A Look into the Vulnerabilities of Automatic Dependent Surveillance-Broadcast

Christian Clay
Department of Computing
East Tennessee State University
Johnson City, United States of America
clayck@etsu.edu

Dr. Mohammad Khan
Department of Computing
East Tennessee State University
Johnson City, United States of America
khanms@etsu.edu

Dr. Biju Bajracharya
Department of Computing
East Tennessee State University
Johnson City, United States of America
bajracharya@etsu.edu

***Abstract*—Automatic Dependent Surveillance-Broadcast (ADS-B) is an emerging technology used to aid ATC manage the flow of air traffic. Compared to previous technologies, such as radar, ADS-B provides more accurate positioning data and more efficient traffic management. ADS-B has significant security flaws. ADS-B is an unencrypted protocol and features no authentication methods allowing trivial attacks to be performed over the protocol. This study provides a background on ADS-B and why it is used, an overview of its security vulnerabilities, and an analysis on other researcher's solutions to the protocol's security problem. In addition, A python based simulation was created to interface with X-Plane 11 to visually study ADS-B attacks on aircraft. This study found that in certain scenarios performed in the simulations, ADS-B attacks could have potentially catastrophic consequences.**

***Index Terms*—ADS-B, Aviation, Cybersecurity, ATC, IoT, IoV.**

I. Introduction

Automatic Dependent Surveillance-Broadcast (ADS-B) is a surveillance technology which aids Air Traffic Control (ATC) and maintains an efficient, safe airspace. ADS-B is one of the technologies of the Federal Aviation Administration's (FAA) Next Generation Air Transportation System (NextGen), a multibillion-dollar infrastructure program to modernize the U.S. National Airspace System [1]. The FAA mandate 14 CFR 91.225 states that aircraft must be equipped with ADS-B transponders in order to fly in most airspaces after January 1, 2020. Some drones, such as the ones manufactured by DJI, are also equipped with technology to receive ADS-B data and incorporate it into their systems. ADS-B uses global navigation satellite systems (GNSS) to transmit positional data to air traffic controllers. When compared to primary surveillance radar (PSR) and secondary surveillance radar (SSR), ADS-B allows for more precise and accurate transmissions of information from aircraft to ATC [2], enables more efficient spacing, self-separation, and traffic flow management [3].

ADS-B provides ground-to-air, air-to-air, air-to-ground, and surface message transfers [4]. Two implementations, 1090 MHz Extended Squitter (1090ES) and 978 MHz Universal Access Transceiver (UAT978), exist for relaying messages.

This paper will focus on the 1090ES implementation as chosen by the FAA in 2002 to be used for most purposes; however, it should be noted researchers such as Khandker *et al.* have demonstrated UAT978 and 1090ES implementations to be comparable [5]. An aircraft receives ADS-B messages from active airplanes which can be routed into onboard systems such as the Traffic Collision Avoidance System (TCAS). TCAS displays can be used to give pilots a visual representation of ADS-B data mid-flight. Various models of TCAS displays include plots of airplanes, associated altitudes, and velocity vectors.

ADS-B provides no security features such as encryption or signature-based authentication. Studies show that ADS-B is vulnerable to attacks including jamming, ghost aircraft injection, Denial-of-Service (DoS) attacks, position deviation attacks, and other similar attacks.

The Federal Aviation Administration expects activity at towered airports to increase at an average rate of 1.5 percent a year through 2042 from 50.7 million in 2022 to close to 68.4 million in 2042. The U.S. commercial fleet is forecast to increase from 5,815 in 2021 to 8,894 in 2042, an average annual growth rate of 2.0 percent a year [6]. With an increasingly complex and congested airspace, ADS-B security becomes more important. Aircraft crashes, such as the Air France flight 447, have already occurred due to erroneous and inconsistent data shown on computers [7]. The Bureau of Enquiry and Analysis for Civil Aviation Safety showed that the emotional factors, such as stress and anxiety, of the pilots had a significant effect on the crash. ADS-B attacks could potentially increase the mental load on pilots and lead to loss of life and financial loss. Raising awareness of ADS-B vulnerabilities to pilots and security researchers is the motivation of this paper. The contributions of this work are:

1) A comprehensive and systematic breakdown of ADS-B attacks
2) A simulation of ADS-B attacks on pilots utilizing X-Plane 11 flight simulator and Python 3 scripts
3) A detailed analysis on the simulation and a proposal for further research

II. Related Studies

Following the emergence of ADS-B usage in both civil and commercial aircraft, enforced by the Federal Aviation Administration's mandate 14 CFR 91.225, ADS-B and its

979-8-3503-3286-5/23/31.00

insecurities have captured the attention of researchers around the world.

Costin and Francillon [8] sought to raise awareness of the many ADS-B protocol vulnerabilities and potential attack vectors at the Black Hat 2012 conference. Notably, they discovered that ADS-B had no security mechanisms in place, which could allow malicious actors to perform exploits such as ADS-B message injection, message tampering, and eavesdropping. In addition, they noted that these attacks could be performed trivially and with cheap, easily obtainable hardware and preexisting software.

Shortly after Costin and Francillion's paper, The United States Air Force Institute of Technology published a similar study. Finke *et al.* [9] evaluated the limitations of the ADS-B protocol and explored the feasibility of employing the FFX algorithm in the ADS-B environment. The researchers pointed out that the United States Air Force has successfully implemented asymmetric encryption, a form of encryption consisting of a public and private key pair, for Identification Friend or Foe (IFF) transmissions. They found an encryption algorithm could mitigate some of the security concerns of the ADS-B protocol, key management is an issue that remains to be addressed.

Many studies similar to Finke *et al.'s* paper attempted to address key management, a glaring problem in many cryptographic solutions to ADS-B security. Wu *et al.* [10] proposed one solution to this issue. The researchers shied away from symmetric encryption methods, due to the communication parties being required to pre-share a secret key and the notion that a single private key leak will compromise the security of the entire system. They addressed the issue of key management by proposing that a list of public keys should be uploaded before the aircraft's flight. This proposal remains to be questioned, as many flights could last more than one hour and ICAO data shows that aircraft take off at a rate of over 400 departures per hour [11]. The researchers noted that real-time publication could be communicated over satellite or ground data links; however, that would add both a significant overhead to infrastructure and a complexity to key management.

Braeken [12] introduced a system called Holistic Air Protection (HAP) capable of providing different levels of security by offering authentication of the payload with potential encryption of the identifier and/or payload of the message. Braeken suggested the usage of an elliptic curve qu vanstone mechanism, an authenticated protocol for key agreement, which allows for a small certificate size, protection from key escrow, and allowance for mechanism variables to be sent over an open channel. They noted that, due to the high packet loss of approximately 70%, caused by regulations set in the standard, HAP will not be able to offer the required performance in practice at the moment.

Some authors have attempted to provide mathematical models to ADS-B protocol attacks. Li and Wang [13] analyzed common attack pattern models and designed detection methods according to flight and ground station capabilities. They integrated several detection methods including flight plan validation, single node data detection, and group data detection. Li and Wang found that their sequential collaborative detection strategy was efficient on effectiveness and accuracy.

Researchers applied machine learning attempting to mitigate vulnerabilities in the ADS-B protocol. Machine learning requires no changes to the ADS-B protocol. Luo *et al.* [14] offered an anomaly detection model which considered temporal correlations and distribution characteristics of ADS-B data. They used a variational autoencoder (VAE) to reconstruct ADS-B data and used support vector data description (SVDD) to generate a false positive rate and false negative rate of anomaly detection. They observed their VAE-SVDD model was more adaptable than other machine learning methods and had a lower false negative and false positive rate. The researchers noted that the detection performance is greatly reduced when large amounts of ADS-B data is lost. In theory, jamming attacks could be used to compromise a machine learning model. In addition, they noted that a large amount of packet loss could result in the reduction of detection performance. Braeken stated that, due to regulations set in the standard, ADS-B had a high packet loss of approximately 70% [12]. Since Luo *et al.* used preexisting data from an OpenSky dataset, their machine learning method may be greatly stunted in real world use.

A similar study by Fried *et al.* utilized a non-recurrent autoencoder classifier [15]. Their data showed a consistently lower false positive rate than Luo *et al.'s* data on the categories of constant position deviation attack and random position deviation attack. Fried *et al.* did not bring to attention the issue of packet loss on the machine learning model.

Several researchers have studied alternative protection mechanisms for ADS-B attacks. Rudys *et al.* [16] proposed a method and system architecture based on physical layer signal analysis for verification of received signal authenticity on ADS-B In enabled aircraft. Their proposed methods protect against message injection attacks. Unlike cryptographic approaches, minimal changes to infrastructure are needed, and their proposed changes added additional protection to the ADS-B protocol in events such as a GNSS blackout. In addition, unlike cryptographic and machine learning approaches, Rudys *et al's.* method provided some levels of protection against jamming.

Various researchers have performed attacks on real hardware that utilizes the ADS-B protocol. Khandker *et al.* [5] explored the cybersecurity posture of various mobile cockpit information system (MCIS) setups for ADS-B technology. They tested six portable MCIS devices and 21 electronic flight bag (EFB) devices against radio-link-based attacks by transmission-capable software-defined radio. They found that many devices experienced a system crash due to Packet-level denial of service (DoS) attacks. They fuzzed and tested both hardware and software devices and demonstrated one of the first ever attacks over UAT978, an ADS-B protocol implementation. They also demonstrated that the UAT978 and 1090ES implementations are comparable and vulnerable to generic and available cyber attacks.

Many authors have recently, as of 2022, reviewed the security issues and development flaws of Aeronautical communication protocols. Mäurer *et al.* [17] looked at digital aeronautical communication systems such as ADS-B from a security-oriented point of view and observed that most systems had been thoroughly analyzed within the academic security community with many papers proposing concrete solutions to missing cybersecurity features, and concluded that there is a systematic problem in the design process of aeronautical communication systems. They pointed out many issues arise when common security properties are not met and present aeronautical systems, such as ADS-B, do not offer the desired security properties.

Manesh *et al.* [18] further discussed ADS-B vulnerabilities and attacks that leverage the ADS-B protocol stack. They also presented the security requirements, attack detection techniques and countermeasures, and an overall risk analysis of the ADS-B system. The authors compared both cryptographic and non-cryptographic solutions. The researchers stated that many attacks are difficult to perform and that network equipment is difficult to come by, but researchers such as Costin and Francillon and Khandker *et al.* have shown attacks to be trivial to execute and equipment easy to come by. [8]

Wu *et al.* studied the security issues of the ADS-B system in information leakage and tampering. They showed that a single solution does not fully protect the security of the ADS-B system. [19]

Dave *et al.* [20] systematically analyzed wireless technologies in aviation, including ADS-B, from a communication, navigation, and surveillance perspective, and presented potential software defined radio attacks targeting popular wireless technologies.

III. Types of ADS-B Attacks

The ADS-B protocol is vulnerable to a wide range of attacks as a result of being unencrypted. ADS-B attacks can be difficult to classify, with many attacks being derivatives of others. In this study, three different attack techniques are proposed to provide a unique collection to perform experiments on. The basic algorithm's used in the simulation are provided as well.

A. Selective Jamming Attack

A selective jamming attack comprises of a non-trivial technique where an attacker can effectively drop ADS-B messages from a specific target. Selective jamming differs from traditional jamming attacks with factors in complexity and specificness. The product of this attack can be achieved in a few different ways. An attacker can transmit an inverse of the ADS-B signal, destroying the original message. A similar technique can be performed using properties of constructive interference to induce enough bit errors in the message to be discarded by receiving systems. The least complex technique to perform a selective jamming attack is for an attacker to jam every ADS-B signal and then repeat all messages except the target's.

Algorithm 1: Selective Jamming Attack

Input: Aircraft Target, CSV File
Output: CSV File
Data: Collected RTTFC Data

```
/* This program simulates a selective jamming
   attack, writing the output to the CSV File
   to be used with X-Plane 11                  */
Open (filename)
for row ← 0 to EOF do
    // column 9 is cs_icao (ICAO call sign)
    if column[9] == args.target then
        Remove (current_row)
```

B. Deviation Attack

An attacker replacing genuine positional data with fake data in an ADS-B message can be classified as a deviation attack. This attack can be performed using the same techniques discussed for the selective jamming attack. ADS-B message fields such as longitude, latitude, altitude, and airspeed can be altered by an attacker.

Algorithm 2: Deviation Attack

Input: Aircraft Target, CSV File
Output: CSV File
Data: Collected RTTFC Data

```
/* This program simulates a deviation attack,
   writing the output to the CSV File to be
   used with X-Plane 11                        */
Open (filename)
for row ← 0 to EOF do
    // column 9 is cs_icao (ICAO call sign)
    // column 2 is the latitude, column 3 is the
       longitude
    if column[9] == args.target then
        deviated_coords = (col[2] +
          deviation_value,col[3] + deviation_value)
        WriteValues (deviated_coords,
          current_row)
```

C. Ghost Injection Attack

A ghost injection attack can be defined as an attacker transmitting ADS-B messages for an aircraft that does not exist. In this attack, an attacker could generate positional/dynamic data using an algorithm and assign static data such as the ICAO callsign while crafting the message. Then, the attacker would need to transmit the message over supporting hardware.

Algorithm 3: Ghost Injection Attack

Input: Fake Callsign, CSV File
Output: CSV File
Data: A program generated object we can call "ghost"

```
/* This program simulates a ghost injection
   attack, writing the output to the CSV File
   to be used with X-Plane 11                */
Def GenerateCoordinates():
    track = []
    difference = point_2 - point_1
    // 1000 points are generated but this can be
       easily altered
    num_coords = 1000
    coord_step = 1 / num_coords
    previous_point = point_1
    for i ← 0 to num_coords do
        this_point = previous_point + difference *
         coord_step
        previous_point = this_point
        WriteValues (this_point)

Function Main:
    // generate static data
    // the idea is to build up "ghost" and then
       pass it to generate coords which will do
       the dynamic data generation and write it
       to the csv file
    GenerateAltitude()
    GenerateAttitude()
    GenerateSpeed()
    // generate dynamic data
    GenerateCoordinates()
    return 0
```

D. Summary of Attacks

While the selective jamming and deviation attacks can be complex to execute, the ghost injection attack can be performed trivially. It should be noted that all of the listed attacks can be executed with prewritten scripts and hardware purchased from the internet.

IV. Experiment Setup

Three Python 3.10.6 programs utilizing the provided algorithms were constructed to simulate each type of ADS-B attack on a data set. Each program performed work on an existing data set of live traffic data or generated a data set with "ghost" data points which was then provided to X-Plane 11. The programs outputted data in RealTraffic's comma-separated values (CSV) format. The CSV file was transmitted via UDP to an instance of X-Plane 11 running on the local machine. This specific instance of X-Plane 11 with the LiveTraffic plugin was configured to receive UDP data over port 49005.

LiveTraffic is an X-Plane 11 plugin used to populate the flight simulator with realtime public traffic data from services such as OpenSky Network and ADS-B Exchange; however, in this context, LiveTraffic was used offline to read in the CSV data from the generated files and position the aircraft accordingly. A program called RealTraffic generated the data set of live traffic data which was utilized as inputs to the selective jamming and deviation attack algorithms.

The RealTraffic CSV format is defined as follows:

```
RTTFC, hexid, lat, lon,
baro_alt, baro_rate, gnd, track,
gsp, cs_icao, ac_type, ac_tailno,
from_iata, to_iata, timestamp, source,
cs_iata, msg_type, alt_geom, IAS,
TAS, Mach, track_rate, roll,
mag_heading, true_heading, geom_rate,
emergency, category, nav_qnh,
nav_altitude_mcp, nav_altitude_fms,
nav_heading, nav_modes, seen, rssi,
winddir, windspd, OAT, TAT,
isICAOhex, augmentation_status,
authentication
```

RealTraffic's CSV format has enough similarity with the ADS-B message structure to accurately demonstrate these attacks in the simulation. In particular, both formats have the ICAO aircraft address, position, barometric altitude, and velocity.

One program provided by LiveTraffic, `SendTraffic.py`, was used to send the CSV data to X-Plane 11. The comprehensive full code will be available for viewing on GitHub.

V. Discussion

The following figures visually demonstrate the aircraft positional data as derived from the processes in section four.

A. Selective Jamming Attack

A commercial aircraft approaching John F. Kennedy International Airport (KJFK) was chosen as a target for the selective jamming attack scenario. DAL205 can be seen approaching KJFK. After running the attack and playing the simulation in X-Plane, DAL205 is missing from the list of contacts in figure 2 and figure 3. An attack like this could complicate ATC procedures, confuse pilots and ATC controllers, and potentially cause a collision.

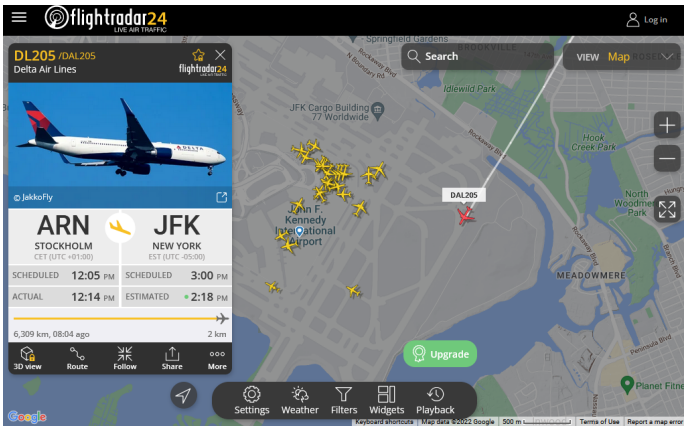

Fig. 1. Our target airplane

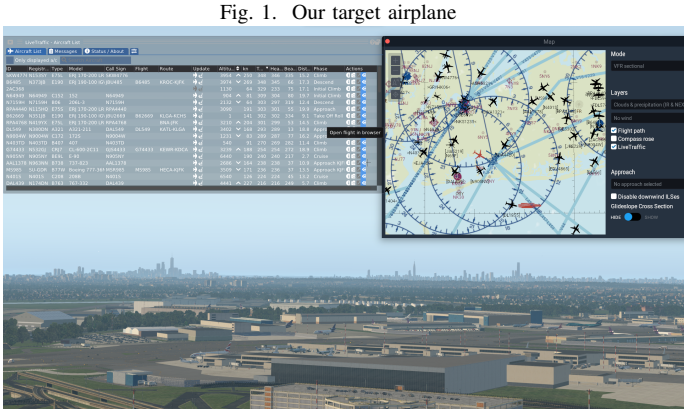

Fig. 2. All of the detected airplanes

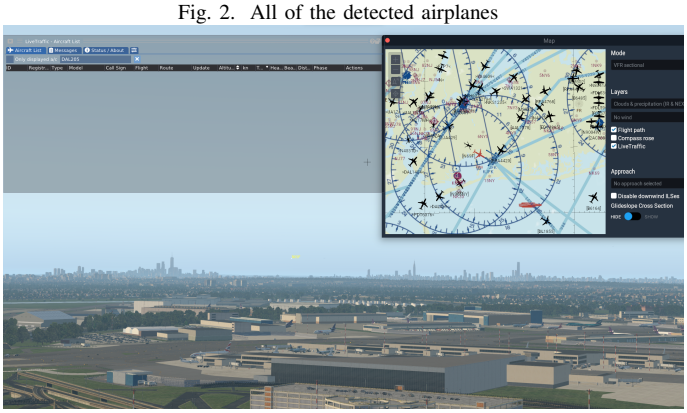

Fig. 3. Our target airplane has been jammed

B. Deviation Attack

For the deviation attack, a scenario where a passenger aircraft's ADS-B messages are altered to show the aircraft flying over the White House is chosen. This particular aircraft was approaching Ronald Reagan Washington National Airport (KDCA) to land. Figure 4 shows the location of the White House on the X-Plane map. After performing the attack and running the simulation, the target plane can be seen headed directly over the White House in figure 5. An attack like this could confuse ATC at KDCA. United States Air Force interceptors could scramble considering similar attacks have occurred, such as the Sept. 11 attacks on the Pentagon, World Trade Center, and failed White House attack.

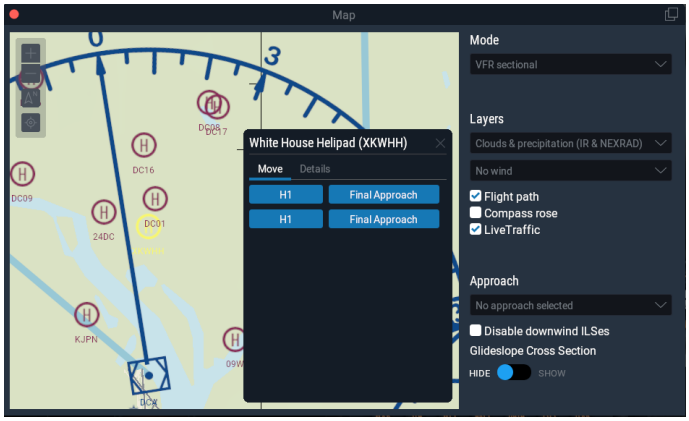

Fig. 4. The location of the White House on the map

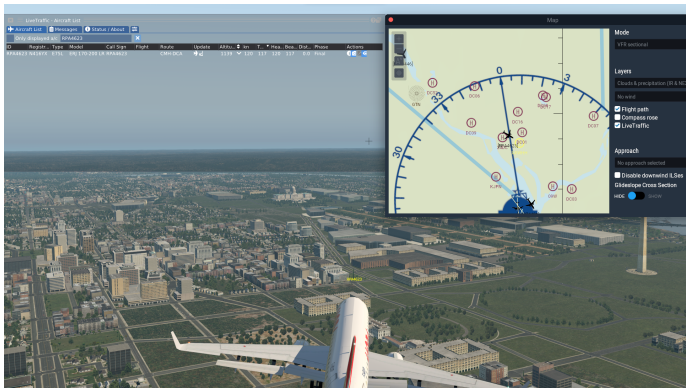

Fig. 5. Our target plane appears to be flying directly over the White House

C. Ghost Injection Attack

In figure 6, A plane can be seen sitting on the end of the runway preparing to take off. A ghost aircraft, marked as an orange diamond on the TCAS display, has been generated to fly towards the taking off aircraft at high speeds and low altitude. Such an attack could cause unwanted control input or audio warnings from the TCAS linked autopilot, disorient the pilots, and cause confusion within the ATC tower. Emotional factors, such as anxiety, could be high considering the similar Tenerife airport disaster, where two passenger jets collided on the runway.

Fig. 6. TCAS displaying a rogue aircraft headed straight over the runway during takeoff

VI. Conclusion

This paper presented an overview of ADS-B, it's vulnerabilities, an analysis of related studies to mitigate these vulnerabilities. Furthermore, a collection of python programs and an experimental framework were created to assist in simulating and visually observing ADS-B attacks. More work should be carried out to refine the python simulations. There is a large gap in research on finding practical solutions to ADS-B insecurities. Further research should be narrowed down to solutions that can be implemented with the current FAA ADS-B infrastructure, allow for possible high packet loss, and comply with the low latency needs of the system. Additionally, solutions that allow for data fusion between existing infrastructure such as primary and secondary search radars, should be encouraged. Such solutions would allow safety measures to be implemented with the shortest amount of time and money.

References

[1] "Next Generation Air Transportation System (nextgen)," Next Generation Air Transportation System (NextGen) — Federal Aviation Administration, 20-Jul-2022. Available: https://www.faa.gov/nextgen.

[2] Automatic Dependent Surveillance— Broadcast (ADS–B) Out Performance Requirements To Support Air Traffic Control (ATC) Service, Vol. 75, No. 103 (May 28, 2010) (14 CFR Part 91). Available: https://www.govinfo.gov/content/pkg/FR-2010-05-28/pdf/2010-12645.pdf.

[3] E. A. Lester and R. J. Hansman, "Benefits and Incentives for ADS-B Equipage in the National Airspace System," MIT International Center for Air Transportation, Aug. 2007. Available: http://dspace.mit.edu/bitstream/handle/1721.1/38468/Lester-ADS-B.pdf.

[4] Technical Provisions for Mode S Services and Extended Squitter, 2nd ed., International Civil Aviation Organization., Montreal, Quebec, 2012.

[5] S. Khandker, H. Turtiainen, A. Costin and T. Hämäläinen, "On the (In)Security of 1090ES and UAT978 Mobile Cockpit Information Systems–An Attacker Perspective on the Availability of ADS-B Safety- and Mission-Critical Systems," in IEEE Access, vol. 10, pp. 37718-37730, 2022, doi: 10.1109/ACCESS.2022.3164704.

[6] Federal Aviation Administration, "FAA Aerospace Forecast Fiscal Years 2022–2042", June 2022, Available: https://www.faa.gov/sites/faa.gov/files/2022-06/FY2022_42_FAA_Aerospace_Forecast.pdf

[7] Bureau d'Enquêtes et d'Analyses, "Final Report On the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro - Paris", July 2012, Available: https://bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf.

[8] Costin, Andrei & Francillon, Aurélien. (2012). Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices.

[9] Finke, Cindy & Butts, Jonathan & Mills, Robert & Grimaila, Michael. (2013). Enhancing the security of aircraft surveillance in the next generation air traffic control system. International Journal of Critical Infrastructure Protection. 6. 3–11. 10.1016/j.ijcip.2013.02.001.

[10] Z. Wu, A. Guo, M. Yue and L. Liu, "An ADS-B Message Authentication Method Based on Certificateless Short Signature," in IEEE Transactions on Aerospace and Electronic Systems, vol. 56, no. 3, pp. 1742-1753, June 2020, doi: 10.1109/TAES.2019.2933957.

[11] "Future of aviation," Future of Aviation. [Online]. Available: https://www.icao.int/Meetings/FutureOfAviation/Pages/default.aspx. [Accessed: 21-Nov-2022].

[12] A. Braeken, "Holistic Air Protection Scheme of ADS-B Communication," in IEEE Access, vol. 7, pp. 65251-65262, 2019, doi: 10.1109/ACCESS.2019.2917793.

[13] Tengyao Li, Buhong Wang, Sequential collaborative detection strategy on ADS-B data attack, International Journal of Critical Infrastructure Protection, Volume 24, 2019, Pages 78-99, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2018.11.003. (https://www.sciencedirect.com/science/article/pii/S1874548218300167)

[14] Peng Luo, Buhong Wang, Tengyao Li, Jiwei Tian, ADS-B anomaly data detection model based on VAE-SVDD, Computers & Security, Volume 104, 2021, 102213, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102213. (https://www.sciencedirect.com/science/article/pii/S0167404821000377)

[15] Asaf Fried, Mark Last, Facing airborne attacks on ADS-B data with autoencoders, Computers & Security, Volume 109, 2021, 102405, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102405. (https://www.sciencedirect.com/science/article/pii/S0167404821002297)

[16] Saulius Rudys, Jurgis Aleksandravicius, Rimvydas Aleksiejunas, Andriy Konovaltsev, Chen Zhu, Lukasz Greda, Physical layer protection for ADS-B against spoofing and jamming, International Journal of Critical Infrastructure Protection, Volume 38, 2022, 100555, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2022.100555. (https://www.sciencedirect.com/science/article/pii/S1874548222000385).

[17] Nils Mäurer, Tobias Guggemos, Thomas Ewert, Thomas Gräupl, Corinna Schmitt, Sophia Grundner-Culemann, Security in Digital Aeronautical Communications A Comprehensive Gap Analysis, International Journal of Critical Infrastructure Protection, Volume 38, 2022, 100549, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2022.100549. (https://www.sciencedirect.com/science/article/pii/S187454822200035X)

[18] Manesh, Mohsen Riahi & Kaabouch, Naima. (2017). Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. International Journal of Critical Infrastructure Protection. 19. 10.1016/j.ijcip.2017.10.002.

[19] Z. Wu, T. Shang and A. Guo, "Security Issues in Automatic Dependent Surveillance - Broadcast (ADS-B): A Survey," in IEEE Access, vol. 8, pp. 122147-122167, 2020, doi: 10.1109/ACCESS.2020.3007182.

[20] Gaurav Dave, Gaurav Choudhary, Vikas Sihag, Ilsun You, Kim-Kwang Raymond Choo, Cyber security challenges in aviation communication, navigation, and surveillance, Computers & Security, Volume 112, 2022, 102516, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102516. (https://www.sciencedirect.com/science/article/pii/S0167404821003400)