EasyChair Preprint

№ 851

Security of ADS-B: Attack Scenarios

Kayvan Faghih Mirzaei, Bruno Pessanha de Carvalho and
Patrick Pschorn

March 23, 2019

Security of ADS-B: Attack Scenarios

Kayvan Faghih Mirzaei Bruno Pessanha de Carvalho Patrick Pschorn

***Abstract*—Automatic Dependent Surveillance-Broadcast (ADS-B) is the successor surveillance technology which is used in aviation, and according to Federal Aviation Administration (FAA) and European Aviation Safety Agency (EASA), the vast majority of aircraft must be equipped with it by January and June 2020, respectively. However, ADS-B, as it is utilized today, is not free from problems. This paper discusses observed attacks and corresponding methods that can be realized over ADS-B surveillance technology and consequently, compromise its availability, integrity or confidentiality. Nonetheless, as an opening, the paper studies essential characteristics of ADS-B, functionality, deployment status and other relevant facts and figures for a better understanding of the basics, current state, and pitfalls of the state-of-the-art technology for air traffic surveillance and control. We afterward proceed to study complexity, severity, and effect of the attacks by providing some examples. Ultimately, we complement the previous sections by presenting an outline of the proposed solutions and mitigation techniques and survey the most distinguished ones.**

***Index Terms*—ADS-B, air traffic control, air traffic surveillance, attack scenarios, attacks, aviation, mitigation techniques, security, vulnerabilities**

I. Introduction

The methods that are currently being used in aviation for air traffic surveillance and control can be categorized as cooperative and non-cooperative methods [1]. In the non-cooperative method, aircraft has no particular communication facility or has no intention to communicate with the ground stations or other surveillance systems on-board of the aircraft. Radar-based surveillance systems which are considered as the predecessor technology to ADS-B, can be categorized as primary and secondary surveillance radar systems (*PSR* and *SSR*) [1]. Although these radar systems due to their particular characteristics are still being used, the technology that is utilized in them is nevertheless very old. Therefore, these systems are not appropriate for surveillance of the ever-increasing airspace traffic of the world today. ADS-B, which is considered a cooperating surveillance technology, enables pilots in addition to the ground-based traffic controllers to perform aircraft surveillance with higher accuracy while lowering the costs of maintenance and installation that exist in the former surveillance systems [2]. Moreover, it is considered a viable solution in areas where implementations of ground-based Air Traffic Control (ATC) facilities would appear unpractical, uneconomical or even impossible (e.g., non-industrialized areas, oceanic airspace) [3].

While ADS-B OUT considered as an airspace requirement and already being used in many parts of the world (such as Australia, Canada, and China [4]), according to FAA and EASA mandates, all aircraft flying in designated controlled airspace must be equipped with compliant ADS-B Out avionics by January and June 2020, respectively [5], [6]. The only exception (U.S. airspace) is for the aircraft that fly in uncontrolled airspace and aircraft without electrical systems such as gliders and balloons. Estimates show that the number of airplanes equipped with the ADS-B Out transponders is continuously increasing and the equipped aircraft fleet for commercial jet airliners are by far the most equipped group [7].

The goal of this paper is to study various attacks and examine the scenarios in order to discover the threats and vulnerabilities of ADS-B surveillance technology. To this end, understanding the basics of ADS-B technology would be necessary. Accordingly, the paper first in section II practices studying the characteristics of this technology and other relevant technologies. Afterward, in section III security status and concerns will be reflected. Section IV surveys the attack scenarios by classifying them into passive and active attacks. In section V the paper goes through the complexity, severity, and effect of the attacks by analyzing them. In chapter VI, the most distinguished solutions will be studied. Finally, chapter VII concludes the paper.

II. ADS-B Basics

As described by [8], the operation of ADS-B is categorized into two different parts: *ADS-B OUT* and *ADS-B IN*. ADS-B OUT continuously broadcasts ADS-B dataset which consists of velocity, position, altitude, "IDENT" and other important information. On the other hand, ADS-B IN, which is the receiver part of the system, enables the pilot to receive traffic information (1090 MHz) and UAT broadcasts (978 MHz only), which consists of aircraft traffic information along with other information such as weather and aeronautical data on the cockpit [9].

According to [8], the following characteristics distinguish ADS-B as a surveillance technology:

- ***A**utomatic*: transmission of data (i.e., location and velocity) is done automatically, every second, without any interrogation.
- ***D**ependent*: ADS-B depends on the data from a compliant navigation system and signal transmitter.
- ***S**urveillance*: ADS-B provides information such as the aircraft's position and velocity using GNSS.
- ***B**roadcast*: transmission model is based on the broadcast communication model; therefore, every ADS-B compatible receiver in proximity can receive broadcast data.

A. ADS-B Functionality

As demonstrated in [8], ADS-B employs the Global Navigation Satellite System (GNSS), more specifically, Global Positioning System (GPS) which is the operational and predominant satellite navigation system today, to determine the aircraft's position and velocity. The resulting coordinates together with the other information such as velocity and altitude will then be transmitted (broadcast) once per second (or better) to the ground stations or the other aircraft in the vicinity [8]. The ADS-B avionics integrates this data with the other data collected from other aircraft systems such as the Flight Management System (FMS), altimeter, and Traffic Collision Avoidance System (TCAS) units to generate a set of data for the aircraft. This data is then transmitted by the ADS-B on one of the ADS-B datalinks at the predefined rate. Aircraft within line-of-sight and ground stations up to approximately 280 miles away, are able to receive the broadcast data (ADS-B Out) [8]. The ground stations equipped with ADS-B receivers then process this data and display it to ATC for use in air traffic control. As a temporary service for encouraging early equipage of ADS-B, this information together with other surveillance data gathered from radar and Wide Area Multilateration (WAM) will be forwarded back to the airplane as Traffic Information Service-Broadcast (TIS-B) [8].

B. ADS-B Signal

As stated in [10], there are three categories of ADS-B transmission frequencies, namely Very High-Frequency Data Link (VDL) Mode 4, 978 MHz Universal Access Transceiver (UAT), and 1090 MHz *Extended Squitter* (ES). However, since the Extended Squitter datalink is viewed as an extension of existing Mode S transponders, it is regarded as the most cost-effective way of transmission of ADS-B data [10]. According to [11], in SSR radar systems, upon interrogation, Mode S transponder responds with a globally-unique 24-bit aircraft identifier to the ground-based radar with a data rate of 1 Mbps and the frame size of either 56 or 112 bits. In order to enable the Airborn Collision Avoidance System (ACAS), the transponder also transmits the unsolicited 56-bit transmissions called Mode S *Short Squitter* once per second which consist only the identifier. However, 1090 Mhz ES uses the Extended Squitter format which consists of 112 bits including a 56-bit data field which comprises the location data with the accuracy of approximately 5.1 meters [11]. The message format of Extended Squitter is shown in Fig. 1.

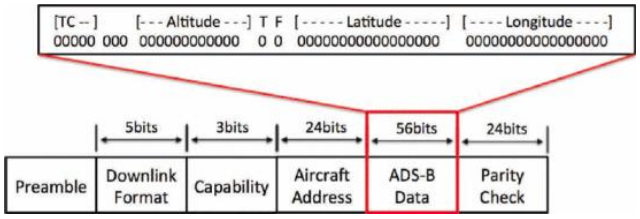

Fig. 1. ADS-B Extended Squitter message format [11]

C. ADS-B Protocol Hierarchy

Fig. 2 demonstrates the correlation between the transponder and ADS-B protocols. As it is illustrated, the 1090ES protocol is an entirely different protocol from Universal Access Transceiver (UAT) and developed on top of the current Mode S protocol. UAT has been developed specifically for the aviation domain and provides a bandwidth of 1 Mbps on 978 Mhz frequency [1]. Accordingly, 1090ES protocol enhances the message fields for ADS-B surveillance data. Therefore, it allows the ADS-B employment in the existing mode-S transponders. Thus, equipage of aircraft can be done with 1090ES which considered to be less expensive than installing new avionics which is necessary for UAT implementation [9].

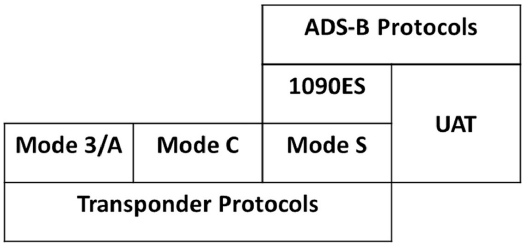

Fig. 2. ADS-B protocol hierarchy [12]

D. ADS-B Message Format

As shown in Fig. 1, the 1090ES data link uses a message format which consists of a preamble followed by a 112-bit message. First 5 bits which are indicated as *Downlink Format field*, indicates the message type. A value of 17 in the aforementioned field indicates the Extended Squitter message type. In this case transmission of 56 arbitrary bits in the *ADS-B Data field* is allowed. The *Capability field* reflects the capabilities of the Mode S transponder. The *Aircraft Address field* carries the unique 24-bit identifier obtained from International Civil Aviation Organization (ICAO). Furthermore, the *Parity Check field* carries a 24-bit CRC error detection code which enables the detection of errors in case of message corruption. Recipients are able to correct up to 5 bits of error using a fixed generator polynomial of degree 24 [1].

III. ADS-B Security Status and Concerns

According to FAA Federal Regulation, the minimum required Message Element Set for ADS-B Out is to broadcast information such as length and width of the aircraft, barometric pressure, latitude and longitude, geometric altitude, the aircraft's "IDENT," and velocity [13]. However, since the communication channel in ADS-B is unencrypted [9], it is relatively easy to collect and spoof this information by attackers with malicious purposes. Costin and Francillon [14] have argued that the aforementioned is possible by using affordable and easily-available, "off-the-shelf" hardware and software. This information enables attackers to capture, modify, delete or inject messages of the communication channel, and use other attack techniques such as jamming and spoofing in order to perform their attacks.

According to [11], ADS-B lacks a secondary mechanism to confirm the location in case of transmitter malfunction. Therefore, even without the existence of attacks, wrong ADS-B data could be transmitted unwittingly. There have been some reports concerning the malfunctions in ACAS (TCAS) and other avionics that have caused dangerous situations previously [15]. Therefore, unverified ADS-B data can cause a significant risk in air transportation of tomorrow. Currently, air traffic surveillance and control over the world is mostly done by the available Primary and Secondary Surveillance Radars. However, once ADS-B is fully deployed and adopted, ATC services rely only on ADS-B technology. Therefore the trustworthiness of ADS-B data is crucial for the future safety of aviation.

IV. Attack Scenarios (ADS-B Vulnerabilities)

In this chapter, different attack scenarios will be described. As in ADS-B there are no mechanisms of authentication or encryption, this system is vulnerable to all attacks that are typically possible in the physical layer [12].

The *Attacker Model* defined in [14] will be used in this chapter in order to classify multiple attack scenarios. This model could be later used to mitigate the security flaws found in ADS-B. According to this model, the attack can be categorized based on the following criteria:

1) *Place in the System*; either external or internal according to whether the attacker is from a trusted party of the aviation control.
2) *Physical Position*; whether the attacker is ground-based or airborne.
3) *Goals*; the nature of the attack can have a wide range of motivations and in [14], four main types of attackers were defined: pranksters, abusive users, criminals, military/intelligence.

In [14], Costin and Francillon also describe the main vulnerabilities found in ADS-B. These issues are the missing security mechanisms which enable a malicious user to be successful in attacking the protocol. Table I shows which security requirement is violated by each type of attack. The main vulnerabilities are:

1) *Lack of authentication*; which could prevent an unauthorized user from sending and receiving messages.
2) *Lack of message signature*; which could prevent message adulteration and would also provide means of correct identification of message sender.
3) *Lack of encryption*; which could protect sensitive data being sent in the wireless channel from being read by third parties.
4) *Lack of MAC or nonces*; which could prevent replay attacks.
5) *Lack of short-lived identifiers*; which could enable data privacy.

The remaining part of this chapter will describe the attacks to ADS-B following an ascending order security risk, which will be discussed in the next chapter. This chapter is organized as follows: in Section IV-A, a passive attack of eavesdropping will be discussed and in Section IV-B, several scenarios of active attacks with potentially catastrophic consequences will be presented. Table II shows an overview of the attacks scenarios described in this paper alongside with the methods exploited to enable the attack.

TABLE I
ADS-B Attacks vs. Security Requirements [9]

Method	Security Requirement Violated
Eavesdropping	Confidentiality
Message Deletion	Integrity
Message Modification	Integrity
Jamming	Availability
Message Injection	Authentication

TABLE II
ADS-B Attack Scenarios [1]

Scenario	Method
Aircraft Reconnaissance	Eavesdropping
Aircraft Disappearance	Message Deletion
Aircraft Spoofing	Message Deletion
Virtual Trajectory Modification	Message Modification
Virtual Aircraft Hijacking	Message Modification
Ground Station Flood Denial	Jamming
Aircraft Flood Denial	Jamming
Aircraft Ghost Injection	Message Injection
Ground Station Ghost Injection	Message Injection

A. Passive Attacks

The lack of confidentiality in the wireless channel due to no encryption and authentication mechanism used in ADS-B enables an attacker to listen to the messages being sent. An attacker with appropriate hardware can acquire sensitive data about an aircraft. This attack is called eavesdropping or ***Aircraft Reconnaissance*** [1].

In [12], the authors have tracked over 18000 flights during a period of a week using a low-cost ADS-B receiver. As shown in Fig. 1, in the 112 bits of an ADS-B message, 56 bits are reserved for data. This data includes identification, position, velocity, urgency code and quality level. 24 bits are reserved for aircraft address identification (ICAO). The ICAO must be unique, but by realizing this attack, this identification could be replicated.

B. Active Attacks

Contrary to passive attacks, active attacks may be a direct threat to the safety of air-traffic control [12]. In this section, various attack scenarios will be described using multiple attack techniques. These active attacks are based on interfering

with the RF channel. In the following subsections, the attack scenarios listed in Table II will be described.

1) Message Deletion: The legitimate ADS-B message can be deleted using two main strategies [1]:

- *Destructive Interference*: this method sends the inverse of the message signal being sent to attenuate or completely destroy the original message.
- *Constructive Interference*: in this method, a high number of bit errors are sent. As the CRC can only correct up to 5-bit errors per message, the receiver of the spoofed message would drop this corrupted message [1].

Taking advantage of these techniques, the following scenarios of attack would be possible:

- ***Aircraft Disappearance***: in this scenario, the attacker would delete all messages of an aircraft making it invisible to other aircraft using ADS-B as an anti-collision system [12].
- ***Aircraft Spoofing***: this can be executed by spoofing the ICAO 24 bit address [12]. This attack can be achieved by a combination of message deletion and message injection. With an internal attacker with access to the aircraft cabin, it would also be possible to change the aircraft's ICAO.

2) Message Modification: Message Modification attack methods can be used by attackers to produce an attack that can be done without any communicating parties being aware of it. Due to this fact, the wrong instruction might be given by air traffic controllers and it could also impact anti-collision systems which might perceive an aircraft to be further away from its real location.

The ADS-B message can be modified by an attacker in two different ways [1]:

- *Overshadowing*: a message with a strong signal high enough to replace parts of the entire message being sent.
- *Bit-flipping*: in this approach, the attacker could flip an arbitrary number of bits from 0 to 1 or vice-versa.

Using the two approaches highlighted above, it enables the following attack scenarios:

- ***Virtual Trajectory Modification***: in this attack, the attacker modifies the original message from an aircraft and alters its position slightly [12]. Another variant would just delete the message and send a new modified one.
- ***Virtual Aircraft Hijacking (False Alarm Attack)***: this attack is similar to the Virtual Trajectory Modification except that this time, the message is modified to send a fake alarm. This could be used by pranksters and causes a lot of confusion in the air traffic control.

3) Jamming: Jamming is a common Denial of Service attack technique used in the wireless data channel. It is based on the fact that there is no physical barrier to access the data link. Therefore, the attacker can use this method to send data at the same Radio Frequency as the real communicating parties. In the case of ADS-B, that would be using the 1090MHz frequency of Mode S as stated in [1]. The attack happens when a malicious user floods the channel with messages which causes the degradation of the communication or complete denial of service.

The attacker using this technique can use multiples strategies to achieve its goal to disrupt the communication according to [16]:

- *Constant Jammer*: which constantly emits either noise, tone or random bits. This can be easily detected as jamming and filtered by the receiver.
- *Deceptive Jammer*: constantly generates valid packets making it more difficult to distinguish the messages sent by the attacker and a valid user.
- *Random Jammer*: it takes turns behaving as a constant and deceptive jammer while going into sleep mode after jamming for a period of time.
- *Reactive Jammer*: this strategy only executes while messages are being sent; this condition is recognizable by sensing activity on the radio channel. This scheme reduces the chance of detection.

According to the attacker model defined at the beginning of this chapter IV, this technique could be exploited by an attacker who is either external or internal, ground-based or airborne and could have diverse goals: pranks, abuse or military. The attacker could follow different ways to disrupt the communication whether with Message Injection, Deletion or Modification. According to [17], the following attack scenarios would be possible using this type of attack:

- ***Ground Station Flood Denial***: this attack would prevent an Air Traffic Control to work accordingly. It is a ground-based attack which impact would be limited to the locally affected area. Despite its low difficulty to be implemented [17], this attack could cause major disruption in areas with a high density of air traffic [12].
  However, for a group of orchestrated attackers with criminal goals, a distributed attack targeted at multiple airports could massively increase the chance of accidents due to the lack of alternative airports not being attacked which could receive the diverted incoming air traffic.
- ***Aircraft Flood Denial***: this attack is similar to the one above, but in this one, the aircraft becomes the target to the attack. In this scenario an aircraft which is about to land or to take off would be affected.
  This attack could be realized with a high-powered ground-based Jamming device. The downfall of this attack would be that the aircraft would eventually go out of reach. An airborne attack would also be theoretically possible with an on-board attacker with such device [17].

4) Message Injection: Due to the lack of authentication in the specification of ADS-B, an attacker can generate valid ADS-B messages. This enables multiple attack scenarios to be executed which can compromise the safety of aircraft, airports and surrounding areas. This method enables the following attack scenario [1]:

- ***Aircraft Ghost Injection***: in this scenario, an attacker could send valid ADS-B messages of an aircraft which does not exist [12]. The target for this attack would be

an aircraft. This attack would often be ground-based, but a successful more complex attack could be made using techniques to simulate the speed and location of a valid airplane. This would make it challenging for a pilot to distinguish the fake messages from real ones especially in an environment with low-visibility capability. In addition, aircraft with Traffic Collision Avoidance System (TCAS) could confuse pilots. This attack is only limited by the bandwidth of the data channel.

- ***Ground Station Ghost Injection***: this scenario is very similar to the one above, except that in this scenario the ADS-B ground station would be the target of the attack. In this case, a fake aircraft would be visible to air traffic controllers.

V. Complexity, Severity, and Effect of the Attacks

The previously identified attack scenarios differ in the impact they have on the target system and the likelihood for an attacker to execute the attack successfully. Manesh and Kaabouch [9] examine their overall risk and compare the described methodologies as depicted in Fig. 3.

		Attack Impact		
		Low	Medium	High
Attack Likelihood	High	Eavesdropping (Low Risk)		
	Medium		Jamming (Medium-High Risk)	Message Injection (High Risk)
	Low		Message Deletion (Medium Risk)	Message Modification (Medium-High Risk)

Fig. 3. ADS-B Risk Analysis [9]

Because of the lack of encryption and authentication in ADS-B, aircraft reconnaissance or eavesdropping attacks are easy to perform due to the availability of the technology (e.g., ADS-B/Mode S broadcasts demonstrated for free by flightradar24.com) and are thus likely to be implemented successfully. However, the impact of this kind of attack is relatively low as it does not harm the aircraft control system directly. Although, reconnaissance is a critical issue for military settings and might be the first step to more sophisticated active attacks [17].

Active attacks are generally more safety critical than conventional eavesdropping, as they try to confuse or harm onboard systems and ground control stations directly which may produce fatal outcomes [12]. Message deletion techniques used for aircraft disappearance or spoofing attacks are categorized as a medium risk factor since time synchronization is required to destroy or interfere the transmission at the right moment, which reduces the likelihood of this attack. Furthermore, multilateration techniques and traditional systems would still support localization of the aircraft as a backup [9]. Message Modification techniques exploited for virtual trajectory modification or hijacking attacks can lead to confusion and fatal outcomes without disclosing an attack and are thus classified as having a high impact on air traffic. However, the likelihood of this attack is the least since precision and time synchronization is required to apply overshadowing or bit-flipping techniques presented in Section IV-B2. Jamming attacks are categorized as a medium-to-high risk since they can lead to a loss of surveillance for a ground control station which has a critical impact on flight control. This can be easily achieved by an attacker who is in proximity to the ground control and disrupts all 1090 MHz transmissions with a portable low power jamming device [17]. Software Defined Radios (SDR) that can be used as jamming devices are highly available and therefore increase the likelihood of this attack. Considering the strategies identified in Section IV-B, jamming can be very effective whilst concealing the actual attack.

The authors of [9] identify message injection as the biggest security threat on ADS-D because of the possibly severe impacts and an increased likelihood of an attacker successfully executing it due to the availability of SDRs. Especially flooding ground control stations with a large number of fake ADS-B message injections can confuse operators and cause traffic disruptions and more fatal consequences. As the attack requires some skill to perform using the ADS-B messaging protocol to create well-formatted messages such that fake aircraft appear on the ground control system, this method is categorized as having a medium likelihood.

The analyzed techniques can harm communication in air traffic, and introduce false information to software, operators and authorities that may draw wrong conclusions based on assumptions relying on the reliability of ADS-B. The authors of [9] state that especially dangerous situations can appear when incorrect and unreliable data affects other information systems causing cascading effects in the whole air traffic control system.

VI. ADS-B countermeasures

In this chapter, we will briefly examine and analyze countermeasures that have been proposed to eliminate the security threats imposed by the ADS-B protocol. The literature generally divides ADS-B countermeasures in (i) secure broadcast authentication solutions and (ii) secure location verification solutions. Secure broadcast authentication solutions aim to secure the ADS-B broadcasting protocol and enabling the receiver to verify the authenticity of a message. This category can be further sub-divided into cryptographic schemes like Public-Key Infrastructure in combination with (retroactive) µTESLA [9] and non-cryptographic schemes such as Fingerprinting [18] and Random Frequency Hopping/Spreading [1]. On the other hand, secure location verification solutions compose a multitude of approaches that try to determine and thereby verify the location of an aircraft by other means including distance bounding, Kalman filtering, multilateration, group verification, data fusion and traffic modeling [9]. This taxonomy is depicted in Fig. 4.

Works from Strohmeier et al. [1] or Manesh and Kaabouch [9] elaborately explain each of these concepts and analyze their value by considering feasibility in terms of cost and difficulty

TABLE III
ADS-B COUNTERMEASURES COMPARISON [9]

Countermeasure	Implementation	Security Level
Lightweight PKI	Very difficult	High
Spread Spectrum	Very difficult	High
Kalman Filtering	Simple	Moderately high
Data Fusion	Moderately simple	Moderately high
PKI + μTESLA	Moderately difficult	Moderately high
Fingerprinting	Moderately difficult	Moderately high
Distance Bounding	Difficult	Low
Multilateration	Simple	Low

of implementation as well as coverage of security threats and security requirements such as data integrity and availability. Therefore, we will now focus on extracting and presenting the most efficient and effective solutions to the overall system problematic.

Table III shows a comparison of the efficiency of implementation versus the gain of security that is sustained by the corresponding solution. The table is ranked by effectiveness in cost and benefit of the approach from top to bottom. As can be seen, the most effective approaches are Lightweight Public Key Infrastructure, Spread Spectrum, Kalman Filtering and Data Fusion. We will, therefore, provide an overview on the underlying concepts and discuss advantages and disadvantages of each solution in the following.

1) Public Key Infrastructure: Encrypting messages using a public key infrastructure has a long tradition in wireless networks. The concept is encompassed by a certificate authority that registers and verifies any communicating party and provides a public and private key to it. These keys can then be used for asymmetric key encryption [19]. Manesh and Kaabouch [9] argue that the benefits of this method would highly increase the security of ADS-B against eavesdropping, message injection, modification, and deletion attacks. However, the challenges that have to be faced in order to implement such a comprehensive solution are hardly feasible. Strohmeier et al. [1] reveal natural disadvantages of using a cryptographic solution due to large communication overhead, a break of compatibility with already equipped hardware and software and major difficulties in the distribution of keys in a decentralized setting. As one possible solution to overcome these issues, they reference a ”lightweight” Primary Key Infrastructure that uses retroactive key publication. For this approach, the sender distributes a signature over several ADS-B messages to reduce the communication overhead for a single message. The receivers buffer incoming messages until the entire signature has arrived at which time the buffered messages can be authenticated. They suggest that for this method the necessary key distribution could be done during the aircraft's scheduled maintenance time.

2) Spread Spectrum: Countermeasures can be employed on the whole communication stack. On the physical layer, an effective approach to secure communication against (narrowband) jamming and message modification attacks is the use of Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Using a shared hopping pattern makes it hard to follow or jam the communication for an attacker without knowing the pattern. Since these patterns need to be pre-shared to synchronize the communication, the authors of [1] argue that these codes would not stay secret for long. To overcome this limitation, this approach has been refined to circumvent the need for pre-shared keys by [20]. By hopping between channels without coordination and relying on a statistical chance that sender and receiver are communicating on the same channel, the attacker is not able to interrogate the communication efficiently. However, this technique reduces the performance of the communication and requires an increased bandwidth which makes it difficult to adapt to the existing ADS-B infrastructure in practice [9]. Further, it can only secure the communication against replay attacks in combination with a Primary Key Infrastructure and timestamps [1].

3) Kalman Filtering: Kalman filtering is an algorithmic approach used to observe and statistically predict future variable values. It is already used filtering and smoothing of GPS data to avoid aircraft collisions on runways and taxiways [9]. It is further used in air traffic control (ground stations) to verify the trajectory changes in ADS-B messages by analyzing motion and intent of the aircraft. Abnormal values on speed and other features concluded from ADS-B messages can thus be detected [1]. However, this countermeasure is vulnerable to the so-called frog-boiling attack: an attacker jams the original signal and injects ADS-B messages with increasingly different simulated coordinates, for example, generated by a flight simulation software [21]. Filtering incoming ADS-B messages greatly increases the complexity of any attack and is comparatively simple to implement since it does not require any changes to the ADS-B protocol. However, it exposes new vulnerabilities to DoS attacks because every receiver has to cope with increased computational complexity.

4) Data Fusion: One generally accepted best practice to increase the reliability of security and safety-critical systems is using redundant systems to verify each other. The fusion of ADS-B data and independent sources can also improve the precision of location tracking in practice by aggregating and overlaying the redundant positioning data. Possible sources of data include multilateration data, traditional radar PSR/ SSR data and even flight plan data can be considered to reduce the risk of any of the respective positioning systems working with flawed or fake parameters. To facilitate data fusion, a prior analysis of trustworthiness of the data source is required as described by [1]. The advantage of this solution is the compatibility with legacy systems that are already installed. Since only algorithms to fuse the reported data need to be implemented, there is no need to change ADS-B protocol. However, for air spaces with no legacy systems, this means exponentially increased cost for building these redundant systems.

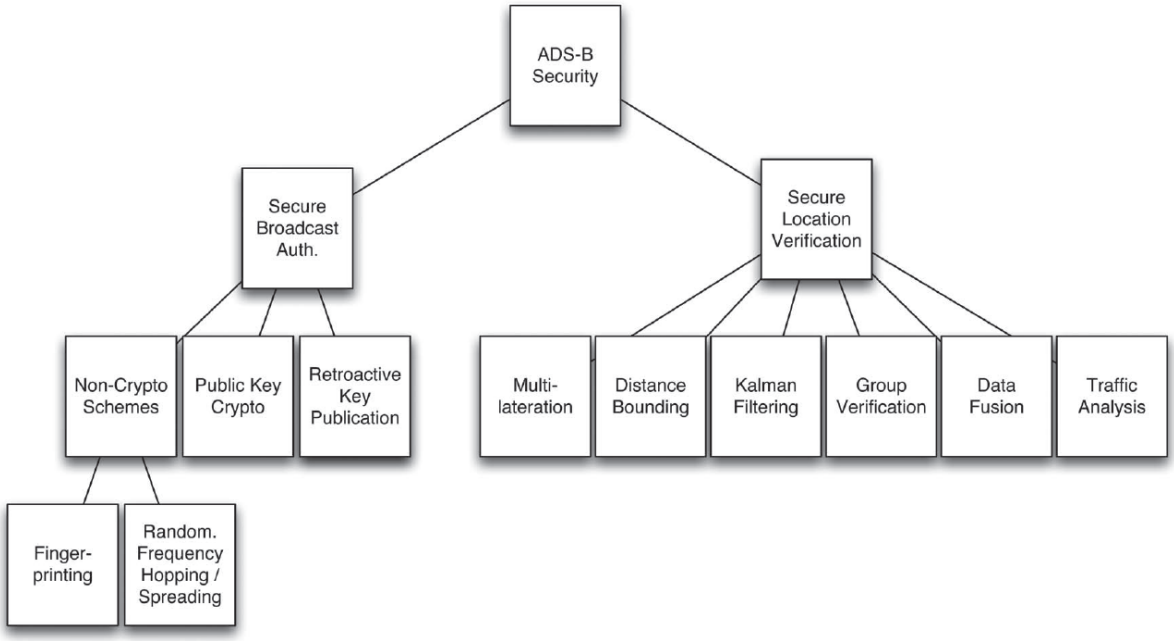

Fig. 4. Taxonomy of ADS-B countermeasures [1]

Since ADS-B hardware and software is already deployed in many aircraft, changing the communication protocol is inherently connected to high costs. Manesh and Kaabouch [9] state that there is no one solution that would be sufficient to solve the problems in ABS-B at the current time. They further state that the key to adopting a feasible solution on ADS-B relies on backward compatibility to avoid the high upfront cost and an incremental introduction of changes to the system. In the end, not securing ADS-B might be worse than realizing a costly solution that imposes a high security level.

VII. Conclusion

Despite many pitfalls that exist in the deployment model of ADS-B technology and the existence of security flaws due to the lack of authentication and encryption in the technology, worldwide acceptance of ADS-B is continuously increasing. As a result, this technology will be widely used by air traffic controllers and airlines over the world. Therefore, ADS-B will eventually replace old surveillance technologies such as PSR and SSR that are currently being used in many countries as the primary surveillance technology for air traffic control. However, surveys have shown that different attack scenarios with different malicious purposes can be executed over ADS-B which can result in massive disruption and disastrous result. Moreover, the growing number of Unmanned Aerial Vehicles (UAVs) is raising concerns (e.g., collision occurrence) due to the lack of appropriate security considerations in ADS-B.

This paper has studied the fundamentals of ADS-B technology. Afterward, different attack scenarios have been inspected in details and categorized into passive and active attacks; furthermore, the possibility of execution, consequences, and severity of the attacks in case of occurrence have been argued. Moreover, the paper summarized some prominent solutions by dividing the countermeasures into Secure Broadcast Authentication and Secure Location Verification methods. These are solutions which have been proposed so far in order to mitigate the security flaws existing in ADS-B technology. However, it has been shown that the implementation of the countermeasures is mostly unfeasible due to lack of backward compatibility, high costs or introduction of additional threats. Additionally, it is argued that each measure does not provide a fully-secure protocol solely. Therefore, future researches should arguably be focused on creating an innovative multi-layer security patch with the consideration of backward compatibility, reducing costs of implementation, and widespread acceptance.

References

[1] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

[2] A. Abdulaziz, A. S. Yaro, A. A. Adam, M. T. Kabir, and H. B. Salau, "Optimum receiver for decoding automatic dependent surveillance broadcast (ads-b) signals," *American Journal of Signal Processing*, vol. 5, no. 2, pp. 23–31, 2015.

[3] G. Galati, G. Perrotta, S. Di Girolamo, R. Dellago, S. Gentile, and F. Lanari, "Study of an integrated communication, navigation and surveillance satellite system for air traffic management," in *Radar, 1996. Proceedings., CIE International Conference of.* IEEE, 1996, pp. 238–241.

[4] E. Hableel, J. Baek, Y.-J. Byon, and D. S. Wong, "How to protect ADS-B: Confidentiality framework for future air traffic communication," in *Computer Communications Workshops (INFOCOM WKSHPS), 2015 IEEE Conference on.* IEEE, 2015, pp. 155–160.

[5] Faa.gov, "No kidding: ADS-B deadline of Jan. 1, 2020, is firm," 2018, accessed 25-December-2018. [Online]. Available: https://www.faa.gov/news/updates/?newsId=90008&omniRss=news_updatesAoc&cid=101_N_U

[6] "ADS-B: On track for the mandate!" *EASA SEASONAL TECHNICAL COMMUNICATION*, Jun 2018. [Online]. Available: https://www.easa.europa.eu/sites/default/files/dfu/EASA_STC_NEWS_JUNE_2018.pdf

[7] M. Chase and M. Foye, "Whats the current status on ADS-B? — avbuyer," 2018, [Accessed: 26- Dec-2018]. [Online]. Available: https://www.avbuyer.com/articles/avionics/what-s-the-current-status-on-ads-b-112141

[8] T. F. SURVEILLANCE and B. S. OFFICE, "ADS-B 101 what it is, and what it means to you," *FAA Safety BRIEFING*, vol. 56, no. 2, pp. 10–12, March/April 2017.

[9] M. R. Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system," *International Journal of Critical Infrastructure Protection*, vol. 19, pp. 16–31, 2017.

[10] R. Francis, R. Vincent, J.-M. Noël, P. Tremblay, D. Desjardins, A. Cushley, and M. Wallace, "The flying laboratory for the observation of ADS-B signals," *International Journal of Navigation and Observation*, vol. 2011, 2011.

[11] Y. Kim, J.-Y. Jo, and S. Lee, "ADS-B vulnerabilities and a security solution with a timestamp," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 11, pp. 52–61, 2017.

[12] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *International Conference on Applied Cryptography and Network Security*. Springer, 2013, pp. 253–271.

[13] Federal Aviation Administration, DOT., "Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements To Support Air Traffic Control (ATC) Service, vol. 1491225, no. 91334." 2010, https://www.ecfr.gov/cgi-bin/text-idx?node=14:2.0.1.3.10#se14.2.91_1227.

[14] 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*, pp. 1–12, 2012.

[15] "Loss of separation between Airbus A330 VHEBO and Airbus A330 VH EBS," Australian Transport Safety Bureau, near Adelaide, South Australia, Aviation Occurrence Investigation AO-2013-161, Mar. 5, 2015, Available at https://www.atsb.gov.au/media/5214362/AO-2013-161%20final.pdf.

[16] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, May 2006.

[17] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78 – 87, 2011.

[18] M. Strohmeier, I. Martinovic, M. Fuchs, M. Schäfer, and V. Lenders, "Opensky: A swiss army knife for air traffic security research," in *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*. IEEE, 2015, pp. 4A1–1.

[19] S. M. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in *Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on*. IEEE, 1992, pp. 72–84.

[20] M. Strasser, P. Christina, S. Capkun, M. Cagalj *et al.*, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *2008 IEEE Symposium on Security and Privacy*. IEEE, 2008, pp. 64–78.

[21] M. Roeling, "False data injection in Kalman Filters in an aerospace setting; ADS-B data with simulated noise," 2016.