Cyber security challenges in aviation communication, navigation, and surveillance

Dave, Gaurav; Choudhary, Gaurav; Sihag, Vikas; You, Ilsun; Choo, Kim Kwang Raymond

Published in:
Computers and Security

Link to article, DOI:
10.1016/j.cose.2021.102516

Publication date:
2022

Document Version
Peer reviewed version

Journal Pre-proof

Cyber Security Challenges in Aviation Communication, Navigation, and Surveillance

Gaurav Dave, Gaurav Choudhary, Vikas Sihag, Ilsun You, Kim-Kwang Raymond Choo

PII: S0167-4048(21)00340-0
DOI: https://doi.org/10.1016/j.cose.2021.102516
Reference: COSE 102516

To appear in: *Computers & Security*

Received date: 1 January 2021
Revised date: 11 October 2021
Accepted date: 19 October 2021

Please cite this article as: Gaurav Dave, Gaurav Choudhary, Vikas Sihag, Ilsun You, Kim-Kwang Raymond Choo, Cyber Security Challenges in Aviation Communication, Navigation, and Surveillance, *Computers & Security* (2021), doi: https://doi.org/10.1016/j.cose.2021.102516

Cyber Security Challenges in Aviation Communication, Navigation, and Surveillance

Gaurav Dave[a], Gaurav Choudhary[b], Vikas Sihag[a], Ilsun You[c,*], Kim-Kwang Raymond Choo[d]

[a] *Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, India.*
[b] *Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Denmark*
[c] *Department of Information Security Engineering, Soonchunhyang University, Asan-si 31538, the Republic of Korea.*
[d] *Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA.*

Abstract

As the aviation sector becomes digitized and increasingly reliant on wireless technology, so has its attractiveness to cyber attackers including nation-state actors and terrorists. For example, vulnerabilities in the broad range of interconnected devices and (sub)systems, their implementations, as well as design flaws, can be exploited to carry out nefarious activities. Therefore, in this paper we review the existing literature to understand the diverse attack vectors associated with communication, navigation, and surveillance systems, and how some of these security issues can be mitigated. Although a number of survey and review articles have analyzed various wireless technologies in aviation, to the best of our knowledge, no work has systematically analyzed them from communication, navigation and surveillance perspectives collectively. Furthermore, we present potential software defined radio (SDR)-based attacks targeting popular wireless technologies. Based on our in-depth review, we highlight existing limitations and discuss potential research opportunities.

Keywords: Aviation, Security, Communication, Navigation, Surveillance, Software defined radio (SDR)

1. Introduction

An aviation ecosystem is complex, with many different building blocks. For example, key infrastructure components of the aviation ecosystem include Air Traffic Management (ATM), which comprise different Communication, Navigation, and Surveillance (CNS) systems. Communication systems generally comprise devices that facilitate the exchange of information (e.g., commands, voice and other data information) between devices, systems and users (e.g., Air Traffic Control (ATC) and pilot), for example, to facilitate navigation. Data from both communication and navigation systems (e.g., onboard systems and radars), as well as the supporting infrastructure, also facilitate surveillance. The challenge in ensuring cybersecurity in aviation is compounded by the volume of air traffic. For example, Chicago OHare International Airport is one of the busiest airports in the world and accounted for 904,300 takeoffs and landings in 2019 [1]. While forecasts project a steady increase in air traffic on a global scale, challenges to the underlying technologies are also intensifying with rapid advances in technical capabilities.

Ensuring cybersecurity in aviation is increasingly important, as more devices and systems become digitized and interconnected with many of the services and communications carried out wirelessly. However, the wireless nature of the communications can be targeted by malicious attacks [2]. Examples of communication-related attacks include those targeting communication signals (e.g., signal jamming and false data / command injection). Navigation-related attacks include GPS spoofing or blocking attacks, signal jamming and eavesdropping, single tone frequency attacks, navigation modification attacks, and surveillance-related attacks include those seeking to conduct illicit / unauthorized surveillance of aircraft and their movements as well as signal jamming, signal modification and deletion. The risk is real. For example, few years ago in 2013, a security consultant claimed to have hacked into an aircraft's control system using his PlainSploit Android application [3]. In another revelation, a group of researchers were able to accomplish a remote, non-cooperative, penetration on a Boeing 757 aircraft [4]. There have also been several other media reports on the insecurity of wireless aviation technologies [5, 6, 7]. The importance of aviation security is also reinforced in the U.S. White House's call for a cyber secure aviation ecosystem [8].

Motivated by the importance of cybersecurity in aviation, here we will review and classify existing attacks on the aviation ecosystem, categorized based on the target CNS systems. In particular, we focus on the protocols, corresponding attacks, targeted security properties and solutions available in the literature. This survey would be beneficial to developers and researchers in their understanding of the current state of aviation security. In our review, we perform searches using keywords such as air traffic, aviation, aerial vehicle networks, security, attacks, communication, navigation, and surveillance, as well as their synonyms and different keyword combinations, on Google Scholar and other academic databases. A snapshot of the publication trend can be observed in Figure 1.

*Corresponding author
Email addresses: spu18cs03@policeuniversity.ac.in (Gaurav Dave), gauravchoudhary7777@gmail.com (Gaurav Choudhary), vikas.sihag@policeuniversity.ac.in (Vikas Sihag), ilsunu@gmail.com (Ilsun You), raymond.choo@fulbrightmail.org (Kim-Kwang Raymond Choo), yyyy (Kim-Kwang Raymond Choo)

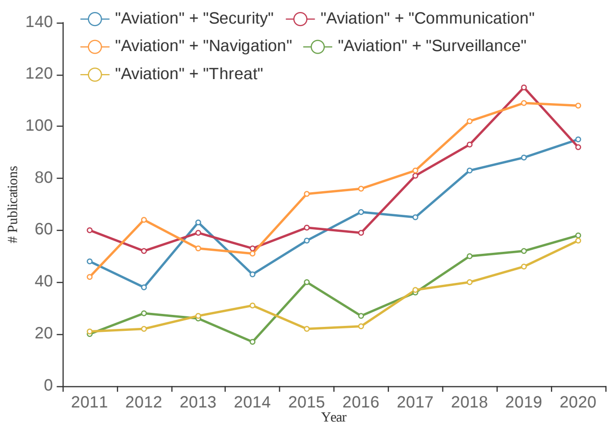

Figure 1: Number of publications with keywords, such as aviation, security, communication, navigation, surveillance and threat, in its title or abstract.

During our keyword searches, we locate a number of other existing related reviews / surveys – see Table 1. For example, Kriaa et al. [9] discussed the safety and security approaches for industrial control systems, and Knowles et al. [10] studied the different approaches for managing and quantifying industrial control system security. More closely related to our paper is the work of Lykou et al. [11], who discussed ATM-related cybersecurity issues. The authors also presented a risk-based framework to address security threats and increase the aviation system's resilience against future attacks. Nobles [12] discussed the emerging cyber threats in civil aviation, cybersecurity frameworks. Khatun et al. [13] discussed the existing millimeter wave systems for airports and short-range communications, and Stewart and Mueller [14] focused on the cost-benefit assessment of United States aviation security measures, while Lee et al. [15] focused on operations research applications in aviation security. Lykou et al. [16] studied the implementation rate of cybersecurity measures in the aviation industry. Strohmeier et al. [17] focused on the aviation community concerning the security of wireless systems. The authors also considered the factors which impact the technological environment and affect the security of aviation technologies, current, and future. However, we observe that no survey or review article has focused on the potential cybersecurity threats to the communication, navigation and surveillance systems, which is the gap we seek to address in our work.

In Sections 2 and 3, we present an overview of the aviation system and the wireless technologies and their associated security issues, respectively. Section 4 defines the identified threats, attack taxonomy, and existing security frameworks and solutions in the aviation domain. Finally, we conclude this work in Section 5.

2. Overview of Aviation System

Before proceeding with aviation security we need to have an understanding of the working of the aviation system. Aviation system comprises sub-systems and wireless technologies responsible for three main applications namely, communication, navigation, and surveillance. CNS is also very much responsible for aviation security. Figure 2 presents an architectural overview of the aviation system. An aircraft needs to transit from one location to another and land on the airstrip. Ground stations, satellites, and other peer aircraft assist it in doing so effectively. The pilot uses communication protocols (such as Very High-Frequency(VHF), High-Frequency(HF), and Controlled Pilot Data-Link Communication(CPDLC)) to have a voice or message-based information exchange from ground station and satellite. It uses navigation protocols (such as VHF Omni-directional Range(VOR), Instrument Landing System(ILS), and Distance Measuring Equipment(DME)) to transit and has a successful landing. The ground station employs surveillance protocols (such as Primary Surveillance Radar(PSR), Secondary Surveillance Radar(SSR), and Automatic Dependent Surveillance-Broadcast(ADS-B)) to keep track of aircraft movement and check for intruders in air space. These systems are always active during aircraft transit and landing.

The Air Traffic Management(ATM) system is responsible for aviation system connectivity. So Air traffic control is the larger body in the ATM system used to connect with aircraft as well as with satellites. Ground networks and data centres are connected with ATC, where data centres are connected with the internet. Ground networks are responsible for satellite and other aspects such as aircraft networks. The aviation system primarily works on the ground station and aircraft connectivity. Most of the time the ground station is responsible for establishing contact with an approaching aircraft. The ground station is comprised of an ATC, which is also responsible for connectivity with supporting ground units (data centres, ground radars, and towers) [18].

VHF and CPDLC are responsible for maintaining voice communication between aircraft and ATC. VHF provides voice-based communication, whereas CPDLC uses VHF datalink to provide message-based communication. Digital Satellite Communication Networks (DSCN) are used to provide connectivity with satellites. DSCN is used both for communication and navigation. DME, VOR, and ILS are dedicated to navigation and smooth landing. DME measures the distance between the aircraft and the station. VOR is short-range and responsible for aircraft to determine its position and stay on course. ILS is responsible for guidance during landing. PSR and SSR are used for surveillance to detect flying crafts. Moreover, ADS-B is also introduced lately for efficient surveillance between aircraft or with a ground station. The aviation system uses above briefed key protocols for smooth air traffic operations.

3. Aviation Protocols in CNS Systems

In this section, we introduce wireless technology employed in the aviation system. We have divided protocols of aviation ecosystem systems based on their application into the communication, navigation, and surveillance domain. Communication system deals with voice or message-based aircraft-to-ATC or aircraft-to-aircraft communication. A navigation sys-

Table 1: Other related survey or review articles on aviation security.(*: Only discussions)

Year	Surveys	Aviation Security	Surveillance Security	Communication Security	Vulnerabilities Considerations	Attacks Considerations
2008	Stewart and Mueller [14]	✓				
2008	Lee et al. [15]	✓				✓ *
2015	Kriaa et al. [9]				✓	
2015	Knowles et al. [10]				✓	✓
2016	Strohmeier et al. [17]	✓	✓	✓	✓ *	✓ *
2017	Khatun et al. [13]					
2019	Lykou et al. [11]	✓	✓	✓		
2019	Calvin Nobles [12]	✓				✓ *
2019	Lykou et al. [16]	✓	✓	✓	✓ *	✓ *
2021	Proposed Survey	✓	✓	✓	✓	✓

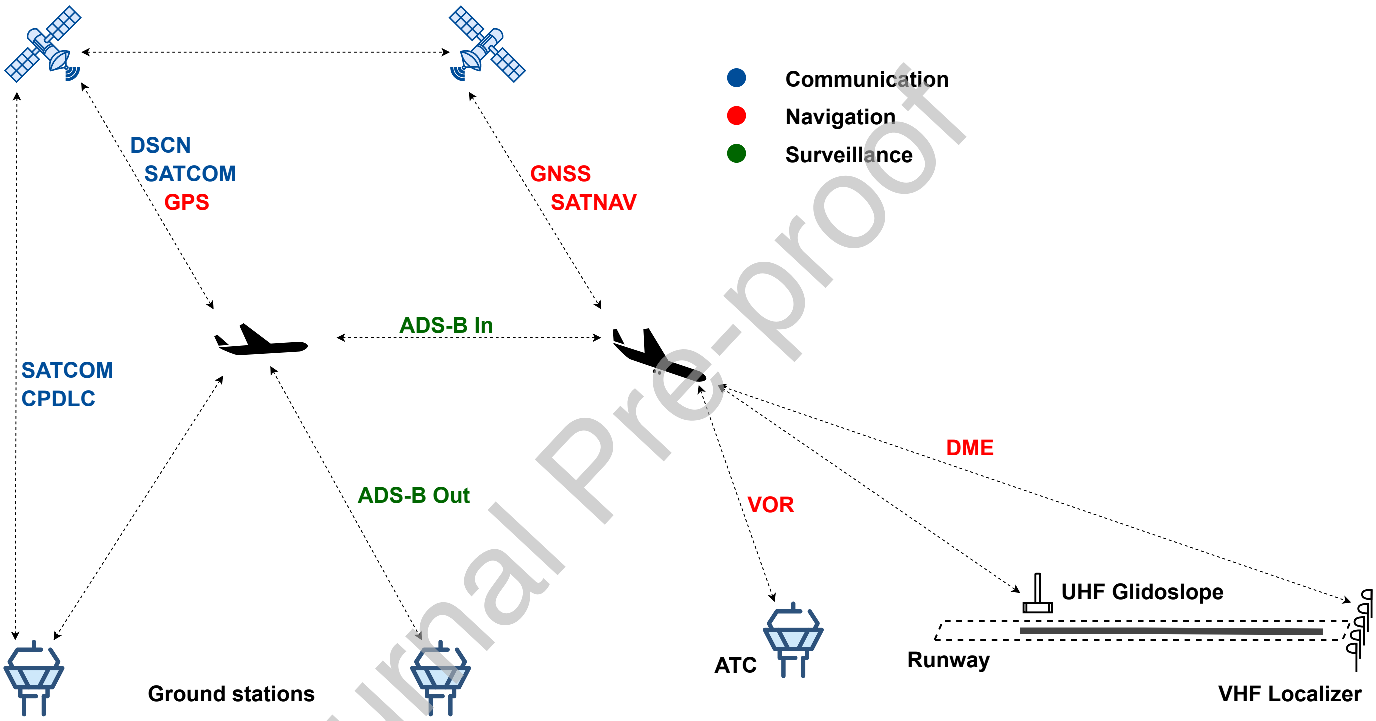

Figure 2: An exemplary overview of Aviation Architecture.

tem comprises protocols that help in aircraft navigation during transit and landing. Furthermore, a surveillance system consists of protocols for aircraft surveillance. Technologies discussed complement and/or supplement each other. Moreover, we brief security issues related to each technology. A comparative analysis of protocols in the CNS system is presented in Table 2.

3.1. Communication Protocols

The communication between aircraft and controllers is managed by ATC protocols. They are responsible for establishing the location and intent information of an aircraft. In this paper, we have discussed protocols responsible for aircraft-to- aircraft and aircraft-to-ATC communication.

3.1.1. Very High Frequency (VHF)

Voice communication, which is over VHF is the primary means of communication between ATC and pilot. It is used for clearance, reports, requests, and instruction exchanges. Moreover, additional information like a weather report, information broadcast is also performed over it. Due to its operation on a very high frequency, it tends to have limited coverage. Voice communication outside its range is conducted over high frequency (HF) [19].

Security Issues. VHF is one of the oldest communication technology used in aviation. Due to its wireless nature, it is susceptible to various attacks. It relies on the correct understanding of voice messages by the parties for successful communication. Voice over VHF is prone to denial of service attacks (partial or full) depending upon targeted frequencies. VHF employs am-

Table 2: The state-of-the-art comparison of existing ATC protocols.

	VHF	CPDLC	DSCN	DME	VOR	ILS	PSR	SSR	ADS-B
Use	Voice (ATC-Aircraft)	Message (ATC-Aircraft)	SATCOM (ATC-Aircraft)	Distance	Bearing	Approach guidance	Non-cooperative detection and positioning	Cooperative detection and positioning	Collision avoidance
Type	Selective and Broadcast	Selective	Selective and Broadcast	Interogate	Broadcast	Broadcast	Broadcast	Interogate	Broadcast
Sender	Aircraft and Ground station	Aircraft and Ground station	Aircraft and Ground station	Ground station	Ground station	Ground Antenna Array	Ground station	Aircraft	Aircraft
Receiver	Aircraft and Ground station	Aircraft and Ground station	Aircraft and Ground station	Aircraft	Aircraft	Aircraft	Original sender	Aircraft and Ground station	Aircraft and Ground station
Frequency (MHz)	3.4-23.35, 117.975-143.975, 225-400	136.975	117.975-143.975	962-1213	108.975-117.975	75, 108-111.975, 328.6-335.4	1-2, 2-4 GHz	1030, 1090	978, 1090
Signal	Analog	Digital	Digital	Morse code	Morse code	Morse code	Analog	Digital	Digital

plitude modulation. As it is broadcast in nature, channel override over destined communication is hard to control when targeted by an attacker. Authentication over VHF is not applied in civil flights because of its computational overhead, but is used in military flights. VHF is considered the less trusted protocol. An attacker with a transmitter-receiver antenna and radio station can perform eavesdropping and jamming. On failure of VHF, ATC has to rely on Controlled Pilot Data Link Communication (CPDLC) for communication [20].

3.1.2. Controller Pilot Data Link Communications (CPDLC)

One of the major problems with voice-over VHF is all pilots communicating with an ATC are channeled into the same frequency. With increased traffic, number of pilots tuned in increases. Thus increasing the probability of accidental overrides. ATC controller has a saturation point, further which it will not be able to handle incoming connection. CPDLC, an alternative to VHF-based voice communication is a message-based service, which uses VHF Data Link Version 2 (VDL) as its data link [21]. Information exchange between ATC and pilot is performed using predefined request, reply, report, and free text messages over the terminal. It is operator-friendly, efficient, faster, and safer than VHF due to reduced voice misunderstanding and message logging. Being a message-based service, it can easily be integrated with automated services [20]. Message exchanges outside the range of VHF are done using satellite instead of radio frequency, which has other spreading issues. As aircraft are getting CPDLC-enabled, VHF still remains the primary communication channel.

Security Issues. CPDLC uses unauthenticated data links for message exchange. An attack on it may go undetected [22, 23]. It does not provide confidentiality and integrity of the message exchanged. Being unauthenticated and insecure, an attacker with a transmitter-receiver antenna and radio station can perform jamming, eavesdropping, message injection, replay, modification, and deletion attacks over it. Predefined request, reply, and clearance messages can be spoofed using software defined radio (SDR) [24, 25].

3.2. Navigation Protocols

Technological advancements in navigation systems enable location-based services for aircraft movement with accuracy, effectiveness, consistency, and continuity. It lies under the air traffic management system [17]. The navigation system comprises of Global Positioning System (GPS) for aircraft tracking, which is possible with the help of the Global Navigation Satellite System (GNSS) [26]. Below we discuss protocols responsible for navigation systems.

3.2.1. VHF Omnidirectional Range (VOR)

VOR is the standard navigation system that works over VHF. It broadcasts VHF radio beacons consisting of station identity and angle to its location with reference to the directional signals. Due to the radial nature of the signal received, the aircraft is able to calculate within which direction it lies from the VOR system. The VOR frequency range is 112-118MHz. VOR is used to determine the bearing or angular divergence from magnetic northward to well-established ground stations. Station identity (2 or 3 letter identifier in morse code) is encoded and broadcasted.

Security Issues. VOR assists the pilot in navigation based on ground station location. Intentionally designed with a lack of confidentiality (to prevent computational overhead), it is susceptible to passive attacks like eavesdropping [27, 28].

3.2.2. Instrument Landing System (ILS)

ILS is used when the pilot is not able to establish visual contact with the runway. It is performed using a radio navigation system that provides horizontal and vertical guidance to aircraft for landing. ILS is responsible for providing a complete picture for guidance to the aircraft for landing. The VOR helps to navigate aircraft to the runway after which ILS is used for landing. ILS is fixed on an airstrip and helps to find the distance from the reference point of landing. For landing purposes, the vertical and horizontal guidance is provided by the ground-based instrument approach by using the combination of radio signals, high-intensity lighting arrays which help during Instrument Meteorological Conditions (IMC) such as fog, rain, or blowing snow. When an aircraft approaches the runway ILS receiver in the aircraft guides it by modulation depth comparisons. ILS consists of two independent subsystems one is UHF glideslope for vertical guidance and VHF localizer for lateral or horizontal guidance. Three terms are used under the ILS device: localizer, glide path, and fan markers. The localizer is a radio beam that gives directional guidance to and along the runway. Localizer provides horizontal guidance. It uses the VHF transmitter and the localizer operates on the frequency range of 108.10-111.9 5MHz with a channel separation of 50KHz. The localizer receives the signal on onboard equipment in the aircraft. The glide path provides vertical guidance to the aircraft by the use of a radio beam. It has a frequency of UHF which lies between 320.30-335 MHz. Marker beacons are used for aircraft safe landing. It has three marker beacons, first is an outer marker (OM) which is also called non-directional beacon (NDM) which is blue. The second is the middle marker (MM) which is yellow and the last is an inner marker (IM) which is white. These are arranged at a certain range and guide to aircraft. The Instrument Landing System is shown in Figure 3. There are radio transmitters that are used to instruct aircraft when it approaches the dock. Four radio transmitters are used for the landing approach. In the center, the localizer antenna is placed. in this AM 90Hz and 150Hz signals are used in which one signal is on left concerning the centerline and another one on right regarding the centerline. The beams are modulated with morse code on audible tones at different frequencies.

Security Issues. ILS is a de-facto approach used for aircraft landing. It accurately provides vertical and horizontal guidance. Sathaye et. al. in [28] demonstrates susceptibility of ILS to wireless attacks by showing controlling in real time the course deviation indicators in aviation-grade ILS receivers. They designed an autonomous ILS spoofer and exhibit an off-runway landing. The overshadow attack, single tone attack and GPS spoof attack are also possible with the ILS system [29, 30].

3.2.3. Distance Measuring Equipment (DME)

DME is a transponder-based radio navigation technology to measure slant range distance by timing the propagation delay of VHF or UHF radio signals. It is very similar to Secondary Surveillance Radar (SSR). Aircraft use DME to determine their distance from a land-based transponder by sending and receiving pulse paired of fixed duration and separation. Aircraft uses the direction finder to determine the angle of arrival of the signal [31]. Generally, VORs are used for ground stations so these are collocated with VORs. The DME uses the Rho-Theta navigation system, which is based on the polar coordinate system of azimuth and distance. VOR and DME are the primary components of the Rho-Theta navigation system in which VOR provides azimuth information mean theta to the pilot and DME used provides distance information means rho so that the pilot receives continuous navigation relative to a known ground location. DME is an easy-to-use device as the pilot has to only tune to DME frequency and read the signal display once the DME has locked up with the ground station [32]. Generally, the DME frequency lies between 960-1215MHz, the interrogator transmits on a frequency of 1025 up to 1150MHz. There are 126 frequency bands of 1MHz spacing defined. DME station replies to 63MHz lower or upper frequency. DME receives control frequency with VOR.

Security Issues. DME is employed with VOR for navigation. They are susceptible to SDR-based attacks. Another possible attack is on rho-theta navigation, where rho and theta are dependent on DME and as well as VOR control frequency. A similar attack can be performed on azimuth angle [33].

3.3. Surveillance Protocols

The term surveillance concerning aviation is to identify an aircraft's identity, location and position passively. It is classified into dependent and independent surveillance based on dependence on onboard equipment. Radar-based systems are generally employed for it. Below we discuss protocols responsible for surveillance and their related security issues.

3.3.1. Primary Surveillance Radar (PSR)

PSR works on the principle of signal reflection for distance and position calculation. It consists of a primary rotating radar, which radiates a high power directional frequency beam on a low GHz band. Upon striking an object or target the signal frequency is reflected and received by the radar receiver [34]. The bearing and round-trip time of the received signal gives the object's position. PSR is a passive system independent of any onboard equipment integration. It is affected by the environment and weather disturbances. It is often used to locate non-cooperative aircraft or during transponder failure. PSR provides only direction and distance information of an aircraft.

Security issues. The PSR works on the principle signal-based detection approach so message injection is not possible but jamming is still possible. When jamming occurs in PSR it does not affect the main target information such as altitude. There is a difference between military PSR and civil PSR as military PSR has security over transmitting radio signals. The sensor system of PSR is also vulnerable to time-based attacks (GPS attacks) [35, 36].

3.3.2. Secondary Surveillance Radar (SSR)

SSR works on the principle of interrogation. SSR sends associate degree interrogation, which is received by the target craft. The craft transponder device sends back a coded reply to the measuring device. The coded signal has the craft decision sign, altitude, speed, and destination. SSR uses modulation for interrogation at the frequency of 1030MHz and the reply at the frequency of 1090MHz [37]. Mode A, Mode C, and Mode S transponder are the main part of the SSR. It is more informative than PSR. Modes A and C were used earlier to detect aircraft identity and altitude respectively. The mode S has replaced the two, to offer unicast aircraft targeting instead of broadcasts used previously. However, it requires the aircraft's position to be resolved by other surveillance protocols (ADS-B or PSR).

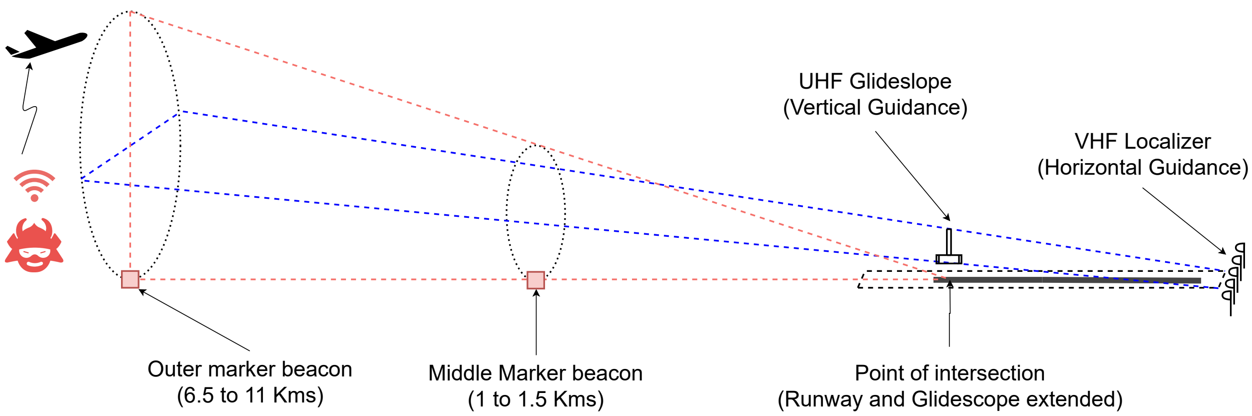

Figure 3: Architectural diagram of Instrument Landing System.

Security Issues. Due to limitations in computational and cryptographic capabilities of civil aviation, SSR was designed intentionally without confidentiality, thus making it susceptible to eavesdropping [28, 27]. SSR is vulnerable to SDR attacks with its dump available on the internet[1], whereas altering, blocking, injection in Mode A, Mode C, and Mode S messages are possible. Researchers have demonstrated injection of ghost aircraft by fake SSR messages and were also able to delete SSR messages [38]. Mode S aircraft identifiers are susceptible to spoofing and alteration. It is also vulnerable to amplification attacks, using which attackers can make generated interrogation requests and collect legitimate aircraft interrogation replies. An amplification attack can lead to a partial DoS attack [39, 40]. With limited interrogation capacity of ATC transponder, an attacker with a Mode-S transponder can saturate it by sending multiple requests with different identifier codes. It will also make other aircraft respond to interrogations thus increasing attack range(amplification or partial DoS attack) [40, 41]. Even moderately busy ATCs are susceptible to this attack with relevant significant data from genuine aircraft getting lost.

3.3.3. *Automatic Dependent Surveillance-Broadcast (ADS-B)*

ADS-B is automatic and dependent on a satellite-based GNSS system for surveillance. An onboard GNSS receiver is used to determine the aircraft's location and velocity. Aircraft continuously broadcasts its location parameters and additional information to be received by other aircraft and ground stations. It enhances pilot traffic awareness. The main ADS-B is divided into two parts one is ADS-B OUT which establishes the automated transmission facilities between the aircraft and ATC. In this ATC transponders transmit information from the ground using Mode-S 1090MHz extended squitter with a refresh rate of 0.5 seconds. Another one is ADS-B IN, which automates transmission between aircraft themselves. Information available to pilot consists of aircraft ID, absolute bearing / 2D distance, heading / track, wake / vortex category, relative / absolute altitude, ground speed, and vertical velocity [42]. ADS-B is now mandatory in Australia, American, and Europe.

[1] dump1090 `https://github.com/MalcolmRobb/dump1090`.

Security Issues. Use of unauthenticated data link 1090 Extended Squitter is vulnerable to active and passive attacks [43]. Selective jamming of an aircraft, false injection of aircraft is possible. As discussed earlier, the ADS-B broadcast the position information of the aircraft which can further be exploited by an attacker. It is easy to inject false messages and even spoof a genuine aircraft [44]. Another possible threat is to nearly change the mechanical phenomenon of the craft by electronic blocking the airships information's and also altered the information signal. Furthermore, ADS-B is unencrypted opening other attack paradigms [45, 46].

4. Aviation Security Threats, Attacks and Solutions

4.1. *Aviation Security Threats*

Threat modeling is efficiently specifying all potential threats that might influence a framework or the aviation network. Over the years, various threat modeling approaches have been developed ranging from generic approaches to domain-specific ones [54, 55, 56]. A practical threat modeling approach can be created from domain-specific analysis of potential threats and risks. Various tools that can be used in the threat modeling process are PASTA, Trike, and Microsoft SDL. A security threat can bring about a condition with an adverse impact on the security of aviation frameworks, including resources and individuals or groups adversely affecting the airplane and its services. In our research, we have evaluated various potential security threats and attacks relevant to aviation, communication, and surveillance. Figure 4, illustrates a hierarchical view of threats on Aviation with reference to CNS system. We expand the threats to Aviation system along three key security properties namely: confidentiality, integrity and availability. For completeness, they are defined as:

- *Availability*: the ability of a system to ensure that an asset can be used by authorized parties.
- *Integrity*: the ability of a system to ensure that an asset is modified only by authorized parties.
- *Confidentiality*: the ability of a system to ensure that an asset is viewed only by authorized parties

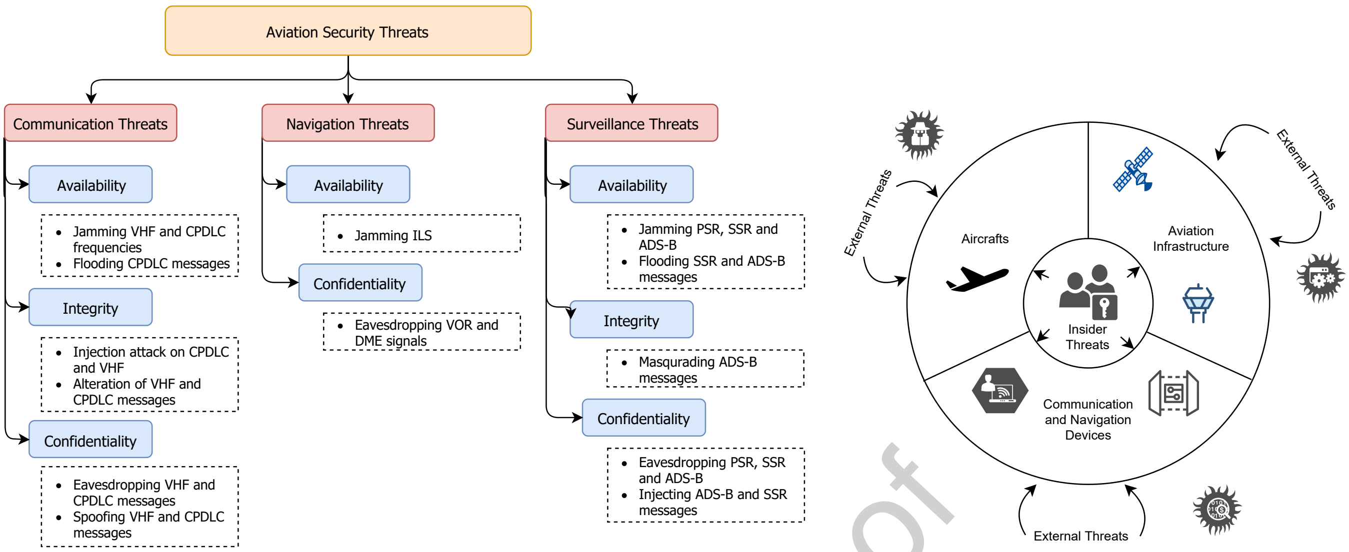

Figure 4: Hierarchical view of security threat on aviation system (CNS) and Threat diagram of aviation system

Table 3: A comparative analysis of threat models presented in literature and their key contributions.

Authors	Key Contributions	Aviation Threat Modeling Mechanism	Security Threats			Case Study / Scenario	Risk Modeling
			Comm.	Nav.	Surv.		
Baquero et al. [47]	Discussed issues of security in aviation and presented threat modeling as a method to identify security threats	SDL Threat Modeling Tool	✓			✓	
Cioaca et al. [48]	Risk Modeling	Threat origins, aviation targets and dimensions	✓	✓	✓		✓
Haass et al. [49]	Graph-based communication oriented framework	Threats to ADS-B system	✓	✓	✓	✓	✓
Kiesling et al. [50]	Model-based approach for aviation cyber security risk assessment	Structured Threat Information eXpression (STIX)	✓	✓	✓	✓	✓
Li et al. [51]	Focused on ADS B attack data strategies	Classical attack patterns on ADS-B data and formal expression	✓	✓	✓	✓	✓
Lykou et al. [11]	Analyzed resilience aspects in the aviation sector	Threat agent characterization	✓	✓	✓		✓
Lykou et al [16]	Discussed Smart Airports Cyber Security	Malicious threats that evolve due to IoT and smart devices installed	✓	✓	✓	✓	✓
Schmitt et al. [52]	Focused cyber-threat situations with flight plan data processing	Abnormal system behavior caused by unintentional acts and intentional manipulations	✓	✓	✓	✓	✓
Strohmeier et al. [27]	Discussed recent advancement of avionics on the security of aviation protocols	Classified the relevant threat agents based on their motivation and wireless capabilities	✓	✓	✓	✓	
Ukwandu et al. [53]	Explored the cyber-security situation in civil aviation industry	Advance Persistent Threat (APT) groups	✓	✓	✓		

We included various security threats omitted from aviation, surveillance & navigation and categorized them. The potential threat actors can be insider or external, and the e-enabled connected aircraft security vulnerabilities can exploit various attack surfaces. The inclusive impact of potential threats can be high and dangerous. Therefore, the modeling of such threats before security designing can help to mitigate the risk of attacks.

Table 3, presents a comparative analysis of threats models discussed in the literature and their key contributions. In the domain of aviation threat modeling, Ukwandu et al. [53] provided a detailed survey about cyber-security challenges in the aviation industry. The authors categorized the threat actors according to various impacts and execution surfaces. The authors also surveyed the aviation attacks in the period of 2000-2020. Furthermore, classify the attack components based on cyber-attack surfaces and their mitigation. Schmitt et al. [52] focused on cyber-threat situations with flight plan data processing and considered abnormal system behavior caused by unintentional acts and intentional manipulations. Li et al. [51] focused on attacks possibilities on ADS-B by classical attack patterns and converted it into formal expressions. Lack of any authentication provides no integrity, and the ability to jam signals brings into question availability. The current threats considerations included the formalism to address multiple systems within the aviation industry [57].

4.2. Attacks on Aviation Security

Modern aircraft and ATC rely on various wireless technologies during multiple phases of a flight. While designing them security was never conceptualized, making them insecure. Recent attack demonstrations by researchers on these wireless technologies have exposed their vulnerabilities [71]. Shift to modern communication methods is principled on the concept of redundancy of services.

The availability of advanced capable radio frequency transceivers such as SDR has provided the technical advantage of the aviation sector to attackers. SDR is a system for radio communication where traditional hardware components of radio (such as mixers, lters, ampliers, detectors, etc.) are implemented as software. SDR is responsible for transmission and reception of radio frequency signals [72]. A few of the popular SDRs are HackRF One, USRP, BladeRF, and RTL-SDR. They all have reception capability (passive attack) but some having transmission capability too (active attack). They have different operational frequencies: HackRF One (30MHz-6GHz), USRP(50MHz-6GHz), BladeRF(300MHz-3.8GHz) and RTL-SDR [73]. Cheap SDRs ($10 to $100)are emerging as tools of threat readily available to threat actors [17].

Table 4 presents a taxonomy of attacks on wireless technologies and proposed solutions available in the literature. Furthermore, it summarizes the existing literature on the basis of attack types and security properties compromised. Attacks considered are (i) Eavesdropping: passive attack such as listening to control traffic; (ii) Jamming: active attack such as channel blockage; (iii) Flooding: active attack targeting service to genuine user request; (iv) Injection: active attack by injecting unauthorized messages for eg. ghost messaging; (v) Alteration: an active attack performed by altering genuine message; and (vi) Spoofing or masquerading: an active attack performed by taking the identity of another user. Eavesdropping, jamming, and alteration compromises message confidentiality, availability, and integrity respectively. Masquerading targets authentication and non-repudiation. Whereas, injection leads to compromising all.

4.3. Aviation Security Frameworks and Solutions

Despite the fact that the avionics industry is not the only one to battle network protection issues, the difficulties in transportation frameworks are also crucial. The aviation sector is still attempting to comprehend cybersecurity threats, risks, and management. Various standard bodies and organizations such as Aviation Information Sharing and Analysis Center (ISAC), International Aviation Transport Association, and International Civil Aviation Organization, are providing guidelines and instruction about new emerging risks and attack vectors. The objectives of such standard organization to incorporate recognizing online protection weaknesses, evaluating dangers, and discovering standard alleviations to deal with the dangers to the aviation security framework. Security isn't yet as inserted as unwavering quality into the design life pattern of aviation frameworks. Regular avionics framework concerns, for example, safety, the performance of flights, environmental impact, fuel efficiency, and airspace security. A comparison of existing security frameworks and solutions for the aviation domain is shown in Table 5.

Mirchandani and Adhikari [74] gave aviation cyber threat vector audit matrix. Tamasi and Demichela [2] discussed a set of methodologies to assess the risk in the Security of civil aviation. Sam Adhikari [75] presented a comparison of aviation cybersecurity frameworks such as NIST and COBIT frameworks. Adhikari and Davis [76] discussed the applicability of blockchain with aviation cybersecurity framework and authors argued that blockchain can provide the needed digital data security for aviation operations. Kiesling et al. [50] gave a model-based approach for aviation cybersecurity risk assessment.

Mirchandani and Adhikari [77] focused on Integrated Risk Assessment with aviation cybersecurity framework. Furthermore, Jaatun and Koelle [78] discussed cyber incident response management for the aviation domain. Baron et al. [79] developed a framework including trustworthiness requirements and models for aviation. Haass et al. [49] give a graph-based communication-oriented framework for aviation cybersecurity. Dhafer Fayez Alqushayri [84] discussed cybersecurity threats and countermeasures of avionics network systems, and their associated defense safety mechanisms. Sampigethaya and Poovendran [85] gave a CPS framework for future aviation information systems.

The new aviation security frameworks being developed should not only address current dangers, but also envision the need to address conceivable future concerns that were not a piece of prior plans. The aviation frameworks being developed for flight control, position, and programmed pilot abilities must incorporate security, authenticity, and privacy. The future communication framework in the aviation business must be considered for

Table 4: Taxonomy classification of attacks and proposed solutions on securing wireless aviation System.

[E: Eavesdropping, J: Jamming, F: Flooding, I: Injection, A: Alteration, S: Spoofing, C: Confidentiality, I: Integrity, A: Availability, NR: Non-Repudiation] (*Partial)

Protocols	Attacks	Type of Attacks						Attack on				Proposed Solutions
		E	J	F	I	A	S	C	I	A	NR	
VHF	[58], [59],[60]	✓	✓		✓	✓	✓	×	×	×	×	[61], [62], [63], [64]
CPDLC	[22], [20], [24],[25]	✓	✓	✓	✓	✓	✓	×	×	×	×	[20], [65], [66]
VOR	[31], [62], [63]	✓						×				[62],[63]
DME	[31], [62], [63]	✓						×				[62],[63]
ILS	[29], [28], [30]		✓							×	×	[29]
PSR	[31], [35], [36]	✓	✓					×		×		[62],[63]
SSR	[29], [17], [25]	✓	✓*	✓	✓			×		×	×	[29]
ADS-B	[67], [68], [42], [45], [46]	✓	✓	✓	✓	✓	✓	×	×	×	×	[69], [70]

its capability to identify the blocked, spoofed, intercepted, and possibly altered communication as well as intruders.

5. Conclusion and Future Research Opportunities

Attacks on aviation systems and the various building blocks (e.g., communication, navigation, and surveillance systems) are not likely to disappear in the foreseeable future. This reinforces the importance of cybersecurity in the aviation industry, and hence motivated this research. We hope that the findings presented in this research will benefit the security community and other stakeholders (e.g., policy- and decision-makers), particularly those in the aviation industry.

We also identify a number of potential future research directions, as discussed below.

- Minimize operational overheads and increase dynamic load balancing: In a distributed aviation network, the exhibition of the framework can rely mainly upon splitting work successfully over the coordinating systems [11, 90]. Dynamic load adjusting has the capability of performing in a way that is better than static techniques. Therefore, the operational overheads should be balanced for better performance. Dynamic load balancing in the aviation industry can be considered as an efficient arrangement and a theme to follow for additional exploration.

- Operation Cost Minimization: The security solution should not provide a burden to existing security frameworks. The aviation industry is a real-time consumer of resources in terms of networks, therefore, the air traffic monitoring tools should be effectively installed and maintained. The Industry control frameworks are hard to maintain and operate and it is getting progressively hard to meet the functional requirements of innovations in the industrial context [91].

- Reliability and Performance: The Aviation Information Sharing and Analysis Center fills in as a clearinghouse for best practices from industry and the scholarly community intending to singular frameworks. The airlines are dashing to offer types of assistance to travellers, flight upholds for the team, and more productive instruments for diagnostics and support [92]. The online protection of these activities may not be staying up with the hurry to the serious commercial center. To understand resource efficiency and reliability, consumption-focused indicators should be incorporated in the aviation industry [85].

- Dynamic Routing Adaptability: The dynamic topologies and adaptive routing encourage on-request and sensible conditions for avionics. The dynamic routing topologies uphold waypoint coordination in flying organizations. The conventional delays exhibited through the general routing algorithms do not efficiently accommodate flight coordination. Therefore, adaptive routing mechanisms should be implemented for dynamically changing topologies. Existing aviation systems do comprise protocols such as CPDLC and ADS-B, which were designed with a significantly weaker threat model in mind. Advancements in disruptive techniques have exposed them. In long term, secure data link development needs to be a priority over which other communication technologies can rely upon. In short term with an existing data link, secure network layer solutions should be developed.

- Adaptive Security Solutions: The on-demand security in the aviation sector, open the door for various level of authentications. The military and civil aviation sectors are the prominent sectors to adopt adaptive security in various domains. Secure ATM and air communications are still open for future research. Penetration testing of usable wireless technologies should be allowed to assess their strength and vulnerabilities. Moreover, independent analysis of technology does not present the real picture unless tested on the complete system [93].

- Real-world penetration testing: To gauge the full impact of attacks on all wireless technologies used in aviation, penetration testing of the systems as used in practice is required. While attacks on any single technology are trivial, little is known about the concrete effects in the real world. Many of the deployed ATC systems are highly proprietary and essentially acting as a black box between

Table 5: A comparison of existing security frameworks and solutions for aviation domain. (*: discussions only)

Research	Key contributions	Considerations					
		Attack	Security	Risk	Protocols	Vulnerabilities	Threat
Tamasi and Demichela [2]	Gives a set of methodologies to assessing the risk in the security of civil aviation	✓	✓	✓		✓	✓
Mirchandani and Adhikari [74]	Presents aviation cyber threat vector audit matrix	✓	✓	✓		✓	✓
Sam Adhikari [75]	Presents a comparison of aviation cybersecurity framework	✓	✓	✓			
Adhikari and Davis [76]	Discusses the applicability of blockchain with aviation cybersecurity framework		✓	✓			
Mirchandani and Adhikari [77]	Integrated risk assessment with aviation cybersecurity framework		✓	✓		✓	
Jaatun and Koelle [78]	Discussed cyber incident response management for the aviation domain.	✓*	✓	✓			
Baron et al. [79]	Developed a framework including trustworthiness requirements and models for aviation	✓	✓	✓		✓	✓
Haass et al. [49]	Gives a graph-based communication-oriented framework for aviation cybersecurity	✓	✓	✓*	✓*		✓
Bhatia et al. [80]	Gives and N2N model for aviation rransportation and ryber rhreats	✓*	✓*	✓			✓*
Kiesling et al. [50]	Gives a model-based approach for aviation cyber security risk assessment	✓	✓	✓			✓
Haass et al. [81]	Discussed the advancements in aviation cyber security	✓*	✓	✓			✓*
Anna Baron Garcia [82]	Gives two information security framework for aviation systems	✓*	✓	✓		✓*	✓
Kumar and Xu [83]	Gives a vulnerability assessment framework for aviation CPS security	✓	✓	✓	✓*	✓	
Dhafer Fayez Alqushayri [84]	Discusses cybersecurity threats and countermeasures of avionics network systems, and their associated defense safety mechanisms	✓	✓	✓		✓	✓
Sampigethaya and Poovendran [85]	Gives a CPS framework for future aviation information systems		✓				✓
Taleqani et al. [86]	Discussed cyber threats in the aviation industry and machine learning solutions	✓	✓				✓
Kagalwalla et al. [87]	discusses the need for cyber-security in aviation and presents the solutions	✓	✓	✓		✓	✓
Sampigethaya and Kopardekar [88]	Discussed UTM cyber security needs and issues.	✓	✓	✓		✓	✓
Chirichiello at al. [89]	Discussed research advances in ATM	✓	✓				✓

the reception of wireless messages and, for example, their final display on ATC radar screens.

- Advanced security mechanisms for tactical and strategic operations: The operations of air traffic services are organized into tactical and strategic operations. The VHF-AM voice communications are used for tactical operations. The information conveyed over the VHF medium are relevant for tactical context. A high level of security of analogue voice communications may be tricky and costly to implement. The future advanced mechanisms for security voice-based communications may explore voice scrambling, digital ciphering and voice print authentication methods. The implementation of advanced security features in the voice communication infrastructure shall be conservative for the existing operational procedures and shall not affect the perception of voice communications by the pilots and the controllers.

- Secure data link communication: Although the security issues have not been actually addressed in the standardization of data link protocol, there is still an opportunity to add security features such as authentication of the data-link communication provider, integrity, anti-replay protection and proof of origin.

- Optimal tradeoff between security and performance of aviation frameworks: While designing protocols pseudonym identifiers with a limited lifetime be considered for anonymity, in case of a leakage. Multiple CNS protocols such as SSR, CPDLC acts as a secondary redundant system. The addition of a redundant system introduces new attack surfaces to be exploited. A weak redundant system may lead to information leakage. Therefore, future generation frameworks should sustain among security as well as the performance [94, 95].

- AI-driven Solutions: Security system enhanced with machine learning-based prediction models to identify intrusion or outlier among existing systems transactions should be researched for attack detection as a proactive approach [96].

Acknowledgement

This research is partially supported by the Soonchunhyang University Research Fund.

Appendix

Table 6 lists acronyms used in the paper.

Table 6: Summary of Acronyms used

Notations	Used Acronym
ADS-B	Automatic Dependent Surveillance-Broadcast
ATC	Air Traffic Control
ATM	Air Traffic Management
CNS	Communication, Navigation and Surveillance
CPDLC	Controlled Pilot Data Link Communication
DME	Distance Measuring Equipment
DSCN	Digital Satellite Communication Network
GNSS	Global Navigation Satellite System
HF	High Frequency
ILS	Instrument Landing System
PSR	Primary Surveillance Radar
SSR	Secondary Surveillance Radar
TCAS	Traffic alert and Collision Avoidance System
VDL	VHF Data Link
VHF	Very High Frequency
VOR	VHF Omni-directional Range

References

[1] E. Mazareanu, Leading airports worldwide by aircraft movements (10 2020).
URL https://www.statista.com/statistics/226823/largest-airports-worldwide-by-flight-operations/

[2] G. Tamasi, M. Demichela, Risk assessment techniques for civil aviation security, Reliability Engineering & System Safety 96 (8) (2011) 892–899.

[3] H. Teso, Aircraft hacking: Practical aero series, in: 4th Hack in the Box Security Conference in Europe, 2013.

[4] R. Hickey, Dhs led team demonstrates that commercial aircraft can be remotely hacked (11 2017).
URL https://www.defensedaily.com/dhs-led-team-demonstrates-commercial-aircraft-can-remotely-hack cyber/

[5] C. Cimpanu, Dhs warns about can bus vulnerabilities in small aircraft (07 2019).
URL https://www.zdnet.com/article/dhs-warns-about-can-bus-vulnerabilities-in-small-aircraft/

[6] P. Hollinger, Can your flight be hacked? (10 2018).
URL https://www.ft.com/content/2e416eca-4e3d-11e8-ac41-759eee1efb74

[7] N. McAllister, Faa: 'no, you can't hijack a plane with an android app' (04 2013).
URL https://www.theregister.com/2013/04/13/faa_debunks_android_hijack_claim/

[8] J. Smith, White house call for stronger aviation security includes cyber, uas (02 2019).
URL https://www.meritalk.com/articles/white-house-call-for-stronger-aviation-security-includes-cyber-

[9] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, Y. Halgand, A survey of approaches combining safety and security for industrial control systems, Reliability engineering & system safety 139 (2015) 156–178.

[10] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, K. Jones, A survey of cyber security management in industrial control systems, International journal of critical infrastructure protection 9 (2015) 52–80.

[11] G. Lykou, G. Iakovakis, D. Gritzalis, Aviation cybersecurity and cyber-resilience: Assessing risk in air traffic management, in: Critical Infrastructure Security and Resilience, Springer, 2019, pp. 245–260.

[12] C. Nobles, Cyber threats in civil aviation, in: Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications, IGI Global, 2019, pp. 119–141.

[13] M. Khatun, H. Mehrpouyan, D. Matolak, I. Guvenc, Millimeter wave systems for airports and short-range aviation communications: A survey of the current channel models at mmwave frequencies, in: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), IEEE, 2017, pp. 1–8.

[14] M. G. Stewart, J. Mueller, A risk and cost-benefit assessment of united states aviation security measures, Journal of Transportation Security 1 (3) (2008) 143–159.

[15] A. J. Lee, A. G. Nikolaev, S. H. Jacobson, Protecting air transportation: a survey of operations research applications to aviation security, Journal of Transportation Security 1 (3) (2008) 160.

[16] G. Lykou, A. Anagnostopoulou, D. Gritzalis, Smart airport cybersecurity: Threat mitigation and cyber resilience controls, Sensors 19 (1) (2019) 19.
[17] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, I. Martinovic, On perception and reality in wireless air traffic communication security, IEEE transactions on intelligent transportation systems 18 (6) (2016) 1338–1357.
[18] M. N. Jamil, M. S. Hossain, R. U. Islam, K. Andersson, Technological innovation capability evaluation of high-tech firms using conjunctive and disjunctive belief rule-based expert system: A comparative study, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 11 (3) (2020) 29–49.
[19] I. Annex, 10–aeronautical telecommunications, Volume II: Communication Procedures.
[20] A. Gurtov, T. Polishchuk, M. Wernberg, Controller–pilot data link communication security, Sensors 18 (5) (2018) 1636.
[21] R. F. SC-186, Minimum Operational Performance Standards (MOPS) for Aircraft Surveillance Applications (ASA) System, RTCA, Incorporated, 2011.
[22] M. S. B. Mahmoud, A. Pirovano, N. Larrieu, Aeronautical communication transition from analog to digital data: A network security survey, Computer Science Review 11 (2014) 1–29.
[23] R. Bembenik, K. Falcman, Ble indoor positioning system using rssi-based trilateration, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 11 (3) (2020) 50–69.
[24] D. Di Marco, A. Manzo, M. Ivaldi, J. Hird, Security testing with controller-pilot data link communications, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, 2016, pp. 526–531.
[25] O. Osechas, M. Mostafa, T. Graupl, M. Meurer, Addressing vulnerabilities of the cns infrastructure to targeted radio interference, IEEE Aerospace and Electronic Systems Magazine 32 (11) (2017) 34–42.
[26] R. Bauernfeind, T. Kraus, A. S. Ayaz, D. Dötterböck, B. Eissfeller, Analysis, detection and mitigation of incar GNSS jammer interference in intelligent transport systems, Deutsche Gesellschaft für Luft-und Raumfahrt-Lilienthal-Oberth eV, 2013.
[27] M. Strohmeier, M. Schäfer, M. Smith, V. Lenders, I. Martinovic, Assessing the impact of aviation security on cyber power, in: 2016 8th International Conference on Cyber Conflict (CyCon), IEEE, 2016, pp. 223–241.
[28] H. Sathaye, D. Schepers, A. Ranganathan, G. Noubir, Wireless attacks on aircraft landing systems, in: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, ACM, 2019, pp. 295–297.
[29] M. Neffe, T. Van Pham, H. Hering, G. Kubin, Speaker segmentation for air traffic control, in: Speaker Classification II, Springer, 2007, pp. 177–191.
[30] M. Smith, M. Strohmeier, J. Harman, V. Lenders, I. Martinovic, Safety vs. security: Attacking avionic systems with humans in the loop, arXiv preprint arXiv:1905.08039.
[31] D. Adamy, EW 101: A first course in electronic warfare, Vol. 101, Artech house, 2001.
[32] E. Kim, Analysis of dme/dme navigation performance and ground network using stretched-front-leg pulse-based dme, Sensors 18 (10) (2018) 3275.
[33] S. C. Lo, P. Enge, Assessing the capability of distance measuring equipment (dme) to support future air traffic capacity, NAVIGATION, Journal of the Institute of Navigation 59 (4) (2012) 249–261.
[34] J. M. Headrick, S. J. Anderson, M. Skolnik, Hf over-the-horizon radar, Radar handbook 20.
[35] F. Edition, Electronic warfare and radar systems.
[36] D. Adamy, EW 103: Tactical battlefield communications electronic warfare, Artech House, 2008.
[37] I. Annex, 10–aeronautical telecommunications, Volume IV: Sureveillance and Collision Avoidance Systems.
[38] M. Mostafa, O. Osechas, M. Schnell, Vulnerability analysis of the cns-infrastructure: An exemplarily approach, in: 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), IEEE, 2016, pp. 1–9.
[39] N. Akshay, R. Shruthi, K. Sushmitha, R. Vanitha, K. Rekha, Live aircraft detection with mode-s transponder using rtl-sdr, International Journal 7 (5).
[40] G. X. Gao, M. Sgammini, M. Lu, N. Kubo, Protecting gnss receivers from jamming and interference, Proceedings of the IEEE 104 (6) (2016) 1327–1338.
[41] A. Abhishta, W. van Heeswijk, M. Junger, L. J. M. Nieuwenhuis, R. Joosten, Why would we get attacked? an analysis of attacker's aims behind ddos attacks, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 11 (2) (2020) 3–22.
[42] D. McCallie, J. Butts, R. Mills, Security analysis of the ads-b implementation in the next generation air transportation system, International Journal of Critical Infrastructure Protection 4 (2) (2011) 78–87.
[43] R. F. SC-186, Minimum Operational Performance Standards for 1090 MHz Automatic Dependent Surveillance-broadcast (ADS-B), RTCA, 2000.
[44] W. Chung, R. Staab, A 1090 extended squitter automatic dependent surveillance-broadcast (ads-b) reception model for air-traffic-management simulations, in: AIAA modeling and simulation technologies conference and exhibit, 2006, p. 6614.
[45] L. Kenney, J. Dietrich, J. Woodall, Secure atc surveillance for military applications, in: MILCOM 2008-2008 IEEE Military Communications Conference, IEEE, 2008, pp. 1–6.
[46] M. Leonardi, E. Piracci, G. Galati, 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.
[47] A. J. Kornecki, Z. Janusz, Threat modeling for aviation computer security, crosstalk 21.
[48] C. Cioaca, M. Boscoianu, An introduction in the risk modeling of aviation security systems, in: Proceedings of the 12th WSEAS international conference on Mathematics and computers in biology, business and acoustics, 2011, pp. 100–105.
[49] J. C. Haass, J. P. Craiger, G. C. Kessler, A framework for aviation cybersecurity, in: NAECON 2018-IEEE National Aerospace and Electronics Conference, IEEE, 2018, pp. 132–136.
[50] T. Kiesling, M. Krempel, J. Niederl, J. Ziegler, A model-based approach for aviation cyber security risk assessment, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, 2016, pp. 517–525.
[51] T. Li, B. Wang, F. Shang, J. Tian, K. Cao, Threat model and construction strategy on ads-b attack data, IET Information Security 14 (5) (2020) 542–552.
[52] A. R. Schmitt, C. Edinger, T. Mayer, J. Niederl, T. Kiesling, Simulation-supported aviation cyber-security risk analysis: a case study, CEAS Aeronautical Journal 10 (2) (2019) 517–530.
[53] E. Ukwandu, M. A. B. Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis, X. Bellekens, Cyber-security challenges in aviation industry: A review of current and future trends, arXiv preprint arXiv:2107.04910.
[54] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, C. Woody, Threat modeling: a summary of available methods, Tech. rep., Carnegie Mellon University Software Engineering Institute Pittsburgh United (2018).
[55] A. Shostack, Threat modeling: Designing for security, John Wiley & Sons, 2014.
[56] T. UcedaVelez, M. M. Morana, Risk Centric Threat Modeling: process for attack simulation and threat analysis, John Wiley & Sons, 2015.
[57] G. Kasturi, A. Jain, J. Singh, Detection and classification of radio frequency jamming attacks using machine learning, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 11 (4) (2020) 49–62.
[58] T. H. Stelkens-Kobsch, A. Hasselberg, T. Mühlhausen, N. Carstengerdes, M. Finke, C. Neeteson, Towards a more secure atc voice communications system, in: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), IEEE, 2015, pp. 4C1–1.
[59] R. Zhang, G. Liu, J. Liu, J. P. Nees, Analysis of message attacks in aviation data-link communication, IEEE Access 6 (2017) 455–463.
[60] N. Ghose, L. Lazos, Verifying ads-b navigation information through doppler shift measurements, in: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), IEEE, 2015, pp. 4A2–1.
[61] R. Fantacci, S. Menci, L. Micciullo, L. Pierucci, A secure radio communication system based on an efficient speech watermarking approach, Security and Communication Networks 2 (4) (2009) 305–314.
[62] H. Hering, G. Kubin, et al., Safety and security increase for air traffic management through unnoticeable watermark aircraft identification tag transmitted with the vhf voice communication, in: Digital Avionics Sys-

tems Conference, 2003. DASC'03. The 22nd, Vol. 1, IEEE, 2003, pp. 4–E.

[63] M. Hagmüller, H. Hering, A. Kröpfl, G. Kubin, Speech watermarking for air traffic control, in: 2004 12th European Signal Processing Conference, IEEE, 2004, pp. 1653–1656.

[64] J. Prinz, M. Sajatovic, B. Haindl, S/sup 2/ev-safety and security enhanced atc voice system, in: 2005 IEEE Aerospace Conference, IEEE, 2005, pp. 1924–1930.

[65] J. H. Griner, An elliptic curve based authentication protocol for controller-pilot data link communications.

[66] T. McParland, V. Patel, W. Hughes, Securing air-ground communications, in: 20th DASC. 20th Digital Avionics Systems Conference (Cat. No. 01CH37219), Vol. 2, IEEE, 2001, pp. 7A7–1.

[67] A. Costin, A. Francillon, Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices, Black Hat USA (2012) 1–12.

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

[69] M. R. Manesh, N. Kaabouch, Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ads-b) system, International Journal of Critical Infrastructure Protection 19 (2017) 16–31.

[70] P. Park, H. Khadilkar, H. Balakrishnan, C. J. Tomlin, High confidence networked control for next generation air transportation systems, IEEE Transactions on Automatic Control 59 (12) (2014) 3357–3372.

[71] O. V. Baranov, N. V. Smirnov, T. E. Smirnova, Y. V. Zholobov, Design of a quadrocopter with pid-controlled fail-safe algorithm, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 11 (2) (2020) 23–33.

[72] V. R. Gannapathy, T. Ibrahim, A. Fayeez, Z. Zakaria, A. R. Othman, N. Q. Jalaudin, A review on various types of software defined radios (sdrs) in radio communication, International Journal of Research in Engineering and Technology (IJRET) 3 (12) (2014) 203–209.

[73] L. Pucker, Channelization techniques for software defined radio, in: Proceedings of SDR Forum Conference, 2003, pp. 1–6.

[74] S. Mirchandani, S. Adhikari, Aerospace cybersecurity threat vector assessment, in: ASCEND 2020, 2020, p. 4116.

[75] S. Adhikari, An analysis of aiaa aviation cybersecurity framework in relation to nist, cobit and dhs frameworks, in: AIAA AVIATION 2020 FORUM, 2020, p. 2930.

[76] S. Adhikari, C. Davis, Application of blockchain within aviation cybersecurity framework, in: AIAA AVIATION 2020 FORUM, 2020, p. 2931.

[77] S. Adhikari, S. Mirchandani, Integrating risk assessment modeling with aviation cybersecurity framework, in: AIAA AVIATION 2020 FORUM, 2020, p. 2932.

[78] M. G. Jaatun, R. Koelle, Cyber security incident management in the aviation domain, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, 2016, pp. 510–516.

[79] A. Baron, R. F. Babiceanu, R. Seker, Trustworthiness requirements and models for aviation and aerospace systems, in: 2018 Integrated Communications, Navigation, Surveillance Conference (ICNS), IEEE, 2018, pp. 1B3–1.

[80] U. Bhatia, S. Chatterjee, A. R. Ganguly, J. Gao, M. Halappanavar, M. Oster, K. Clark, R. Brigantic, R. Tipireddy, Aviation transportation, cyber threats, and network-of-networks: Modeling perspectives for translating theory to practice, in: 2018 IEEE International Symposium on Technologies for Homeland Security (HST), IEEE, 2018, pp. 1–7.

[81] J. Haass, R. Sampigethaya, V. Capezzuto, Aviation and cybersecurity: opportunities for applied research, TR News (304) (2016) 39.

[82] A. B. Garcia, Building and integrating an information security trustworthiness framework for aviation systems.

[83] S. A. Kumar, B. Xu, Vulnerability assessment for security in aviation cyber-physical systems, in: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, 2017, pp. 145–150.

[84] D. F. Alqushayri, Cybersecurity vulnerability analysis and countermeasures of commercial aircraft avionic systems.

[85] K. Sampigethaya, R. Poovendran, Cyber-physical integration in future aviation information systems, in: 2012 IEEE/AIAA 31st Digital Avionics Systems Conference (DASC), IEEE, 2012, pp. 7C2–1.

[86] A. R. Taleqani, K. E. Nygard, R. Bridgelall, J. Hough, Machine learning approach to cyber security in aviation, in: 2018 IEEE International Conference on Electro/Information Technology (EIT), IEEE, 2018, pp. 0147–0152.

[87] N. Kagalwalla, P. P. Churi, Cybersecurity in aviation: An intrinsic review, in: 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), IEEE, 2019, pp. 1–6.

[88] K. Sampigethaya, P. Kopardekar, J. Davis, Cyber security of unmanned aircraft system traffic management (utm). in 2018 integrated communications, navigation, in: Surveillance Conference (ICNS)(pp. 1C1-1). IEEE, 2018.

[89] A. Chirichiello, C. Porretti, A. Berardi, Cyber threat intelligence for supporting the atm security management., in: ITASEC, 2017, pp. 253–257.

[90] D. P. Johnson, Civil aviation and cybersecurity, Pobrane z: http://sites. nationalacademies. org/cs/groups/depssite/documents/webpage/deps_084768. pdf.

[91] K. Sampigethaya, R. Poovendran, Security and privacy of future aircraft wireless communications with offboard systems, in: 2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011), IEEE, 2011, pp. 1–6.

[92] K. Sampigethaya, R. Poovendran, Aviation cyber–physical systems: Foundations for future aircraft and air transport, Proceedings of the IEEE 101 (8) (2013) 1834–1855.

[93] R. Sabatini, T. Moore, S. Ramasamy, Global navigation satellite systems performance analysis and augmentation strategies in aviation, Progress in Aerospace Sciences 95 (2017) 45–98.

[94] H. Sedjelmaci, S. M. Senouci, Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution, The Journal of Supercomputing 74 (10) (2018) 4928–4944.

[95] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, C. Royalty, Future e-enabled aircraft communications and security: The next 20 years and beyond, Proceedings of the IEEE 99 (11) (2011) 2040–2055.

[96] H. Kim, J. Ben-Othman, L. Mokdad, J. Son, C. Li, Research challenges and security threats to ai-driven 5g virtual emotion applications using autonomous vehicles, drones and smart devices, IEEE Network.

Gaurav Dave: Software and Implementation; Gaurav Choudhary: Data curation, Writing- Original draft preparation, Visualization; Vikas Sihag: Data curation, Writing- Original draft preparation, Visualization; Ilsun You: Visualization, Investigation, Supervision, Reviewing, and Editing; Kim-Kwang Raymond Choo: Visualization, Investigation, Supervision, Reviewing, and Editing.

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Gaurav Dave is a Junior Security Engineer at Norsk Hydro, India. He is a security researcher having a keen interest in aviation security, drone security, and communication security. He has done a Master of Technology in Cyber Security from the Sardar Patel University of Police and a Bachelors in Computer Science.

Gaurav Choudhary received a Ph.D. in Information Security Engineering from Soonchunhyang University, South Korea. He is presently working as an Assistant Professor in the School of Computer Science and Engineering (SCSE) at VIT Bhopal University. Before joining VIT Bhopal, he worked at Mobile Internet Security Laboratory (MobiSec Lab), South Korea as a Security Researcher on various projects funded by reputed organizations such as the Institute for Information and Communications Technology Promotion (IITP), National Research Foundation of Korea (NRF), and the Air Force Office of Scientific Research (AFOSR), USA. His current research interests include Threat Intelligence, IoT and CPS Security, Cyber Security, Vulnerability Assessment, 5G Security, Drone Security, and Cryptography. He has authored or co-authored many reputed SCI journal/conference papers and book chapters. He also serves as a Reviewer for various IEEE, ACM, and other journals.

Vikas Sihag has been an Assistant Professor with the Department of Cyber Security, Sardar Patel University of Police since 2013. He is also associated as a researcher with the Department of Computer Science and Engineering, National Institute of Technology, Raipur. He has received his Masters in Information Security from Motilal Nehru National Institute of Technology, Allahabad. His current research interests include Android security, malware analysis, digital forensics and protocol security. He is a British Standards Institution certified Information Security Management Systems - Lead auditor. He is also a CEH (Certified Ethical Hacker) and CEI (Certified EC-Council Instructor). He has organized various international and national training programs for Law Enforcement Agencies. He also has (co-)authored many journal/conference papers and book chapters.

Ilsun You (SM'13) received the MS and PhD degrees in computer science from Dankook University, Seoul, Korea, in 1997 and 2002, respectively. He received the second PhD degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was at the THINmultimedia Inc., Internet Security Co., Ltd. and Hanjo Engineering Co., Ltd. as a research engineer. Now, he is a full professor at Department of Information Security Engineering, Soonchunhyang University. He has served or is currently serving as a General Chair or a Program Chair of international conferences and workshops such as WISA'19-20, MobiSec'16-19, AsiaARES'13-15, MIST'09-17, MobiWorld'08-17, and so forth. Dr. YOU is the EiC of Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) and Journal of Internet Services and Information Security (JISIS). He is in the Editorial Board for Information Sciences (INS), Journal of Network and Computer Applications (JNCA), IEEE Access, Intelligent Automation & Soft Computing (AutoSoft), International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Computing and Informatics (CAI), and Journal of High Speed Networks (JHSN). Especially, he has focused on 4/5G security, security for wireless networks & mobile internet, IoT security and so forth while publishing more than 180 papers in these areas. He is a Fellow of the IET and a Senior member of the IEEE.

Kim-Kwang Raymond Choo holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He is the recipient of the 2019 IEEE TCSC Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Endowed Research Award for Tenured Faculty, IEEE Access Outstanding Associate Editor of 2018, British Computer Society's 2019 Wilkes Award Runner-up, 2019 EURASIP JWCN Best Paper Award, Korea Information Processing Society's JIPS Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian

Computer Society, an IEEE Senior Member, and Co-Chair of IEEE MTCT's Digital Rights Management for Multimedia Interest Group.