Choudhary *et al. J Surveill Secur Saf* 2022;3:27-40
DOI: 10.20517/jsss.2021.17

Journal of Surveillance, Security and Safety

Original Article

Open Access

Aviation attacks based on ILS and VOR vulnerabilities

Gaurav Choudhary[1], Vikas Sihag[2], Shristi Gupta[3], Shishir Kumar Shandilya[3]

[1]DTU Compute, Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU),Kongens Lyngby, 2800 Denmark.
[2]Department of Cyber Security, Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, 342037, India.
[3]School of Computer Science and Engineering (SCSE),VIT Bhopal University, Bhopal, 466114, India.

Correspondence to: Dr. Gaurav Choudhary, DTU Compute, Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Kongens Lyngby, 2800, Denmark. E-mail: gauravchoudhary7777@gmail.com;

How to cite this article: Choudhary C, Sihag V, Gupta S, Shandilya SK. Aviation attacks based on ILS and VOR vulnerabilities. *J Surveill Secur Saf* 2022;3:27-40. http://dx.doi.org/10.20517/jsss.2021.17

Received: 23 Oct 2021 **First Decision:** 24 Nov 2021 **Revised:** 11 Jan 2022 **Accepted:** 1 Apr 2022 **Published:** 20 May 2022

Academic Editor: Kshirasagar S. Naik **Copy Editor:** Xi-Jun Chen **Production Editor:** Xi-Jun Chen

Abstract

Aim: As the aviation industry grows more digital and reliant on wireless technology, it has grown more appealing to cyber criminals, including nation-state actors and terrorists. Vulnerabilities in a wide range of networked devices and (sub)systems, as well as their implementations and design defects, can be used to carry out malicious operations. The purpose of this study is to provide a comprehensive survey threats on aviation communication models.

Methods We describe an overview of aviation threat model and attacks. A detailed taxonomy predicated on security vulnerability is presented. Further, this paper discusses the research aspects and challenges to be taken care of in aviation security and communication Finally, we conclude with a summary of the current state of threats and their consequences for widely-used aviation models.

Results The main findings of this study is to introduce fundamental security vulnerabilities of aviation model and classify into categories to efficiently analyze them. Vulnerabilities of VOR, ILS systems and their impact are also discussed. Moreover, we describe and assess mitigation systems to defense these attacks.

Conclusion We conclude that the aviation system is still exposed to various attacks. We examine key technological challenges that have been serving as a deterrent to adopting more secure alternative approaches, as well as research avenues where further progress is needed.

Table 1. List of air traffic control technologies

ADS-B	Automatic dependent surveillance-broadcast
SSR	Secondary surveillance radar
PSR	Primary surveillance radar
MLAT	Multilateration
VHF	Very high frequency voice transmission
CPDLC	Controller-pilot data link communication

Keywords: Aviation, attacks, vulnerability, ILS, VOR

INTRODUCTION

An aircraft ecology is complicated, with several components. Air traffic management (ATM), which includes various communication, navigation, and surveillance (CNS) systems, is an example of critical infrastructural components of the aviation ecosystem. To aid navigation, communication systems typically consist of devices that permit the flow of information among devices, systems, and users [e.g., air traffic control (ATC) and pilot]. Surveillance is made easier by data from communication and navigation systems (such as onboard devices and radars), as well as supporting infrastructure. The amount of air travel adds to the difficulty of guaranteeing aviation cybersecurity[1]. A lot of effort has been made in envisioning better and safer systems that not only serve as a minor upgrade but significantly improve upon the existing state of the art. The aviation security market was worth USD 10.78 billion in 2019 and is expected to reach USD 11.45 billion by 2027 at a CAGR of 7.62%[2]. Aircraft manufacturers have not yet fully adopted the practice of proactively redesigning communication systems within the aircraft. More secure aviation communication systems have been long overdue, arguing that cases of existing vulnerabilities being exploited historically are sparse. The absence of worldwide standards and regulations within the aviation sector has also been a point of contention in the implementation of stronger security standards.

Researchers have explored security flaws in widely adopted methods such as automatic dependent surveillance-broadcast (ADS-B) and proposed changes that enhance security while maintaining an acceptable efficiency and latency trade-off. They cover a range of sub-domains:

- Judiciary challenges in enforcing new security models.
- Technical challenges in implementing new methods while ensuring backward compatibility.
- Threat and attack analysis of widely adopted methods and technologies.
- Behavioral analysis of different stakeholders.

While these works add tremendous value to the field, a few concerning patterns are observed. There has been very little testing on real aircraft, and the majority of findings have been obtained by running simulations in a sandbox or by reverse engineering proprietary hardware and constructing prototypes. Methods with strict security constraints are seen to be less efficient and, as a result, introduce latency in the process. The list of air traffic control technologies is shown in Table 1.

Problem statement and our contributions

The aviation sector is the most prominent candidate in the emerging civilian and military activities market. In the aviation system, instead of a wired system, wireless technology is used; thus, these systems have maximum possibilities of attacks. Many departments lie under the aviation sector and still have vulnerabilities to attacks. The existing technology of aviation is not using hiding techniques and still uses Morse code techniques. The frequency-dependent devices are more vulnerable because most devices are open source.

1. This paper presents the state of the art for existing security issues with aviation, surveillance, and commu-

nication.

2. It also identifies new variants of threats and security vulnerabilities and discusses the possible countermeasures to these attacks.
3. A detailed taxonomy predicated on security vulnerability is also discussed. Further, this paper discusses the research aspects and challenges to be taken care of in aviation security and communication.

The purpose of this work is to examine threats in aviation system, as well as to give a taxonomy and demonstration of attack. Furthermore, we examine the vulnerabilities and recent assaults on the aviation sector, as well as their future trends.

The paper is organized as follows. In Section 2, the related work is presented. In Section 3, aviation communication technologies are discussed. Section 4 provides a state-of-the-art overview of the current and upcoming aviation attack vectors. The current technical issues in ILS and VOR are discussed in Section 5. Finally, Section 6 concludes the paper.

RELATED WORK

Attacks on aviation systems and their different subsystems are unlikely to go away in the near future. This emphasizes the significance of cybersecurity in the aviation business. Security researchers are trying to make air travel more secure. Ashdown[3] discussed judiciary challenges in designing better security models for aviation systems, especially in an international context, such as the lack of enforcement power held by aviation laws to hold attackers accountable. Suggestions are further made on how organizations such as the International Civil Aviation Organization (ICAO) should handle attacks that are likely to happen as aviation systems transition from legacy communication infrastructure based on radar and ground-based air traffic control to modern communication technologies that tap into the Internet.

The accelerated advancement of unmanned aerial vehicles (UAVs), because of their decreasing price, inflated aerial moveables, and broad scope of implementations, put forward the latest prospects for a line of work in public and private applications. The residing UTM's range is relevant to VLL airspaces that reinforce BVLOS indefinite levels; nonetheless, in the future, UTM will focus on higher airspace levels together with PAVs and CAVs. The faultless BVLOS functioning in both VLL and higher altitudes is indispensable since it accomplishes manned/unmanned airspace integration and collaboration in the middle of them. The aDAA should utilize 360-degree radial computer vision-based spotting mechanics that acknowledge reliable as well as shielded BVLOS functioning. The instantaneous DAA could be accomplished by utilizing conglomerate transmission mechanics such as broadcasting location, V2X communication, satellite, optical, and wireless communication[4–6].

WID is a wireless communication structure that makes use of drones as infrastructure that propounds aerial wireless following appliances where ground connectivity is not effortlessly attainable. The definite principle upper hand of WID is the popular wireless network investiture. NR-U WID authorizes wireless technologies to be executed at a low price and with high certainty. The utilization of an unauthorized band has a power ordinance that limits NR-U to be constricted within the compact range region. This is a crucial pitfall for the terrestrial NR-U as the signal, for the most part, agonizes from trail deprivation attenuation, in addition to fading effects[7,8]. The trade for making use of compact unmanned aerial systems (sUAS) to examine the profitability of transmission plus distribution infrastructure is anticipated to extend to 4.1B dollars annually by 2024. Given the fact of diminutive measurement along with the heaviness limitations, sUAS cannot be provided with supplementary assets for security, which makes sUAS uncomplicated to attack set side by side with military UAS, but military UAS are more susceptible to attack due to the way they are utilized. Major (6 attacks) and minor UAS (5 attacks) attacks are equitably endangered; however, small materialistically available

Table 2. Possible attacks concerning technologies. (P1: Jamming, P2: Injection, P3: Message inception, P4: Message modification, P5:DOS, P6: Intrusion, P7: Spoofing)

Technology	P1	P2	P3	P4	P5	P6	P7	Ref's
ADS-B	Y	Y	Y	Y		Y	Y	[14–17]
SSR	Y	Y		Y	Y			[18,19]
PSR	Y							[20–22]
MLAT		Y					Y	[23,24]
VHF	Y	Y			Y		Y	[25–27]
ACARS		Y	Y			Y		[19,28]
CPDLC	Y	Y	Y	Y	Y		Y	[29–32]

Table 3. Security issues concerning technologies. (R1: Confidentiality, R2: Authentication, R3: Privacy, R4: Integrity, R5: Availability)

Technology	R1	R2	R3	R4	R5	Ref's
ADS-B	Y	Y	Y	Y	Y	[14,15,17]
VHF		Y		Y		[26]
CPDLC	Y	Y		Y		[19,33]
ACARS	Y	Y	Y	Y		[29–32]
Secure-ACARS			Y		Y	[34]

UAS might be more at risk than large UAS. There has been a narrowly single openly announced authentic attack on sUAS, and it was a GPS Jamming attack. A questionable GPS jamming along with a GPS spoofing attack was implemented on RQ-170, an enormous fastened wing UAV by Lockheed Martin, ensuring the apprehension of the UAV with slight destruction on its left wing[9,10].

Nguyen *et al.*[11] proposed the utilization of phase-shift keying modulation to increase the payload of current automatic dependent surveillance-broadcast (ADS-B) and use this extra space as a digital signature to authenticate messages in aviation systems. This method requires no additional modifications to integrate with existing systems (as the resultant modulation on combining standard pulse-position modulation and phase-shift keying modulation is compatible with ADS-B In/Out and can operate along with ADS-B. While this study was performed in the laboratory using hardware-in-the-loop (HIL) simulations and actual flights, tests in commercial airlines are yet to be conducted, which would be a more vital testament to the method's effectiveness. Santamarta.[12,13] uncovered vulnerabilities within SATCOM systems that would allow unauthenticated malicious actors to abuse and remotely take control of devices within the system by exploiting backdoors, hardcoded credentials, undocumented and insecure protocols, and weak encryption algorithms. They detailed several methods to exploit vulnerabilities within the system in question, ranging from methods as simple as sending a specially crafted SMS message to gaining access to credentials concealed within the system. While the implications of this study are wide-reaching, it is to be noted that all testing was done without physical access to the equipment. Instead, research was performed by reverse engineering all the devices. The possible attacks concerning technologies are shown in Table 2, while security issues concerning technologies are shown in Table 3.

COMMUNICATIONS, NAVIGATION, AND SURVEILLANCE

The Air Route Traffic Control Center is responsible for controlling the air traffic traveling at and above 18,000 feet within designated control sectors. Terminal Radar Approach Control (TRACON) Facility controls aircraft within a 30 nautical mile radius of the larger airports within the ATC system. Airport control towers are responsible for controlling aircraft within a five nautical mile radius of the airport[35]. An exemplary view of aviation communication technologies is shown in Figure 1.

The National Airways System (NAS) has three techniques to track aircraft: procedural ATC, primary surveillance radar (PSR), and secondary surveillance radar (SSR). Procedural ATC is a dependent surveillance tech-

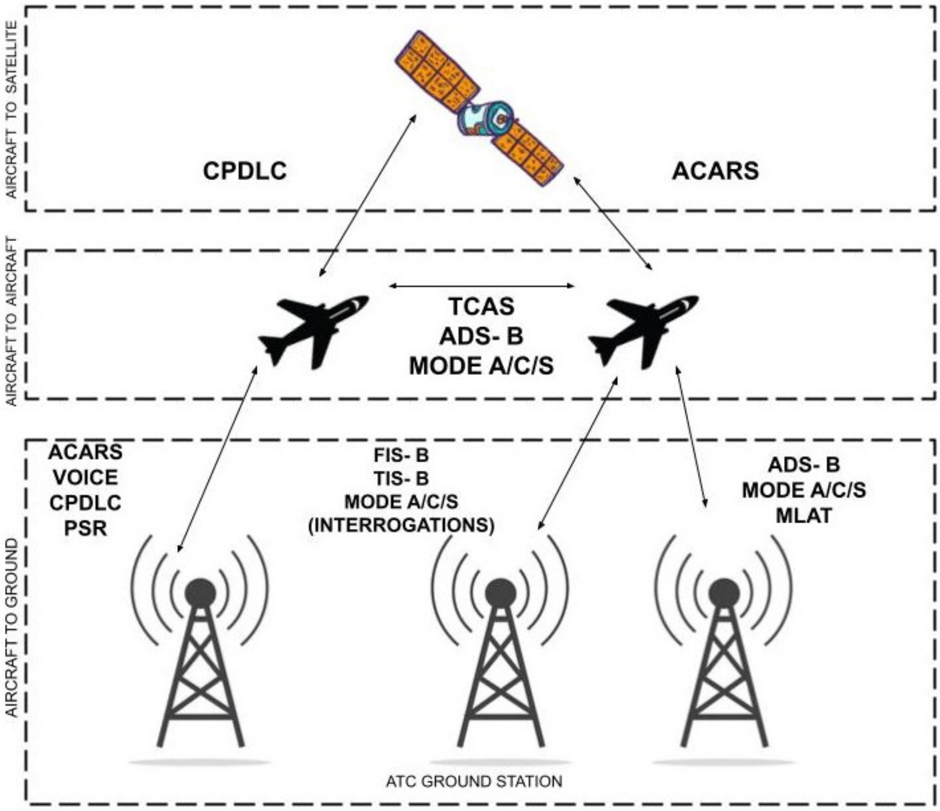


Figure 1. An exemplary scenario of aviation communication technologies[36].

nique; it depends on input from individual aircraft. Pilots are required to report their position using radio communications periodically. It is predominately used in little or no radar coverage areas such as the ocean and remote area flight operations. PSR is an independent and non-cooperative surveillance radar system; it does not depend on any input from the aircraft. TRACON is used in busy terminal areas. SSR is a partially independent and cooperative surveillance radar system; it determines the aircraft's position by combining radar target return and aircraft transponder reply when interrogated by a ground station. It is used for route tracking.

ATC has been in service for more than half a century. Its installation, operation, and maintenance are challenging and costly, especially the ground-based SSR and PSR radar systems. With increased air traffic and aging equipment, although the air transportation system performs adequately, it is reaching its limit. The expected growth in air traffic will likely create costly flight delays and increased flight safety hazards unless a new system is launched. The FAA began working on the Next Generation Air Transportation System (NextGen) in response to these concerns. NextGen is primarily focused on significantly increasing the safety and capacity of air transportation operations. The upgrade requires the actual conversion of the entire NAS, including incorporating satellite-based technologies for surveillance operations and the shutdown of many ground-based systems currently in use. The critical component of NextGen is a position reporting and tracking technology called automatic dependent surveillance-broadcast (ADS-B).

Air traffic control

ATC is the major body in the air traffic management system that connects with both planes and satellites. ATC connects ground networks and data centers, whereas data centers link to the Internet. Satellite and other components, such as aircraft networks, are handled by ground networks. Air traffic controllers use radar to

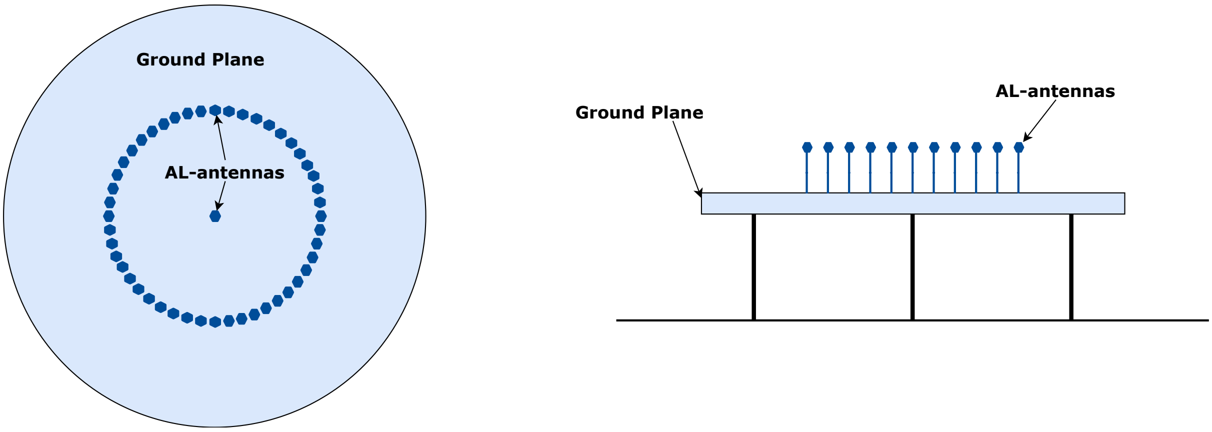


Figure 2. Top-view and side-view of DVOR antenna consisting of 48 Alford Loop antennas.

Table 4. Comparison between the popular SDRs

	RTL-SDR	Hack RF	USRP	BLADE-RF
Frequency	500 kHz to 1.7 GHz	10 MHz to 6 GHz	56 MHz to 6 GHz	300MHz to 3.8GHz
Tx / Rx	Receiver	Transfer and Receiver	Transfer and Receiver	Transfer and Receiver
ADC Bits	8-bit Resolution	8-bit Resolution	12-bit Resolution	12-bit Resolution
Price	30$	300$	50$	800$

track the position of aircraft in their allotted zone and communicate with pilots through radio. ATC employs the VOR (VHF omnidirectional range) system for aircraft location. The conventional navigation system that operates over VHF is VOR. It transmits VHF radio beacons that provide the station's name as well as the angle to its position relative to the directional signals. Because of the radial character of the received signal, the aircraft can compute the direction it is traveling from the VOR system. The frequency range of the VOR is 112–118 MHz. Doppler VOR (DVOR), a type of VOR consisting of circular installed antennas, is shown in Figure 2.

ADS-B

ADS-B (automatic dependent surveillance-broadcast) technology allows the aircraft to identify its location using satellite navigation and broadcast it on a regular basis; surveillance technology allows the aircraft to be followed.

The lack of security in the ADS-B protocol has been highlighted by security experts and hackers[14]. The research demonstrates the physical restrictions necessary to manage the 1090 MHz ADS-B channel, such as distance and transmitting power[15,16]. Although no security problems have been documented thus far, exploit kits for faking ADS-B signals are widely accessible online, implying that assaults are simply a matter of time[17].

As authorities make the use of ADS-B mandatory in all flights under instrument flight rules, with no exceptions for military, government, or business flights, tracking sensitive aircraft data has become easier. There have been instances of classified military operations being disclosed as a result of the use of ADS-B data[37].

Primary surveillance radar (PSR)

PSR is the conventional radar sensor that sends an electromagnetic wave and receives back the reflected wave from the target (aircraft) to calculate its latitude, altitude, etc. As the detection is based on the reflection of its signal, it is not possible to modify or inject any message. The jamming attack can be performed, but the requirements to carry out the attack makes it infeasible.

Table 5. List of information services technologies

ACARS	Aircraft Communications Addressing and Reporting System
TCAS	Traffic Alert and Collision Avoidance System
FIS-B	Flight Information System - Broadcast
TIS-B	Traffic Information System - Broadcast

Secondary surveillance radar (SSR)

SSR is a radar system that responds to interrogation signals from aircraft equipped with radar transponders by delivering encoded data such as the aircraft's identifying code, altitude, etc. Because SSR/Mode S share the same underlying protocol as ADS-B, they are also vulnerable[17]. Further investigation reveals the possibility of radio frequency interference, which might result in ghost aircraft, jamming, or transponder lockouts[19].

In June 2014, a real-world event involving SSR jamming and over-interrogation caused multiple airplanes to vanish from controllers' radar screens in Central Europe on two different occasions[18]. The European Aviation Safety Agency inquiry, however, was unable to identify the perpetrator and declared the attack to be non-malicious. Security experts emphasize that such hostile assaults are feasible[18]. Software-defined radio (SDR) tools play an integral part in attack execution. A comparison of popular SDRs is presented in Table 4.

MLAT

Multilateration is a technique for establishing the position of a target (aircraft) by measuring the "time of arrival"(TOA) of energy waves whose speed is known. MLAT is a verification mechanism for unauthenticated wireless networks that works in tandem with ADS-B. If the ADS-B message received is incorrect, the sender's position can still be determined. Despite the fact that MLAT provides security through physical layer attributes and is difficult to manipulate, real-world MLAT systems rely on combining location and message contents to validate a target's identity and altitude. Because of the reliability of MLAT over ADS-B, the entire system is open to exploits such as Mode A/C/S or ADS-B. A well-coordinated and synchronized attacker might influence the time of arrival of a message to an MLAT system's dispersed receivers and hence fabricate location data[23].

Very high frequency (VHF)

The primary mode of communication utilized to send ATC commands to the aircraft and the pilot's requests to the ATC is voice communication. While VHF remains the primary ATC communication channel to this day, the analog nature of the channel, as well as the fact that broadcasts are not encrypted, allow nearly anybody to listen in on local voice communication and identify aircraft registration numbers. An investigation showed that speech recognition algorithms could be used to automate and scale a tracking strategy, even if blocking measures were utilized to prevent public websites from obtaining the data[38]. Real-world instances of air traffic controller impersonation in Turkish airspace[25] and at Melbourne airport created concern for controllers.

Controlled pilot data link communication (CPDLC)

CPDLC is a two-way data-link technology that allows controllers to send non-urgent strategic signals to an aircraft instead of using voice communications. CPDLC has no authentication or confidentiality and is vulnerable to a variety of attack vectors. The German Aerospace Center has described how CPDLC technology may be deceived and spammed[19]. While there have been no public allegations of malicious tampering, CPDLC's resistance to outside manipulation is unclear. Several investigations have been undertaken for duplicate, delayed, or missing CPDLC communications and unauthenticated ground station logins.

Information services

Technology that provides the pilot with information to improve their situational awareness is known as information services. A list of information services technologies is presented in Table 5.

ACARS

ACARS is a digital communication system that allows messages to be sent between aircraft and ground stations. ACARS may be classified into three kinds based on their contents: air traffic control (ATC), aeronautical operation control (AOC), and airline administrative control (AAC). ACARS flaws can allow for falsified ATC certifications via unauthenticated data transfers. Hugo Teso demonstrated the possibilities of exploiting ACARS to remotely attack a flight management system (FMS) using second-hand gear in 2013. The authors of[32] investigated the insertion of external ACARS signals into FMS.

AVIATION ATTACK VECTORS

Aviation communication technologies being wireless makes access control mechanisms challenging. In addition, the broadcast nature of radiofrequency makes the system prone to various attacks. These attacks have become practical and easily accessible due to the escalation of software-developed radios (SDRs).

Message injection

Because the data connection layer lacks any authentication measures, it is simple for an attacker to construct a transmitter capable of producing appropriately modulated and structured signals. Schafer *et al.*[15] used an example to demonstrate how ADS-B may be attacked with minimum knowledge and easily available basic technological tools. Other implications of failing to authenticate include denying that a node transmitted any data or claiming to have received contradictory data, making accountability difficult.

Message deletion

Using destructive or constructive interference, attackers can physically destroy genuine communications. Constructive interference can induce bit errors into a message making it unreadable. Due to the necessity of precise and complex timing requirements, destructive interference can be quite difficult. If the conditions are satisfied, the attacker can send the inverse of the signal broadcast by the genuine sender. Because of superposition, the signal may be attenuated or eliminated.

Message modification

Messages can be modified during transmission using techniques such as overshadowing and bit-flipping. During overshadowing, the attacker sends a powerful signal to replace all or part of the target message. The attacker uses bit-flipping to superimpose the signal, altering any number of bits from 1 to 0 or 0 to 1. The authors of[39,40]discussed the feasibility of message manipulation.

Eavesdropping

Listening in on an unsecured broadcast transmission is referred to as eavesdropping. When the protocol broadcasts unsecured communications, attackers may easily eavesdrop. It can be used as a reconnaissance medium for other strikes. It is practically impossible to detect and presents privacy issues. The authors of[41,42] provided a way for users to monitor and track the aircraft's present position, trip trajectory, and other details, thus posing concerns.

Jamming

The attacker uses a sufficiently high-power frequency to prevent a single node or numerous participants from transmitting or receiving messages. Because of the critical nature of data, the impact of jamming in aviation communication technology is significantly greater than in other wireless technologies. Jamming of ATC frequencies is illegal, and while it is feasible to track down the perpetrator, it is insufficient to preserve the ATC system. Wilhelm *et al.*[43] discussed the viability of jamming.

Defense methods

It is fair to assume that wireless networks always include listeners; hence, the traditional attacker–defender concept would be limited. The cyber-physical method focuses on threat detection and only deploys extra protection if considered essential. Physical layer security ensures confidentiality by utilizing the physical layer features of the communication [44]. Time differences of arrival [23,45], Doppler shifts [46], direction of arrival [47], and angle of arrival [48] are different ways to identify spoofing attack. Methods of watermarking/fingerprinting are used to identify and authenticate wireless devices and their users. Watermarking entails inserting indicators throughout the communication stream that authentication algorithms can exploit. Fingerprinting works by taking advantage of technological flaws in the hardware and software that enable the connection. Researchers investigated the possibility of watermarking VHF communication [49,50], exploiting differences in transponder implementations on the data-link layer [51].

The application of machine learning to identify intrusion in the wireless aviation system may be handled in two ways. The first is classification, in which the characteristics of a specific valid user are discovered and confirmed against saved patterns. The use of behavioral biometric speech data from pilots conversing over VHF radio is presented in [25,52]. Second, there is anomaly detection, in which the characteristics of the system's normal state are learned over time, and any divergence from these patterns is alerted for security issues. The authors of[25,52] identified aberrant stress levels and anxiety in the pilot's speech through VHF radio, thereby attempting to discover abnormalities. To avoid false-positives, careful calibration and engineering are necessary.

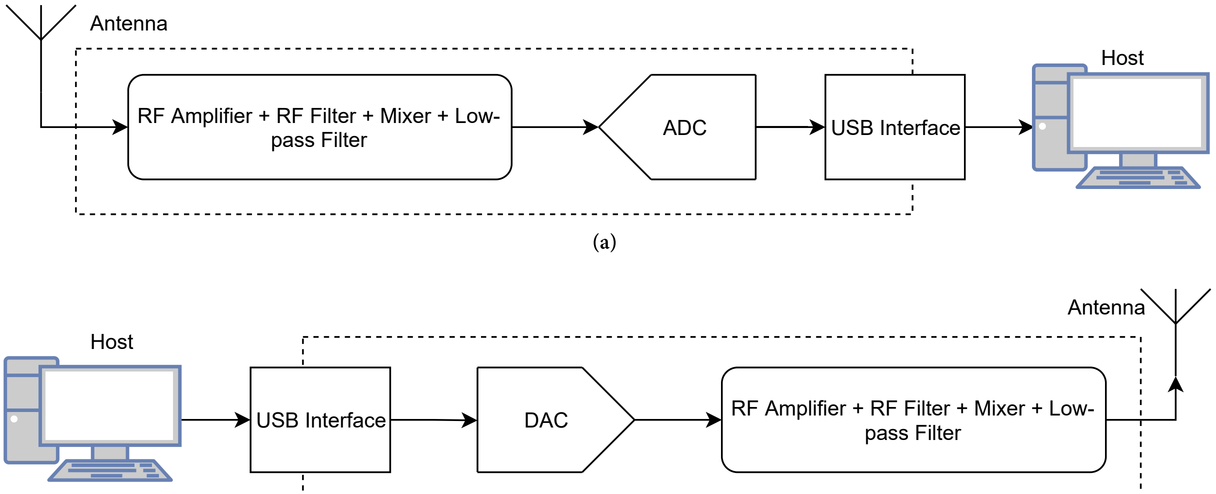
The authors of[53] discussed the changes in the user experience that occur with the introduction of formal security requirements into an ATC system and investigated whether ADS-B position reports should be utilized as an aircraft's main location source. The authors of[54] summarized the risk and requirement analysis carried out via the ATM system utilizing VHF communication. Creating rules and procedures aids in the enhancement of aviation communication security; they are far easier to implement in practice than implementing new systems and technological adjustments to existing technology. The authors of[55] comprehensively reviewed aviation security activities undertaken by aviation authorities and industry. Flight simulators should simulate cyber attacks [56,57] and release test-run data and mitigation options [58,59] Aviation professionals and passengers should be educated about the ADS-B security vulnerabilities [58].

Cryptography can efficiently protect the secrecy, authenticity, and integrity of any digital communication's content. The research provides experimental techniques that might solve the security issues associated with unencrypted communication in ACARS [31], ADS-B [60], and CPDLC [61,62]. Identity-based encryption [63,64], format preserving encryption [65–67], retro-active publication [68,69], use of public key infrastructure [70,71], and blockchain [72,73] are also being studied.

SATCOM is used in aviation, maritime, and military sections. The military department is secured, but aviation is not as secured as others. The malware used to attack the aviation SATCOM is the "Mirai BOT". It is a very effective malware, and it is associated with IoT devices. This bot is used to attack the antenna control unit, which is essential for aviation SATCOM. On a recent international flight, two unexpected things were observed: the IP address assigned to the passenger is routable, and something else is a network scanning the routable IPs by an external host. The security analyst has a crucial role in aviation [74]. After landing, the security analyst scanned the internal network and said that the FTP, TELNET, and WWW were available for specific IPs. He discovered that the backdoor on the plane's satellite modern data unit (MDU) and the public IP are trying to connect to the telnet service. Further analysis discovered that the compromised router is a part of the IoT botnet, and it is collateral damage. The security analyst finally concluded that the attacker was trying to "brute force attack" SATCOM. The IT infrastructure of the aviation industry is a segment commonly attacked using malwares [75]. The most prominent of them being malicious hacking (ransomware, phishing and DDoS) with intent to gain unauthorised access [76–79]. Block diagram depicting working of SDR in operation is given in

Table 6. The existing and new security vulnerabilities of ATC protocols

Channel	Protocols [36]	Vulnerabilities [36]	Recently Identified	Mitigation
Communication	VHF, CPDLC, DSCN	DOS, AM, Jamming, Spoof clearance, replay attacks, Malware passive attacks [80]	Voice based(VHF CPDLC) SDR Attacks, Satellite useful information extraction(DSCN) attacks	Blocked the open aviation frequency, Used high power LNAs
Navigation	DME, VOR, ILS	Time base attacks, DOS attacks,GPS jamming, Spoofing, RAIM attacks [81]	Frequency based SDR attack(DME), Beacons transmission in Morse code (VOR) SDR attack, Eavesdropping and Landing disruption by manipulating the frequency, Wireless attack by SDR (ILS)	Using suitable Encryption technique instead of Morse code, Blocked open and easily available Aviation frequency, High power LNAs
Surveillance	PSR, SSR, ADS-B	Time base attacks, Jamming on operation frequency, Emergency code injection, Jamming, Amplification Attack, DOS attack, Passive or Active attacks, Jamming and Injection attacks [82]	1030MHz frequency based attack and 1090MHz replay attack (SSR), 1090MHz Aircraft messages alteration attack(ADS-B)	Blocked 1030 and 1090MHz frequency which is open source, Used High end LNAs


Antenna
RF Amplifier + RF Filter + Mixer + Low-pass Filter
ADC
USB Interface
Host
Host
USB Interface
DAC
RF Amplifier + RF Filter + Mixer + Low-pass Filter
Antenna

(a)

(b)

Figure 3. Block diagram of SDR (a) receiver and (b) transmitter.

Figure 3. The existing and new security vulnerabilities of ATC protocols are shown in Table 6.

CURRENT TECHNICAL ISSUES

Current ATC Communication systems such as ADS-B, primarily being broadcast based, are prone to eavesdropping and are limited because they need to balance elements of the CIA (confidentiality, integrity, and availability) triad. Stronger encryption processes mean lower real-time relaying of messages. Relying on a fixed range of frequencies also means that it is prone to jamming and does not offer HA capabilities. Current systems are also not designed for redundancy. Aircraft fallback to legacy systems when primary systems fail, but this process is inherently flawed, as falling back to previous generation technologies leads to a significant degradation in the quality of service. This means that an attacker could lead an aircraft into losing several navigational capabilities effortlessly. FAA's NextGen model bypasses the challenges of being a broadcast-based system by routing data over the Internet. While it removes many challenges associated with broadcasting to all listeners in proximity, it has to tackle a whole new range of cybersecurity challenges that any service operating through the Internet would face.

Components within ATC systems could take up to two decades to go from development to full deployment. In a world where new software updates are shipped daily, such an elongated development lifecycle is a significant setback that massively slows down the adoption of newer technologies. The slow certification process is a substantial component of this challenge, adding many years between development and deployment phases. Compatibility requirements enforced by law are another judicial component that slows down the development of new and better technologies within the ATC system. While it might seem pragmatic to reuse existing hardware components and delay significant redesigns, the cost of clearing technological backlogs in the long term is immense.

CONCLUSION

Technological advancements were made to meet the requirement of cheaper and more precise air communication. Safety and security factors in the development did not meet the required level of perfection; although no major attacks have been publicly reported, the threats remain unchanged. People need to be aware of the existing issues in the communication system and work to find a better, safer solution. Different approaches are made to advance existing technologies by integrating security aspects into them. The emphasis on domain-specific knowledge and aviation requirements should be placed on the whole system rather than isolated problems for future security developments. Security threats might not be limited to misuse of easily accessible software-defined radios; unforeseen disruptions are bound to happen in the future. Hence, aviation authorities need to understand the current developments and issues regarding them and work on developing processes that can adapt to the changes and challenges of the future.

DECLARATIONS

Authors' contributions

Made substantial contributions to the conception and design of the survey and analysis of the research, performed data curation: Shristi G, Choudhary G, Sihag V

Performed data acquisition, as well as provided administrative, technical, and material support: Shandilya SK

Availability of data and materials

Not applicable.

Financial support and sponsorship

None.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Copyright

REFERENCES

1. Dave G, Choudhary G, Sihag V, You I, Choo KKR. Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security* 2022;112:102516. Available from: https://doi.org/10.1016/j.cose.2021.102516.
2. Insights FB. Airport Security Market Size, Fortune Business Insights; 2020. https://www.prnewswire.com/news-releases/airport-security-market-size-to-reach-usd-11-45-billion-by-2027-increasing-flight-travels-safety-due-to-amid-covid-19-will-aid-growth-says-fortune-business-insights-301070663.html.
3. Ashdown LK. Preventing a cyber-9/11: how universal jurisdiction could protect international aviation in the digital age. *J Air L & Com* 2019;84:3. Available from: https://scholar.smu.edu/jalc/vol84/iss1/2.
4. Shrestha R, Oh I, Kim S. A survey on operation concept, advancements, and challenging issues of urban air traffic management. *Front Future Transp* 2021;2:626935. Available from: https://doi.org/10.3389/ffutr.2021.626935.
5. You IS, Sharma V, Choudhary G, KO YH. Method for verifying drone included in industrial internet of things system, by using petri-net modeling. Google Patents; 2021. US Patent App. 17/255,497. Available from: https://patents.google.com/patent/US20210279339A1/en.
6. Choudhary G, Sharma V, You I. Sustainable and secure trajectories for the military Internet of Drones (IoD) through an efficient Medium Access Control (MAC) protocol. *Computers & Electrical Engineering* 2019;74:59–73. Available from: https://doi.org/10.1016/j.compeleceng.2019.01.007.
7. Krishna CL, Murphy RR. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In: 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR). IEEE; 2017. pp. 194–99. Available from: 10.1109/SSRR.2017.8088163.
8. Choudhary G, Sharma V, Gupta T, Kim J, You I. Internet of Drones (IoD): threats, vulnerability, and security perspectives. arXiv preprint arXiv:180800203 2018. Available from: https://arxiv.org/abs/1808.00203.
9. Bajracharya R, Shrestha R, Jung H. Wireless infrastructure drone based on NR-U: a perspective. In: 2021 International Conference on Information and Communication Technology Convergence (ICTC). IEEE; 2021. pp. 834–38. Available from: 10.1109/ICTC52510.2021.9620869.
10. Choudhary G, Sharma V, You I, et al. Intrusion detection systems for networked unmanned aerial vehicles: a survey. In: 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE; 2018. pp. 560–65. Available from: 10.1109/IWCMC.2018.8450305.
11. Nguyen A, Amrhar A, Zambrano J, et al. Application of phase modulation for secure automatic dependent surveillance-broadcast. Available from: https://lassena.etsmtl.ca/relanlassena/IMG/pdf/-144.pdf.
12. Santamarta R. A wake-up call for satcom security. Technical White Paper 2014. Available from: https://www.secnews.gr/wp-content/uploads/Files/Satcom_Security.pdf.
13. Santamarta R. SATCOM terminals: Hacking by air, sea, and land. DEFCON White Paper 2014. Available from: https://docs.huihoo.com/blackhat/usa-2014/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf.
14. Costin A, Francillon A. Ghost in the air (traffic): on insecurity of ADS-B protocol and practical attacks on ADS-B devices. Black Hat USA 2012:1–12. Available from: https://s3.eurecom.fr/docs/bh12us_costin.pdf.
15. Schäfer M, Lenders V, Martinovic I. Experimental analysis of attacks on next generation air traffic communication. Springer; 2013. Available from: https://doi.org/10.1007/978-3-642-38980-1_16.
16. Leonardi M, Piracci E, Galati G. ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions. In: 2014 Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV). IEEE; 2014. pp. 41–46. Available from: 10.1109/TIWDC-ESAV.2014.6945445.
17. Wireless Attack Launch Box;. https://github.com/crescentvenus/WALB.
18. Strohmeier M, Martinovic I, Lenders V. Securing the air–ground link in aviation. In: The Security of Critical Infrastructures. Springer; 2020. pp. 131–54. Available from: https://doi.org/10.1007/978-3-030-41826-7_9.
19. Osechas O, Mostafa M, Graupl T, Meurer M. Addressing vulnerabilities of the CNS infrastructure to targeted radio interference. *IEEE Aerosp Electron Syst Mag* 2017;32:34-42. Available from: https://doi.org/10.1109/MAES.2017.170020.
20. Adamy D. EW 101: A first course in electronic warfare. vol. 101. Artech house; 2001. Available from: https://ieeexplore.ieee.org/abstract/document/9100068.
21. Adamy D. EW 102: a second course in electronic warfare. Artech House; 2004. Available from: https://ieeexplore.ieee.org/abstract/document/9100226.
22. Adamy D. EW 103: Tactical battlefield communications electronic warfare. Artech House; 2008. Available from: link.gale.com/apps/doc/A361848257/AONE?u=anon~2af1a93f&sid=googleScholar&xid=e2c63e44.
23. Moser D, Leu P, Lenders V, et al. Investigation of multi-device location spoofing attacks on air traffic control and possible countermeasures. In: Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking; 2016. pp. 375–86. Available from: https://doi.org/10.1145/2973750.2973763.
24. Shang F, Wang B, Yan F, Li T. Multidevice false data injection attack models of ADS-B multilateration systems. *Security and Communication Networks* 2019;2019:1-11. Available from: https://doi.org/10.1155/2019/8936784.
25. Stelkens-Kobsch TH, Hasselberg A, Mühlhausen T, et al. Towards a more secure ATC voice communications system. In: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC). IEEE; 2015. pp. 4C1. Available from: https://doi.org/10.1109/DASC.2015.7311419.
26. Melbourne Airport hoax caller Paul Sant pleads guilty to making fake flight calls, aborting Virgin landing. https://www.abc.net.au/news/2017-09-05/melbourne-airport-hoax-caller-paul-sant-pleads-guilty/8873984.
27. Meet the NATS pirate hunters. https://nats.aero/blog/2015/05/meet-the-nats-pirate-hunters/.
28. Di Marco D, Manzo A, Ivaldi M, Hird J. Security testing with controller-pilot data link communications. In: 2016 11th International

Conference on Availability, Reliability and Security (ARES). IEEE; 2016. pp. 526–31. Available from: https://doi.org/10.1109/ARES.2016.104.

29. Teso H. Aircraft hacking: Practical aero series. In: 4th Hack in the Box Security Conference in Europe; 2013. Available from: https://www.pnc-contact.com/doc/Hugo%20Teso%20-%20Aircraft%20Hacking.pdf.
30. Blanchet B. Symbolic and computational mechanized verification of the ARINC823 avionic protocols. In: 2017 IEEE 30th Computer Security Foundations Symposium (CSF). IEEE; 2017. pp. 68–82. Available from: https://doi.org/10.1109/CSF.2017.7.
31. Risley C, McMath J, Payne B. Experimental encryption of aircraft communications addressing and reporting system (ACARS) aeronautical operational control (AOC) messages. In: 20th DASC. 20th Digital Avionics Systems Conference (Cat. No. 01CH37219). vol. 2. IEEE; 2001. pp. 7D4/1-7D4/8. Available from: https://doi.org/10.1109/DASC.2001.964200.
32. Zhang R, Liu G, Liu J, Nees JP. Analysis of message attacks in aviation data-link communication. *IEEE Access* 2018;6:455-63. Available from: https://doi.org/10.1109/ACCESS.2017.2767059.
33. Wernberg M. Security and privacy of controller pilot data link communication; 2018. Available from: https://www.diva-portal.org/smash/get/diva2:1305189/FULLTEXT01.pdf.
34. Smith M, Strohmeier M, Lenders V, Martinovic I. On the security and privacy of ACARS. In: 2016 Integrated Communications Navigation and Surveillance (ICNS). IEEE; 2016. pp. 1–27. Available from: https://pdfs.semanticscholar.org/7ad9/83c960d531968355647d68e3f116cccbe55c.pdf.
35. Comendador FG, Valdes RA, PerezSanz L. Evolution of Air Traffic Services in Spain for the European Single Sky regulation. *IEEE Aerosp Electron Syst Mag* 2011;26:23-9. Available from: https://doi.org/10.1109/MAES.2011.5958760.
36. Strohmeier M, Schäfer M, Pinheiro R, Lenders V, Martinovic I. On perception and reality in wireless air traffic communication security. *IEEE Trans Intell Transport Syst* 2016;18:1338–57. Available from: https://doi.org/10.1109/TITS.2016.2612584.
37. Exploited ADS-B Information Exposed. Online flight tracking provides interesting details about Russian air bridge to Syria. https://theaviationist.com/2015/09/11/ads-b-exposes-russian-air-bridge-to-syria/.
38. Hoffman D, Rezchikov S. Busting the BARR: Tracking “untrackable” private aircraft for fun & profit. DEF CON 2012;20.
39. Pöpper C, Tippenhauer NO, Danev B, Capkun S. Investigation of signal and message manipulations on the wireless channel. In: European Symposium on Research in Computer Security. Springer; 2011. pp. 40–59. Available from: https://doi.org/10.1007/978-3-642-23822-2_3.
40. Wilhelm M, Schmitt JB, Lenders V. Practical message manipulation attacks in IEEE 802.15. 4 wireless networks. In: MMB & DFT 2012 Workshop Proceedings; 2012. pp. 29–31. Available from: https://www.lenders.ch/publications/conferences/Pilates12.pdf.
41. Flight Aware Live Flight Tracking;. https://uk.flightaware.com/live/.
42. Flightradar24 Live Air Traffic. http://flightradar24.com.
43. Wilhelm M, Martinovic I, Schmitt JB, Lenders V. Short paper: reactive jamming in wireless networks: how realistic is the threat? In: Proceedings of the fourth ACM conference on Wireless network security; 2011. pp. 47–52. Available from: https://doi.org/10.1145/1998412.1998422.
44. Zhou X, Song L, Zhang Y. Physical layer security in wireless communications. Crc Press; 2013. Available from: http://users.jyu.fi/~timoh/TIES327/WPLS.pdf.
45. Baker R, Martinovic I. Secure location verification with a mobile receiver. In: Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy; 2016. pp. 35–46. Available from: https://doi.org/10.1145/2994487.2994497.
46. Schäfer M, Leu P, Lenders V, Schmitt J. Secure motion verification using the doppler effect. In: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks; 2016. pp. 135–45. Available from: https://doi.org/10.1145/2939918.2939920.
47. Wang W, Chen G, Wu R, Lu D, Wang L. A low-complexity spoofing detection and suppression approach for ADS-B. In: 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS). IEEE; 2015. pp. K2–1. Available from: https://doi.org/10.1109/ICNSURV.2015.7121236.
48. Murphy TA, Harris WM. Device, system and methods using angle of arrival measurements for ADS-B authentication and navigation. Google Patents; 2019. US Patent 10,365,374. Available from: https://patents.google.com/patent/US9476962B2/en.
49. Fantacci R, Menci S, Micciullo L, Pierucci L. A secure radio communication system based on an efficient speech watermarking approach. *Security Comm Networks* 2009;2:305-14. Available from: https://doi.org/10.1002/sec.70.
50. Hagmüller M, Hering H, Kröpfl A, Kubin G. Speech watermarking for air traffic control. In: 2004 12th European Signal Processing Conference. IEEE; 2004. pp. 1653–56.
51. Strohmeier M, Martinovic I. On passive data link layer fingerprinting of aircraft transponders. In: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy; 2015. pp. 1–9. Available from: https://doi.org/10.1145/2808705.2808712.
52. Finke M, Stelkens-Kobsch TH. A practical example for validation of ATM security prototypes. *CEAS Aeronautical Journal* 2018;9:157–70.
53. Nuseibeh B, Haley CB, Foster C. Securing the skies: In requirements we trust. *Computer* 2009;42:64–72. Available from: https://doi.org/10.1109/MC.2009.299.
54. Montefusco P, Casar R, Koelle R, Stelkens-Kobsch TH. Addressing security in the ATM environment: from identification to validation of security countermeasures with introduction of new security capabilities in the ATM system context. In: 2016 11th International Conference on Availability, Reliability and Security (ARES). IEEE; 2016. pp. 532–41. Available from: https://doi.org/10.1109/ARES.2016.67.
55. Mahmoud MSB, Pirovano A, Larrieu N. Aeronautical communication transition from analog to digital data: A network security survey. *Computer Science Review* 2014;11:1-29. Available from: https://doi.org/10.1016/j.cosrev.2014.02.001.
56. Nguyen D, Shelton JW, Mitchell TM. System and method for evaluating cyber-attacks on aircraft. Google Patents; 2017. US Patent 9,836,990. Available from: https://patents.google.com/patent/US9836990B2/en.

57. Smith M, Strohmeier M, Harman J, Lenders V, Martinovic I. Safety vs. security: Attacking avionic systems with humans in the loop. arXiv preprint arXiv:190508039 2019. Available from: https://doi.org/10.48550/arXiv.1905.08039.
58. Strand DA. Automatic dependent surveillance: broadcast (ADS-B) vulnerabilities. Utica College; 2017. Available from: https://www.proquest.com/openview/317ac3b8f115065e3e9fbc69ac6a831d/1?cbl=18750&pq-origsite=gscholar.
59. Viveros CAP. Analysis of the cyber attacks against ADS-B perspective of aviation experts. Master's thesis, University of Tartu; 2016. Available from: https://core.ac.uk/reader/83597530.
60. Jochum JR. Encrypted mode select ADS-B tactical military situational awareness. MASSACHUSETTS INST OF TECH CAMBRIDGE DEPT OF ELECTRICAL ENGINEERING AND …; 2001. Available from: https://apps.dtic.mil/sti/citations/ADA402100.
61. McParland T, Patel V, Hughes W. Securing air-ground communications. In: 20th DASC. 20th Digital Avionics Systems Conference (Cat. No. 01CH37219). vol. 2. IEEE; 2001. pp. 7A7/1-7A7/9. Available from: https://doi.org/10.1109/DASC.2001.964187.
62. Olive M. Efficient datalink security in a bandwidth-limited mobile environment-an overview of the Aeronautical Telecommunications Network (ATN) security concept. In: 20th DASC. 20th Digital Avionics Systems Conference (Cat. No. 01CH37219). vol. 2. IEEE; 2001. pp. 9E2/1-9E2/10. Available from: https://doi.org/10.1109/DASC.2001.964255.
63. Hableel E, Baek J, Byon YJ, Wong DS. How to protect ADS-B: Confidentiality framework for future air traffic communication. In: 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE; 2015. pp. 155–60. Available from: https://doi.org/10.1016/j.ijcip.2013.02.001.
64. Yang A, Tan X, Baek J, Wong DS. A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification. IEEE Transactions on Services Computing 2015;10:165–75. Available from: https://doi.org/10.1109/TSC.2015.2459709.
65. Agbeyibor R, Butts J, Grimaila M, Mills R. Evaluation of format-preserving encryption algorithms for critical infrastructure protection. In: International Conference on Critical Infrastructure Protection. Springer; 2014. pp. 245–61. Available from: https://doi.org/10.1007/978-3-662-45355-1_16.
66. Finke C, Butts J, Mills R. ADS-B encryption: confidentiality in the friendly skies. In: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop; 2013. pp. 1–4. Available from: https://doi.org/10.1145/2459976.2459986.
67. Finke C, Butts J, Mills R, Grimaila M. Enhancing the security of aircraft surveillance in the next generation air traffic control system. *International Journal of Critical Infrastructure Protection* 2013;6:3-11. Available from: https://doi.org/10.1016/j.ijcip.2013.02.001.
68. Berthier P, Fernandez JM, Robert JM. Sat: Security in the air using tesla. In: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC). IEEE; 2017. pp. 1–10. Available from: https://doi.org/10.1109/DASC.2017.8102003.
69. Martinovic I, Strohmeier M. On the Security of the Automatic Dependent Surveillance- Broadcast Protocol. *IEEE Commun Surv Tutorials* 2015;17:1066-87. Available from: https://doi.org/10.1109/COMST.2014.2365951.
70. Lee SH, Han JW, Lee DG. The ADS-B protection method for next-generation air traffic management system. In: Ubiquitous Computing Application and Wireless Sensor. Springer; 2015. pp. 105–13. Available from: https://doi.org/10.1007/978-94-017-9618-7_10.
71. Yue M, Wu X. The approach of ACARS data encryption and authentication. In: 2010 International Conference on Computational Intelligence and Security. IEEE; 2010. pp. 556–60. Available from: https://doi.org/10.1109/CIS.2010.127.
72. Arora A, Yadav SK. Batman: Blockchain-based aircraft transmission mobile ad hoc network. In: Proceedings of 2nd International Conference on Communication, Computing and Networking. Springer; 2019. pp. 233–40. Available from: https://doi.org/10.1007/978-981-13-1217-5_23.
73. Reisman R. Blockchain serverless public/private key infrastructure for ADS-B security, authentication, and privacy. In: AIAA Scitech 2019 Forum; 2019. p. 2203. Available from: https://doi.org/10.2514/6.2019-2203.
74. Fouda RM. Security vulnerabilities of cyberphysical unmanned aircraft systems. *IEEE Aerosp Electron Syst Mag* 2018;33:4-17. Available from: https://doi.org/10.1109/MAES.2018.170021.
75. Ukwandu E, Ben-Farah MA, Hindy H, Bures M, Atkinson R, et al. Cyber-security challenges in aviation industry: a review of current and future trends. *Information* 2022;13:146. Available from: https://doi.org/10.3390/info13030146.
76. Sihag V, Vardhan M, Singh P. BLADE: robust malware detection against obfuscation in android. Forensic Science International: Digital Investigation 2021;38:301176. Available from: https://doi.org/10.1016/j.fsidi.2021.301176.
77. Sihag V, Vardhan M, Singh P, Choudhary G, Son S. De-lady: Deep learning based android malware detection using dynamic features. *Journal of Internet Services and Information Security (JISIS)* 2021;11:34–45. Available from: https://doi.org/10.22667/JISIS.2021.05.31.034.
78. Sihag V, Choudhary G, Vardhan M, Singh P, Seo JT. PICAndro: Packet InspeCtion-Based Android Malware Detection. *Security and Communication Networks* 2021;2021:1-11. Available from: https://doi.org/10.1155/2021/9099476.
79. Sihag V, Vardhan M, Singh P. A survey of android application and malware hardening. *Computer Science Review* 2021;39:100365. Available from: https://doi.org/10.1016/j.cosrev.2021.100365.
80. Gurtov A, Polishchuk T, Wernberg M. Controller–pilot data link communication security. *Sensors (Basel)* 2018;18:1636. Available from: https://doi.org/10.3390/s18051636.
81. Sathaye H, Schepers D, Ranganathan A, Noubir G. Wireless attacks on aircraft landing systems. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks. ACM; 2019. pp. 295–97.
82. McCallie D, Butts J, Mills R. Security analysis of the ADS-B implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection* 2011;4:78-87. Available from: https://doi.org/10.1016/j.ijcip.2011.06.001.