Survey of Cyber Threats in Air Traffic Control and Aircraft Communications Systems

Elad Harison and Nezer Zaidenberg

Abstract Air traffic control systems based on the ADS-B standard have been widely adopted in civil aviation to the point that they are now considered the de facto standard. ADS-B provides major benefits to airports and airlines by increasing the safety of air traffic management and control and allowing more flights to travel near busy airports. However, the ADS-B technology lacks sufficient security measures. The ADS-B system is vulnerable and exposed to cyberattacks. We survey the potential known threats and attacks against ADS-B and assess the potential cybersecurity threats to air traffic management and control. The widespread use of ADS-B and the lack of security features in it, i.e., all the ADS-B messages are unauthenticated and unencrypted!, makes this necessary. As we demonstrate in the survey, ADS-B's lack of security features allows injection of false flight data, as well as jamming the wireless communications between airplanes and control towers and preventing the detection of commercial aircrafts by ADS-B ground stations, control towers, and other aircrafts.

Keywords Cyber · Security · ADS-B · Air traffic communications

1 Introduction

One of the recent major technological advances in air traffic control (ATC) systems was the adoption of ADS-B protocol. The ADS-B protocol allows for a cooperative air traffic surveillance technology (hereby SSR or *secondary surveillance radar*).

E. Harison (✉)
School of Industrial Engineering and Management, Shenkar College of Engineering and Design, Ramat Gan, Israel
e-mail: eladha@shenkar.ac.il

N. Zaidenberg
Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland
e-mail: nezer@trulyprotect.com

M. Lehto and P. Neittaanmäki (eds.), *Cyber Security: Power and Technology*, Intelligent Systems, Control and Automation: Science and Engineering 93,
https://doi.org/10.1007/978-3-319-75307-2_12

The ADS-B approach augments the prior approach of an uncooperative system in which elements operated independent surveillance tools (i.e., hereby PSR or *primary surveillance radar*). In contrast, in the ADS-B approach, all elements work together in a dependent manner in order to enhance airline safety (for example, Horowitz and Santos 2009, Ali et al. 2015, and others). An older PSR system was designed using a set of independent elements and systems. These independent elements each function by transmitting high-frequency radar signals. These high-frequency signals are reflected from the target object they hit. The reflection of signals is a physical process; therefore, they are reflected by any object. Reflection of signals does not require cooperation from the inspected aircraft (or other inspected objects) or any of the aircraft's systems and software. The reflection echo of the transmitted radar signals identifies the object. The distance (range) between the transmitting and reflecting objects can be calculated based on the amount of time that elapses until we receive the echo. The angular direction of the inspected aircraft, as well as its velocity, can be calculated based on the time and direction differences of two returned signals. Likewise, the size and the shape of the object can also be measured. The returned signals are processed by the air traffic control. After processing the returned signals, the control tower can receive a relatively good estimate of the direction, speed, and distance associated with any aircraft. In contrast to the older PSR, the newer SSR system utilizes data that is received from transponders installed in the aircraft. These transponders intercept SSR requests and transmit responses to the requests, i.e., in contrast to PSR, SSR is an active system that responds to "request" signals. These signals can be received from either ground stations or other airplanes. The response from the SSR transponders includes information about the aircraft's precise altitude, heading, identification codes, and technical details. Naturally, SSR requires the transponders to be installed and programmed in such a way as to respond to the request. Without the inspected aircraft cooperation SSR would have been impossible. When SSR is compared to old fashion PSR, SSR systems such as ADS-B are significantly more accurate, both in terms of the localization and in terms of the identification of inspected aircraft. However, in SSR systems all the surveillance data collected by the system, i.e., the position, velocity, and status of all aircrafts involved, is received from the inspected aircraft, as opposed to measured by the inspection system. Thus, SSR systems, such as ADS-B, are also very dependent on data received from the aircraft and on the reliability of communication, as well as the cooperation between the aircraft itself and the ground stations and that these communications are not fabricated or attacked.

Automatic dependent surveillance-broadcast (ADS-B) is an air traffic communications protocol. ADS-B is used for transmitting location, velocity, and heading data between aircraft and ground stations. ADS-B is an SSR system for locating aircrafts and avoiding collision risks. ADS-B is rolled out as a significant achievement of the next generation of air traffic control systems. ADS-B is planned to be the most significant part in a system that protects over two billion passengers boarding commercial aircraft per annum.

Each aircraft that uses the ADS-B SSR system retrieves its own position, heading, and velocity from a GPS receiver that is placed on board. The ADS-B communication

system consists of two components. Communication is sent using broadcast transmitters. The ADS-B transmitter is called "ADS-B OUT". The second components are broadcast receivers. The broadcast receivers that interpret ADS-B communication are called "ADS-B IN". The aircraft that use ADS-B periodically broadcast their positions via the ADS-B OUT messaging system to virtually all who can receive their position, specifically the air traffic management and control towers. However, the rapid adaptation of ADS-B and installation of a growing number of ADS-B IN receivers in aircraft raise a new set of cybersecurity challenges. For example, how can a receiving party authenticate the identity of a transmitting aircraft? This authentication procedure needs to be efficient, as it takes place over and over for each signal in real time! How can information received about positions and flight paths of each of the aircraft be trusted, *inter alia* (for analysis of security concerns, see Benda 2015 and Hainess 2012)?

At the physical network level, ADS-B operates at two specific radio frequencies: 1030 MHz for active transmissions (i.e., transmissions from ATC towers, radars, or other aircraft) and 1090 MHz for active responses and normal broadcasts (both from other aircraft and from airport vehicles). ADS-B is supported by two different data links radio frequencies, 1090 MHz Extended Squitter (1090ES) and the Universal Access Transceiver (UAT).

ADS-B has multiple purposes with the following benefits:

- Increases the safety of air traffic control by dramatically improving the situational awareness of pilots and providing them with access to real-time air traffic data of the aircraft that surround them.
- Improves air traffic conflict detection and resolution systems by informing aircraft about their relative positions to other planes ahead of time, independent of ground facilities in control towers and other air traffic control stations.
- Improves accuracy of air traffic information such as aircraft positions due to the higher resolution data obtained from the ADS-B system, in comparison to older traditional radar systems.
- Provides altitude information, in addition to all information provided by older radar systems. The older radars systems usually cannot provide altitude information.

Figure 1 demonstrates ADS-B protocol.

Therefore, the increasing adaption of ADS-B technology will allow for much more efficient use of the airspace around busy international airports by reducing the required flight distance between planes, due to ADS-B's improved accuracy and interplane exact location (based on GPS) data exchanges.

Since ADS-B is so well designed in terms of airspace efficiency and offers such a great benefit, it is surprising that despite the years invested by regulators in the development of the ADS-B standard, the design of the ADS-B communication protocol that is used in commercial air traffic does not specify any mechanisms to encrypt its messages, or digitally sign or authenticate them. There are no means in the ADS-B protocol to ensure that messages are non-replayed (reply attack) and adhere to other security measures to ensure resilience in the face of even simple and well-known cyberattacks. It is well known today that the ADS-B standard was not developed

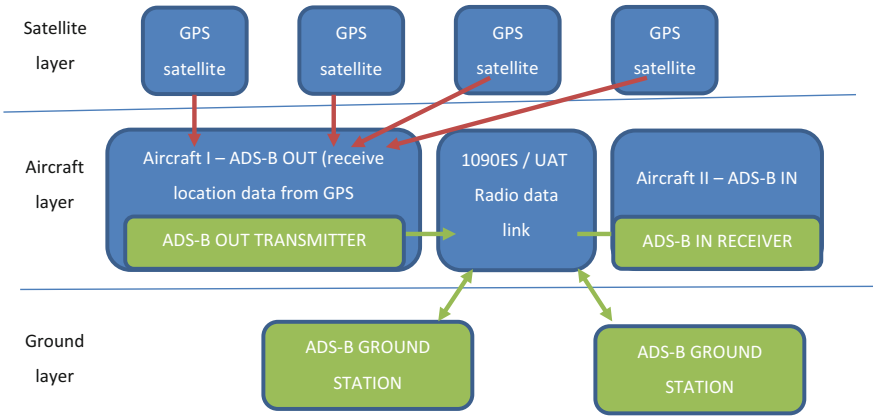

Fig. 1 ADS-B protocol

with security concerns in mind. It is also a well-known fact that ADS-B messages are unauthenticated and unencrypted and, therefore, are susceptible to numerous attacks. Attackers can use the same radio frequency as ADS-B transmissions to send rogue messages or disrupt ADS-B messages (as demonstrated by McCallie et al. 2011, Strohmeier et al. 2014). Recently, the ADS-B security problem was widely reported in the press and at major hacker conventions (specifically Defcon 17, 18, 20 and 22, black hat 2012, and others), where the security shortcomings of ADS-B and how to compromise it using off-the-shelf hardware and simple software security were demonstrated on stage. The fundamental principle behind ADS-B communications is as follows: ADS-B aircraft constantly broadcast ADS-B messages to each other. The rate at which these messages are sent is approximately two per second. This allows for messages to be lost and the system can still function with the partial transmission of messages that actually reach their target. The ADS-B messages are all *unencrypted, unauthenticated* messages that include only an error code to protect the plain text messages over radio transmission links. The error code protection prevents random, unindenting alteration of messages due to communication errors, but does not prevent malicious, intentional alteration of messages. These vulnerable messages contain the critical information of the aircraft position, its velocity, and the identification of each participating aircraft, as well as other information related to it, such as the aircraft's make and model, the engine's make and model, and other statistical information.

Since 2015, the installation of ADS-B systems has become a mandatory licensing requirement for all the new manufactured aircraft used in the European airspace. The ADS-B standard and its underlying technology were largely embraced by many commercial airlines worldwide. According to reports from manufacturers and regulatory bodies worldwide, around 70–80% of commercial aircraft today have already been equipped with ADS-B transponders as of 2013. Canada and Australia are already

using ADS-B in their airspace. In fact, in the less populated parts of these countries, ADS-B is the only means of air traffic control (Purton et al. 2010; Davidson 2013).

Cutting costs has consistently been mentioned as one of the important factors that led to the adoption of the new air traffic management technology (Stark et al. 2013). Cybersecurity experience from other industries shows that cutting costs may result in adopting a system with insufficient security implementation and may result in disasters. In an air traffic control system, the risk of implementation without taking cybersecurity into consideration is real, as the ROI from purchasing and implementing the ADS-B system is so tempting, given ADS-B's significant benefits for its users (see, for example, Ali 2016, for a game theory-based analysis of the benefits of airline operators that use ADS-B, as detailed in Alonso et al. 2013). When working properly (and not under attack) the ADS-B systems improve safety and reduce the likelihood of incidents by a large margin. However, if an ADS-B system is breached and exploited by internal or external malicious parties due to nonexistent security standards (unauthenticated, unencrypted, etc.), disasters may occur.

2 Vulnerabilities of the ADS-B Technology

From the very beginning of ADS-B development, researchers and developers of the ADS-B technology intended that the ADS-B system be used for supporting mission critical, automatic, and human decisions that directly affect air traffic safety in multiple ways. Thereupon, it was imperative and critical that the ADS-B standard and underlying technologies meet meticulous operational, performance, and reliability requirements. However, cybersecurity requirements were not on top of the list. Therefore, the main problem that has not been addressed by the ADS-B system designers lies within the domain of technological cybersecurity mechanisms. All ADS-B communication is unauthenticated and unencrypted. Furthermore, the devices that transmit and receive communications are unattested. This leads to the following issues:

- Lack of entity authentication features to protect receivers against message injection from unauthorized entities.
- The standard lacks message signatures or authentication codes to protect against malicious tampering of messages or impersonating aircrafts. The system does include error codes to protect against unintentional modifications of some bits, but a malicious attacker can modify the message and transmit a correct checksum.
- Messages are not encrypted against eavesdropping. Anybody who receives the messages can understand their contents.
- There is no trusted computing implemented in the system that allows recipients to attest that the sending device has not been tampered with.
- The technology lacks challenge-response or any other mechanisms (such as timestamp, sequence numbers, etc.) to protect against replay attacks. Any recipient of

any message can later rebroadcast it at some future time and the message will appear to be genuine ADS-B message.
- No framework that protects against privacy tracking attacks was embedded.

One such framework to address these concerns was proposed by Perrig and Tygar (2003). The proposed framework allows for a deep analysis of the drawbacks of the ADS-B surveillance system in terms of security. The proposed framework suggests two key areas concerning the secure broadcasting shortcomings of ADS-B: that receivers of information must be able to attest and ensure that any acquired information indeed originated from the designated sender and at the present time (and is not replayed). Furthermore, senders must be able to restrict the list of recipients of the location information. In order to prevent attacks against air traffic systems and to avoid revealing trade secrets, the air traffic control technology should additionally guarantee the confidentiality of messages that are sent via ADS-B revealing the location of aircraft. Last, we believe that recipients of ADS-B messages must be able to attest to the authenticity of the sending device and ensure that it has not been tampered with. Throughout the development of the ADS-B surveillance system, such technological cybersecurity concerns and possible security ramifications were indeed considered and have recently become increasingly crucial in the exploration of ADS-B technology. This is in the wake of the practice of production and adoption of second-rate hardware without trusted computing capabilities that further capitalizes on the system's susceptibility.

Based on the aforementioned guidelines, Strohmeier et al. (2013a, b) indicate that any attempt at improving the security of ADS-B must provide assurance that:

- the data received is indeed consistent with the data that was sent and has not been altered by any third party (i.e., data integrity);
- the data was sent from the claimed sender (i.e., source integrity);
- the data was sent from the claimed location (i.e., data origin authentication);
- the data scheme is consistent with existing ADS-B installations and does not largely impact hardware or software systems (i.e., low impact on current operations, protection against flooding);
- exposure of cyberattacks and security-related incidents is prompt and accurate;
- there is sufficient computing power to ensure a secure defense against DoS and brute force attacks (floods and brute force encryption breaking);
- the solution is robust enough to satisfy the needs of consistently augmenting volumes and density of air traffic;
- the system's security is immune to jamming attempts; and
- the signal is powerful enough to prevent loss of data packets.

Non-repudiation (i.e., the encryption algorithm's ability to verify the message's source) was considered a desirable but low priority feature. However, this security feature comes with additional legal considerations.

ADS-B vulnerabilities inherently result from the nature of using RF communication without additional security measures. In contrast with wired networks, there are no practical obstacles for an attacker trying to access a wireless RF network. While

Table 1 Comparison of the various attacks on ADS-B systems

Severity	Complexity	Summary of the attack on ADS-B systems	Method
Low	Low	Aircraft reconnaissance	Eavesdropping
Medium	Low	Ground station flood denial of service	Signal jamming
Medium	Low-medium	Aircraft flood denial of service	Signal jamming
High	Low	Ground station target Ghost injection/flooding Psychological effect	Message injection
Medium	Low-medium	Virtual aircraft hijacking	Message injection
High	Medium	Aircraft target ghost injection/flooding Denial of service Psychological effect	Message modification
High	Medium	Virtual trajectory modification	Message modification
High	Low	Aircraft disappearance	Message deletion
High	Low	Aircraft spoofing	Message modification

a wired network requires physical access, and thus overcoming physical obstacles such as fences or security guards, RF communication in particular is much more vulnerable to attacks by unauthorized users than other wireless protocols (such as Zigbee, Wi-Fi, Bluetooth, etc.), as RF covers a much larger radius, and therefore cannot be protected by simple perimeter defense.

The attacks we describe provide a comprehensive, detailed model of attacks that exploit the inherent vulnerabilities of ADS-B systems, i.e., lack of encryption and authentication (see summary of attacks in Table 1).

Some of the more severe attacks were demonstrated on stage during the Defcon convention.

2.1 Eavesdropping

One of ADS-B's numerous security vulnerabilities is its vulnerability to eavesdropping. As ADS-B communication is not encrypted, it is most susceptible to the interception of its encrypted, unsecured broadcast transmissions. Eavesdropping has been a long-acknowledged susceptibility of ADS-B. In fact, eavesdropping on ADS-B has even been used as a "feature" in several mobile apps for detecting an airplane's flight number and destination (see Hainess 2012). Due to ADS-B's use of unen-

Table 2 Demonstrates an example of the information describing a randomly chosen aircraft, obtained from its ADS-B (left table) and from publicly available sources (such as lists of flights arriving and departing from airports) (right table). Based on Schäfer et al. (2013)

Call sign	AY0798	Flight no.	AY0798
Int. Civil Aviation Org. (ICAO) code	FIN	Owner	Finnair Oyj
Country	Finland	Start	TLV
Position	TLV	Destination	HEL
Altitude	32500 feet	Scheduled arrival	06:00
Heading	135	Aircraft model	Airbus 319
Speed	425 kn.	Seats	156
Climbing rate	901 feet/min.	Engine	CFM56

crypted, unsecured message broadcast channels (Signore and Hong 2000), there are some legitimate examples of the positive use of location technology, such as flightrader24.com, which is a mobile app that is capable of presentation of air traffic in real time, by eavesdropping. However, eavesdropping understandably remains an indisputable privacy concern due to its potential use in elaborate attacks. While the Federal Aviation Administration claims that aircraft equipped with ADS-B systems are no more at risk than aircrafts without ADS-B. It is clear that the knowledge obtained from the interception of ADS-B messages could be used in the planning of attacks. Any data attained from ADS-B systems could be a powerful tool in the hands of attackers, even if only for reply attacks. Furthermore, attackers can combine such information with publicly available data, such as official aviation databases of incoming and outgoing flights; Table 2 provides an example of the information retrieved from a randomly chosen aircraft via ADS-B augmented by information from publicly available sources.

Through extensive eavesdropping on ADS-B data, attackers can generate statistics about behavioral patterns of aircraft fleets, including information about destinations and recurrent delays. Such information can be employed in competitive analysis about the airline's competitors and their business activities. Furthermore, the data can be rebroadcast, since ADS-B is vulnerable to reply attacks. In addition, the data can be used to create a received signal strength (RSS) map, completing RSS maps that allow attackers to locate aircraft through RSS profiling-based localization techniques or multi-literation. This method can succeed despite attempts to disguise the aircraft's position (for example, in the case of a military aircraft).

The issue is complicated by the fact that it is both difficult to prevent eavesdropping over radio lines. The listening party can be very far away, and the receipt of signals does not generate any signals that can be detected. The only way to prevent eavesdropping over radio transmissions is by utilizing rigorous encryption techniques. Few countries have established laws and regulations against eavesdropping on unencrypted broadcasts that are intended for somebody else. But even when such

laws exist, they do not make it impossible to eavesdrop or make the act of doing so easier to detect.

2.2 Jamming

ADB-S systems are also susceptible to signal jamming attacks. Signal jamming attacks occur when an attacker prevents either the transmission of data or the reception of a transmitted signal.

The jammed signal can originate from a ground station, aircraft, or even a broad area with multiple senders or receivers. Jamming can be done by sending high power signal across an ADS-B radio's frequency. Such attacks can be calculated solely to affect airborne targets or even specific aircraft.

While all forms of wireless radio communications are susceptible to jamming attacks, the potential consequences for aircraft are particularly dangerous, especially if the aircraft relies exclusively on ADS-B communication for navigation. As a result of an aircraft's inability to control intrinsic wide-open spaces between other aircraft and the necessity of broadcasting information between aircraft and ground stations, grievous results (including crash landings and collisions) may occur.

As with SSR communication systems like ADS-B, primary radar systems are also vulnerable to signal jamming attacks, particularly jamming attacks in which the receiver, rather than transmitter, is targeted and jammed (PSR systems have both a transmitter and a receiver). PSR systems can be significantly more difficult to jam than ADS-B receivers, particularly by nonmilitary attackers, as these systems contain rotating antennas and higher transmission power. However, because ADS-B receivers are so widely disseminated for air traffic control purposes, substantial effort is required in order to generate a total blackout for a set area. Despite this, a targeted attack that jams even just a fraction of traffic messages has the capacity to bring about significant denial-of-service consequences and safety problems at any airport or other area with dense air traffic. Furthermore, the abundance of ADS-B capable equipment (Costin and Francillon 2012) makes such attacks easier to prepare, and thus more likely.

2.3 Message Injection

ADS-B messages are unauthenticated and unencrypted. The lack of authentication procedures at the data link level between senders and receivers of ADS-B systems results in a critical weakness. Messages can now possibly be injected into a message stream between two (or more) unsuspecting parties. The injection of spurious messages into air traffic communication systems cannot be detected by either party. Sophisticated ADS-B content can be developed by attackers; this content can be modified and configured to resemble legitimate ADS-B messages, yet in reality, the

forged messages would contain misleading information. These forged messages may potentially result in unsafe action taken by its receiver(s) (i.e., other aircraft, air traffic control towers, ground stations, etc.).

For example, a malicious attacker can develop and inject a message into any legitimate ADS-B system that suggests the message's origin is a fictitious or "ghost" aircraft. Upon receiving the message, an aircraft may change its course, putting other airplanes at risk, or a control tower may send unnecessary or even risky instructions to aircraft. Such a sophisticated attack involves carefully crafting a disguise for the ghost aircraft's location, made up of realistic properties such as ID, position, and velocity, to convince the message's receivers of the aircraft's authenticity (as the message itself contains no authentication and signature system). This form of attack can result in confusion or distraction among air traffic controllers attempting to locate the ghost aircraft. When combined with poor visibility, fog, and other conditions that would prevent the tower from immediately noticing that the "ghost" aircraft does not exist, such an attack can also result in denied landings or instructions for airborne aircraft to alter their altitudes and/or flight paths.

Additionally, attackers may focus on the aircraft's on-board ADS-B collision avoidance systems with message injections intended to distract pilots. Attacks against aircraft can be particularly affective in periods of poor visibility conditions in which the pilots are chiefly relying on instruments to detect other aircraft. Therefore, under poor visibility conditions, towers and pilots alike are more prone to be influenced by any malicious interference with such instruments. Attacks prepared by malicious attackers who are familiar with collision avoidance systems and message injection suggesting the presence of a nearby "ghost" aircraft hold a great potential to direct pilots to alter their course, velocity, and altitude, essentially at the attacker's will. While pilots retain enough autonomy to avoid a collision under such circumstances, very quick, life-threatening decisions can continue to be made by misled pilots and air traffic controllers due to a lack of authentication measures. Despite good judgment, with very little time to take action, even experienced pilots may make a mistake. Thus, the end result of the injection of ghost aircraft and fabricated information can be dire.

2.4 Message Flooding

Message injection techniques can also be used by attackers to introduce overwhelming numbers of aircraft and messages into an ADS-B system. Provided the amount is large enough, the system will not be able to handle so many concurrent messages and may also miss the handling of important messages. This is a denial-of-service attack similar to IP network attacks such as ping flood. In the ADS-B environment, this type of attack is referred to as message flooding. Message flooding also involves the conception of multiple ghost aircrafts, each appearing as real planes. The multitude of messages from all the ghost airplanes will result in denial of service for the ADS-B subsystem. When the surveillance system is under message flooding attack,

the capacity of the controllers to correspond with the aircraft and react accordingly can be severely hindered by the attacker. While the source of such an injection attack is usually more easily detectible than in the case of a single ghost aircraft injection, the lack of surveillance technologies, even for a limited time, continues to pose danger. Such attacks make it impossible for air traffic controllers to differentiate ghost aircraft from real aircraft even momentarily. This in turn renders the management of runways and airspace impossible.

2.5 Ground Station Flooding

Similar to aircraft message flooding from the previous section, there are attacks that focus on flooding ground sensors. This attack can lead to the loss of a large number of messages and cause communication failures. This will subsequently lead to the dissolution of air traffic control services based on ADS-B. Not only do such attacks force air traffic control to switch to inferior radar-based surveillance and control methods, the resulting malfunction of surveillance or collision avoidance systems can additionally lead to misguided judgments and human errors with potentially disastrous outcomes in highly dense areas (e.g., ground and airspace areas of major international airports). Air traffic controllers are ultimately required to use voice radio to blindly guide passing or landing aircraft into other airspaces. This process is bringing about additional concerns, as the voice radio system could also be attacked and affected.

Powerful flooding attacks could additionally flood communications between aircraft, resulting in the malfunction of their collision avoidance systems, and ultimately in a much higher chance of collisions and disasters. This is particularly true in instances of climbing or descending, during which pilots have limited vision, and thus a greater potential to overlook nearby aircraft.

2.6 Message Deletion

Attackers have the potential to "delete" messages across ADS-B systems. Any ADS-B message including authentic messages that are sent from authentic sources can be deleted. An attacker may have a destructive interference, whereby the signal transmitted by an authentic sender is countered with an "opposite" signal. This overlaying of signals causes the original, authentic signal to be negated, or at least to be severely undermined. A message deletion attack is quite challenging, as it requires exact and complex timing. Conversely, the attacker is not necessarily required to coordinate the attack with the legitimate message, but must only yield a significant quantity of errors within the original sender's authentic message for the receiver to simply discard and disregard it as corrupted. Though the message is discarded, the original sender is not notified. By deleting all the target messages, an attacker can effectively

thwart a targeted aircraft from being identified by some or all ADS-B ground stations at a given airport or by other aircraft through this method of deleting that aircraft's messages. Though message deletion is comparable to the previously described attack on a ground station through flooding, message deletion is more elusive than flooding due to the fact that the identified absence of a single aircraft is likely to be attributed to a failure of avionics (rather than issues in the ground station hardware). Should issues with the affected aircraft be noticed, the affected aircraft would be landed for safety checks, resulting in disruption of its flight schedule and operation. However, if the issues remain undetected, it could result in fatal consequences due to the affected aircraft no longer being protected by ADS-B-based systems, including the ADS-B collision avoidance system.

2.7 Message Modification

Since ADS-B messages are not encrypted or signed, malicious attackers can modify any message's contents on the physical network level (radio transmission) during transmission through two well-known approaches: *overshadowing* and *bit-flipping*. Overshadowing ensues when the attackers send specific high-powered signals designed to replace a portion of a message or even an entire message, while bit-flipping occurs when the attackers overlay the communication signals by converting any number of bits within the communication signal from 1 to 0, or vice versa. These methods are not specific to ADS-B, and any radio transmission can be attacked through these methods. What makes ADS-B specifically vulnerable is that messages are not signed, encrypted, or authenticated. Messages can also be modified via a combination of both message deletion and injection techniques.

Modifying the contents of a message can be considered an even more threatening attack than message injection, as the receivers receive the altered message and perceive that it is genuine. This attack method can be used to attack airplane traffic and automatic pilots, as was demonstrated by Hainess (2012). In both message injection and message modification, arbitrary information can be introduced into the message. As the message is unauthenticated, the recipient has no way to separate genuine and fabricated messages. Likewise, the sender has no way to tell that the message has been fabricated.

Attackers may use the aforementioned message modification techniques to implement attacks against air traffic, for example, modification of a trajectory report. Should the attacker remain undetected through a smooth takeover or other means, such an attack could result in erroneous or unnecessary instructions sent from air traffic controllers to other aircraft or in the delayed reaction of critical collision avoidance systems, and in extreme cases, even force other aircraft to make unnecessary, risky maneuvers.

2.8 False Alarm

In a false alarm attack against ADS-B, the attacker makes use of the ADS-B systems' ability to communicate emergencies or other unlawful interferences (e.g., hijacking) to the air traffic control. This attack is committed by deleting, then re-injecting or modifying the targeted aircraft's messages to deliberately suggest a false emergency with the aircraft to air traffic control. The air traffic control tower, law enforcement agencies, and policymakers would subsequently be misinformed and may take counteractions about the "emergency"/"hijacking", etc. With their attention shifted to focus on the aircraft in question the attacker may actually be interested in another aircraft. The attack may additionally launch further processes affecting other aircrafts, including the denial of permission to land or imposing penalty charges for airlines. Recognizing false alarm attacks remains complex matter as transmissions from supposed hijacked aircrafts or aircrafts in distress are typically deemed to be unreliable.

2.9 Aircraft Spoofing

An amalgamation of message deletion and message injection attacks can be used in an aircraft spoofing attack. In a new type of attack, the communication address of the ADS-B system may be spoofed with the intent to outsmart the ADS-B surveillance capabilities. The communication address in transponders can easily be modified and set to a spoofed address by anyone with access to the aircraft cockpit. In an aircraft spoofing attack, any alarm triggered by the discovery of an unanticipated aircraft by other surveillance technologies like PSR would be avoided by designating the aircraft as friendly.

Spoofing an aircraft that may crash into other aircraft or the control tower itself may cause psychological affects for the tower crew, causing them to neglect other tasks (that appear to be less crucial), etc.

This was actually demonstrated on stage at Defcon.

3 Profiles of Potential ADS-B Attackers

Costin and Francillon 2012 suggest that constitution of a proper adversary model for the purpose of evaluating the potential of threats and damages of attacks on the ADS-B system is of paramount importance. Attackers of ADS-B systems may have multiple goals, and thus are typically categorized based on their relationship to the attacked organization, their position within the attacking organization, and their physical location and/or their desired outcomes.

In terms of their relationship to the attacked organization, an attacker can be either external or internal. As ADS-B is unauthenticated and unencrypted, no special organizational knowledge is required. Therefore, an external attack is more likely, as the attacker can execute many low-cost attacks without the need for authentication or authorization; neither would they need any special knowledge or expensive or hard to come by equipment. Internal attacks can be made by a trusted employee (e.g., pilot, air traffic controller, airport technician), but these attacks are much rarer, either as a result of company loyalty or vigorous processes. However, there have been several instances when the motivations of an internal "attacker" were unintentional.

In terms of physical location, most attacks are committed using ground-based attackers that are typically within range and have the capacity to broadcast ADS-B and disable ADS-B transmissions. Since these attacks are limited by range and prohibited by law, ground-based ADS-B attacks are somewhat limited. Modern technologies (such as drones, unmanned aerial vehicles or UAV, autonomous checked luggage, small electronic devices carried on the attacker's body) are much more typically employed.

Finally, the following types of attackers can be categorized according to their motivations and awaited outcomes:

- *Pranksters* are considered the least aggressive of attackers, but their potential influence on aviation security should not be underestimated. A prankster may be a pilot, a technician or more likely a curious technology geek. The "prankster" may remain unaware of the potential significances of his/her actions. Potential "Pranksters" have given lectures on the potential of air traffic attacks at the most recent hacker's conventions. "Pranksters" also represent the largest possible group of attackers.
- *Abusive users* can have a wide range of motivations—from money and fame to conveying messages. These potential attackers may even belong to privacy-breaching groups (e.g., the paparazzi). This potential attackers group can also include aircraft pilots who want to deliberately exploit their access to ADS-B technology and achieve or express goals.
- *Terrorists and criminals* may target the aviation industry with a desire to perpetrate extensive monetary damage, affect the stock market, etc. Criminals are typically motivated by money, while terrorists are motivated by a desire to generate a public feeling of terror, fear of flight, and disruption of normal life.
- *Military and intelligence* attackers tend to have greater access to resources, as well as sophisticated technology and secure information. Such resources may include means for cryptographic code breaking. Such attackers may have goals regarding covert operations or spying and sabotage activity. As a result, these entities often have state-level motives and may group together with a range of military or intelligence agency personnel in their effort to conduct an attack. As the system is mostly civilian, we have not proposed special countermeasures against such adversaries.

4 Proposed Improvements to ADS-B Systems

Among the trivial improvements that can benefit ADS-B usage are using private/public key pair signatures and timestamps on each message that can prevent fabrication and reply attacks and provide efficient authentication. The ground station can also generate queries (challenges) that require specific response to prevent ghost plane injection.

Since the message content will differ in a random way due to signatures, it will also be more difficult to jam the signals.

5 Discussion

The analyses of potential attacks and attacker profiles, as described in the previous sections, suggest that the ADS-B technology and communication protocol suffer from various vulnerabilities that can be exploited to induce potentially massive damage in aerial transport. Many of the proposed attacks can be easily prevented by introduction of state-of-the-art security standards, and thereupon dramatically enhance the safety of aircraft. For instance, by adding signature and integrity verification to ADS-B messages—that is, relatively simple development and modification of the state-of-the-art ADS-B systems—message alteration and injection can be prevented. By implementing trusted computer programming in ADS-B systems, attacks by pilots and airport staff on ADS-B systems can be prevented. We propose that certified ADS-B IN devices can securely verify the validity of the broadcasts of other aircrafts with verification of their digital signatures and remotely attest the broadcasting devices. This way, message injection attacks will become much more difficult to accomplish, or even next to impossible, with standard computational means and without breaking state-of-the-art cryptographic standards. In today's state-of-the-art situation, signature keys are gathered from the broadcasts of aircraft, and as the receiving party cannot fully verify the identity of the transmitting airplane, the broadcast messages cannot be fully trusted. The key distribution problem, i.e., devising a system for providing all the aircraft in the world with unique and trusted signatures, can be easily solved by establishing the certification authority of avionics devices, specifically ADS-B OUT systems. Even today, avionics devices have to pass rigorous regulatory and safety certification procedures, as well as comply with guidelines of other aviation regulatory authorities (i.e., the FAA, EUROCONTROL, and CASA). As part of the proposed certification process, security integrity checks of messages, as well as those of the hardware and software of devices, will be executed. Trusted computing components such as TPM will be implemented for underlying key distribution (Zaidenberg et al. 2015). TPM and other such devices on all communication software allow, in particular, for all the communications devices to be remotely attested by the recipient. The public key distribution of all aircrafts in the area can be handled by control towers.

The proposed communication model consists only of unidirectional broadcasts. Although there is growing research in the field of *aeronautical* ad hoc *networks* that provide multi-hop communication networks (see, for example, Qiu et al. 2015, Rosati et al. 2016), the present state of the art is that real-world implementations are based solely on single-hop, unidirectional broadcast links. Every few hundred milliseconds, aircraft periodically broadcast their positions, velocity, and directions as measured by GPS using plain text messages. This method of constant periodical transmission of one's location is known as *beaconing*. In the current communications model, the transmission's reliability, i.e., the issues of packet loss of data packets of transmitted messages, is yet to be considered. The ADS-B communication protocol does not have means to prevent collisions of transmitted signals. The sender is unaware of the problems in receipt of its messages (if any problems exist). The sender does not retransmit the location packets until it is time to send the next packet. Therefore, there are no guarantees of full and proper receipt of messages by either involved party. (The sender does not know if any or all packets were received; the receiver is unaware of any missing packets). With packet error rates hovering at around a mean of 33%, independent of the channel, it is clear that substantial packet loss is taking place on the physical level. Moreover, the rate of packet loss is expected to increase further as the channel utilization rises over the next decade due to more aircraft using ADS-B when it becomes mandatory and the ever-increasing air traffic, particularly around busy airports.

The ADS-B communication network to and from aircraft is an ad hoc and highly mobile network, as many nodes (aircraft) in the ADS-B network are constantly moving at a velocity of up to 1,000 km/h or more and a relative velocity of up to 2000 km/h. The network is therefore extremely dynamic and often results in communication between two nodes that lasts only a few seconds before the nodes leave communication range. And yet, ongoing message transmission, such as messages indicating the locations of the aircraft involved, is very important, as aircraft trajectories are not physically restricted, although in some areas, common routes and airspaces are defined or restricted by the air traffic control authorities.

Overhauling the existing communication technologies of aircrafts and upgrading current airports to the ADS-B system involves great investment of both monetary and temporal resources. Approximately, $1.7 billion in investments was planned for the upgrade, ADS-B through 2014 by the Federal Aviation Administration (FAA). Furthermore, in order to ensure smooth transition in the upgrade an additional $1 billion of funding projected for the years 2014–2020. However, the exact costs and timelines needed for the full execution of ADS-B and the full realization of ADS-B paybacks remain uncertain at the present. The U.S. Federal Aviation Administration has increased its original estimate for the total assumed costs for ADS-B adaptation by the year 2035 by $400 million, for a total to $4.5 billion, and there remains the potential for additional costs and additional delays due to the ongoing alterations to crucial program activities. Table 3 lists the current FAA's approved funding for key activities involved in the realization of the ADS-B overhaul through the year 2020, revealing mounting ADS-B implementation costs over time.

Table 3 ADS-B estimated costs for key program activities (in millions of USD) *Source* U.S. Federal Aviation Administration (2014)

Key activities	2007 baseline segments 1 and 2 FY 2007–2014	2012 baseline segment 3 FY 2014–2020	Total
Ground infrastructure development and upgrades	$707.9	$19.4	$727.3
Upgrades to the FAA automation platforms	305	5.6	310.6
Avionics development, software testing, and certification for ADS-B Out and ADS-B In standards	45.7	1.3	47
Operational procedures costs and the development and implementation support costs	40.7	172.8	213.5
Subtotal	$1,099.3	$199.1	$1,298.4
Service subscription charges annually	612.1	761.3	1,373.40
Total	$1,711.4	$960.4	$2,671.8

The security concerns listed in this chapter suggest that the Federal Aviation Administration has not been fully aware of all risks and has not provided a secure, full-blown, reliable technology. We have shown that insufficient resources have been provided in order to meet the scope of the complete project. In addition to the aforementioned cybersecurity concerns, certification and flight standard officials have mentioned one additional concern in the adoption of the ADS-B standard. That concern is that ADS-B security may, in fact, encumber the airline industry. It has been suggested by certification and flight standard officials that some (or many) regional inspectors are not equipped to learn and fully understand the Federal Aviation Administration's certification and installation policies for ADS-B systems. This lack of skill frequently results in the potential for poor execution of these systems. One additional concern is that the aircraft maintenance and avionics industry as a whole are currently not outfitted in order to meet the demand for ADS-B installation and modification. Other flight officials have highlighted the possibility that some current GPS and navigation systems are incompatible with ADS-B. All these issues demonstrate the need for further financing and resource allocation, as the Federal Aviation Administration's current ADS-B installation budget is estimated at 4 billion USD excluding the costs that relate to the delays in the certification process, technical errors in implementation, and the unavailability of aircraft during the installation

of avionics systems, as well as loss of profits (U.S. Federal Aviation Administration 2014; also in Gillen and Morrison's 2015, for in-depth analysis of the costs associated with aviation security).

6 Conclusions

The introduction of the ADS-B protocol and communication systems, as well as ADS-B adaptation by virtually all aircraft manufacturers and airlines, is one of the major innovations in the field of air traffic control in recent decades.

ADS-B offers more accurate methods of communications and reporting between ground facilities and aircraft. ADS-B improves the reliability of these channels, allowing more flights to land and take off safely from each airport, and thus improves the safety of passengers. ADS-B provides pilots with real-time data and air traffic information, allowing more accurate decisions to be made. ADS-B can provide more accurate data compared to the PSR data provided to air traffic controllers by through the use of SSR. Additionally, ADS-B can enhance the accuracy of the detection of aircraft positions due to the higher resolution of air traffic information.

However, the development and specification of ADS-B have dangerously ignored the risks of cyber-intrusion. The ADS-B design has not foreseen cyber threats and has not included even the most trivial countermeasures, such as authentication and encryption. Recently, the scopes of potential threats and terrorist-specific interest in airplanes have made ADS-B vulnerabilities a tight spot. Malicious activities are aimed at the intentional delivery of false information to aircraft systems. Such information can mislead pilots and automatic pilots, thus affecting their decision-making and putting their entire aircraft in peril.

ADS-B systems are now widespread through airports all over the world. The abundance of ADS-B-based airports, along with the lack of security countermeasures, presents a potential cyber threat to modern aviation. The cyber threats presented in this chapter stress the need for re-evaluation of the lack of security measures in the ADS-B technology and call for a provision of an advanced technological solution that can maintain ADS-B's benefits but prevent its malicious exploitation.

References

Ali BS (2016) System specifications for developing an automatic dependent surveillance-broadcast (ADS-B) monitoring system. Int J Crit Infrastruct Prot, forthcoming

Ali BS, Majumdar A, Ochieng WY, Schuster W, Chiew TK (2015) A causal factors analysis of aircraft incidents due to radar limitations: The Norway case study. J Air Transp Manag 44–45:103–109

Alonso JJ, Bonnefoy PA, Bono J, Fan A, McConnachie D, Tracey BD, Wolpert D, Xie D (2013) Application of game theoretic models to evaluate airline equipage dynamics of nextgen technologies. In: Aviation technology, integration, and operations conference, Los Angeles, Aug 2013

Benda P (2015) Harnessing advanced technology and process innovations to enhance aviation security. J Air Transp Manag 48:23–25
Costin A, Francillon A (2012) Ghost in the air (Traffic): on insecurity of ADS-B protocol and practical attacks on ADS-B devices. Black hat 2012. https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf
Davidson J (2013) ADS-B requirements coming into effect. universal weather, 23 Sept 2013. http://www.universalweather.com/blog/2013/09/ads-b-requirements-coming-into-effect/. Retrieved 30 Dec 2016
Gillen D, Morrison WG (2015) Aviation security: costing, pricing, finance and performance. J Air Transp Manag 48:1–12
Hainess B (2012) Defcon 20 − Hacker + Airplanes = No good can come of this. https://www.youtube.com/watch?v=CXv1j3GbgLk
Horowitz BM, Santos JR (2009) Runway safety at airports: a systematic approach for implementing ultra-safe options. J Air Transp Manag 15(6):357–362
McCallie D, Butts J, Mills R (2011) Security analysis of the ADS-B implementation in the next generation air transportation system. Int J Crit Infrastruct Prot 4(2):78–87
Perrig A, Tygar D (2003) Secure broadcast communication in wired and wireless networks. Springer Science, New York
Purton L, Abbass H, Alam S (2010) Identification of ADS-B system vulnerabilities and threats. In: Australian transport research forum proceedings, Canberra, pp 1–16, Oct 2010
Qiu Q, Fang Z, Gong C (2015) Study on key techniques of aeronautical ad hoc network MAC and network layer. Proced Eng 99:280–291
Rosati S, Kruzelecki K, Heitz G (2016) Dynamic routing for flying ad hoc networks. IEEE Trans Veh Technol 65(3):1690–1700
Schäfer M, Lenders V, Martinovic I (2013) Experimental analysis of attacks on next generation air traffic communication. In: Jacobson M, Locasto M, Mohassel P, Safavi-Naini R (eds) Applied cryptography and network security. Springer, Heidelberg
Signore TL, Hong Y (2000) Party-line communications in a data link environment. In: Proceedings of the 19th digital avionics systems conference, Philadelphia, Oct 2000
Stark B, Stevenson B, Chen YQ (2013) ADS-B for small unmanned aerial systems: case study and regulatory practices. In: Proceedings of the international conference on unmanned aircraft systems (ICUAS), Atlanta, pp 152–159, May 2013
Strohmeier M, Lenders V, Martinovic I (2013) Security of ADS-B: state of the art and beyond. Report No CS-RR-13-10, Department of Computer Science, University of Oxford
Strohmeier M, Lenders V, Martinovic I (2013) On the security of the automatic dependent surveillance-broadcast protocol, Jul 2013. http://arxiv.org/pdf/1307.3664.pdf
Strohmeier M, Schäfer M, Lenders V (2014) Realities and challenges of nextgen air traffic management: the case of ADS-B. IEEE Commun 52(5):111–118
U.S. Federal Aviation Administration (2014) Office of inspector general ADS-B program audit report. Report No AV-2014-105, U.S. Department of Transportation
Zaidenberg N, Neittaanmäki P, Kiperberg M, Resh A (2015) Trusted computing and TPM in cyber security: analytics, technology and automation. Book 3, pp 205–212. ISBN 978-3-319-18301-5