IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 20, 2022, accepted March 21, 2022, date of publication April 4, 2022, date of current version April 13, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3164704

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

SYED KHANDKER, HANNU TURTIAINEN, ANDREI COSTIN, AND TIMO HÄMÄLÄINEN
Faculty of Information Technology, University of Jyväskylä, 40014 Jyväskylä, Finland

Corresponding author: Andrei Costin (ancostin@jyu.fi)

This work was supported in part by the Engage Consortium's Knowledge Transfer Network (KTN) Project 204, in part by the Finnish Grid and Cloud Infrastructure—FGCI (persistent identifier urn:nbn:fi:research-infras-2016072533), in part by the Research Dean for Research through the Faculty of Information Technology of the University of Jyväskylä, and in part by the Finnish Cultural Foundation under Grant 00221059.

ABSTRACT Automatic dependent surveillance-broadcast (ADS-B) is a key air surveillance technology and a critical component of next-generation air transportation systems. It significantly simplifies aircraft surveillance technology and improves airborne traffic situational awareness. Many types of mobile cockpit information systems (MCISs) are based on ADS-B technology. MCIS gives pilots the flight and traffic-related information they need. MCIS has two parts: an ADS-B transceiver and an electronic flight bag (EFB) application. The ADS-B transceivers transmit and receive the ADS-B radio signals while the EFB applications hosted on mobile phones display the data. Because they are cheap, lightweight, and easy to install, MCISs became very popular. However, due to the lack of basic security measures, ADS-B technology is vulnerable to cyberattacks, which makes the MCIS inherently exposed to attacks. Attacks are even more likely for the MCIS, because they are power, memory, and computationally constrained. This study explores the cybersecurity posture of various MCIS setups for both types of ADS-B technology: 1090ES and UAT978. Total six portable MCIS devices and 21 EFB applications were tested against radio-link-based attacks by transmission-capable software-defined radio (SDR). Packet-level denial of service (DoS) attacks affected approximately 63% and 37% of 1090ES and UAT978 setups, respectively, while many of them experienced a *system crash*. Our experiments show that DoS attacks on the reception could meaningfully reduce transmission capacity. Our coordinated attack and fuzz tests also reported worrying issues on the MCIS. The consistency of our results on a very broad range of hardware and software configurations indicate the reliability of our proposed methodology as well as the effectiveness and efficiency of our platform.

INDEX TERMS Cybersecurity, attacks, ADS-B, ATC, ATM, UAT978, 1090ES, availability, DoS.

I. INTRODUCTION

THE demand for air transportation has been steadily increasing over the last few decades. The Federal Aviation Administration (FAA) predicts that the number of passengers in commercial aviation will increase to 1.15 billion by 2033 [1]. On the other side of the Atlantic, Eurocontrol predicts 1.6 billion air passengers in its sky per year by the early 2030s [2]. In addition, air cargo transportation, military aircraft, and unmanned aerial vehicles are expected to boost air traffic in the coming years. As a result, the number of aircraft in the airspace will continue to increase, and the airspace will become even more crowded. For reasons such as the safety of navigation, increased airspace capacity, improved flight safety, and future navigation needs, in 2004 the FAA initiated the Next Generation Air Transportation System (NextGen) project. NextGen focuses on the modernization of America's air transportation system to make flying even safer, more efficient, and predictable. One of its aspirations is to gradually transform the current obsolete

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenbao Liu.

and imprecise radar-based air traffic control (ATC) and air traffic management (ATM) systems into a fully digital and satellite-based navigation system. To implement this, the FAA chose the Automatic dependent surveillance-broadcast (ADS-B) system to be a core part of future air navigation technology in the US. In 2011, the EU also mandated a gradual ADS-B requirement starting in June 2020 [3]. The core idea of ADS-B is to periodically broadcast the position and other flight-related information of an aircraft to the ATC and other aircraft in the vicinity via radio frequency (RF) data link. The ADS-B communication system's construction and maintenance costs are expected to be only one-tenth of radar-based navigation [4]. This simplified air navigation technology is gaining popularity all over the world.

Light weight yet effective ADS-B technology is easy to adapt and use. For example, the ADS-B transceiver and smartphone-based mobile cockpit information system (MCIS) is very trendy in the general aviation (GA) sector. In this system, a small ADS-B transceiver is connected to a smartphone or other smart device that displays the navigation data to the pilot through an electronic flight bag (EFB) application. It also transmits global navigation satellite system (GNSS) location, flight information, and other useful information via the ADS-B antenna. MCIS setups cost around 500–1000 dollars. The affordable price and the ease of installation make such setups attractive to pilots of private planes.

Studies show that firmware vulnerabilities are quite common in Internet-of-Things (IoT) and embedded devices [5], [6] and this is also the case for ADS-B technology. The main reason for this insecurity is that ADS-B does not utilize basic security measures such as authentication and encryption. There have been many reports of ADS-B exploitation in the industry [7], [8] and in academia [9]–[12]; therefore, MCISs can be labelled inherently insecure. Even though many studies investigated the security of ADS-B, the security assessment of MCIS remains particularly under-researched. Compared to the powerful transponder or desktop setups, these power-, memory-, and computationally constraint mobile setups could be more vulnerable against cyberattacks. Nonetheless, the use of mobile setups is increasing rapidly. The 21 EFB applications used in this study were downloaded more than 650,000 times from the Google play store, leaving alone other non-tested applications and iOS platform's download numbers aside. Assessing the security of such safety- and mission-critical systems against modern cyberattacks has motivated us to conduct this research. Our main contributions with this work are:

1) We present a systematic and comprehensive study of the (in)security of different commercial-grade MCISs.
2) We test the impacts of the attacks on a large number of EFB applications.
3) To the best of our knowledge, we implement and demonstrate the first-ever ADS-B attacks over UAT978.
4) We demonstrate that the UAT978 and 1090ES implementations are comparably vulnerable to generic and available cyberattacks.

The rest of this article is organized as follows: Section II introduces the relevant background on ADS-B and MCIS. Related studies are discussed in Section III. Details of our test platform and experiment setup are presented in Section IV. Attacks on MCIS are explained in Section V. Attack results are evaluated in Section VI. We discuss some solutions in Section VII. Finally, with Section VIII we conclude this article.

II. BACKGROUND

Modern aviation has relied only on primary surveillance radar (PSR) for a long time. With PSR, the position of the aircraft is measured by the distance and the angle to the radar, but the identity of the aircraft remains unknown. For this purpose, secondary surveillance radar (SSR) was developed. SSR transmits interrogation pulses using RF signals, which are known as Mode A and Mode C. These pulses allow the SSR to continuously interrogate the identity and the barometric altitude of an aircraft. However, the SSR systems have reached the limit of their operational capability. Mode A communication is limited to 4096 unique codes, which poses an issue for very busy modern air transportation. Therefore, a more advanced aircraft communication protocol is needed. Mode S was designed to solve these problems. Mode S is an SSR process that allows selective interrogation of aircraft according to an aircraft's unique 24-bit code called the International Civil Aviation Organization (ICAO or ICAO24) address. Based on Mode S, ADS-B's concept was evolved and it is now considered the future replacement of SSR.

ADS-B is a surveillance technique that relies on aircraft broadcasting their identity, position, and other information derived from onboard systems periodically without the need for interrogation. Besides the ground station, other aircraft also can receive the broadcast to have situational awareness and self-separation. The most important part of the ADS-B is position information, which is determined by GNSS. There are two main functionalities in ADS-B: ADS-B IN and ADS-B OUT. ADS-B IN refers to receiving, processing, and displaying the ADS-B signals from the ATC, aircraft, and other ADS-B OUT-equipped vehicles. ADS-B OUT refers to transmitting an aircraft's position, identity, velocity, and additional flight-related information. For data transmission, two datalink solutions are used as the physical layer for the ADS-B: 1090 MHz Extended Squitter (1090ES) and Universal Access Transceiver at 978 MHz (UAT978). Figure 1 depicts the ADS-B protocol in SSR.

A. 1090ES

1090ES uses the 1090 MHz radio frequency to transmit ADS-B OUT via a Mode-S transponder. Squitter refers to a burst or broadcast of aircraft-tracking data transmitted periodically by a Mode S transponder without interrogation

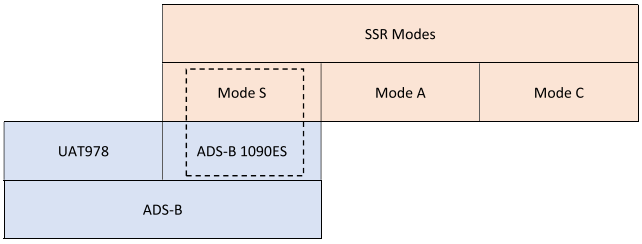

FIGURE 1. ADS-B protocol within SSR.

from the controller's radar. There are two types of squitters: short squitter and extended squitter. As short squitter includes downlink format capability, ICAO24 address, and cyclic redundancy check (CRC). An extended squitter contains all the information of a short squitter but it also includes altitude, position, heading, and velocity. To analyze all the information, we have focused on the extended squitter in this study. The ADS-B 1090ES signal is modulated using pulse position modulation (PPM), which is 112 bits long. A 0.8μs preamble should precede the data block.

B. UAT978

UAT978 applies to aircraft that fly below 18,000 feet in the US, mainly focusing on GA. If an aircraft flies above 18,000 feet, it must be equipped with an ADS-B 1090ES transmitter. Besides navigation, UAT978 also provides services such as flight information system-broadcast (FIS-B) and traffic information system-broadcast (TIS-B). UAT978 uses continuous phase frequency shift keying (CPFSK) modulation with a modulation index of 0.6 and a data rate of 1.041667 Mbps. There are two types of UAT ADS-B downlink messages: basic and long. A basic message contains 144 bits, while a long message has 272 bits. Forward error correction (FEC) is performed using a systematic Reed–Solomon error correction code. For the basic message, the FEC should be 96 bits long, and for the long message, the FEC should be 112 bits long. *1110101011001101110110100100111100010* is the default synchronization bit pattern for both types of messages in UAT978.

C. MOBILE COCKPIT INFORMATION SYSTEM

Compared to SSR, ADS-B is very handy and lightweight. With this simplified version of the air navigation technique, many manufacturers offer portable ADS-B transceivers. Some of these transceivers can fit in the plane's cockpit; some are hung on the window. They transmit and receive the ADS-B signals with a built-in antenna or via the aircraft's antenna port. EFB applications hosted on smartphones or tablets are connected to the transceiver device via WiFi. EFB application displays all the necessary navigation data to the pilot. These portable transceivers are programmable via computer or mobile application. A needed change in the static information (e.g., ICAO24 address, flight number, squawk code) can be done via the nominated program. In contrast,

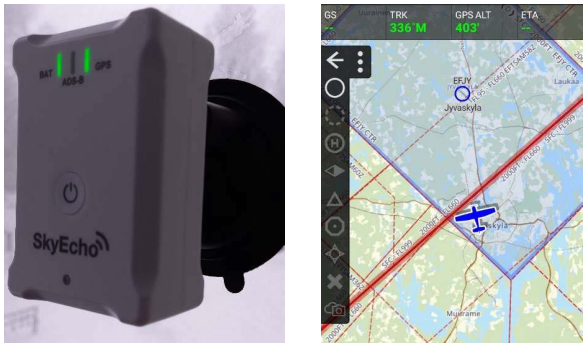

FIGURE 2. SkyEcho2 with OzRunways EFB application.

dynamic data (e.g., location, altitude) are changed automatically via the GNSS receiver of the device. Figure 2 shows a MCIS setup, where data ADS-B data from the SkyEcho2 transceiver is displayed on OzRunways EFB application via WiFi network.

D. TERMINOLOGY CLARIFICATIONS

During different phases of the experiment in this study, we observed different behavior from various tested configurations and MCISs. Below we explain the terminology and meaning of states, as used throughout this paper:

- **Crash:** If a MCIS totally shuts down unexpectedly or ungracefully due to software misbehaviour from the Denial-of-Service (DoS) attack inputs, we classify that as a crash. Commonly, this is the first and immediate step before an attacker can perform remote code execution (RCE) or arbitrary code execution (ACE) attacks- This means the attacker can execute their own code (e.g., ransomware, malware) on the affected system (e.g., device, software, MCIS).
- **Unresponsive:** Some setups did not crash but they could not handle the overwhelming amount of data. As a result, they hang on, which is described as unresponsive.
- **Output clogged:** Some setups, perhaps to avoid a system crash or due to design limitations, can decode or display a limited number of aircraft. The setups cyclically show the ADS-B message within that capacity. Sometimes the ADS-B messages from new aircraft replace the old ones within that limit, or new aircraft from valid ADS-B signals do not appear at all. This situation is called output clogged.
- **Unreadable screen:** When the system is flooded with attacker ADS-B signals, the very large number of data fields and aircraft icons make it impossible to read the screen. However, the system keeps functioning without crashing or becoming unresponsive, though most of the time, the system becomes slower.
- **No effect:** Despite the attack, if the system behaves normally without any visible/observable DoS or side-effects, we called that no effect. However, none of the tested MCISs were able to handle a massive amount of

ADS-B messages (e.g., 200,000 or more). For instance, we observed in many MCISs a significant amount of valid messages being dropped (i.e., the number of processed/displayed ADS-B messages is significantly lower than the number of input ADS-B messages we send). In such cases, we called this no effect but make a side comment that messages were dropped.

III. RELATED STUDIES

Securing the ADS-B has drawn massive attention from researchers due to its direct connection to aircrafts' safe navigation and the effects that failures have on passengers' life. As early as 2004, Krozel and Andrisani [15] reported that data dropouts, erroneous inputs, and deception might degrade data integrity from ADS-B-equipped aircraft. They proposed verification and validation techniques to ensure data integrity using a Kalman filter. The filter would smooth out noise in measured ADS-B signals, identify and suppress erroneous data, coast between data dropouts, and provide the current best state estimates. Since then, there have been many kinds of studies to enhance ADS-B communication's authenticity, security, confidentiality, and integrity [16]–[18].

Sampigethaya [19] focused on the security of ADS-B and proposed a framework for broadcast data link-based navigation and surveillance for the ADS-B-enabled aircraft. Costin and Francillon [9] presented the first public implementation and results of launching ADS-B message injection and spoofing attacks. Strohmeier *et al.* [20] analyzed the 1090 MHz communication channel to understand the behavior of ADS-B 1090ES under increasing traffic load and security challenges. They concluded that the cheap and easily available SDRs posed a significant threat to ADS-B communication and could be used for practical RF-based attacks. Schäfer *et al.* [11] implemented attacks on ADS-B 1090 using USRP N210 as the transmitter and SBS-3 as the receiver. They showed that active attacks such as ghost aircraft injection, ghost aircraft flooding, ground station flooding, and virtual trajectory modification are easily implemented using low-cost devices.

McCallie *et al.* [21] analyzed the security vulnerabilities associated with ADS-B implementations. They classified the attacks and examined the potential damage that the attacks may have on air transportation operations. They stated that ADS-B exploitation could cause disastrous consequences, confusion, aircraft groundings, and in the worst case even plane crashes. Manesh *et al.* [22] used Piccolo autopilot and a portable ground station to observe the autopilot's ghost aircraft injection response. They injected fake ADS-B messages causing ghost aircraft to appear in the vicinity of the Piccolo autopilot (ownership). This caused the autopilot to take evasive measures to avoid the collision. Subsequently, they pushed the ghost aircraft very close to the autopilot. The sudden appearance of false aircraft caused the pilot to execute a steep turn and start descending to regain well-clear as soon as possible. Eskilsson *et al.* [23] demonstrated ADS-B and controller–pilot data link communications (CPDLC) attacks using HackRF. They used freely available *ADSB_Encoder.py* Python script [24] to encode ICAO, latitude, longitude, and altitude information into an IQ file. Later the file was transmitted over the air using a HackRF device and decoded by *dump1090* software. They stated that simple implementation, systematic documentation, and relatively inexpensive equipment could also result in an increasing number of people carrying out an attack. The acquisition of more attacking devices can lead to a large-scale attack.

Tabassum *et al.* [25], [26] concluded ADS-B systems are prone to message and payload loss. In their exploratory analysis, they found that message contents are sometimes inconsistent with nominal conditions. They spotted message dropout, partial message content losses, data drift from the nominal value, and discrepancies between geometric and barometric altitude. They suggested that prior to the complete implementation of ADS-B, it is important to address, understand and monitor these deficiencies.

Air communication modes are also a significant source of big data that must be handled securely and effectively. Mink *et al.* [27] analyzed the unaddressed big data issues for NextGen. They evaluated the NextGen system using five differentiated qualitative characteristics of big data: volume, velocity, variety, veracity, and value. They estimated that all modes (Mode A, C, and S) combined would generate 41 TiB data per year at a velocity of 13 messages per millisecond with no encryption. These findings indicate that the NextGen system has several big data challenges that must be addressed it it is to obtain its maximal potential. However, no such study in Europe has been conducted yet.

Wu *et al.* [10] did a survey of the security issues of ADS-B. They noted that the attack intention could be for economic benefit, terrorism, cyber warfare, or personal interest. The authors modeled the attacker as professional hacking groups, terrorist organizations, military organizations, or amateurs. The survey showed that a single solution does not fully protect the ADS-B system's security. The public key infrastructure or spread spectrum technology can resist most attacks, but there are still deficiencies. They proposed a multi-layered security framework.

Most recently, Leonardi *et al.* [28] studied the effect of jamming attacks in crowd-sourced air traffic surveillance. They found that ground-based communication link jamming can disrupt ADS-B communication more easily and effectively than an air-based jammer and it is easy to implement the attack from the ground. Their work complements our study in the sense that it analyzes DoS attacks on air traffic surveillance (including ADS-B). However, they performed the DoS on the communication link where we performed it on the datalink ADS-B layers.

Dave *et al.* [29] reviewed the cybersecurity challenges in aviation communication, navigation, and surveillance. According to them, as the aviation sector becomes digitized and increasingly reliant on wireless technology, cyberattackers in this sector are also increasing. From old VHF, CPDLC, and PSR to today's ADS-B technology, all are proven to

TABLE 1. Comparison with related work shows different types of ADS-B attacks *demonstrated* throughout the state of the art.

Reference	Injection	Spoofing	Flooding Display (operational DoS)	Software Attacks (application DoS, RCE)	Logical Vulnerabilities	Coordinated Attackers N-to-1	Coordinated Attackers N-to-N	ADS-B UAT978 (any attacks)	Unified Attack Platform (1090ES and UAT978)
Costin et al. [9]	✓	✓	–	–	–	–	–	–	–
Schäfer et al. [11]	✓	✓	✓	–	–	–	–	–	–
Shang et al. [13]	–	–	–	–	–	–	✓(theoretical, simulated)	–	–
Khandker et al. [14]	✓	✓	–	–	✓	✓	✓(supported, untested)	–	–
This work	✓	✓	✓	✓	–	–	–	✓	✓

be vulnerable to cyberattacks. Moreover, the unencrypted nature of ADS-B opens many other attack paradigms. SDR availability is one of the most technical advantages for attackers. Many GA pilots use MCIS, which is very handy and easy to install. Lundberg *et al.* [30] found that this type of mobile setup is not a part of the onboard systems. Thus, its reliability does not meet the standards applied to traditional avionics such as radio technical commission for aeronautics, aeronautical radio incorporated, and the European organisation for civil aviation equipment. They tested three sets of hardware and applications: Appareo Stratus2 receiver with the ForeFlight app, Garmin GDL 39 receiver with the Garmin Pilot app, and SageTech Clarity CL01 with the WingX Pro7 application. They reported that all of them were vulnerable, allowing an attacker to manipulate information presented to the pilot. They recommended a device should sign the data sent from the receiver to the app and vice versa. They also recommend regularly updating the firmware, implementing EFB updates, and to following security-aware software development in order to enhance the security of such mobile cockpit information systems.

Even though the security of ADS-B is heavily researched, Lundberg *et al.* [30] have provided as the sole contribution to MCIS security. However, technology and the demand for MCIS have drastically changed since that study. Many new ADS-B transceivers and software have been developed. Attackers have new tools and ideas as well. Therefore, evaluating the attacks on MCIS against current technology is essential. In comparison with Lundberg *et al.* [30], our work provides comprehensive qualitative and quantitative security feature testing of MCIS. Last but not least, the present paper complements our research work and the results in [14], [31].

Table 1 compares this article's attacks and contributions against the relevant attacks presented in the literature.

IV. EXPERIMENT SETUP

In this section, we describe our approach for attacking MCIS. We performed the experiments in well-controlled lab environments using low power, placing the receivers and transmitters in close proximity, and employing signal attenuators.

A. ATTACK PLATFORM

We used Python programming language to generate the attack payloads. Then a program called GNU radio companion (GRC) was used to produce the IQ values, subsequently transmitted on the air using transmission-enabled SDR. Three transmission-enabled SDRs were used: HackRF, BladeRF, and PlutoSDR. One type of device was sufficient for the attacks in this study. However, we tested three of them to check the feasibility of attacks by heterogeneous devices. To encode the position and altitude into the ADS-B 1090ES signal, we used Yusupov's example script [24]. Later we extended the software's service by writing the codes for other necessary data fields of the ADS-B 1090ES, such as flight information, velocity, and squawk. Yusupov also provided a UAT978 long-message generator [32], and we used that script to experiment with UAT978 data encoding. We slightly modified Larroque's Reed–Solomon codec to generate the FEC [33]. Later, by adding synchronization bits and proper serialization, we generated the final UAT978 attack payload. We used GRC's CPFSK block to transmit the UAT978 signal over the air. Our written software can send *1-to-N* 1090ES and UAT978 messages by *1-to-N* transmitters. It is controlled by several arguments in a command-line interface or with a graphical user interface. To generate a fake ADS-B radio signal, we generate N messages to a CSV file. Then, we create the IQ file of those messages for the 1090ES or UAT978 signal. We duplicate each message 5–10 times to ensure that the tested receiver caught each one. In the end, we transmitted all the N messages very quickly to push the receiving software to its limits. Figure 3 shows how a Python-generated attack payload reaches the MCIS through a radio link. Below we present the ADS-B fields and other parameters that can be set in our software to send individual or multiple messages using 1090ES or UAT978 protocols.

- **icao24:** set an ICAO address to the message.
- **squawk:** set a squawk code to the message.
- **flightnum:** set a flight number.
- **velocity:** set airspeed of the aircraft.
- **lat:** set GPS latitude coordinate.
- **lon:** set GPS longitude coordinate.
- **alt:** set GPS altitude.
- **gain:** set the transmit gain.
- **modetx** set the protocol 1090ES or UAT978.
- **devtx:** set a specific transmitter device.
- **file** set the paths of attack file.
- **ts:** set a timestamp in milliseconds.
- **crc:** set a CRC checksum. For UAT978, this argument refers to the Reed–Solomon FEC.
- **multiprocessing:** set the number of parallel transmitters to use at once.

B. MOBILE COCKPIT INFORMATION DEVICES

We tested six mobile cockpit information devices from different manufacturers. Some of them had ADS-B transmission capability, while others were limited to receive only. Because

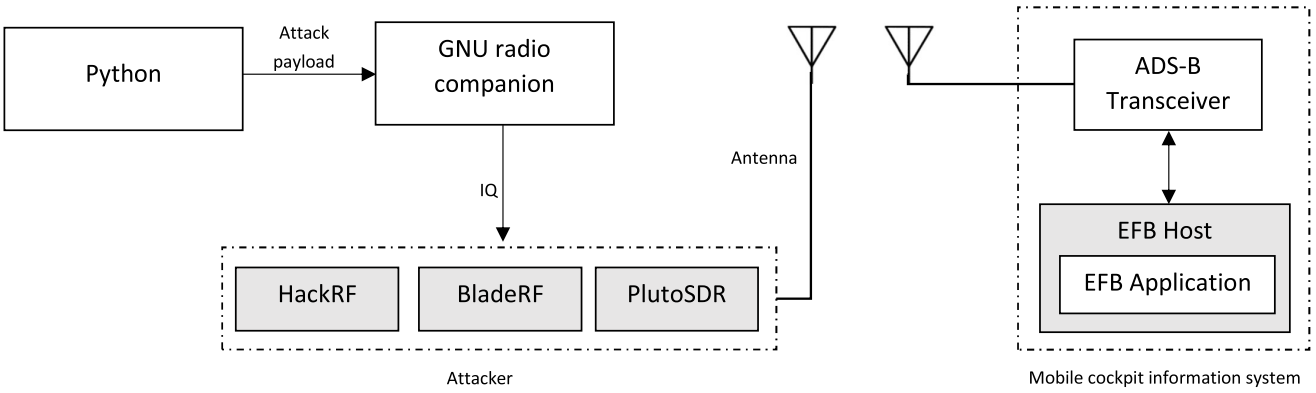

FIGURE 3. Attacker model.

TABLE 2. List of tested mobile cockpit information devices.

Device Name	Receive mode	Transmit mode
uAvionix SkyEcho2	1090ES UAT978	1090ES
uAvionix echoUAT	1090ES UAT978	UAT978
ForeFlight Sentry	1090ES UAT978	No
Garmin GDL 52	1090ES UAT978	No
ADL 180	1090ES	No
Helios Avionics SensorBox	1090ES	No

ADS-B is not fully functional in many parts of the world, some devices did not support transmission. Table 2 shows the list of tested devices.

C. ELECTRONIC FLIGHT BAG APPLICATIONS

A variety of EFB applications support the devices listed in Table 2. However, not all the applications were compatible with all the devices, because some devices use proprietary protocols to exchange data with applications. The most popular protocol is GDL-90 [31], which most applications, such as AvPlan, FLyQ, OzRunways, use. However, the GarminPilot application worked only with the Garmin GDL-52 device, while SensorBox worked with their developed Horizon application. Table 3 shows the list of tested EFB applications. We included the world-wide installation number for Android platform applications (reliably available) to get an idea of how many users could be affected by an application failure. Some applications were not available for a specific platform, device, or our region. We cross-marked if we could not test it on a platform. Tested applications per platform are check-marked. Missing information was marked NA (not available). All the EFB applications did not support all the tests (see VI-D).

TABLE 3. List of tested EFB applications.

Application name	Tested platform		Installation number
	Android	iOS	Android
ADSB Flight Tracker	✓	×	100k+
ADSB Flight Tracker Lite	✓	×	10k+
ADS-B for Pilot PRO	✓	×	10k+
ADL Connect	✓	✓	1k+
AirMate	×	✓	50k+
Avare ADSB	✓	×	100k+
Avare ADSB Pro	✓	×	5k+
AvPlan	✓	✓	1k+
EasyVFR4	✓	✓	1k+
FlyQ	×	✓	10k+
ForeFlight	×	✓	NA
Garmin Pilot	✓	✓	100k+
Horizon	✓	✓	10k+
iFlightPlanner	×	✓	NA
Levil Aviation	×	✓	NA
Naviator	✓	×	100k+
OzRunways	✓	✓	50k+
Pilots Atlas	×	✓	50+
SkyDemon	✓	✓	100k+
Stratus Insight	×	✓	NA
Xradio ADS-B Receiver	✓	×	10k+

V. ATTACKS ON MOBILE COCKPIT INFORMATION SYSTEMS

We implemented RF-link-based attacks on the MCISs. Being portable and lightweight, MCISs have limited computation power, memory capacity, and screen size. Therefore, an ADS-B packet-level DoS attack would be a good choice to check their resilience under a cyberattack. In this study, we primarily focused on DoS attacks on the MCISs. DoS attacks disrupt the availability of services by clogging or

shutting down service entities or networks. The intention is to prevent legitimate users from accessing the service or to prevent legitimate data from reaching its destination. This is accomplished by crashing the service with malicious data or by flooding its input with garbage data or fake messages beyond its capabilities. Because ADS-B does not use authentication or encrypted wireless traffic, it is virtually impossible for it to block a malicious source of fake signals. Therefore, identifying and properly handling the messages is the key to defending against these attacks. The effects of DoS attacks on wireless traffic and wireless sensor networks have been the subject of extensive and prolific research. Osanaiye *et al.* [34] and Ghildiyal *et al.* [35] concluded that DoS attacks could be detrimental to the operation of the system, and defending against them is not trivial. Strohmeier *et al.* [20] addresses the security issues of ADS-B broadcasts, stating that the system is sensitive to RF attacks. DoS attacks can lead to an unresponsive or disabled system, which can lead to poor decision-making within ATC or the malfunction of automated systems because of the authentic information. Our attack system operated on a click-and-run approach, where we first generated random yet valid ADS-B messages and transmitted those messages via transmission-enabled SDRs in a rapid burst. While attacking, we visually observed the effect of the attack and recorded the observations. We noted if the software had any crashes, errors, malfunctions, or unresponsiveness. If not, we noted if the output of the software was clogged enough to miss ADS-B messages.

We also tested coordinated attacks on the MCISs. In these attacks, multiple attackers targeted a single aircraft (or ICAO24 address). Multiple attackers continuously sent sporadic information about the targeted aircraft. To a receiver, this seems like the targeted aircraft is erratically changing its location or other important flight-relevant information. We showed that such attacks lead to logical vulnerabilities [14].

Finally, we conducted fuzz testing for the EFB applications. This is an automated software testing method for finding implementation and input sanitization bugs using intentionally malformed or randomized inputs. The ADS-B devices communicated to the mobile application following some protocols. Among them, GDL-90 is the most popular. By following this protocol but using malformed input, we conducted fuzz tests of the EFB applications [31].

VI. RESULTS AND EVALUATION

We identified many candidate EFB applications for various tests. After a few trial-and-error setups (e.g., successful installation and configuration with hardware), 17 applications were selected for RF-link-based attacks, and 15 applications were selected for fuzz tests. Some applications supported both types of tests, while some were limited to only one. In total, 21 distinct EFB applications were tested in this study. Furthermore, six MCIS devices were tested. Of them, four supported UAT978, while all six supported the 1090ES protocol.

In the receive mode, compared with other MCIS devices such as SkyEcho2 or Sentry, the echoUAT receives and processes both 1090ES and UAT978 messages at a considerably lower ($\approx 100 \times -140\times$ less) number of messages per minute. Subsequently, it forwards a significantly smaller number of ADS-B messages to the decoding application. Therefore, we construe this as being the main reason that none of the tested mobile apps crashed during the DoS attack tests while using echoUAT hardware. SkyEcho2 and Sentry can receive up to 55k distinct ICAO24 addresses per minute, but echoUAT surprisingly has a *hardware limitation* that processes approximately 400 distinct ICAO24 addresses per minute. We are not sure about the core reasons for this functional discrepancy. The maximum transmission rates of messages per second for 1090ES and UAT978 were 6.2 and 1, respectively [36], [37]. However, we have not found the maximum or minimum receiving resolution of the ADS-B system. In our experiment, we found that SensorBox and Garmin GDL-52's decoding capacity was approximately 10,000 and 30 distinct ICAO24 addresses, respectively. Because these two devices work with their proprietary application only, we could not find out whether the limitation was in the hardware or the software. During the test, we found the the ADL 180 device displayed approximately 75 aircraft at a time in both Android and iOS applications.

A. DoS ATTACK RESULTS FOR UAT978

DoS attacks on UAT978 were tested on a number of hardware and software combinations:

- 4 MCIS devices
- 2 mobile operating systems
- 9 EFB applications
- 24 different setup combinations

Overall, our DoS attack affected 9 out of 24 tested configuration for UAT978. The configurations crashed, clogged, or were unresponsive. Some applications were not affected during the DoS attack. Instead they dropped a significant number of legitimate messages and displayed only a tiny portion of the transmitted signal. In practice, with the limited memory, computational power, and display capacity, it is nearly impossible for the MCISs to display and update the ADS-B data for a huge number of distinct aircraft flawlessly (e.g., attack payload of 200,000 ICAO24 address or more). Despite the applications not crashing, we believe that clogging the system and disabling the capability of the system to show all required signals to the user was a successful DoS attack as it disrupted the availability of required data. We marked these situations as non-impacted to distinguish the systems that showed even some resilience to the attacks from the ones that crashed consistently. Therefore, we believe that the non-impacted setups are also not adequate for safety and mission-critical systems. Table 4 presents a summary of the results of the attacks.

TABLE 4. DoS attack results for UAT978.

EFB application	Receiving device	EFB host and operating system	Effect	Time to DoS (seconds)	Observation note
AirMate 2.3	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	90	
AirMate 2.3	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
AvPlan 7.10.7	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	30	
AvPlan 7.10.7	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
AvPlan 1.3.14	SkyEcho2	Samsung A21s & Android 10	**Crash**	60	
AvPlan 1.3.14	echoUAT	Samsung A21s & Android 10	No effect	NA	Valid message dropped
EasyVFR4 4.0.866	SkyEcho2	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
EasyVFR4 4.0.866	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
EasyVFR4 4.0.870	SkyEcho2	Samsung A21s & Android 10	No effect	NA	Valid message dropped
EasyVFR4 4.0.870	echoUAT	Samsung A21s & Android 10	No effect	NA	Valid message dropped
FlyQ EFB 5.0	SkyEcho2	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
FlyQ EFB 5.0	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
ForeFlight 13.0.1	Sentry	iPhone 11 & iOS 14.4	**Crash**	15	
ForeFlight 13.0.1	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	15	
ForeFlight 13.0.1	echoUAT	iPhone 11 & iOS 14.4	No effeact	NA	Valid message dropped
Garmin pilot 10.5.7	GDL 52	iPhone 11 & iOS 14.4	**Output clogged**	10	Maximum 30 aircraft display
Garmin pilot 8.0.0	GDL 52	Samsung A21s & Android 10	**Output clogged**	10	Maximum 30 aircraft display
OzRunways 10.10	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	420	
OzRunways 10.10	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
OzRunways 4.4.1	SkyEcho2	Samsung A21s & Android 10	**Unresponsive**	NA	
OzRunways 4.4.1	echoUAT	Samsung A21s & Android 10	No effect	NA	Valid message dropped
Pilots Atlas 5.11.10	SkyEcho2	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
Stratus Insight 5.17.3	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	60	
Stratus Insight 5.17.3	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped

B. DoS ATTACK RESULTS FOR 1090ES

The attacks on ADS-B 1090ES were tested on a number of hardware and software combinations:

- 6 MCIS devices and 1 RTL-SDR
- 2 mobile operating system
- 15 EFB applications
- 44 total configuration combinations

We found that some EFBs worked with the RTL-SDR through SDR driver v.3.10 in the Android platform. Thus, we used RTL-SDR as the RF front-end for EFBs. Overall, out of 44 tested configurations for DoS attacks on ADS-B 1090ES, 28 were affected. Table 5 presents a summary of the results of the attacks.

C. ADS-B OUT IMPACT

We also investigated the impact of DoS attacks on the performance of ADS-B OUT. Among the MCIS devices, SkyEcho2 transmits the 1090ES signals and echoUAT transmits the UAT978 signals. Table 6 shows the results of the ADS-B OUT impact experiment. In all the ADS-B OUT scenarios, we performed the attacks with a burst of 10k unique ICAO ADS-B messages. However, changing attack intensity numbers (i.e., increasing to bursts of 20k or 30k ICAO24 address) did not significantly change the impact. Each test was were carried out 15 times for each scenario. The results show that the DoS attack on ADS-B IN reduced the ADS-B OUT capacity of SkyEcho2 by approximately 15%, while no significant impact was observed on the echoUAT. However, it is still unclear whether the described impact on SkyEcho2 ADS-B OUT also had a *qualitative impact*. In other words, it remains for future work to investigate if the decline was due to some critical ADS-B OUT messages being dropped or being sent with unacceptable delay. For example, if some ADS-B OUT packets are delayed or dropped altogether, this could dramatically impact the effectiveness of the traffic collision avoidance system.

D. FUZZING

The communication between the MCIS devices and the EFB was mostly conducted via WiFi using the GDL-90 protocol by Garmin. However, the MCIS devices used insecure WiFi connections through which malformed data can be passed to

TABLE 5. DoS attack results for 1090ES.

EFB application	Receiving device	EFB host and operating system	Effect	Time to DoS (seconds)	Observation note
ADL Connect 8.95	ADL 180	iPhone 11 & iOS 14.4	**Unresponsive**	300	
ADL Connect 8.90	ADL 180	Samsung A21s & Android 10	**Output clogged**	60	Maximum 75 aircraft display
ADSB Flight Tracker v 30.9	RTL-SDR	Samsung A21s & Android 10	**Output clogged**	600	
ADSB Flight Tracker Lite v 8.4.1	RTL-SDR	Samsung A21s & Android 10	**Output clogged**	600	
ADS-B for Pilot PRO v 1.8	RTL-SDR	Samsung A21s & Android 10	**Output clogged**	600	
Avare ADSB v 4.9.1	RTL-SDR	Samsung A21s & Android 10	**Output clogged**	600	CRC errors reported
Avare ADSB Pro v 4.9.1	RTL-SDR	Samsung A21s & Android 10	**Output clogged**	600	CRC errors reported
AirMate v 2.3	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	1200	
AirMate v 2.3	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
AvPlan v 7.10.7	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	120	
AvPlan v 7.10.7	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
AvPlan v 7.10.7	ADL 180	iPhone 11 & iOS 14.4	**Output clogged**	60	Maximum 75 aircraft display
AvPlan v 1.3.14	SkyEcho2	Samsung A21s & Android 10	**Crash**	180	
AvPlan v 1.3.14	echoUAT	Samsung A21s & Android 10	No effect	NA	Valid message dropped
AvPlan v 1.3.14	ADL 180	Samsung A21s & Android 10	**Output clogged**	60	Maximum 75 aircraft display
EasyVFR4 v 4.0.866	SkyEcho2	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
EasyVFR4 v 4.0.866	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
EasyVFR4 v 4.0.866	ADL 180	iPhone 11 & iOS 14.4	**Output clogged**	60	Maximum 75 aircraft display
EasyVFR4 v 4.0.870	SkyEcho2	Samsung A21s & Android 10	No effect	NA	Valid message dropped
EasyVFR4 v 4.0.870	echoUAT	Samsung A21s & Android 10	No effect	NA	Valid message dropped
EasyVFR4 v 4.0.870	ADL 180	Samsung A21s & Android 10	**Output clogged**	60	Maximum 75 aircraft display
FlyQ EFB v 5.0	SkyEcho2	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
FlyQ EFB v 5.0	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
FlyQ EFB v 5.0	ADL 180	iPhone 11 & iOS 14.4	**Output clogged**	60	Maximum 75 aircraft display
ForeFlight v 13.0.1	Sentry	iPhone 11 & iOS 14.4	**Crash**	120	
ForeFlight v 13.0.1	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	120	
ForeFlight v 13.0.1	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
ForeFlight v 13.0.1	ADL 180	iPhone 11 & iOS 14.4	**Output clogged**	60	Maximum 75 aircraft display
Garmin pilot 10.5.7	GDL 52	iPhone 11 & iOS 14.4	**Output clogged**	10	Maximum 30 aircraft display
Garmin pilot 8.0.0	GDL 52	Samsung A21s & Android 10	**Output clogged**	10	Maximum 30 aircraft display
Horizon v 3.1	SensorBox	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
Horizon v 3.1	SensorBox	Samsung A21s & Android 10	No effect	NA	Valid message dropped
OzRunways v 10.10	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	120	
OzRunways v 10.10	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
OzRunways v 10.10	ADL 180	iPhone 11 & iOS 14.4	**Output clogged**	60	Maximum 75 aircraft display
OzRunways v 4.4.1	SkyEcho2	Samsung A21s & Android 10	**Unreadable screen**	600	
OzRunways v 4.4.1	echoUAT	Samsung A21s & Android 10	No effect	NA	Valid message dropped
OzRunways v 4.4.1	ADL 180	Samsung A21s & Android 10	**Output clogged**	60	Maximum 75 aircraft display
Pilots Atlas v 5.11.0	SkyEcho2	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
Pilots Atlas v 5.11.0	ADL 180	iPhone 11 & iOS 14.4	**Output clogged**	60	Maximum 75 aircraft display
Stratus Insight v 5.17.3	SkyEcho2	iPhone 11 & iOS 14.4	**Crash**	180	
Stratus Insight v 5.17.3	echoUAT	iPhone 11 & iOS 14.4	No effect	NA	Valid message dropped
Stratus Insight v 5.17.3	ADL 180	iPhone 11 & iOS 14.4	**Output clogged**	60	Maximum 75 aircraft display
Xradio ADS-B Receiver v 5.106	RTL-SDR	Samsung A21s & Android 10	**Crash**	20	

TABLE 6. Impact on ADS-B OUT when executing a DoS attack.

Device	ADS-B OUT support	ADS-B IN support	Numbers of test runs	ADS-B OUT at normal operation (avg. msg/min)	ADS-B OUT at DoS attack (avg. msg/min)	Performance Impact (%)
uAvionics SkyEcho2	1090ES	1090ES	15	268	227	– 15%
		UAT978	15	NA	228	– 15%
uAvionix echoUAT	UAT978	1090ES	15	NA	60	0%
		UAT978	15	60	60	0%

the application, and this may affect the integrity and security of the overall system.

We performed extensive fuzz-testing for the EFBs by using the American fuzzy lop (AFL) Python implementation. AFL was set up to send malformed data to the IP address of the EFB application host. Table 7 highlights our fuzz-testing results. To compare the result with the DoS tests, we also show in Table 7 the corresponding ADS-B DoS test result on corresponding EFBs. In the table, we marked as NA whenever we could not configure an EFB for the test (e.g., due to unavailability, or some other limitation). In addition, some applications (e.g., EFB apps, desktop software) did not work with our MCIS devices. However, they worked with GDL-90 and the fuzzing setup, which can also be seen in Table 7 in their corresponding rows. The results show that 3 out of 7 or approximately 42% applications were affected by the fuzzing test on the Android platform. On the iOS platform, the impact rate was around 53% for 7 affected EFB applications out of 13. Some EFBs applications, such as AvPlan, were crashed by both tests. Some EFB were crashed by one of the tests, while only EasyVFR4 and Pilot Atlas survived both tests.

One particular observation from Table 7 is as follows. If the tested application is vulnerable to ADS-B DoS attacks (e.g., crash), it is extremely likely that it will be found vulnerable by GDL-90 fuzzing with very likely the same consequences (e.g., crash). Examples include AirMate, AvPlan, OzRunways, and Stratus Insight. Likewise, if an application did not present any major issues during ADS-B DoS attacks, it will very likely pass the GDL-90 fuzzing tests. Although, exceptions to this rule are iFlightPlanner and Levil Aviation. This shows strong efficiency and correlation of cybersecurity testing by ADS-B DoS and/or GDL-90 fuzzing. This means that insufficiently secured applications (e.g., see Table 7) that result in serious consequences (e.g., software/EFB crash) will eventually be discovered with sufficient testing when using the methodology and the pentesting platform design that we propose in this paper and in our related works [14], [31].

E. LOGICAL VULNERABILITIES

For an aircraft, ADS-B traffic information in the MCIS updates with the reference of the ICAO24 address. If multiple sources of ADS-B signal containing the same ICAO24 address emit the position information from different places, it appears that aircraft is changing its position erratically.

TABLE 7. Comparing ADS-B DoS results with GDL-90 fuzzing results [31].

Fuzzed EFB (has GDL-90)	Application platform		Result during ADS-B DoS (for comparison)
	Android	iOS	
AirMate	NA	**Crash**	**Crash**
AvPlan	**Crash**	**Crash**	**Crash**
EasyVFR4	No effect	No effect	No effect
FlyQ EFB	NA	**Unresponsive**	No effect
ForeFlight	NA	No effect	**Crash**
Horizon	No effect	No effect	**Clogged**
iFlightPlanner	NA	**Crash**	NA
Levil Aviation	NA	**Crash**	NA
Naviator	**Unresponsive**	NA	NA
OzRunways	**Crash**	**Crash**	**Crash**
Pilots Atlas	NA	No effect	No effect
SkyDemon	No effect	No effect	NA
Stratus Insight	NA	**Crash**	**Crash**
Traffic	No effect	NA	NA
Xavion	NA	No effect	NA

Also, we found that none of the tested MCIS setups check the received data's integrity. For example, many aircraft might have the same flight number or irrational altitude and speed relationship [14]. Such a situation may raise logical vulnerabilities for the MCIS user.

VII. DISCUSSION

We did not observe any hardware crashes. However, this does not mean the devices we tested do not have potential bugs or security vulnerabilities at their hardware or firmware level. In fact, firmware vulnerabilities are quite common in IoT and embedded devices [5], [6] and as Muench *et al.* [38] demonstrated, when memory is corrupted in embedded devices, the results are different from desktop systems. Looking more into the future, we argue that the possibilities of the presented attacks may have impacts beyond the ground-, and aircraft-based ADS-B systems and well into the aerospace domain. The emergence and deployment of satellite-based ADS-B surveillance and receivers [39]–[41] and the increase of ADS-B application in unmanned aerial vehicles (UAVs) [42],

[43] could increase the attack sphere and severely amplify the potential impact of attacks [44].

To address the security vulnerabilities of MCISs demonstrated in this study, we present some solutions. First, the hardware, firmware, and software should be rigorously and continuously tested through automated means such as our platform. The testing should start from the development environment and extend to the operational environment, because development environments do not fully represent the proper use cases. Kacem *et al.* [45] proposed a crypto and radio-location-based hybrid solution to thwart ADS-B attacks. Their proposed framework called ADS-Bsec provides authenticity and integrity for ADS- B packets by using a keyed-hash message authentication code (HMAC). The minimum size of an HMAC is 128 bits which need to be distributed among several ADS-B messages. Although their proposed framework supports backward compatibility with the current ADS-B protocol; however, the CRC checks must be disabled.

Kassab [46] surveyed safety-critical software development and concluded that although safety-critical applications are tested more frequently, quality assurance testing is mostly performed in the very late stages of software development. According to him, the software development practices must be of a higher standard. Possible attack vectors must be identified during software development, and mitigation must be implemented. The iterative development cycle between testing and mitigation implementation should be enforced. For example, a subset of DO-178B (Software Considerations in Airborne Systems and Equipment Certification) could be developed and explicitly required for MCISs. Furthermore, proper memory management must be implemented in the software. The software that crashed, hung up, or went unresponsive does not have appropriate memory management implemented. Therefore, it can be assumed that the EFBs were not tested against DoS attacks during the software development. Researchers have proposed several defense strategies against attacks on ADS-B. However, the effectiveness of the proposed attack detection and prevention methods are yet to be tested in academia and industry. Nonetheless, some defense strategies are available.

Li and Wang [47] proposed a sequential collaborative attack detection strategy based on ADS-B data. According to them, time series and position, the law of motion, historical data, etc., can be used to detect injection, DoS, replay, and ghost attacks. However, the authors did not consider the physical or signal pattern of the attacks. They solely trusted the data. The position-related data of a commercial aircraft change a bit within 30 seconds. However, our study shows that a successful DoS attack can be performed within this short time. In contrast, it may take much more time to apply their proposed method to establish collaboration among the nodes such as ground stations and aircraft in the vicinity to detect the DoS attack. Ying *et al.* [48] proposed a deep neural network (DNN)-based spoofing detector. That method allows a ground station to examine each incoming message based on physical layer features such as IQ samples and phases to flag suspicious messages. The classifier predicts the ICAO24 address of the received ADS-B message and compares it against the claimed ICAO24 address. The rate of the change in the signal phase indicates the carrier frequency offset, which is a sum of frequency offsets and the Doppler shift. They used this feature for classification purposes. However, the main limitation of their method is the supervised learning method for a dynamic environment. An unknown legitimate aircraft flying over the region can initiate a false alarm. Moreover, radio propagation, receiver characteristics, and measurement noise also can affect the system. Our attacking approach can generate any ICAO24 address, which can be regarded as an aircraft flying for the first time in the air space with no historical data, thus bypassing the security or generating a false alarm. Jansen *et al.* [49] proposed a non-invasive trust evaluation system to detect attacks on ADS-B-based air-traffic surveillance. They used a ''Wireless Witnessing'' method to detect the attacks, which is essentially sharing the observations of geographically distributed sensors. An ADS-B receiving sensor should always receive the signals within its coverage. During a spoofing or an injection attack, sensors may receive such ADS-B signals that the signal's encoded position information exceeds the sensor's range. Multiple sensors' wireless witnessing would increase the probability of attack detection. By collecting scores from all the sensors, they calculated a total that indicated and ADS-B attack. Their proposed method is a post-processing method. It is not suitable for a real-time attack. As our study has shown, an attack can be made within a few minutes. A quick DoS attack may cause substantial negative consequences.

VIII. CONCLUSION

This work performed the largest and the most comprehensive cybersecurity assessment of DoS availability attacks on popular MCIS setups by modelling the attacker via remote unauthenticated and unauthorized RF-link. We developed a cybersecurity pentesting platform consisting of a large and comprehensive list of ADS-B transceivers, SDRs, and different EFB applications. Furthermore, we developed a flexible software suite that allows us to perform cybersecurity tests. We tested 44 1090ES and 24 UAT978 MCIS setups, for a total of 68 test configurations. Our ADS-B packet-level DoS attack affected availability on approximately 63% and 37% of 1090ES and UAT978 setups, respectively. The most concerning finding of this study was the very high number of MCISs and ADS-B software that crashed as a result of the performed attacks, where such crashes further expose the affected systems to potential ACE attacks.

The test results show that many, if not most, popular MCISs are vulnerable to many types of cyberattacks, including attacks on availability with resulting software crashes. Relevant overseeing and regulatory bodies (such as FAA, EASA, and ICAO) should investigate these issues further,

and propose practical steps and approaches to ensure further resilience of MCISs to cyberattacks.

ACKNOWLEDGMENT

The authors acknowledge the grants of computer capacity from the Finnish Grid and Cloud Infrastructure (persistent identifier urn:nbn:fi:research-infras-2016072533). Major parts of this research supported by cascade funding from the Engage Consortium's Knowledge Transfer Network (KTN) project "Engage-204-Proof-of-concept: practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity" (SESAR Joint Undertaking under the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No. 783287). All and any results, views, and opinions presented herein are only those of the authors and do not reflect the official position of the European Union (and its organizations and projects, including Horizon 2020 program and Engage KTN). The authors thank Dr. Andrei Costin for facilitating and managing a partially-supporting grant Decision of the Research Dean on research funding within the Faculty (07.04.2021) of the Faculty of Information Technology, University of Jyväskylä (JYU). Hannu Turtiainen also thanks the Finnish Cultural Foundation/Suomen Kulttuurirahasto (https://skr.fi/en) for supporting his Ph.D. dissertation work and research (under grant decision no. 00221059) and the Faculty of Information Technology, JYU, in particular, Prof. Timo Hämäläinen, for partly supporting and supervising his Ph.D. work at JYU in 2021–2022. *(Syed Khandker and Hannu Turtiainen are co-first authors.)*

REFERENCES

[1] The Federal Aviation Administration. (2013). *FAA Aerospace Forecast, Fiscal Years 2013–2033*. Accessed: Feb. 24, 2021. [Online]. Available: https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/2013_forecast.pdf

[2] EUROCONTROL. (2019). *European Aviation in 2040*. Accessed: Mar. 2, 2021. [Online]. Available: https://www.eurocontrol.int/sites/default/files/2019-07/challenges-of-growth-2018-annex1_0.pdf

[3] EASA. (2018). *EASA Seasonal Technical Commission*. Accessed: Mar. 2, 2021. [Online]. Available: https://www.easa.europa.eu/sites/default/files/dfu/EASA_STC_NEWS_JUNE_2018.pdf

[4] Z. Wu, A. Guo, M. Yue, and L. Liu, "An ADS-B message authentication method based on certificateless short signature," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 3, pp. 1742–1753, Jun. 2020.

[5] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares," in *Proc. 23rd USENIX Secur. Symp.*, 2014, pp. 95–110.

[6] A. Costin, A. Zarras, and A. Francillon, "Automated dynamic firmware analysis at scale: A case study on embedded web interfaces," in *Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, May 2016, pp. 437–448.

[7] R. Mark. (2017). *FAA Warns of ADS-B False Alerts*. Accessed: Jun. 6, 2021. [Online]. Available: https://www.flyingmag.com/faa-warns-ads-b-false-alerts

[8] N. Morgan and G. D. Vynck. (2015). *WestJet Says it Never Sent Hijack Alarm, Wasn't in Danger*. Accessed: Jun. 4, 2021. [Online]. Available: https://www.bloomberg.com/news/articles/2015-01-10/westjet-hijack-signal-called-false-alarm

[9] A. Costin and A. Francillon, "Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," in *Proc. Black Hat USA*, 2012, pp. 1–12.

[10] Z. Wu, T. Shang, and A. Guo, "Security issues in automatic dependent surveillance—Broadcast (ADS-B): A survey," *IEEE Access*, vol. 8, pp. 122147–122167, 2020.

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

[12] M. R. Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system," *Int. J. Crit. Infrastruct. Protection*, vol. 19, pp. 16–31, Dec. 2017.

[13] F. Shang, B. Wang, F. Yan, and T. Li, "Multidevice false data injection attack models of ADS-B multilateration systems," *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, Mar. 2019.

[14] S. Khandker, H. Turtiainen, A. Costin, and T. Hamalainen, "Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures," *IEEE Trans. Aerosp. Electron. Syst.*, early access, Dec. 31, 2021, doi: 10.1109/TAES.2021.3139559.

[15] J. Krozel, D. Andrisani, M. Ayoubi, T. Hoshizaki, and C. Schwalm, "Aircraft ADS-B data integrity check," in *Proc. AIAA 4th Aviation Technol., Integr. Oper. (ATIO) Forum*, Sep. 2004, p.6263.

[16] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ADS-B research," in *Proc. IEEE Aerosp. Conf.*, Mar. 2006, pp. 1–7.

[17] R. G. Wood, "A security risk analysis of the data communications network proposed in the NextGen air traffic control system," Ph.D. dissertation, School Educ. Found., Leadership Aviation, Oklahoma State Univ., Stillwater, OK, USA, 2009.

[18] L. Purton, H. Abbass, and S. Alam, "Identification of ADS-B system vulnerabilities and threats," in *Proc. 33rd Australas. Transp. Res. Forum (ATRF)*, 2010, pp. 1–16.

[19] K. Sampigethaya, R. Poovendran, and L. Bushnell, "A framework for securing future e-enabled aircraft navigation and surveillance," in *Proc. AIAA Infotech@Aerosp. Conf.*, Apr. 2009, pp. 1–10.

[20] M. Strohmeier, M. Schafer, V. Lenders, and I. Martinovic, "Realities and challenges of NextGen air traffic management: The case of ADS-B," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 111–118, May 2014.

[21] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *Int. J. Crit. Infrastruct. Protect.*, vol. 4, no. 2, pp. 78–87, Aug. 2011.

[22] M. R. Manesh, M. Mullins, K. Foerster, and N. Kaabouch, "A preliminary effort toward investigating the impacts of ADS-B message injection attack," in *Proc. IEEE Aerosp. Conf.*, Mar. 2018, pp. 1–6.

[23] S. Eskilsson, H. Gustafsson, S. Khan, and A. Gurtov, "Demonstrating ADS-B AND CPDLC attacks with software-defined radio," in *Proc. Integr. Commun. Navigat. Surveill. Conf. (ICNS)*, Sep. 2020, pp. 1B2-1–1B2-9.

[24] L. Yusupov. (2021). *Lyusupov/ADSB-Out*. Accessed: Feb. 24, 2021. [Online]. Available: https://github.com/lyusupov/ADSB-Out

[25] A. Tabassum, N. Allen, and W. Semke, "ADS-B message contents evaluation and breakdown of anomalies," in *Proc. IEEE/AIAA 36th Digit. Avionics Syst. Conf. (DASC)*, Sep. 2017, pp. 1–8.

[26] A. Tabassum and W. Semke, "UAT ADS-B data anomalies and the effect of flight parameters on dropout occurrences," *Data*, vol. 3, no. 2, p. 19, Jun. 2018.

[27] D. Mink, W. B. Glisson, R. Benton, and K.-K. R. Choo, "Manipulating the five V's in the next generation air transportation system," in *Security and Privacy in Communication Networks*, X. Lin, A. Ghorbani, K. Ren, S. Zhu, and A. Zhang, Eds. Cham, Switzerland: Springer, 2018, pp. 271–282.

[28] M. Leonardi, M. Strohmeier, and V. Lenders, "On jamming attacks in crowdsourced air traffic surveillance," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 6, pp. 44–54, Jun. 2021.

[29] G. Dave, G. Choudhary, V. Sihag, I. You, and K.-K.-R. Choo, "Cyber security challenges in aviation communication, navigation, and surveillance," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102516.

[30] D. Lundberg, B. Farinholt, E. Sullivan, R. Mast, S. Checkoway, S. Savage, A. C. Snoeren, and K. Levchenko, "On the security of mobile cockpit information systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 633–645.

[31] H. Turtiainen, A. Costin, S. Khandker, and T. Hamalainen, "GDL90fuzz: Fuzzing—GDL-90 data interface specification within aviation software and avionics devices—A cybersecurity pentesting perspective," *IEEE Access*, vol. 10, pp. 21554–21562, 2022.

[32] L. Yusupov. (2021). *Lyusupov/UAT-Test-Signal*. Accessed: Feb. 24, 2021. [Online]. Available: https://github.com/lyusupov/UAT-test-signal

[33] S. Larroque. (2020). *Tomerfiliba/Reedsolomon*. Accessed: Mar. 15, 2021. [Online]. Available: https://github.com/tomerfiliba/reedsolomon/blob/master/reedsolo.py
[34] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, 2018.
[35] S. Ghildiyal, A. K. Mishra, A. Gupta, and N. Garg, "Analysis of denial of service (DOS) attacks in wireless sensor networks," *Int. J. Res. Eng. Technol.*, vol. 3, no. 22, pp. 140–143, Jun. 2014.
[36] P. Prakash, A. Abdelhadi, and M. Pan, "Secure authentication of ADS-B aircraft communications using retroactive key publication," 2019, *arXiv:1907.04909*.
[37] ICAO. (2003) *Manual for the Universal Access Transceiver (UAT)*. Accessed: Mar. 2, 2021. [Online]. Available: https://www.icao.int/safety/acp/Inactiveworkinggroupslibrary/ACP-WG-C-UA T-2/UAT-SWG02-WP04-DraftTechManualV0-1.pdf
[38] M. Muench, J. Stijohann, F. Kargl, A. Francillon, and D. Balzarotti, "What you corrupt is not what you crash: Challenges in fuzzing embedded devices," in *Proc. NDSS*, 2018, pp. 1–15.
[39] M. A. Garcia, J. Stafford, J. Minnix, and J. Dolan, "Aireon space based ADS-B performance model," in *Proc. Integr. Commun., Navigat. Surveill. Conf. (ICNS)*, 2015, pp. C2-1–C2-10.
[40] M. Garcia, J. Dolan, and A. Hoag, "Aireon's initial on-orbit performance analysis of space-based ADS-B," in *Proc. Integr. Commun., Navigat. Surveill. Conf. (ICNS)*, Apr. 2017, pp. 1–28.
[41] S. Kaul, "Smallsats, hosted payload, aircraft safety, and ADS-B navigation services," in *Handbook of Small Satellites: Technology, Design, Manufacture, Applications, Economics and Regulation*. Cham, Switzerland: Springer, 2020, pp. 1011–1027.
[42] A. Pahsa, P. Kaya, G. Alat, and B. Baykal, "Integrating navigation & surveillance of unmanned air vehicles into the civilian national airspaces by using ADS-B applications," in *Proc. Integr. Commun., Navigat., Surveill. Conf.*, May 2011, pp. J7-1–J7-7.
[43] M. Consiglio, B. J. Duffy, S. Balachandran, L. Glaab, and C. Munoz, "Sense and avoid characterization of the independent configurable architecture for reliable operations of unmanned systems," NASA, Washington, DC, USA, Tech. Rep., 2019. [Online]. Available: https://www.nasa.gov/sites/default/files/atoms/files/2019_consiglio_isaac_atm2019_tpsas_v9-508_0.pdf
[44] J. Pavur, M. Strohmeier, V. Lenders, and I. Martinovic, "In the same boat: On small satellites, big rockets, and cyber trust," in *Proc. 13th Int. Conf. Cyber Conflict (CyCon)*, May 2021, pp. 151–169.
[45] T. Kacem, A. Barreto, D. Wijesekera, and P. Costa, "ADS-Bsec: A novel framework to secure ADS-B," *ICT Exp.*, vol. 3, no. 4, pp. 160–163, Dec. 2017.
[46] M. Kassab, "Testing practices of software in safety critical systems: Industrial survey," in *Proc. 20th Int. Conf. Enterprise Inf. Syst.*, 2018, pp. 359–367.
[47] T. Li and B. Wang, "Sequential collaborative detection strategy on ADS-B data attack," *Int. J. Crit. Infrastruct. Protection*, vol. 24, pp. 78–99, Mar. 2019.
[48] X. Ying, J. Mazer, G. Bernieri, M. Conti, L. Bushnell, and R. Poovendran, "Detecting ADS-B spoofing attacks using deep neural networks," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 187–195.
[49] K. Jansen, L. Niu, N. Xue, I. Martinovic, and C. Pöpper, "Trust the crowd: Wireless witnessing to detect attacks on ADS-B-based air-traffic surveillance," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2021, pp. 1–17.

SYED KHANDKER received the M.Sc. degree in web intelligence and service engineering from the University of Jyväskylä, Finland, in 2016, where he is currently pursuing the Ph.D. degree with the Faculty of Information Technology. Since his childhood, he has been a Radio Enthusiast and holds an Amateur Radio Operator License. His research interests include the field of RF fingerprint positioning, automatic dependent surveillance-broadcast, automatic identification systems, wireless communications, and artificial intelligence.

HANNU TURTIAINEN received the B.Sc. degree in electronics engineering from the University of Applied Sciences, Jyväskylä, Finland, and the M.Sc. degree in cybersecurity, in 2020. He is currently pursuing the Ph.D. degree in software and communication technology with the University of Jyväskylä. His research interests include machine learning and artificial intelligence in the cybersecurity and digital privacy field. He is also working in the IoT field as a Cybersecurity Engineer and a Software Engineer at Binare.io, a deep-tech cybersecurity spin-off from the University of Jyväskylä.

ANDREI COSTIN received the Ph.D. degree from EURECOM/Telecom ParisTech, in 2015, under co-supervision of Prof. Francilon and Prof. Balzarotti. He is currently a Senior Lecturer/an Assistant Professor in cybersecurity with the University of Jyväskylä, Finland, with a particular focus on IoT/firmware cybersecurity and digital privacy. He has been publishing and presenting at more than 45 top international cybersecurity venues, both academic (Usenix Security and ACM ASIACCS) and industrial (BalckHat, CCC, and HackInTheBox). He is the author of the first practical ADS-B attacks (BlackHat 2012) and has literally established the large-scale automated firmware analysis research areas (Usenix Security 2014)—these two works are considered seminal in their respective areas, being also most cited at the same time. He is also the CEO/Co-Founder of Binare.io, a deep-tech cybersecurity spin-off from the University of Jyväskylä, focused on innovation and tech-transfer related to IoT cybersecurity.

TIMO HÄMÄLÄINEN has over 25 years of research and teaching experience related to computer networks. He has lead tens of external funded network management related projects. He has launched and leads Master Programs with the University of Jyväskylä (currently SW and Communications Engineering) and teaches network management related courses. He has more than 200 internationally peer-reviewed publications and he has supervised 36 Ph.D. theses. His current research interests include wireless/wired network resource management (the IoT, SDN, and NFV) and network security.