories. As shown in Figure 4, and the detailed description of the security requirements of the ADS-B system shows in Table 4 [37].

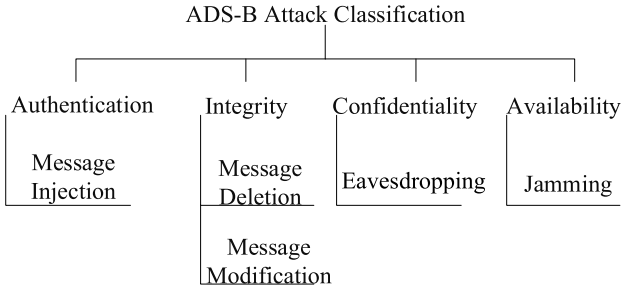

FIGURE 4. ADS-B attack classification.

The following is a detailed analysis of the different attack categories for the ADS-B system.

TABLE 4. Security requirements of the ADS-B system.

Security Requirement	Description
Authentication	Identity authentication means that the communication recipient should be capable of accurately identifying the true identity of the aircraft transmitter at all hours. However, by injecting the message into the communication of the legal entity and changing the AA address in the ADS-B message, the malicious node can broadcast the ADS-B message using the false identity that cannot be authenticated.
Integrity	During the transmission, ADS-B data cannot be revised, deleted, interposed, and forged accidentally or intentionally is required by the ADS-B data integrity. Therefore, message deletion and message modification attacks are directed at data integrity. So, classify them as this category.
Confidentiality	Confidentiality means that during the transmission process, illegal users cannot read the information. Only the authorized person can use the data in the network. Any activity that leads to information leakage to unauthorized or malicious users violates confidentiality. Therefore, eavesdropping falls into this category.
Availability	Availability means subscribers or licensors must always get ADS-B messages and services. For example, an attacker can easily jam an ADS-B ground station and perform a denial of service attack. Therefore, jamming and flooding attacks fall into this category.

1) MESSAGE INJECTION

Because ADS-B technology does not have an authentication mechanism, attackers can use existing technology to construct legitimate fake information and inject fake messages into existing air traffic communications. Schäfer *et al.* [26] shows a low-cost broadcast of fake messages using limited knowledge and common techniques. Similar to jamming attacks, an attacker can perform message injections on ground stations/aircraft, such as ground station target ghost injections and aircraft target ghost injections. In order to perform a ground station target ghost attack, the attacker needs to

create and broadcast fake ADS-B messages with the same attributes as the real ADS-B message, including speed, location, and identification number, so that the receiver cannot distinguish between normal ADS-B signal and false ADS-B signal. Eventually, the false target will appear on the network of the legitimate node, achieving the purpose of the ghost attack.

2) MESSAGE DELETION

As for this type of attack, the legal message from the ADS-B net can delete by an attacker. One way is for an attacker to generate a sufficient number of bit errors in an ADS-B message. The ADS-B message has a 24-bit parity data segment that supports the correction of up to 5-bit errors. Any message that exceeds 5-bit errors will be considered a corrupted message and will be discarded. Alternatively, the attacker can generate a synchronization signal with the target ADS-B that is opposite in phase to the target ADS-B signal, so that it can partially or eliminate and destroy the ADS-B message. However, implementing such attacks requires strict time synchronization, which is technically complex and inefficient. In both cases, the aircraft will disappear on the surveillance system, increasing the risk of aircraft collisions.

3) MESSAGE MODIFICATION

Because such attacks require modification of messages from legitimate nodes in the network, they are the most difficult of all attacks. Implementing such an attack requires an attacker to access legitimate network devices, which is too hard in reality. However, there are other ways to perform such an attack. For example, overlay, bit flipping, and combined message deletion and injection [37].

In an overlay attack, an attacker can replace or change a legitimate message by transmitting a high-power signal. This type of attack is different from a jamming attack. The coverage target is a specific node rather than the entire channel. The target of the jamming attack is the entire channel. Bit flipping means that the attacker achieves the purpose of flipping the bit in the message by superimposing the fake information. Of course, simultaneously implementing message deletion and modification can also achieve the purpose of modifying the message. See the survey by Pöpper *et al.* [38] and Wilhelm *et al.* [39] for details.

4) EAVESDROPPING

Eavesdropping, message interception, or aircraft reconnaissance attacks are all categories of eavesdropping, which refers to the behavior of an attacker maliciously collecting and analyzing wireless signals. Since ADS-B sends plaintext information over an unencrypted wireless channel. It is naturally open, and any third party can receive its information utilizing a radio frequency transceiver. So eavesdropping is the most direct weakness of ADS-B.

Since the advent of ADS-B technology, eavesdropping has been a closely watched issue. While some services can legitimately use this feature to track air traffic, providing services to consumers, for example, the flightradar24.com provides consumers with real-time global flight tracking service through its ADS-B network data across more than 20,000 ADS-B receivers worldwide. However, it does not rule out that some malicious attackers can use this vulnerability to launch some complex attacks. Furthermore, even message encryption may have eavesdropped, let alone the ADS-B message is not encrypted. While a few countries, for example, the United Kingdom, have enacted laws to listen to broadcast information to unintended recipients. The current technical reality has made it difficult to implement these laws effectively.

5) JAMMING

Since ADS-B broadcasts messages in random burst mode and does not have a collision detection mechanism. In a jamming attack, an attacker only needs to send a large amount of strong power data in the same frequency band, which can hinder the real participation in the communication session. The sender sends or receives data, which reduces the service capability of the attack target, and ultimately prevents the attacker from providing normal services to the user. In addition, Wilhelm *et al.* [40] mentions that real-time reactive jamming only for existing data packets in the air has proven to be feasible. Jamming is a common problem in wireless networks. Considering the openness of aviation networks and the special nature of air traffic data, its risk in the aviation industry has been further amplified.

In addition to the ADS-B receiver, the PSR (Primary Surveillance Radar) may also be a jamming target for the attacker. Due to factors such as the rotating antenna of the PSR and high power, it is difficult to implement. In the survey by Adamy *et al.* [41] can find a detailed introduction to radar and jamming.

There are two main types of jamming attacks against ADS-B, namely Ground Station Flood Denial and Aircraft Flood Denial [42]. The purpose of these attacks is to interrupt the monitoring network by jamming the communication channel. Launching a ground station flood attack is easier than an aircraft flood attack. Because the attacker can attack the closest possible target and therefore requires less energy to attack. If the attacker intends to interfere with aircraft signals on the ground, a very high-power interference signal is required, so this situation is hard to occur.

Table 5 summarizes and compares the ADS-B attacks according to the degree of difficulty, the harms generated, etc.

Because ADS-B transmits data over an open and unencrypted wireless channel, it is vulnerable to eavesdropping. Eavesdropping is a passive attack, and eavesdropping itself does not cause any damage to the ATC system, so it is classified as the lowest hazard.

Message deletion attacks are of moderate risk because they require time synchronization, which reduces the possibility of performing this attack. In addition, the impact of message deletion attacks on ATC and surveillance systems is moderate. Even if the attacker's attack causes the aircraft to

TABLE 5. ADS-B vulnerability risk analysis.

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 Inject	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	

disappear from the control terminal, the backup system still supports the surveillance system. For example, multilateral flight, thereby reducing the harm of this attack. Similar to the message deletion attack, jamming attacks have the same risks and may cause the aircraft to disappear. However, because jamming attacks do not require time synchronization, the possibility of such attacks is relatively high and is of moderate risk.

Message modification attacks on air traffic safety impact of the largest. Because the attacker could hijack the aircraft remotely and cause the aircraft to collide [37]. However, message modification attacks require strict time synchronization and higher complexity. Therefore, this possibility of performing this attack is minimal.

Message injection attacks can inject a large amount of fake aircraft information into the communication channel, which can seriously disrupt air traffic and cause aircraft collision. Hence, give this type of attack the highest risk.

IV. CURRENT ADS-B SECURITY SOLUTION

As mentioned above, over the past decade, more and more researchers have participated in the ADS-B security research and proposed various solutions to enhance the security of ADS-B. There are two main types of current ADS-B security solutions [43], secure location verification and secure broadcast authentication. Figure 5 shows the specific classification [44]. In this section, we will analyze the merits and demerits of each scenario in detail.

A. SECURE LOCATION VERIFICATION

Unlike secure broadcast authentication, the aim is to verify the safety position of the aircraft or other communication participant's authenticity of location information cross-checked. The core is to find the real location information of the sender and verify the authenticity by cross-validating with the location information [44]. In addition, this location information

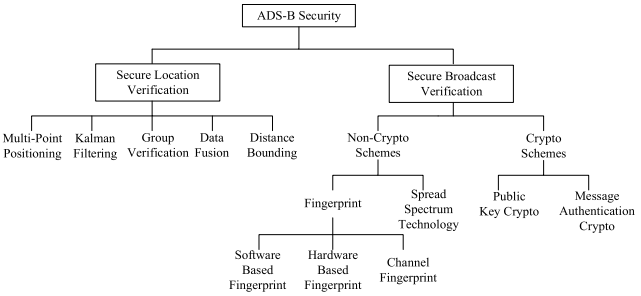

FIGURE 5. ADS-B Solution Classification.

can be used in conjunction with ADS-B and radar to provide an alternative solution when the navigation system fails.

1) MULTILATERATION

Multilateration technology is based on the signal arrival time difference (TDOA) [45] positioning principle. The system calculates multiple (at least three) ground stations by receiving periodic reports from the aircraft, or secondary radar interrogation signals, or TCAS (Traffic Collision Avoidance System) response signals. The time difference of the same signal is received and a hyperbolic equation is established to determine the position of the aircraft. Figure 6 shows the TDOA [46].

Multilateration technology is now applied to the Advanced Scene Motion Guidance Control System (A-SMGCS), in addition to its scalability, easy verification of data availability, high redundancy, and low cost, especially for multi-point monitoring. The system can fully utilize the ADS-B ground station, making it an ideal ADS-B positioning monitoring backup system.

There have been several research literatures on multilateration of ADS-B signals. Kaune *et al.* [47] established an exclusive cut-price test bench that can use ADS-B signals for multilateration. Smith *et al.* [48] proposed a method of

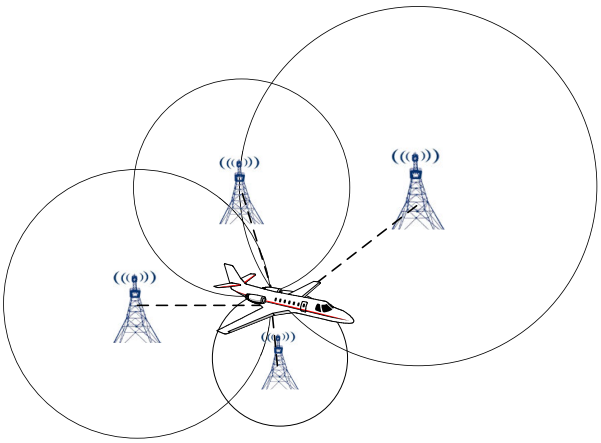

FIGURE 6. TDOA hyperboloid intersection.

multilateral technology that provides authentication and ADS-B communications backup. Johnson *et al.* [49] described their work in the Afghan theater, and the results prove that regional multi-point positioning is an adaptive and reliable monitoring solution. Daskalakis [50] conducted a regional multilateration (WAMLAT(Wide Area Multilateration)) technique to track the low-altitude helicopter and route flight experiments in the Gulf of Mexico, the results show that the effect is comparable to SSR (Secondary Surveillance Radar), surveillance. MITRE [51] analyzed the possibility authorized by the US Federal Aviation Administration established WAMLAT selective navigation system in the United States airspace.

However, ICAO also lists some known shortcomings of multilateration as follows [52].

1) Susceptible to multipath effects.
2) Requires multiple receiving stations to correctly receive signals.
3) The central processing station must be connected to multiple receiving stations.
4) It is difficult and expensive to deploy sensors in remote areas.

In addition, Schuchman *et al.* [53] also mention the method by which an attacker deceives a multilateration system. Multilateration technology requires the cooperation of multiple ground equipment and is not suitable for air-to-air communication scenarios between aircraft and aircraft. However, this technology can be used in conjunction with data fusion technology as a backup system for ADS-B systems. It is worth noting that the use of multilateration technology as a backup system, although increasing the reliability of ADS-B, adding a backup system, indirectly increasing the running cost of the ADS-B, and weakening the low-cost advantage of the ADS-B system.

2) KALMAN FILTERING

Kalman filtering has been used in ATC systems that GPS signal is filtered to avoid planes collided in the coasting condition [37], [54]. The Kalman filtering method is a method of processing ADS-B data by using a Kalman filtering. The Kalman filtering can clear invalid data, smooth fill missing data, filter signal noise, and obtain ideal and accurate flight status values. It is mainly used for the ground system to filtrate and validate the ADS-B report the aircraft state vector and the track changes, and these data plausibility check [55].

Krozel *et al.* [56] proposed a multivariate Kalman filtering method. The method combines the actual motion of the aircraft with the intent information in the ADS-B information to form a correlation function. Figure 7 shows a schematic diagram of the correlation function [56]. Among them, the validity verification of the intent information is divided into two parts, geometric conformity verification and purpose matching verification. The correlation function is used to find the correlation between the aircraft motion and the broadcast intention, the geometric coincidence verification verifies whether the flight between the turning points of the aircraft meets the required navigation performance. Objective to verify whether the pilot is flying according to the broadcast intention, decompose the aircraft motion state into the horizontal track, vertical track, and speed, respectively establish correlation function, obtain the correlation degree of each corresponding motion state corresponding vector. Then establish the target model and calculate the integrity of the ADS-B intent information is evaluated based on the Required Navigation Performance (RNP).

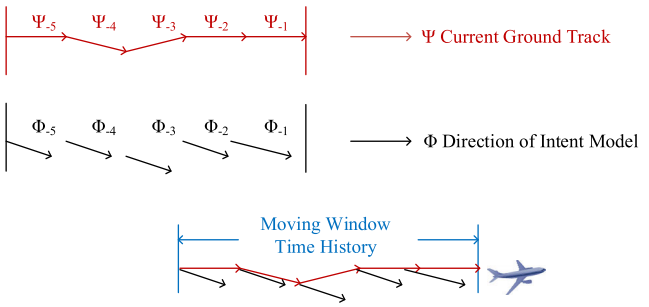

FIGURE 7. Correlation function with previous and current values.

Kovell *et al.* [57] noted Kalman filter has been widely used since the ADS-B related systems, it is necessary to differentiate between the different categories of data processing filter. Such as handling aircraft GPS position information and mentioned in the text the Kalman filtering for handling real-time position information declarations. Kovell *et al.* [57] used the data of the ADS-B system and other monitoring system data for data fusion, and proposed an encryption method and positioning technology for protecting the ADS-B system. In addition, the Kalman filter and group verification are studied to develop more reliable positioning methods.

Kalman filtering is an algorithm that uses the linear system state equation to observe the system input and output data to optimally estimate the state of the system. It is characterized by processing noisy input and observation signals based on linear state space representation to obtain a system state or real signal. In the field of civil aviation, it is mainly used to detect whether the flight route of the aircraft is consistent with

the predetermined route. Perform relevant calculations on the aircraft's real course and flight plan, and determine whether the aircraft is driving normally according to the calculation results. The Kalman filter has a large amount of calculation when the complexity of the operation increases, the operation time becomes longer, which greatly affects the positioning of the aircraft. Moreover, when the moving object is blocked for a long time, the target will be lost.

From the attacker's point of view, there are two main vulnerabilities in the current Kalman filtering method. One is the frog boiling attack [58]. Such an attack can jam the signal of the real node and inject the false position information at a slow rate so that the Kalman filtering cannot know the change of the signal. One is a denial of service attack. Since the Kalman filtering processes data for a long time, as the complexity increases, the probability of being subjected to a denial of service attack is greater.

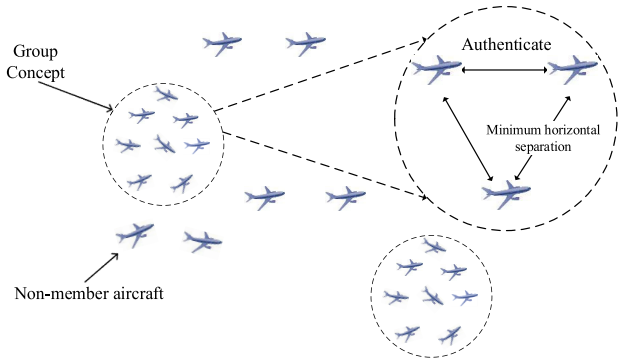

FIGURE 8. ADS-B group concept.

3) GROUP CERTIFICATION

Sampigethaya *et al.* [59] proposes that group authentication can be used to solve ADS-B security and privacy issues. Figure 8 shows the concept of the group [59]. The group authentication mainly uses the multilateration technology between members in the group to verify the location declaration information of the members in the non-group, thereby ensuring the communication security of the ADS-B IN. Four or more aircraft first authenticate each other to establish a trust to become a member of a group. Then utilizing multilateration techniques based on signal strength or signal arrival time difference, the air position of non-group members can be identified. Once a false location report is found, the aircraft in the other group will be notified and appropriate action will be taken.

However, group certification requires the aircraft to be equipped with ADS-B IN to operate multilateration technology [37]. According to the ADS-B specification, ADS-B IN is an optional feature, so not all commercial aircraft have ADS-B IN functionality. Adding additional features will increase the operating cost of the system. In addition, ADS-B is a single communication, and it is more difficult to establish trust between aircraft.

4) DATA FUSION

Data fusion results in more accurate and reliable results than single-source data by fusing and correlating data from different sources. Data fusion can be done in different ways, such as probabilistic modeling and analysis, machine learning, and fuzzy logic [37]. No need to change the ADS-B message format and protocol for data fusion, and is compatible with legacy systems.

Baud *et al.* [60] do the data fusion between radar and ADS-B, and the results showed that the method could improve the actual tracking quality. Regarding ADS-B security, the authors recommend inter-checking ADS-B location data with data from the else isolated source. For example, multilateration, radar systems, and FPD (Flat Panel Display). Mixed estimation arithmetic combining multiple sensors different monitoring techniques (Primary Surveillance Radar, Secondary Surveillance Radar), and FPD is proposed by Liu *et al.* [61].

In fact, multiple integrated systems have been deployed to improve airport security, such as ASDE-X, which essentially uses data fusion technology to fuse multiple subsystem data (ADS-B, multilateration, aircraft technical data, Radar data, etc.).

Tang *et al.* [62] discusses the problem of the coordinate system between ADS-B data and radar data and proposes the use of uniform Cartesian coordinates. In addition to the coordinate system problem, data fusion requires data synchronization between different data sources, such as the location information of the ADS-B system and multilateration or GPS data synchronization.

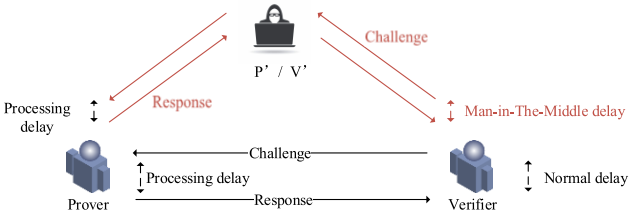

FIGURE 9. Principle of the distance bounding protocols.

5) DISTANCE BOUNDING

This type of secure location verification is an intra-area scheme. The principle that the transmission speed of the signal is the same as the speed of light is the core of this solution [63]. Figure 9 shows the principle. The proof node P passes the challenge message of the verification node V to prove that the node P is within the communication range of the challenge node. The upper limit of the distance between the nodes P and V is determined by proving the turnaround time of the challenge information and the response information between the node P and the verification node V and the signal processing time. The correctness of all nodes claiming location information can verify by the distance between P and V. In addition, triangulation and distance boundaries can determine the practical location of the node.

The survey by Tippenhauer *et al.* [64] studied the influence of the distance bounding on the mobile node, and the results show that the distance bounding is not a suitable choice for nodes moving at high speed. In a high-speed mobile node scenario, the distance bounding takes about 600ms to achieve full positioning. For the aircraft, it has moved hundreds of meters.

Similar to the concept of distance bounding, Kim *et al.* [45] proposed a method for signal transmission time. The basic principle is that when the signal propagates between the sender and the receiver, the propagation time is within a certain range. When there is a spoofed message, the propagation time will increase. With time, the propagation time will be It is longer than the normal signal propagation time, and the time is used as the standard to better identify spoofed messages, to resist spoofed ADS-B messages. This method uses a small timestamp value, which is called ADS-B (ADS-BT) with a timestamp. ADS-BT monitors the difference between the time of flight based on timestamp values and the time of flight based on position data. Experiments show that the scheme can detect deceptive signals to a large extent, with a high recognition rate and low cost, but it needs to modify the current ADS-B protocol.

6) TRAFFIC MODELING

In the case of providing a certain level of security and verify the aircraft's position in the ADS-B transmission network, historical air traffic control data, and data mining techniques can be used to model and use the model to identify false location information or other malicious activities. For example, the received signal strength is inversely proportional to the distance, and the authenticity of the position information can be discriminated by this simple relationship. It is also possible to combine the signal arrival angle with the received signal strength and determine the authenticity of the position information about the historical data.

Finke *et al.* [65] proposed a statistical model to verify the location information claimed by nodes in the car network. The model considers the difference between the location information and the estimated location information claimed by the node as a random variable over some time. Based on the central limit theorem, when the observed value reaches a certain number, the position difference value conforms to the normal distribution. Therefore, the statistical model can declare the location information of the node.

Zhang *et al.* [66] propose an online 4D-TP method, which consists of the preparation process, calculation process, and updating process. The updating process plays the most important role in the online 4D-TP method. The process including current trajectory updating and aircraft intent updating. The receiver on aircraft could receive the message and decompose and decode the message to determine the flight identification, position, and velocity of every aircraft.

B. SECURE BROADCAST AUTHENTICATION

In the related art, for example, wireless sensor networks and mobile ad hoc networks, broadcast authentication protocols play an important role in protecting data security. Secure broadcast authentication is a preventive/wireless network attacks possible method of detection. The security condition of secure broadcast authentication means that no attacker can forge the correct broadcast data packet. Authentication itself does not prevent malicious nodes from making erroneous data packets to interfere with the operation of the system. Only to ensure that authorized nodes must send the correct data packets. For more information on secure broadcast authentication, please refer to the survey by Perrig *et al.* [67].

Since there is no double-sided communication and trustworthy transmission between ADS-B network participants, compared with the peer-to-peer communications, ADS-B message network identity verification more difficult [37]. Given compatibility and international interoperability, the original designer designed the ADS-B network as an overt, unencrypted protocol. The goal of secure broadcast authentication is to provide an authentication mechanism for ADS-B based on the retention of ADS-B openness. According to different implementations, secure broadcast authentication can be further divided into an encryption method and a non-encryption method.

1) NON-ENCRYPTED SCHEMES

As mentioned earlier, the application is more difficult due to key distribution and management issues with encryption solutions and incompatibility with existing ADS-B infrastructure. The non-encryption method has no key distribution and management problems, mainly including fingerprinting technology and spread spectrum technology. Currently, there are only a few non-encryption schemes to improve the security of ADS-B. Zeng [68] presents three techniques to enhance or replace traditional encryption, software-based fingerprinting, hardware-based fingerprinting, and channel-based fingerprinting. In the survey by Danev *et al.* [69] can find more physical layer identification techniques for wireless devices. Li *et al.* [70] analyzed common attack models for highly concealed ADS-B data attacks. Based on the capabilities of existing ground stations and aircraft, they proposed a comprehensive detection scheme, including flight plan verification and single-node data detection. And group data detection to generate a comprehensive attack probability, and as a reference to judge the attack. The results show that the sequential collaborative detection strategy is effective in terms of effectiveness and accuracy, especially against random deviation injection attacks, constant deviation injection attacks, and DOS attacks.

a: SOFTWARE-BASED FINGERPRINTING

The software-based fingerprinting method distinguishes different devices by different modes or behaviors of software running on the wireless device. For a given network device,

different manufacturers' software development teams typically use a variety of different methods when implementing software. So, classification and identification of different network devices are done through these differences. However, most airlines today use very alike or identical hardware, making them difficult to distinguish even more difficult. On the one hand, they are more susceptible to attack by potential attackers, and on the other hand, they are more easily researched, and copied by potential attackers.

b: HARDWARE-BASED FINGERPRINTING

Hardware-based fingerprinting methods attempt to classify and identify different network devices through hardware differences. For example, radiofrequency fingerprinting, which uses the opening or closing of transient differences or modulation differences of radio signals as device signatures for classification [71]. However, this method is mainly used for non-mobile devices and is close to the transmitting antenna, which makes it difficult to apply in a highly dynamic, long-distance ADS-B network.

Clock skew is another way to distinguish between different hardware. Since there are no two fully synchronized clocks, you can use the time difference to construct distinct signatures for network devices and identities [37]. However, this method requires a timestamp to be added to the message. In addition, an attacker may eavesdrop on the communication information and simulate the jitter of the clock [72].

c: CHANNEL-BASED FINGERPRINTING

This type of fingerprinting identification method utilizes the natural features of the communication channel, such as received signal strength, channel impulse response, and carrier phase [37], and has been documented to replace traditional authentication and verification techniques [73]–[75]. They are relatively easy to implement in wireless systems and can provide reasonable security without much overhead. Mauro *et al.* [76] proposed using the carrier phase as a feature of aircraft classification to distinguish between real and false messages. Finally, the authors point out that combining the carrier phase with other characteristics of the message (carrier frequency stability, pulse shape, message time information, etc.) can be used for more complex classifications, thereby greatly improving the security of ADS-B [77].

d: SPREAD SPECTRUM TECHNOLOGY

Spread spectrum technology is mainly used in wireless communication to combat jamming and eavesdropping, including direct sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS). The transmitter and receiver need to pre-share the spreading code or frequency hopping mode during use. Therefore, similar to the encryption scheme, spread spectrum technology also has key management and distribution issues.

In order to eliminate the problem of pre-shared spreading codes/modes, Strasser *et al.* [78], Pöpper *et al.* [79], and Liu *et al.* [80] proposed the non-coordinated spread spectrum technique. Different from the pre-shared spreading code, in the uncoordinated spread spectrum, the sender and the receiver do not need to pre-share the spreading code, but randomly jump to different channels or randomly use the spreading code, so the attacker cannot be effective eavesdrop or jam the channel. The corresponding disadvantage is that bandwidth resources are wasted because most of the time the communication parties are not on the same channel. Although spread spectrum technology can effectively resist various attacks, its inherently low performance and time extension make it difficult to use in ADS-B systems.

2) ENCRYPTION SCHEMES

In wireless networks, encryption measures are a method of protecting communications that have been tested and put into use. Therefore, it needs to be considered in the ADS-B network. According to whether the encryption key and the decryption key are the same, the encryption method can be divided into symmetric encryption and asymmetric encryption.

a: PUBLIC KEY ENCRYPTION

The digital signature is the reverse application of public-key cryptography. Encrypt the message with the private key, and decrypt the message with the public key. Zhou *et al.* [81] proposed a lightweight IBV signature scheme. Improve the security of batch message authentication and have better resistance to replay attacks. The scheme has strong robustness to adaptive selection message attacks under the random oracle model, point addition computations instead of hash-to-point or pairing operations. Experimental results show that the scheme has a good computational cost and transmission overhead The advantages. However, this scheme is only in the theoretical experimental stage, and cannot be applied in practice.

Wesson *et al.* [82] researched the encryption scheme adopted to protect the security of ADS-B messages. They analyze the advantages and disadvantages of symmetric encryption, asymmetric encryption, digital signature, and corresponding key management in detail. Finally, it is concluded that asymmetric encryption is the only feasible encryption method, and the ECDSA (Elliptic Curve Digital Signature Algorithm) signature length is the smallest, so it is also the best solution. ECDSA signature is 448 bit in length. The author has given two broadcast methods. One is to divide the 560 bit into nine sequences, the first sequence is 112 bit, followed by eight 56 bit sequences, there are delays in both methods. In order to reduce the delay of data, the authors propose that the DME (distance measuring equipment) band can be used to broadcast ADS-B messages containing signatures.

Unlike symmetric encryption, public-key encryption does not require the communication partner to share the pre-key. Pan Weijun *et al.* [83] proposed a data authentication scheme based on elliptic curve cryptography (ECC) and X.509 certificate [44]. Figure 10 shows the certification scheme [84]. The scheme uses the ECSDA algorithm to generate signatures

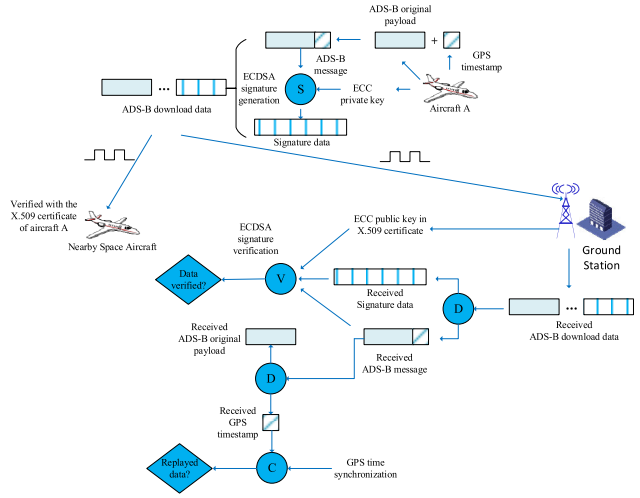

FIGURE 10. Encryption scheme ADS-B data authentication scheme.

for ADS-B data and timestamps, providing integrity and non-repudiation for ADS-B data. Since the signature length is too long, this scheme is only applicable to the UAT data chain rather than the 1090ES data link. The UAT can provide a longer message bit than the 1090ES, with a payload of 16 or 32 bytes when transmitted from the aircraft [85]. In addition, to separate and assemble the signature data, the scheme also requires 5 bit of additional information. Because public-key encryption is used, the communication parties don't need to share the key in advance. However, since it is necessary to ensure the validity and authenticity of the public key, PKI (Public Key Infrastructure) needs to be deployed to manage and store certificates. As the number of aircraft increases, the revocation, update, and storage of certificates will become very frequent, which is not only costly but also less scalable. In addition, the performance of asymmetric encryption is also poorer than symmetric encryption. The main challenge of public-key cryptography is to solve the scalability and cost of public key infrastructure (PKI) for digital signatures [86].

In order to solve the problem of symmetric encryption shared key and improve encryption efficiency, Baek *et al.* [87] proposed a phased hybrid encryption scheme based on identity in 2017. Figure 11 shows the block diagram of the scheme [87]. The scheme divides encryption into two phases, key encryption, and data encryption. Key encryption uses identity-based encryption, so there is no need to manage certificates. Data encryption uses symmetric encryption, which is faster and more efficient than public-key encryption. The first is the key-encryption phase. The sender uses the recipient's ID as the public key of the key-encryption phase. This public key is used to encrypt the private key to be used in the next stage (data encryption stage). Then, the private key encrypts the data, and the receiver first receives the key ciphertext. In order to obtain the private key of the encrypted data, the receiver needs to decrypt the private key of the key-encryption stage to obtain the data encryption key. The receiver can decrypt the received data ciphertext by decrypting the key. However, this solution requires the sender to store the recipient's ID in advance and needs to know the ground station or other aircraft around the aircraft in advance, and only one receiver at a time.

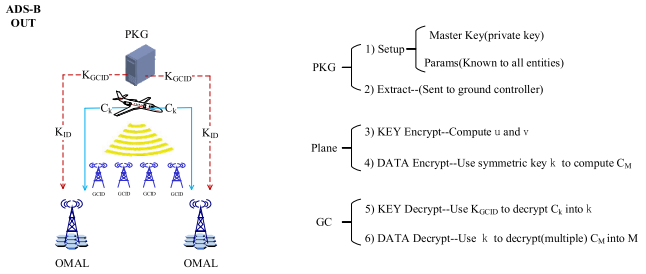

FIGURE 11. Identity-based phased encryption scheme.

To delete PKI in public-key encryption and increase the efficiency of public-key encryption signature, considering the limited computing power of ADS-B airborne equipment, BaeK [84] *et al.* proposed an offline/online signature method in 2013, which is based on the identity signature system does not require the participation of PKI. Since the identity-based cryptosystem mostly requires complex bilinear pairing operations. In order to improve the signature efficiency, the method operates to separate the signature method of varying complexity, and a lot of complex operations that are not related to the messages to be signed during the offline phase is completed [10]. Sign the message with a few low-complexity calculations.

The characteristics of the transmission link with reference to ADS-B data at a lower bandwidth, Yang *et al.* [85] proposed an identity authentication scheme that supports message recovery. Because the message can be recovered from the signature, it indirectly reduces the length of the message, saves communication costs during ADS-B information transmission [10].

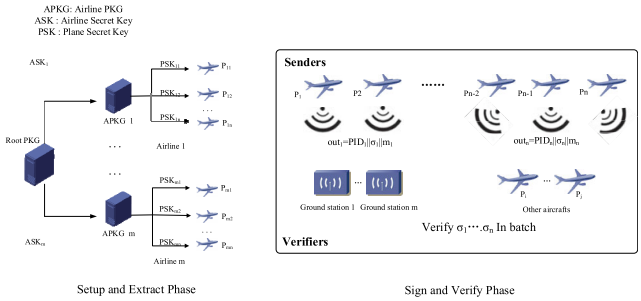

FIGURE 12. ADS-B authentication framework.

From the perspective of improving the efficiency of recipient authentication, Yang *et al.* [43] proposed a hierarchical authentication scheme that supports batch authentication. Figure 12 shows the certification scheme [44]. The program is divided into two sub-programs. Partial batch certification and full batch certification. Partial batch authentication supports multiple authentications of multiple signatures of the same signer at one time. Full batch authentication supports different signatures of multiple different signers at one time, improving authentication efficiency. However, this

method requires complicated "mapped to point" operation in the authentication phase [10]. As the number of signatures increases, the number of computations increases. In addition, in the solution to support full batch certification, this method also requires PKI (Public Key Infrastructure) to ensure the identity of the aircraft or airline, increased operating and maintenance costs of the system.

In order to overcome some of the shortcomings of Yang's scheme. He *et al.* [88] proposed an improved scheme to support batch authentication. Compared with Yang's scheme, He's scheme removes complicated "mapped to point" operations because there is no PKI participation, therefore, it does not require a management certificate. However, both of the communication schemes ADS-B data link cost is increased, the longer the signature generated [10]. To improve the computational efficiency of signatures, Thumbur *et al.* [89] recently proposed a batch authentication scheme to remove bilinear pairs, eliminating complex bilinear pairing operations, reducing the complexity of signatures and improving the efficiency of signature generation.

After analyzing various solutions, Robinson [90] proposed creating a PKI infrastructure for the aircraft assets distribution system (AADS). Figure 13 shows the structure [90]. Although the main focus of this work on the ground to distribute software and data, rather than the ADS-B protocol. The authors identified the requirements and necessities of the aviation industry from the proposed PKI infrastructure. The system can also be used to protect air traffic control data. At the same time, the author points out that since there is no centralized authority in the ad hoc network, the method of using pre-loaded trust certificates can be used as a short-term solution before developing a more structured long-term public key infrastructure.

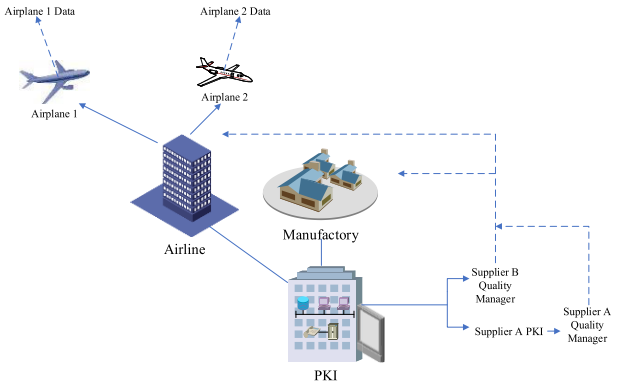

FIGURE 13. PKI structure diagram.

b: SYMMETRIC ENCRYPTION

Samuelson *et al.* [91] proposed using Message Authentication Code and encryption technology to protect the message content of ADS-B. In the authentication scheme, all participants send messages in cleartext. The message authentication code is appended to the normal ADS-B message to provide identity authentication for the participants. Regardless of whether the verification is passed, all participants can see all the data, thus retaining the openness of the ADS-B system. Figure 14 shows the certification scheme [91].

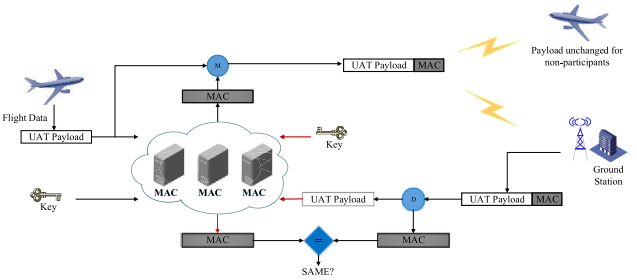

FIGURE 14. Scheme of the message authentication code.

Unlike the authentication scheme, encryption changes the original content of the message, and only the participants of the key can correctly interpret the received message. Since the ciphertext length of the public key encryption is long, the typical length is 1024 bit, and the UAT has only 272 bit of data bit, Samuelson *et al.* believe that encrypting the session key using the public key is an alternative. Figure 15 shows the encryption scheme [91]. After analyzing the feasibility of encrypting ADS-B messages. Jochum *et al.* [92] also proposed a similar encryption scheme, but both gave a rough encryption framework, and no specific encryption algorithm was given.

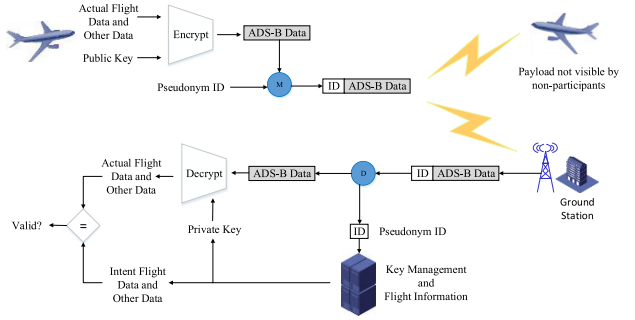

FIGURE 15. Encryption scheme.

Since ADS-B has limited data bit (UAT 272 bit, 1090ES 112 bit), and the ciphertext length of common encryption algorithms is long, in order to reduce the ciphertext length, Finke *et al.* [65] propose to use format-preserving encryption to encrypts ADS-B messages. Fixed-length messages that do not conform to the standard block size (64/128 bit) mainly use reserved format encryption algorithms and is often used to encrypt sensitive data such as credit card numbers and ID numbers in the database [93]. Unlike traditional packet encryption, the reserved format encryption does not extend the data. The ciphertext that retains the format encryption has the same format as the plaintext, thus minimizing the occupation of data bit by the ciphertext.

In order to preserve the openness of the ADS-B system, unlike Finke *et al.* [65] for ADS-B complete data encryption, Yang *et al.* [94] also use the reserved format encryption, but only the AA field of the ADS-B message is encrypted.

After receiving an ADS-B message, an unauthorized user will not be able to correctly decrypt the aircraft's identity information, thereby defending against aircraft reconnaissance attacks. Since the data segment is not encrypted, a certain degree of confidentiality is provided on the basis of ensuring the openness of the ADS-B protocol. Agbeyibor [95] evaluated the applicability of different kinds of reserved format encryption algorithms to ADS-B message encryption in terms of security and performance.

Finke *et al.* [65] assess the limitations of the traditional systems currently used for ATC and discusses the feasibility of using reserved format encryption (especially FFX (Format-preserving, Feistel-based encryption with multiple implementation variances) algorithm) in ADS-B environments, the input data is divided into two parts, and three rounds of FFX calculations are performed. Each round guarantees that part of the data comes from the results of the previous round and the F function is calculated on the rest data. Use message entropy as a metric to examine the algorithm's ability to obfuscate and distract predictable message inputs. Experiments show that a sub-class of the FFX-A2 algorithm is appropriate for ADS-B message encryption. After entropy encryption, the output shows that the method effectively masks the message content. Although the results show that this algorithm can be used to afford the security of the ADS-B message, the key management is still all symmetric encryption difficult to solve.

Yang *et al.* [85] came up with the new encryption solution to ADS-B security. Firstly, they utilized some cryptographic primitives, secondly applied it to air traffic monitoring scenarios. This method could guarantee the concealment and integrity of ADS-B messages. Compared with the previous solution, this solution is not only highly compatible with the existing ADS-B protocol, which due to the use of the FFX encryption and reserved ADS-B message, but also lightweight for congested data links and resource-constrained avionics. In addition, it can tolerate packet loss and confusion that often occur in ADS-B wireless broadcast networks, which is easy to deploy and practical. Experiments based on a large amount of real flight data demonstrate the performance of the scheme, which is extremely suitable for the deployment of actual aviation systems. However, this solution only targets two types of attacks, which are aircraft reconnaissance and aircraft ghost injection. This method only uses FFX to encrypt the unique aircraft identification number issued by ICAO, instead of the whole ADS-B message.

Samuelson *et al.* [96] proposed techniques to enhance the entire security of ADS-B, which includes a MAC (Message Authentication Code) algorithm and encryption methods for securing message content. They use the same encryption key and decryption key to complete this encryption method, which is a symmetric scheme. As a result of the format of ADS-B messages are limited, asymmetric encryption is required for session secret keys, otherwise, they would not use asymmetric cryptography with a single public/private key pair. Samuelson specializes in UAT (universal access transceiver) datalink messages broadcast on the 978 MHz channel. Jochum *et al.* [92] made similar recommendations after studying military applications ADS-B message encryption feasibility. However, none of them gave a specific algorithm.

Wesson *et al.* [82] discussed whether cryptography can secure the ADS-B, and studied the inevitable flaws in using a symmetric encryption algorithm in the ADS-B system. Therefore, the integrity protection of public-key encryption is highly recommended. They thought asymmetric-key elliptic curve digital signature method is the most practical and effective encryption method, and the ADS-B messages are broadcast over alternative authentication channels.

The symmetric encryption scheme chooses the encryption algorithm that does not change the existing ADS-B message protocol to encrypt the open ADS-B message and protect the data. The encryption key can be deduced from the decryption key, and vice versa. In most symmetric algorithms, the same key is used for encryption and decryption, the confidentiality of the data needs to be guaranteed by both parties. It has high encryption efficiency and is suitable for data with a large amount of encrypted data. However, comparing to asymmetric encryption, the encryption strength is not high. The security of the symmetric algorithm depends too much on the key, once the key is leaked, it means that anyone can encrypt/decrypt the message.

Since the reserved format encryption is symmetric encryption. The communication parties must share the key in advance, and it is difficult to deploy in consideration of the mobility of the communication parties [95], [97], [98]. In order to solve multiple system vulnerabilities in the ADS-B system, Thabet *et al.* [99] proposed a hybrid ADS-B security scheme using HMAC (Hash Message Authentication Code) and multilateration technology.

c: TESLA

The TESLA protocol is a variant of traditional asymmetric encryption and is mainly used for identity authentication protocols on broadcast networks [100], [101]. The important feature of the TESLA protocol is that it does not use an asymmetric key algorithm, but a symmetric key algorithm. This greatly reduces the computational difficulty of identity verification broadcasts and increases the speed of broadcast identity verification. The main idea of the protocol is that the MAC is generated by the broadcast node, and encrypt the message is appended to each. MAC key after a certain time or a certain number of messages for decrypting the sender will be released [37]. At this point, the recipient collecting the broadcast message can decrypt the message. Recently, Yang *et al.* [102] proposed the use of the TESLA protocol to ADS-B certification. Figure 16 shows the certification block diagram [102].

TESLA (Time Efficient Stream Loss-tolerate Authentication) broadcast authentication protocol, an efficient protocol with low communication and computational overhead, can be extended to a large number of receivers and tolerates packet

TABLE 6. Comparison of the feasibility of different ADS-B security solutions.

Category	Difficulty	Cost	Scalability	Compatibility
(Lightweight)PKI	High	High	Medium	Need to manage the key, change the agreement
Message Authentication Code	Low	Low	Medium	Need to manage the key, change the message format
TELSA	Medium	Medium	High	Need a new message format
Multilateration	Low	Medium	Medium	Need to add hardware, compatible with the current system
Fingerprinting Technology	Medium	High	Medium	Need to add hardware/software without changing the protocol
Spread Spectrum Technology	High	High	Medium	Need to add hardware, change the agreement
Distance Bounding	High	Medium	Low	Need to add a new agreement
Kalman Filtering	Low	Low	High	Need to add software
Data Fusion	Low	High	Medium	Need to add software
Traffic Modeling	Medium	Low	High	Need to add software and data processing modules

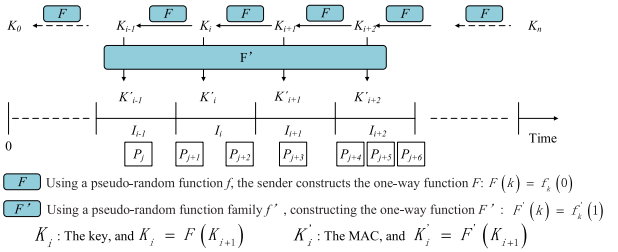

FIGURE 16. Implementation of adaptive-TESLA.

loss. TESLA is based on loose time synchronization between the sender and receiver.

TESLA can use truncated MAC, and verifying digital signatures is more complicated than calculating and generating MAC tags. TESLA has a small amount of calculation, and TESLA is more robust when data is lost. However, the key to TESLA lies in the delayed key release technology (the delay is δ), and the sender and receiver need to synchronize the clocks in advance. When the user's time estimation error $|\delta r| < \delta$, TESLA can ensure the reliability of data authentication. But when $|\delta r| > \delta$, TESLA cannot guarantee the reliability of data verification. Finally, TESLA is still evolving, and its stability needs to be further determined.

The current encryption schemes in the ADS-B security field mainly have the following disadvantages.

Violation of ADS-B openness: Symmetric encryption changes the original message content so that the unauthorized public cannot correctly interpret the received data.

Key management is difficult: Public key encryption requires a CA management certificate. As the number of aircraft increases, the revocation, update, and storage of certificates will become very frequent, which is not only costly but also less scalable.

Poor compatibility: Most of the current schemes need to change the message format, which is costly and difficult, and is not conducive to compatibility between systems.

V. ADS-B SECURITY SOLUTION ANALYSIS

This section in shortly summarizes the merit and demerit of different solutions from the aspects of security and feasibility. As mentioned above, there is no optimal solution when considering the impact on current ADS-B system software/hardware. In order to improve the security of the ADS-B system, most of the solutions need to change the infrastructure of the current ADS-B system. In addition, the current solution does not consider the existing problems of the ADS-B protocol, such as crowded 1090MHz transmission channel, the compatibility of existing hardware and software, which greatly reduces the feasibility of the solution.

Combined with the current status of the aviation industry traffic control system, Table 6 summarizes the feasibility of different methods in terms of difficulty, cost, and scalability. As can be seen from Table 6, the cost and difficulty of different schemes are relatively high. In terms of implementation, PKI and spread spectrum technology are the hardest. They are the most costly solutions, as both solutions require a major change to the infrastructure of current ADS-B systems [37]. For example, spread spectrum technology requires both hardware addition and protocol changes. On the contrary, MAC and Kalman filtering technology are the lowest cost and the easiest way to implement. Nevertheless, the MAC belongs to the symmetric encryption system and therefore requires a management key, which also makes the method harder to implement than the Kalman filtering method [37].

We can also choose a new protocol to solve the potential security problems of the ADS-B system, instead of the security solutions that have been widely used in other fields, but this also brings scalability problems, so this is ultimately a compromise choice. For example, the use of data fusion technology to fuse data from multiple subsystems (PSR, SSR ADS-C (Automatic dependent surveillance - contract), WAMLAT, etc.) is a distinct and required solution, however, ADS-B is proposed to reduce the traditional radar system, the dependence is the common sense of the aviation community. Therefore, in order to solve the potential security problems of ADS-B, choosing to maintain and retain most of the traditional ATC system will become the inversion.

Table 7 shows the attacks that the scheme discussed in this article can defend against. As can be seen from Table 7, most of the solutions can defend against message deletion/injection attacks. First, the openness of the ADS-B system is considered to be an important feature. Although eavesdropping is the basis for launching other attacks, only when there are major changes in current air traffic control and communication methods, eavesdropping needs to be resisted, otherwise, it is not necessary. Second, if there is no complete encryption

TABLE 7. Comparison of security of different ADS-B security solutions.

Category	Eavesdropping	Jamming	Message deletion/injection	DOS attack
(Lightweight)PKI	√	×	√	×
Message Authentication Code	×	×	√	×
TELSA	×	×	√	×
Multilateration	×	×	√	×
Fingerprinting Technology	×	×	√	√
Spread Spectrum Technology	√	√	×	√
Distance Bounding	×	×	√	×
Kalman Filtering	×	×	√	×
Data Fusion	×	×	√	√
Traffic Modeling	×	×	√	×

TABLE 8. Comparison of different ADS-B security solutions from the perspective of security requirements.

Category	Data Integrity	Location Integrity	Confidentiality	Authentication	Availability
(Lightweight)PKI	√	√	√	√	×
Message Authentication Code	×	×	×	√	×
TELSA	×	×	×	√	×
Multilateration	×	√	×	×	×
Fingerprinting Technology	×	×	×	√	√
Spread Spectrum Technology	×	×	√	×	√
Distance Bounding	×	√	×	×	×
Kalman Filtering	√	√	×	√	×
Data Fusion	×	√	×	√	√
Traffic Modeling	×	√	×	×	×

scheme, passive attacks such as eavesdropping are difficult to guard against. Although spread spectrum techniques and PKI are the hardest to implement and costly solutions, they are resistant to most attacks [37]. In contrast, the MAC and the Kalman filtering method are low-cost and relatively easy to implement, but can only resist an attack, so it is not enough to ensure ADS-B communication security [37].

In terms of security requirements, as shown in Table 8. PKI can ensure the integrity of data as well as the integrity of location, authentication, and confidentiality. However, the availability of ADS-B networks cannot be guaranteed [37]. Location, authentication, and practicality ensured by data fusion [37]. It cannot guarantee the data confidentiality and integrity of ADS-B messages, it is not an efficient solution. Other solutions, including multilateration, distance bounding, and message authentication codes, only meet one security requirement, so it is not suitable as an independent security solution [37].

Table 9 gives a comprehensive comparison of the various ADS-B security solutions. The solution to ensure ADS-B security is not only to improve the security of the system but also to consider the practical feasibility of the solution. Although lightweight PKI and spread spectrum technologies have significantly improved system security, due to the limitations of the current ADS-B protocol, which is hard to achieve. Nevertheless, at the current rate of technology development and the appearance of new technologies such as cognitive radio, it can be predicted that the current ADS-B protocol and bandwidth limitations will be well resolved in the future.

TABLE 9. Overall comparison of different ADS-B security solutions.

Category	Achieve	Security Level
(Lightweight)PKI	Difficult	High
Message Authentication Code	Easy	Low
TELSA	General	Medium
Multilateration	Easy	Low
Fingerprinting Technology	General	Medium
Spread Spectrum Technology	Very Difficult	High
Distance Bounding	Difficult	Low
Kalman Filtering	Easy	Medium
Data Fusion	Easy	Medium
Traffic Modeling	General	Low

Both data fusion and Kalman filtering can provide a certain degree of security and are easy to implement. At the same time, these two solutions have little changes to the current

ADS-B system and are compatible with the current system. As mentioned earlier, the Kalman filtering method is one of the easiest solutions for verifying position information. Though its overall security level is limited, this method has less impact on the current ADS-B system, this solution can be integrated into the current monitoring system to improve the security of the system. Data fusion requires additional data sources, which increases the operating cost of the system and runs counter to the original intention of the FAA NextGen plan to reduce costs [10]. Other schemes, for example, distance boundaries and TELSA, provide lower security and are harder to implement [37].

VI. FUTURE RESEARCH DIRECTION

Compared with other schemes, although PKI and spread spectrum techniques are more difficult, these two schemes can resist most attacks. Therefore, in order to improve the overall security of the system, it will become necessary to add confidentiality and spread spectrum technology to the future air traffic system. The ADS-B security solution should provide compatibility with future system development and be able to adapt to future iterations of the system. To this end, we make some suggestions and opinions for future work.

As mentioned earlier, current ADS-B security solutions fail to fully protect ADS-B communications and provide the only certain extent of security. A potential work in the future is to propose a multi-layered security framework that includes detection and defense against different ADS-B attacks.

With the increase of airplanes and other aircraft, the airspace will become more crowded. There are growing concerns about ADS-B and NextGen vulnerabilities security. Shortly, the more application of UAVs (Unmanned Aerial Vehicle), especially with the emergence of awareness and avoidance systems for UAVs, will also affect ADS-B systems. The security of the ADS-B system is the focus of future research.

A. CHALLENGES

ADS-B data is broadcasted in plain text during transmission, which lacks effective data security measures. This is also the inherent vulnerability of ADS-B technology. ADS-B data contains important flight status data and plays an important supporting role in situational awareness [103]. Therefore, ensuring security is the first priority of the ADS-B system. The various attack methods mentioned in this article need to be continuously improved. In addition, the following challenges exist in the future development of ADS-B.

1) 1090ES DATA LINK CHANNEL CONGESTION RISK

At present, most of the global ADS-B systems use the 1090ES data link mode for data transmission. The ADS-B transmission in this mode is implemented based on the mode S, which can be realized by simply upgrading and modifying the existing airborne equipment. However, the working frequency of the traditional secondary radar system is also in the 1090 frequency band. In the high-density area of the air route, it is easy to cause transmission channel blockage, signal interleaving, and mutual interference. As a result, the ADS-B ground station cannot accurately receive or process signals, and targets appear Lost conditions can even lead to serious aviation accidents.

2) GNSS POSITIONING ACCURACY RISK

The ADS-B systems receive data from the GNSS (Global Navigation Satellite System), then processes the data, and broadcasts its status information. Therefore, the integrity of GNSS is a prerequisite to ensure accurate aircraft position information. However, since the ADS-B system itself does not have the function of message verification, it is impossible to verify the data from the GNSS. Therefore, if the positioning of the GNSS is inaccurate, it will cause the information broadcast by the ADS-B system to be wrong. It will cause the ground station to receive inaccurate or incorrect aircraft position messages, which will cause controllers to make incorrect commands, causing a series of follow-up problems.

3) POTENTIAL ADS-B TARGET FRAUD RISK

The ADS-B data broadcasts information in an unencrypted manner, and through low-cost equipment, it can complete the reception and eavesdropping of ADS-B data, obtain aircraft location information, identification information, and so on. Illegal users can also counterfeit ADS-B information, conduct electronic deception, or record the collected information and then transmit it to interfere with the normal reception of ground stations and aircraft.

B. RECOMMENDATIONS

The ADS-B comprehensive security framework is an inevitable result of future development. However, for the current issues, it is always better to adopt backward compatibility rather than completely updating the device. The use of safe location authentication methods, such as multilateration technology, can make up for the problem of safe distance in the near future. In multiple parts, such as signal receiving authentication, broadcasting, the use of fingerprint technology can ensure the security of data and build an intrusion prevention system. It is also possible to improve the performance of the controller by improving the current data fusion algorithm and thus improve system security.

In the future of aviation, there will be more and more aircraft in the airspace, which will cause congestion in the airspace, and the number of ADS-B messages will also increase. How to quickly and accurately receive and process ADS-B messages and expand the transmission range of ADS-B messages on the 1090 frequency band to avoid channel congestion and message loss is the focus of further research.

Blockchain is an integrated system of multiple technologies such as peer-to-peer networks, cryptography, consensus mechanism, smart contract, etc. It can provide a trusted channel for information exchange and exchange in untrusted networks. For its unique public trust mechanism, it can be

applied to the ADS-B system, combined with the group certification method to achieve the authentication and protection of ADS-B messages. And this also will be the main direction of our future research. Su *et al.* proposed an identity recognition technology based on blockchain, which uses the peer-to-peer (P2P) technology to distribute and store data in each node to achieve distributed authentication. The program has the characteristics of high scalability, high reliability, and high security, and supports unified identity authentication on different platforms [104]. Related article ''Aviation Blockchain Infrastructure'' (ABI) is designed to enable aircraft to communicate effectively, safely, and privately with air traffic management and other properly authorized entities. Reisman *et al.* [105] proposed the use of blockchain technology for ADS-B security verification. These articles or reports illustrate the feasibility of applying blockchain technology to the ADS-B system, and provide direction and help for our future research.

In various research and application areas, abnormal data detection is a very important issue. For an open, non-encrypted system like ADS-B, abnormal data detection is even more important. In recent years, various anomaly detection methods based on machine learning have been proposed in various fields. It is worth noting that the anomaly detection methods based on deep learning are becoming more and more popular and applied to various tasks. We feel that in the future ADS-B system attack detection process, deep learning anomaly detection methods can be added. According to the characteristics of fast ADS-B message update and strong time correlation, the deep learning model is used to detect abnormal ADS -B time series, improve the detection effect by increasing the feature dimension of the series. This method does not need to change the existing ADS-B protocol, nor does it need to add new sensors. There are already many articles on the use of deep learning methods to detect ADS-B abnormal information. Habler *et al.* [106], Akerman *et al.*, [107] and Chen *et al.* [108] in their survey have been proposed the methods by deep learning or LSTM to solve the security of ADS-B system. They build models, train data, and detect abnormal data, which will provide good help and basic support for our future research. Li *et al.* [109] proposed a detection scheme against message injection. Based on the hidden Markov model with a viscous hierarchical Dirichlet process, a dynamic time detection method is proposed to detect multiple attack modes.

Moreover, the traditional land-based ADS-B system mainly sends requests from the aircraft to the satellite to obtain information data, and then sends information to surrounding aircraft and ground receivers through its transmitter. However, this plan is difficult to complete in the ocean, mountainous areas with complicated terrain and harsh desert areas, mainly because the establishment of ground stations faces huge challenges. Faced with the limitations of the layout of ground stations, current aircraft can only fly along civil aviation routes, airport terminal areas, and other land areas. The satellite-based ADS-B system can serve the shortcomings of the land-based system and can be used in airspace that is not or difficult to be covered by the land-based system, thereby forming a global ADS-B airspace monitoring network with no dead ends. The satellite-based ADS-B system receives the ADS-B information sent by the aircraft and sends the information to the ground station through the satellite communication channel to achieve monitoring. Therefore, in the future, not only the operation of the land-based ADS-B system should be implemented, but the research of the satellite-based system should also be strengthened. The satellite-based system is the future development trend, which will provide better surveillance and the system security will also be improved (because of the signal source from satellite communications, it is more difficult to be attacked than aircraft sent to the ground), and it will also facilitate other aviation systems.

Finally, the popularity of ADS-B systems is also very important. Compared with traditional radar surveillance systems, ADS-B has obvious advantages. Countries should accelerate the application of ADS-B systems. After that, the research focus should be on satellite-based ADS-B systems to achieve global coverage of ADS-B networks.

VII. CONCLUSION

This paper analyzes the system vulnerability of ADS-B, gives various possible attacks on ADS-B, and classifies the attacks according to the attack intention and security requirements. In addition, we focus on the latest ADS-B security solutions and analyze different solutions in terms of security and feasibility. We find that relying on a single detection/defense solution does not fully protect ADS-B communication security. Therefore, it is necessary to propose a multi-layered security framework that includes detection and defense against different ADS-B attacks. With the development and maturity of technology, it is necessary to use deep learning methods to analyze vulnerabilities, combined with blockchain technology to solve problems.

REFERENCES

[1] *Securing Smart Airports*, Eur. Union Agency Netw. Inf. Secur., Heraklion, Greece, Dec. 2016.
[2] A. Coyne. (2016). *How Airbus Defends Against 12 Big Cyber-Attacks Each Year*. [Online]. Available: http://www.itnews.com.au/news/how-airbus-defends-against-12-big-cyber-attacks-each-year-418131
[3] *Forecast, FAA Aerospace, Fiscal Years 2013–2033*, Federal Aviation Admin., Washington, DC, USA, 2013.
[4] R. De Cerchio and C. Riley, ''Aircraft systems cyber security,'' in *Proc. IEEE/AIAA 30th Digit. Avionics Syst. Conf.*, Oct. 2011, pp. 1–7.
[5] A. Wood. (2016). *Newark Airport GBAS Vulnerable to Truckers' GPS Jammers*. [Online]. Available: http://www.ainonline.com/aviation-news/ainalerts/2011-01-25/newark-airport-gbasvulnerable-truckers-gps-jammers
[6] International Civil Aviation Organization. (2012). *In Twelfth Air Navigation Conference Montréal*. [Online]. Available: http://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP122.1.1.ENonly.pdf
[7] A. Williams. (2014). *Jets Vanishing From Europe Radar Linked to War Games.-Reuters*. [Online]. Available: http://www.reuters.com/article/us-europe-airplanes-safety-idUSKBN0EO1CW20140613
[8] A. Sternstein. (2015). *Exclusive: FAA Computer Systems Hit by Cyberattack Earlier this Year*. [Online]. Available: https://www.nextgov.com/cybersecurity/2015/04/faa-computer-systems-hit-cyberattack-earlier-year/109384/

[9] J. Valero. (2016). *Hackers Bombard Aviation Sector With Over 1,000 Attacks Per Month*. [Online]. Available: https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/
[10] Z. Wu, A. Guo, M. Yue, and L. Liu, "An ADS-B message authentication method based on certificateless short signature," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 3, pp. 1742–1753, Jun. 2020.
[11] E. Atienza, R. Falah, S. García, L. Gutiérrez, M. Á. L. Martínez, and Ó. Robles, "ADS-B: An air navigation revolution," Rey Juan Carlos Univ.-Fuenlabrada Campus, Madrid, Spain, Tech. Rep., 2013.
[12] *NASA—NextGen*. Accessed: 2017. [Online]. Available: http://www.hq.nasa.gov/office/aero/asp/airspace/index.htm
[13] *The Roadmap for Delivering High Performing Aviation for Europe. European ATM Master Plan Executive View Edition*, SESAR Joint Undertaking (EU Body or Agency), Feb. 2016.
[14] *Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B). DO-242A (Including Change 1)*, RTCA Inc., Washington, DC, USA, Dec. 2006.
[15] *Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance—Broadcast (ADS-B) and Traffc Information Services—Broadcast (TIS-B). DO-260B With Corrigendum 1*, RTCA Inc., Washington, DC, USA, Dec. 2011.
[16] *Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance—Broadcast. DO-282B With Corrigendum 1*, RTCA Inc., Washington, DC, USA, Dec. 2011.
[17] P. J. Martone and G. E. Tucker, "Candidate requirements for multilateration and ADS-B systems to serve as alternatives to secondary radar," in *Proc. 20th IEEE/AIAA Digit. Avionics Syst. Conf. (DASC)*, Oct. 2001, pp. 1–12.
[18] C. Rekkas and M. Rees, "Towards ADS-B implementation in Europe," in *Proc. Tyrrhenian Int. Workshop Digit. Commun.-Enhanced Surveill. Aircr. Vehicles*, Sep. 2008, pp. 1–4.
[19] P. Marks. (2011). *Air Traffc System Vulnerable to Cyber Attack*. [Online]. Available: http://www.newscientist.com/article/mg21128295.600-air-traffc-system vulnerable-to-cyber-attack.html
[20] H. Kelly. (2012). *Researcher: New Air Traffic Control System is Hackable*. [Online]. Available: http://edition.cnn.com/2012/07/26/tech/web/air-traffic-control-security/index.html
[21] A. Greenberg. (2012). *Next-Gen Air Traffic Control Vulnerable to Hackers Spoofing Planes Out of Thin Air*. [Online]. Available: http://www.forbes.com/sites/andygreenberg/2012/07/25/next-gen-air-traffic-control-vulnerable-to-hackers-spoofing- planes-out-of-thin-air/
[22] K. Zetter. (2012). *Air Traffic Controllers Pick the Wrong Week to Quit Using Radar*. [Online]. Available: http://www.wired.com/threatlevel/2012/07/adsb-spoofing/
[23] S. Henn. (2012). *Could the New Air Traffic Control System be Hacked?* [Online]. Available: http://www.npr.org/blogs/alltechconsidered/2012/08/16/158758161/could-the-new-air-traffic-control-system-be-hacked
[24] A. Costin and A. Francillon, "Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," Black Hat USA, Las Vegas, NV, USA, Tech. Rep., Jul. 2012, pp. 1–12.
[25] B. Haines, "Hacker + airplanes = no good can come of this," Confidence X, Tech. Rep., 2012.
[26] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *Applied Cryptography and Network Security*. Banff, AB, Canada: Feb. 2013, pp. 253–271.
[27] K. Gopalakrishnan, M. Govindarasu, D. W. Jacobson, and B. M. Phares, "Cyber security for airports," *Int. J. Traffic Transp. Eng.*, vol. 3, no. 4, pp. 365–376, 2013.
[28] Australian Government. (2015). *Loss of Separation Between Airbus A330 VH-EBO and Airbus A330 VH EBS*. [Online]. Available: https://www.atsb.gov.au/media/5214362/AO-2013-161%20final.pdf
[29] A. Hansen. Book review for tracon by Paul McElroy. American Aviation Historical Society, Celebrating Over 60 Years of Service. Accessed: 2019. [Online]. Available: http://www.aahs-online.org/bk_review.php?ibook=45
[30] *ADS-B Benefits are Limited Due to a Lack of Advanced Capabilities and Delays in User Equipage*, Office Inspector Gen., U.S. Dept. Transp., Washington, DC, USA, Sep. 2014.
[31] *Securing Smart Airports*, Eur. Union Agency Netw., Inf. Secur., Heraklion, Greece, Dec. 2016.
[32] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, 4th Quart., 2013.
[33] *Flightradar24 Flight Tracker*. Accessed: 2019. [Online]. Available: https://www.flightradar24.com/
[34] HoID. *How to Track ADS-B Equipped Aircraft on Your Smartphone*. Accessed: 2019. [Online]. Available: https://null-byte.wonderhowto.com/how-to/track-ADS-B-equipped-aircraft-your-smartphone-0179666/
[35] *Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed*, GAO, Washington, DC, USA, 2002.
[36] The Economist. (2011). *No Jam Tomorrow-GPS Jamming*. [Online]. Available: https://www.economist.com/technology-quarterly/2011/03/12/no-jam-tomorrow
[37] M. R. Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system," *Int. J. Crit. Infrastruct. Protection*, vol. 19, pp. 16–31, Dec. 2017.
[38] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel," in *Proc. 16th ESORICS*, 2011, pp. 40–59.
[39] M. Wilhelm, J. B. Schmitt, and V. Lenders, "Practical message manipulation attacks in IEEE 802.15.4 wireless networks," in *Proc. MMB DFT Workshop*, 2012, pp. 1–3.
[40] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" in *Proc. 4th ACM Conf. Wireless Netw. Secur. (WiSec)*, 2011, pp. 47–52.
[41] D. Adamy, *EW 101: A First Course in Electronic Warfare*. Norwood, MA, USA: Artech House, 2001.
[42] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *Int. J. Crit. Infrastruct. Protection*, vol. 4, no. 2, pp. 78–87, Aug. 2011.
[43] A. Yang, X. Tan, J. Baek, and D. S. Wong, "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification," *IEEE Trans. Services Comput.*, vol. 10, no. 2, pp. 165–175, Mar./Apr. 2017.
[44] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1066–1087, 2nd Quart., 2015.
[45] Y. Kim, J.-Y. Jo, and S. Lee, "ADS-B vulnerabilities and a security solution with a timestamp," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 11, pp. 52–61, Nov. 2017.
[46] N. Xu, R. Cassell, C. Evers, S. Hauswald, and W. Langhans, "Performance assessment of multilateration Systems–a solution to nextgen surveillance," in *Proc. Integr. Commun., Navigat., Surveill. Conf.*, Herndon, VA, USA, May 2010, pp. D2-1–D2-8.
[47] R. Kaune, C. Steffes, S. Rau, W. Konle, and J. Pagel, "Wide area multilateration using ADS-B transponder signals," in *Proc. 15th Int. Conf. Inf. Fusion*, 2012, pp. 727–734.
[48] A. Smith, R. Cassell, T. Breen, R. Hulstrom, and C. Evers, "Methods to provide system-wide ADS-B back-up, validation and security," in *Proc. 25th Digit. Avionics Syst. Conf.*, 2006, pp. 1–7.
[49] J. Johnson, H. Neufeldt, and J. Beyer, "Wide area multilateration and ADS-B proves resilient in Afghanistan," in *Proc. ICNS*, 2012, pp. A6-1–A6-8.
[50] A. Daskalakis and P. Martone, "A technical assessment of ADS-B and multilateration technology in the gulf of mexico," in *Proc. IEEE Radar Conf.*, May 2003, pp. 370–378.
[51] F. A. Niles, R. S. Conker, M. B. El-Arini, D. G. O'Laughlin, and D. V. Baraban, "Wide area multilateration for alternate position, navigation, timing (APNT)," MITRE-CAASD, McLean, VA, USA, Tech. Rep., 2012.
[52] J. C. Siu, "ICAO concepts and literatures regarding ADS-B, multilateration and other surveillance techniques," in *Proc. ICAO/FAA Workshop ADS-B Multilateration Implement.*, Sep. 2011, pp. 1–7.
[53] L. Schuchman, "Automatic dependent surveillance system secure ADS-S," U.S. Patent 7 876 259, Jan. 25, 2011.
[54] R. E. Kalman, "A new approach to linear filtering and prediction problems," *J. Basic Eng.*, vol. 82, no. 1, pp. 35–45, 1960.
[55] D. Fox, J. Hightower, L. Liao, D. Schulz, and G. Borriello, "Bayesian filtering for location estimation," *IEEE Pervasive Comput.*, vol. 2, no. 3, pp. 24–33, Jul./Sep. 2003.
[56] J. Krozel, D. Andrisani, M. Ayoubi, T. Hoshizaki, and C. Schwalm, "Aircraft ADS-B data integrity check," in *Proc. AIAA 4th Aviation Technol., Integr. Oper. (ATIO) Forum*, Sep. 2004, pp. 1–11.
[57] B. Kovell, B. Mellish, T. Newman, and O. Kajopaiye, "Comparative analysis of ADS-B verification techniques," M.S. thesis, Univ. Colorado, Boulder, BO, USA, 2012.

[58] E. Chan-Tin, V. Heorhiadi, N. Hopper, and Y. Kim, "The frog-boiling attack: Limitations of secure network coordinate systems," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 3, pp. 1–23, Nov. 2011.
[59] K. Sampigethaya and R. Poovendran, "Security and privacy of future aircraft wireless communications with offboard systems," in *Proc. 3rd Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2011, pp. 1–6.
[60] O. Baud, N. Honore, and O. Taupin, "Radar/ADS-B data fusion architecture for experimentation purpose," in *Proc. 9th Int. Conf. Inf. Fusion*, Jul. 2006, pp. 1–6.
[61] W. Liu, J. Wei, M. Liang, Y. Cao, and I. Hwang, "Multi-sensor fusion and fault detection using hybrid estimation for air traffic surveillance," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2323–2339, Oct. 2014.
[62] T. Yong, W. Honggang, X. Zhili, and H. Zhongtao, "ADS-B and SSR data fusion and application," in *Proc. IEEE Int. Conf. Comput. Sci. Automat. Eng. (CSAE)*, vol. 2, May 2012, pp. 255–258.
[63] S. Brands and D. Chaum, "Distance-bounding protocols," in *Proc. Theory Appl. Cryptograph. Techn.*, 1994, pp. 344–359.
[64] N. O. Tippenhauer and S. Čapkun, "ID-based secure distance bounding and localization," in *Proc. Comput. Secur.—ESORICS*, 2009, pp. 621–636.
[65] C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system," *Int. J. Crit. Infrastruct. Protection*, vol. 6, no. 1, pp. 3–11, Mar. 2013.
[66] J. Zhang, J. Liu, R. Hu, and H. Zhu, "Online four dimensional trajectory prediction method based on aircraft intent updating," *Aerosp. Sci. Technol.*, vol. 77, pp. 774–787, Jun. 2018.
[67] A. Perrig and D. Tygar, *Secure Broadcast Communication in Wired and Wireless Networks*. New York, NY, USA: Springer, 2003.
[68] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.
[69] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv.*, vol. 45, no. 1, pp. 1–29, Nov. 2012.
[70] T. Li and B. Wang, "Sequential collaborative detection strategy on ADS-B data attack," *Int. J. Crit. Infrastruct. Protection*, vol. 24, pp. 78–99, Mar. 2019.
[71] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *Proc. Commun., Int., Inf. Technol.*, 2004, pp. 201–206.
[72] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Trans. Mobile Comput.*, vol. 9, no. 3, pp. 449–462, Mar. 2010.
[73] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2008, pp. 128–139.
[74] J. Zhang, S. K. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–5.
[75] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1422–1430.
[76] M. Leonardi, G. Di Gregorio, and F. Di Fausto, "Air traffic security: Aircraft classification using ADS-B message's phase-pattern," *Aerospace*, vol. 4, no. 4, p. 54, 2017.
[77] M. Leonardi and D. Di Fausto, "ADS-B signal signature extraction for intrusion detection in the air traffic surveillance system," in *Proc. 26th Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2018, pp. 2564–2568.
[78] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2008, pp. 64–78.
[79] C. Pöpper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," in *Proc. USENIX Secur. Symp.*, 2009, pp. 231–247.
[80] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.
[81] J. Zhou and J. Yan, "Secure and efficient identity-based batch verification signature scheme for ADS-B system," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 12, pp. 6243–6259, 2019, doi: 10.3837/tiis.2019.12.024.
[82] K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Can cryptography secure next generation air traffic surveillance?" Radionavigation Secur. Res. UT Austin, Univ. Texas Austin, Austin, TX, USA, Tech. Rep. Mar. 2014.
[83] Z. Feng, W. Pan, and Y. Wang, "A data authentication solution of ADS-B system based on X. 509 certificate," in *Proc. 27th Int. Congr. Aeronaut. Sci. (ICAS)*, 2010, pp. 1–6.
[84] J. Baek, Y.-J. Byon, E. Hableel, and M. Al-Qutayri, "An authentication framework for automatic dependent surveillance-broadcast based on online/offline identity-based signature," in *Proc. 8th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, Oct. 2013, pp. 358–363.
[85] H. Yang, R. Huang, X. Wang, J. Deng, and R. Chen, "EBAA: An efficient broadcast authentication scheme for ADS-B communication based on IBS-MR," *Chin. J. Aeronaut.*, vol. 27 no. 3, pp. 686–688, 2014.
[86] R. V. Robinson, K. Sampigetha, M. Li, S. Lintelman, and R. Poovendran, "Secure network-enabled commercial airplane operations: It support infrastructure challenges," in *Proc. 1st CEAS Eur. Air Space Conf. Century Perspect.*, 2007, pp. 1–6.
[87] J. Baek, E. Hableel, Y.-J. Byon, D. S. Wong, K. Jang, and H. Yeo, "How to protect ADS-B: Confidentiality framework and efficient realization based on staged identity-based encryption," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 690–700, Mar. 2017.
[88] D. He, N. Kumar, K.-K.-R. Choo, and W. Wu, "Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 2, pp. 454–464, Feb. 2017.
[89] G. Thumbur, N. B. Gayathri, P. V. Reddy, M. Z. U. Rahman, and A. Lay-Ekuakille, "Efficient pairing-free identity-based ADS-B authentication scheme with batch verification," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 5, pp. 2473–2486, Oct. 2019.
[90] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, and J.-U. Buber, "Impact of public key enabled applications on the operation and maintenance of commercial airplanes," in *Proc. AIAA ATIO Conf.*, 2007, pp. 1–10.
[91] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ADS-B research," in *Proc. IEEE Aerosp. Conf.*, Big Sky, MT, USA, Oct. 2006, p. 7.
[92] J. Jochum, "Encrypted mode select ADS-B for tactical military situational awareness," M.S. thesis, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2001.
[93] M. Bellare, P. Rogaway, and T. Spies. (2010). *The FFX Mode of Operation for Format-Preserving Encryption, Draft 1.1*. [Online]. Available: https://www.src.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec.pdf
[94] H. Yang, M. Yao, Z. Xu, and B. Liu, "LHCSAS: A lightweight and highly-compatible solution for ADS-B security," in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–7.
[95] R. C. Agbeyibor, "Secure ADS-B: Towards airborne communications security in the federal aviation administration's next generation air transportation system," Air Force Inst. Technol. Wright-Patterson Afb Oh Graduate School Eng. Manage., Wright-Patterson AFB, OH, USA, Tech. Rep. AFIT-ENG-14-M-02, 2014.
[96] E. Valovage, "Enhanced ADS-B research," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 22, no. 5, pp. 35–38, May 2007.
[97] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, "Future E-enabled aircraft communications and security: The next 20 years and beyond," *Proc. IEEE*, vol. 99, no. 11, pp. 2040–2055, Dec. 2011.
[98] K. Sampigethaya, R. Poovendran, and L. Bushnell, "A framework for securing future eEnabled aircraft navigation and surveillance," in *Proc. AIAA Infotech@Aerosp. Conf.*, Apr. 2009, pp. 1–10.
[99] T. Kacem, D. Wijesekera, and P. Costa, "ADS-bsec: A holistic framework to secure ADS-B," *IEEE Trans. Intell. Vehicles*, vol. 3, no. 4, pp. 511–521, Dec. 2018.
[100] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. IEEE Symp. SP*, May 2000, pp. 56–73.
[101] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *Rsa Cryptobytes*, vol. 5, no. 2, pp. 2–13, 2002.
[102] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, "A practical and compatible cryptographic solution to ADS-B security," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3322–3334, Apr. 2019.
[103] T. Li, B. Wang, F. Shang, J. Tian, and K. Cao, "Online sequential attack detection for ADS-B data based on hierarchical temporal memory," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101599.
[104] X. Su, X. Zou, and D. Yong, "An identity identification technology based on blockchain," *ZTE Technol.*, vol. 24, no. 6, pp. 45–52, 2018.

[105] R. Reisman, "Blockchain serverless public/private key infrastructure for ADS-B security, authentication, and privacy," in *Proc. AIAA Scitech Forum*, Jan. 2019, p. 2203.
[106] E. Habler and A. Shabtai, "Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages," *Comput. Secur.*, vol. 78, pp. 155–173, Sep. 2018.
[107] S. Akerman, E. Habler, and A. Shabtai, "VizADS-B: Analyzing sequences of ADS-B images using explainable convolutional LSTM encoder-decoder to detect cyber attacks," 2019, *arXiv:1906.07921*. [Online]. Available: https://arxiv.org/abs/1906.07921
[108] S. Chen, S. Zheng, L. Yang, and X. Yang, "Deep learning for large-scale real-world ACARS and ADS-B radio signal classification," *IEEE Access*, vol. 7, pp. 89256–89264, 2019.
[109] T. Li, B. Wang, F. Shang, J. Tian, and K. Cao, "Dynamic temporal ADS-B data attack detection based on sHDP-HMM," *Comput. Secur.*, vol. 93, Jun. 2020, Art. no. 101789.

ZHIJUN WU received the B.S. and M.S. degrees in information processing from Xidian University, China, and the Ph.D. degree in cryptography from the Beijing University of Posts & Telecommunications, China. He was a Professor with the Department of Communication Engineering, Civil Aviation University of China. His research interests include denial-of-service attacks and security in big data and cloud computing.

TONG SHANG received the B.S. degree in electronic information engineering from the Information Security, Civil Aviation University of China, Tianjin, China, where he is currently pursuing the M.S. degree in electronic information engineering.

His main research interests include cryptography and ADS-B system security.

ANXIN GUO received the B.S. degree in electronic information engineering from the Zhengzhou University of Light Industry, Zhengzhou, China, and the M.S. degree in information security from the Civil Aviation University of China, Tianjin, China.

His research interest includes information security.