Securing the Air–Ground Link in Aviation

Martin Strohmeier, Ivan Martinovic, and Vincent Lenders

1 Introduction

As an increasingly interconnected and digitalized global system of systems, aviation faces new challenges. Passengers, airlines and air navigation service providers (ANSPs) all demand more connectivity; passengers for their entertainment needs, airlines for increased serviceability and more efficient operations, and ANSPs to help facilitate the safe control of the ever increasing flight traffic.

Recently, security researchers in both academia and industry have increasingly treated the aviation system as national and supra-national critical infrastructure similar to power grids, telecommunication and public health infrastructure. Responsible for this renewed focus on aviation security are new technological developments, which have shifted the threat model away from traditional electronic warfare and towards an easy accessibility of wireless systems by a wide variety of threat actors [109]. The ubiquitous availability of low-cost software-defined radio transceiver (SDR) technology enables both innocent amateurs and malicious actors to compromise civil aviation security.

Academic and industrial research on such matters has picked up significantly over the past decade, and those who argue that airports and aircraft are secure with current defenses slowly become the minority. However, there is still a large knowledge and awareness gap in the broader industry on this topic. Until recently, voices from outside and within the industry have been ignored too often and

M. Strohmeier (✉) · V. Lenders
armasuisse W + T, Thun, Switzerland
e-mail: martin.strohmeier@armasuisse.ch; vincent.lenders@armasuisse.ch

I. Martinovic
Department of Computer Science, University of Oxford, Oxford, UK
e-mail: ivan.martinovic@cs.ox.ac.uk

M. M. Keupp (ed.), *The Security of Critical Infrastructures*, International Series
in Operations Research & Management Science 288,
https://doi.org/10.1007/978-3-030-41826-7_9

necessary actions such as information sharing have not been taken or delayed considerably.

It is commonly held that reminding passengers about any potential dangers of flying is likely to be detrimental to the aviation industry as a whole. Consequently, the main goal with regards to cybersecurity is to not scare the public at all costs. In a traditionally very secretive industry, this means that public information is scarce and often unreliable, and cybersecurity is no exception.

In this work, we compile and systematize the existing sources on the topic of wireless security in civil aviation. We first compile recent academic research on vulnerabilities but also real-world reports on possible incidents, such as news articles and analyses conducted by aviation authorities. Then, we discuss the existing strategies suggested by researchers to address the problems of integrity, authenticity and confidentiality. Our aim is to fill the knowledge and awareness gaps that exist around the security and privacy of commonly used communication technologies in aviation. Similarly, we hope to provide a reliable resource for aspiring researchers who look to get started in this field and who seek to understand its most important issues.

To make these contributions, we survey the literature on reported security incidents and privacy breaches and link this evidence to extant research on security and privacy in aviation. We use these insights to create a taxonomy of feasible countermeasures, and we develop recommendations for future aviation security research.

The remainder of this chapter is organized as follows: Sect. 2 discusses and classifies known vulnerabilities and incidents. Section 3 then outlines the existing research on security before it examines the work on privacy. Finally, based on the insights from this discussion, Sect. 4 defines a research agenda for both areas.

2 Classification of Air–Ground Link Incidents and Vulnerabilities

We first survey and systematize all incidents and vulnerabilities across the technologies that underpin modern air traffic management (ATM) that have been reported in the past. We first consider those that impact the security of the system, followed by privacy-related incidents. Table 1 provides a short glossary of the surveyed technologies.

2.1 Security Incidents

Table 2 lists reported incidents and vulnerabilities relating to air–ground links, with attack vectors including denial of service (DoS), jamming, injection and intrusion.

Table 1 Glossary of the analyzed technologies

Abb.	Technology
ACARS	Aircraft Communications Addressing and Reporting System
ADS-B	Automatic Dependent Surveillance-Broadcast
CPDLC	Controller-Pilot Data Link Communication
MLAT	Multilateration
PSR	Primary Surveillance Radar
SSR	Secondary Surveillance Radar
TCAS	Traffic Alert and Collision Avoidance System
VHF	Very High Frequency (voice transmission)

Table 2 Reported security incidents and vulnerabilities related to different air traffic control (ATC) technologies

Technology	Type	Vector	Description	Sources
ADS-B	Vulnerability	Injection	Analysis of different types of message injection in theory and in lab	[19, 88]
	Vulnerability	Jamming	Analysis of jamming with SDR in lab	[56]
	Exploit	Injection	Software enabling ADS-B spoofing with SDRs	[20]
SSR	Incident	DoS	Ground-based over-interrogation of aircraft transponders, causing real-world radar failures.	[85]
	Vulnerability	Jamming, Injection	Lab analysis by German Aerospace Center	[78]
PSR	Vulnerability	Jamming	Traditional electronic warfare	[1–3]
MLAT	Vulnerability	Injection	Proof of concept of an attack on MLAT system in lab	[70, 94]
VHF	Incident	Injection	Spoofing of ATC in Turkish airspace and at Melbourne airport	[100, 134]
	Incident	DoS	Regular communication interference from pirate radio stations and other unlicensed transmitters	[101]
ACARS	Vulnerability	Intrusion	Remote intrusion in lab into flight management system	[118]
	Vulnerability	Injection	Analysis of different types of message injection theoretically and in lab	[12, 86, 137]
CPDLC	Incident	Injection	Delayed CPDLC messages received undetected at aircraft hours later	[5, 93]
	Vulnerability	Jamming, Injection, DoS	Lab analyses conducted by several different aviation authorities	[23, 78]

Additionally, eavesdropping is possible for all considered technologies as none of them uses encryption. While we believe that eavesdropping is not a direct security issue, it does compromize the privacy of both passengers and airline staff. We discuss these implications in Sect. 2.2. It is noteworthy that there have been no academic studies or public incident reports with regards to TCAS, although its vulnerability is similar to the SSR and ADS-B technologies whose information TCAS uses.

2.1.1 ADS-B

The introduction of ADS-B has motivated much research on aviation security. Talks by hackers and academics pointed out the absence of any security in the protocol by the early 2010s (e.g. [19]). Later works analyzed the concrete physical circumstances (distance, sending power) required to manipulate the 1090 MHz ADS-B channel and showed concrete laboratory attacks [56, 88]. The use of ADS-B is only mandatory since 2020, and it is not yet used widely in airline operations. Therefore, no security incidents have been reported to date. However, exploit kits, i.e., tool boxes for SDRs, which enable the spoofing of ADS-B messages are available online (e.g., [20]), such that attacks are presumably only a matter of time.

2.1.2 SSR

While there are no dedicated attack tool boxes available for SSR/Mode S, it shares the same fundamental protocol characteristics with ADS-B. Thus, sending and exploiting Mode S is trivially possible by adapting existing scripts such as [20] or others. Consequently, an analysis by the German Aerospace Center [78] showed that radio frequency interference is possible, enabling ghost aircraft, jamming, or transponder lockouts. There has been one widely reported real-world incident related to SSR jamming and over-interrogation, causing several aircraft to vanish from controllers' radar screens in Central Europe on two separate occasions in June 2014 [85]. The subsequent investigation by the European Aviation Safety Agency could not identify the culprit for this SSR over-interrogation but found it was unlikely the attack was malicious. Still, cybersecurity experts stress that such malicious attacks would be generally feasible [85].

2.1.3 PSR

PSR takes a special role in our survey, since attacks are not feasible with standard software-defined radio transmitters. PSR detection is based on the reflection of its own signals, thus there is no message content that could be injected or modified. It is true that PSR can be jammed, but this requires sophisticated and powerful military equipment. See [1–3] for a detailed account of primary radar jamming and electronic warfare. Since we want to focus on civil aviation, and since there is little research about attacks on PSR, we do not consider this topic any further.

2.1.4 MLAT

Multilateration uses the signals of other wireless protocols, such as SSR or ADS-B. Thus, MLAT is often considered as a verification technology for unauthenticated wireless links [44]. Even if the contents of, e.g., an ADS-B message are wrong, the location of the sender can still be identified. Thus, MLAT offers security by physical layer properties (specifically, by the propagation speed of electromagnetic waves) which are difficult to manipulate. However, real-world MLAT systems must rely on combining location and message content data as they attempt to authenticate the identification and altitude of a target. This dependability makes these systems as vulnerable to exploits as Mode A/C/S or ADS-B. Additionally, a well-coordinated and synchronized attacker may manipulate the time of arrival of a message at the distributed receivers of an MLAT system and hence may falsify location data [70].

2.1.5 VHF

VHF has long been subject to radio interference due to its analogue nature and well-known technological underpinning. Indeed, in a recent survey, aviation experts regarded VHF as the most untrustworthy communication with the highest likelihood of both benign and malicious interference [113], such as spoofed voice communication. For example, the impersonation of air traffic controllers in Turkish airspace [100] and at Melbourne airport [134] caused significant stress among real controllers. Further, VHF communication is regularly interfered with by non-licensed emitters such as pirate radio stations, implying additional workload for controllers who must identify such frequency abuse [101].

2.1.6 ACARS

ACARS vulnerabilities have been described as early as 2001 when a U.S. military official pointed out that forged ATC clearances may be issued by unauthenticated data links [86]. In 2013, Hugo Teso used second-hand hardware to show the potential of using ACARS to remotely exploit a Flight Management System (FMS). Recently, [137] has analyzed the injection of outside ACARS messages into an FMS in both theory and practice.

2.1.7 CPDLC

CPDLC is a relatively new technology; hence, it has only recently been scrutinized by security experts, partly because fully implemented decoders for SDRs have not been openly available. Nonetheless, CPDLC generally offers no authentication or confidentiality and hence is subject to the same attack vectors that are used to compromise ACARS. The German Aerospace Center has recently addressed some vulnerabilities of CPDLC [78], highlighting the ease with which this technology can be spammed and spoofed. While there are no public reports of malicious interference, the robustness of CPDLC against outside interference is questionable. To date, several investigations have been launched into duplicate, delayed or lost CPDLC messages as well as into logins to unauthenticated ground stations [5, 93]. These problems, while yet benign, illustrate the vulnerabilities of the system.

2.2 Privacy Incidents

Table 3 lists the known privacy-related incidents and vulnerabilities with respect to air traffic control communication. We can broadly classify these privacy issues into tracking-related and data link-related leaks. The overwhelming majority of the surveyed privacy incidents relates to the possibility of aircraft tracking, while very few studies discuss aircraft user privacy breaches by compromised data links.

2.2.1 Tracking-Related Privacy Leaks

Privacy is at risk predominantly because almost all ATC technologies allow non-aviation actors to closely track flight movements. Many websites on the Internet (e.g., *Flightradar24*, *ADS-B Exchange*, or the *OpenSky Network*) exploit one or several of these technologies, and they provide easy access to immediate, highly detailed and continuous tracking data. When this information is combined with data from other comprehensive sources (including authoritative ones such as the FAA [29]), individual aircraft users can be tracked at little cost [109].

ACARS transmits flight data, e.g., flight plans, by unencrypted data links, such that aircraft identifications, movements and locations are revealed to the public. The system therefore became an attractive high-value target. Novel SDR technology allows any outside listener to receive ACARS data links. As shown in [95–97], location data sent via satellite can be received far beyond the line-of-sight required for other technologies.

ADS-B has been held responsible for significant tracking and privacy issues ever since it became operational. As authorities in the US, Europe and many other airspaces make the use of ADS-B mandatory in all flights under instrument flight rules, even so for military, government or corporate flights, the effort required to track sensitive aircraft data has decreased substantially. There are reports of sensitive

Table 3 Reported privacy leaks and confirmed vulnerabilities on ATC technologies

Technology	Type of leak	Description of privacy leak	Ref's
ACARS	Tracking	Tracking sensitive aircraft using ACARS	[95, 97]
	Data	Personal data leakage on non-commercial and commercial aircraft	[95, 97, 121]
	Tracking, Data	Weak proprietary cryptography broken	[96]
ADS-B	Tracking	Leak of military operations	[15, 16]
	Tracking	Tracking of personal/governmental assets	[25]
	Tracking	Circumvention of aircraft blocking	[52]
	Tracking	Tracking of business assets	[79]
	Tracking	De-anonymization of transponder IDs	[87]
	Tracking	Fingerprinting of aircraft transponders	[57, 105]
SSR & MLAT	Tracking	Tracking of surveillance drones	[109]
VHF	Tracking	Aircraft tracking using voice recognition	[42]
ATC (general)	Tracking	Correlating CEO vacations with press releases	[131]
	Tracking	Analysis of CEO private aircraft use	[61]
	Tracking	Corporate aircraft movement tracking for merger data	[62, 114]
	Tracking	Large-scale analysis of effects of government and military aircraft tracking	[114, 115]
	Tracking	Use of aircraft blocking to hide merger negotiations	[18]
	Tracking	Analysis of aircraft patterns to uncover surveillance operations	[7]

military missions that were exposed by expoiting ADS-B information (e.g., [16]). Journalists have set up ADS-B receivers and Twitter bots which publicly announce the presence of government aircraft at Geneva airport. These data leaks are not only a privacy concern for users, but they have also been used as evidence in court [25]. Moreover, the public reporting of CEOs' corporate aircraft use has caused reputation and business loss [79]. The National Business Aviation Association (NBAA) has repeatedly criticized that ADS-B data intercepts are compromising the privacy of their members. In particular, they note that attempts to block online services from using these data can be circumvented [52]. Studies on ADS-B have shown that procedures designed to protect privacy in the ADS-B Universal Access Transceiver (UAT) data link are flawed [87] since pseudonyms can be correlated with real transponder IDs. Aircraft transponders can be fingerprinted on the physical and data link layer, such that aircraft can be tracked even if real transponder IDs are unknown [57, 105].

SSR/MLAT: Even if aircraft are not equipped with ADS-B, their location can be obtained by Mode S. Hence, the movements and locations of non-updated military aircraft can be exposed once multiple stations are able to receive the same signal. For example, the combination of SSR and MLAT data on the *Flightradar24* website allowed the public to track movements of the border surveillance drones of the Swiss armed forces [109].

VHF: While VHF remains the most important ATC communication option to date, both its analogue nature and the fact that transmissions are not encrypted enable almost anyone to listen into local voice communication and identify aircraft registration codes. Websites such as *LiveATC*[1] publicly broadcast ATC communication transmitted by VHF. An experimental approach demonstrated that voice recognition algorithms can be used to automate and scale a tracking approach, even if blocking techniques designed to prevent public websites from accessing the data are used [42].

ATC (general): Many privacy issues are rather associated with ATC as a system than with any particular technology. Three studies have used a list of all civil flights in the United States between 2007 and 2011 that the Wall Street Journal obtained from the FAA following a Freedom of Information Act request. Journalists have used this dataset to track CEOs' private aircraft use. The publication of these data led to accusations of under-reported CEO income and increased scrutiny of corporate flight departments [61]. Other authors have used this dataset to establish a correlation between CEOs' holiday schedules and their companies' news announcements to predict stock price volatility [131]. Finally, the data have been used to correlate merger and acquisition activities with corporate flights [62], motivating later research that used ADS-B data to investigate the same issue [114].

Reports indicate that some companies are aware of this vulnerability and therefore attempt to prevent the exposure of their aircraft on public tracking websites [18]. Lastly, aircraft movement data obtained from the ATC system has been used to uncover government and military operations [114, 115] as well as surveillance operations by police entities [7].

2.2.2 Leaks of Personal Data

There have been only sporadic reports of privacy leaks on data links, despite the popularity of ACARS decoders such as acarsd.[2] A Swiss pilot magazine reports several incidents such as the transmission of credit card data, and it describes Internet forums where aviation enthusiasts share potentially sensitive ACARS messages [121]. Academic work has addressed the same issue in a more systematic way. The authors in [95, 97] examine the usage of ACARS in Central Europe. They analyze messages transmitted by VHF and satellite communication, showing that sensitive data such as credit card details, medical records, and passenger manifests were transmitted. In a related study [96], the authors show that there is a clear demand for privacy by ACARS users as some of them use mono-alphabetic

[1] https://www.liveatc.net.

[2] http://www.acarsd.org.

substitution ciphers in an attempt to protect their communication. Naturally, this approach is highly insecure and leaks both tracking information and personal data.

3 Defense

3.1 Security Countermeasures

We create a novel taxonomy that partitions the literature on countermeasures to security and privacy threats into four categories (viz. Table 4). We use this taxonomy to illustrate current research directions.

3.1.1 Cyber-Physical Security

While security has always been a major issue in computer networking, and academic research has developed countless strategies to secure and authenticate data and users, many of these are either bound to the traditional wired paradigm or difficult to deploy in a legacy-oriented aviation environment.

Cyber-physical systems (CPS) such as ATC combine computation and physical processes. Integrated feedback loops between these elements secure system monitoring and control. While classical attacker-defender models for wired networks have been developed, these can be too prohibitive since they do not consider the fact that in wireless networks there are always (if inadvertent) listeners. Hence, new solutions beyond cryptographic measures are required that can take into account the peculiarities of wireless communication. Such a cyber-physical approach to security

Table 4 Existing research on security for ATC technologies

Cyber-Physical Security	
Physical Layer	[9, 34, 50, 54–56, 58, 59, 70–72, 75 80, 90, 94, 106, 117, 124, 127, 133]
Localization	[26, 28, 67, 68, 89, 107, 112]
Watermark/Fingerprinting	[27, 39, 41, 83, 105, 133]
Machine Learning	
Classification	[30, 73, 100, 133]
Anomaly Detection	[30, 38, 54, 55, 59, 106, 108, 111]
Non-technical Measures	
Formal Methods	[12, 66, 69, 76, 116, 119]
Policies/Procedures	[17, 60, 74, 78, 98, 103, 123]
Cryptography	
Cryptographic Measures	[4, 8, 11, 13, 21, 22, 31–33, 35, 37, 43, 45–49, 53, 63, 64, 77, 82, 84, 86, 92, 102, 108, 120, 125, 128–130, 132, 135, 136]

should focus on attack detection in the first place and only deploy additional security measures if these are deemed necessary. Thus, the performance and the security requirements of the CPS may be balanced. To date, the extent research interest on CPS can be partitioned into three (if partially overlapping) areas: physical layer security, localization, and watermarking/fingerprinting.

Physical Layer Security

Physical layer security has recently emerged as a complementary technique to improve the communication security of wireless networks. A fundamentally different approach to cryptography, it establishes secrecy by exploiting the physical layer properties of the channel [138]. It is particularly attractive for the legacy systems found in aviation as it does not require changes to communication protocols or aircraft. The work in this area has identified several methods by which spoofing attacks can be identified, such as time differences of arrival [9, 70, 106], Doppler shifts [34, 90], direction of arrival [124], or angle of arrival [71]. Some authors [72, 117] further suggest the use of beamforming to detect spoofing attacks. Several works also exploit physical layer characteristics to improve defenses against jamming [56, 58, 127].

Localization

The opportunities the physical layer offers to increase security can also be exploited to verify aircraft location data. Hence, the veracity of ADS-B position messages can be checked. As localization is a relatively mature area of research, technical implementations based on multilateration have been realized. This approach seems promising since it is based on physical constants and constraints that are difficult to manipulate (e.g., the speed of light). For the case of ATC, most works have exploited time differences of arrival, often in the form of traditional multilateration [26, 67, 68] but also by alternative techniques [89, 107, 112]. Other approaches have used the angle of arrival to localize aircraft and to verify their position claims [28].

Watermarking/Fingerprinting

Watermarking and fingerprinting are two related approaches that both can identify or authenticate wireless devices and their users. Watermarking installs deliberate markers in the communication process that can be used by authentication algorithms. Fingerprinting exploits technological imperfections of the hardware and software that enable communication. Both techniques can verify the authenticity of the participants' transceivers on the ground and on the aircraft. Hence, they can be deployed to detect both malicious and inadvertent intrusion. Several studies have investigated the option to watermark VHF communication in an attempt to introduce speaker verification[27, 39, 41, 83]. Further, two studies considered the feasibility of fingerprinting the ADS-B protocol. One of them proposes to exploit differences in transponder implementations on the data link layer [105], another approach uses behavioral differences in the frequencies exhibited by different aircraft transponders [57]. Note that none of these approaches offer perfect security, since attackers with a large resource endowment may mimic both watermarks and fingerprints.

3.1.2 Machine Learning

The use of machine learning for security purposes has found widespread adoption over the past years, in particular with respect to intrusion detection in networked systems. Two approaches have been used to detect attacks on wireless aviation systems. The first is classification, whereby the characteristics of particular legitimate users are segmented and verified against these saved patterns. The other is anomaly detection, whereby the parameters of the normal state of the system are learned over time, and deviations from these patterns are marked as an anomaly and potential security concern.

Classification

Currently, classification approaches have mostly been applied to human users using the VHF channel. The authors in [30, 73, 100] use behavioral biometric voice data from pilots communicating via VHF radio to tell apart speakers on the VHF channel in an attempt to verify them and detect potential imposters. Very recent approaches have attempted to classify and segment standardized digital communication using deep learning on ADS-B signal characteristics [133].

Anomaly Detection

Some of the above-cited studies attempt to detect abnormal stress levels and distress in the pilot's voices over VHF radio [30, 100], thereby seeking to detect anomalies with regards to legitimate channel use. In contrast, the authors in [106, 111] suggest to use analogue physical layer features such as received signal strength and time differences of arrival collected from ADS-B/SSR data to learn about the space of states normally occupied by aircraft and detect subsequent diversions from this normal state. Finally, the authors in [38] apply long short-term memory networks to detect spoofed ADS-B location messages in the flight tracks of commercial aircraft.

There are many explanations for irregular aircraft movement, which is why anomaly detection is only one of several elements of an intrusion detection system. Careful calibration and engineering are required to prevent false positives.

3.1.3 Non-technical Measures

Much contemporary research focuses on non-technical measures by which the air-ground link can be secured. By the term ‘non-technical’, we refer to approaches that prefer formal and procedural reform of extant ATC technology landscapes over the development of new technical systems or technologies.

Formal Methods

Early academic work has described changes to user experience following the introduction of formal security requirements into an ATC system and explored whether ADS-B position reports should be used as a primary position source for aircraft [76]. More recently, the authors of [66] conducted a risk and requirements analysis of the ATM system, using VHF communication as a case study.

As the popularity of this research field grows, and as users become more experienced and deploy novel technological tools, research is now at a point where security standards can formally be verified. A complete formal verification of the ACARS Message Security standard ARINC 823 [12] identified several weaknesses that can be exploited. While the analysis confirms the security properties of the protocol, it also highlights that improvements must be made. Other work proposes the use of ontologies [69], modal logic [119], and dynamic queue networks [116] to validate different aspects of the information flow on the air–ground link.

Policies/Procedures

As new systems and technical changes to existing technologies are difficult to deploy in the real aviation environment, researchers have proposed policies and procedures which might improve the security of wireless communications. An overview of security-related initiatives of aviation authorities and the industry can be found in [60].

Both aviation professionals and passengers should be educated about ADS-B security problems [103], and flight simulators should simulate cyberattacks [74, 98]. Further, aviation authorities are advised to release test-run data and mitigation options, to increase the awareness of security vulnerabilities, and to continuously operate primary surveillance radars [103, 123]. While the last recommendation is costly and thus offsets the efficiency advantage of introducing improved protocols, it is mentioned by the FAA as a potential intermediate solution until the 2020 ADS-B adoption requirement [14]. Finally, it is suggested that the next generation of ATC technology should be designed with cyberattacks and radio frequency interference in mind [78, 104].

3.1.4 Cryptography

Cryptography is the most effective measure by which communication can be secured in any scenario. As a result, it is used widely in research that focuses on improving the security of wireless aviation protocols, nonwithstanding some significant obstacles that many analysts have cited (e.g., [108, 125]). Cryptography can effectively secure the content of any digital communication by integrity, authentication, and confidentiality. In particular, there is no alternative means by which confidentiality can be guaranteed. Unfortunately, to date only the ARINC 823 standards on ACARS message security [21, 22], have proposed to introduce cryptograhpic measures, and these standards have not yet been adopted in practice [97].

Earlier work has suggested experimental solutions that might address the security problems of unencrypted communication in both ACARS [86], ADS-B [45], and CPDLC [33, 64, 77] technology. Once the security problems of ADS-B came to the fore, many researchers focused on the development of extant and future protocols. They propose to introduce identity-based encryption [37, 40, 120, 128, 129], format preserving encryption [4, 31, 32, 43] and retro-active key publication [11, 92, 108]. There has also been research on public key infrastructures in the aviation context [53, 136] and the use of blockchain technology [8, 84]. While much work has addressed the downsides of cryptographic countermeasures and their incompatibility with current systems [92, 130, 132], to the best of our knowledge these studies have not yet been considered in detail by aviation authority committees.

3.2 Privacy Countermeasures

Studies that aim to protect the privacy of aircraft users and stakeholders can be categorized into two fundamental areas: First, those which analyze countermeasures to the tracking of private and government aircraft, and second, those which strive to provide greater confidentiality for sensitive data that are sent to or from aircraft.

3.2.1 Countermeasures Against Tracking

Recent works have analysed industry initiatives that propose mitigate the problem of tracking sensitive private and public aircraft. They found that these proposals are likely ineffective in realistic threat scenarios [114]. Alternative proposals in the academic literature can be partitioned into technical and non-technical countermeasures.

Technical Measures

Turn Position Broadcasting Off Since the use of ADS-B is not yet mandatory in all airspaces, around 30% of all aircraft do not broadcast their position [91]. However, since the use of ADS-B is now mandatory in Western airspaces, this share can be expected to decrease; moreoever, there are alternative means by which aircraft can be easily tracked.

Pseudonymous Identifiers Only the UAT data link offers pseudonymous identifiers by design. This link is used by some aircraft under visual flight rules in the US. It offers a built-in privacy mechanism that generates a non-conflicting, random, temporary identifier that inhibits third-party tracking [65]. Unfortunately, this approach is both limited to general aviation aircraft in the US and ineffective as the aircraft's real identifiers can be recovered [87]. Furthermore, the FAA warns that the use of this feature may have serious negative consequences [6]:

> We do not recommend integrating the anonymity features, as the operator will not be eligible to receive ATC services, may not be able to benefit from enhanced ADS-B search and rescue capabilities, and may impact ADS-B In situational awareness benefits.

On the level of the aircraft call sign, commercial firms offer solutions which assign the aircraft to an anonymous "DOTCOM" airline [122], and thus anonymize its call sign. While this approach has potential benefits compared to other blocking solutions, aircraft still broadcast their real transponder IDs, such that this method only neutralizes very weak attacks.

Encryption While few works have actively proposed and developed cryptographic solutions specifically tailored to prevent tracking, the full encryption of a message's identifying information may constitute an effective method. Consequently, cryptographic solutions as discussed in Sect. 3.1.4 may also be effective. However, practical compatibility and implementation problems will likely require separate solutions that can safeguard privacy in both SSR, ADS-B, ACARS, CPDLC and even VHF communication.

Non-technical Measures

Web Tracker Blocking Many stakeholders seek to prevent the live and public display of their aircraft on websites such as *Flightradar24* by using block lists. For a history and legal analysis of the FAA's blocking program in the USA, see [36]. However, the effectiveness of this approach is questionable [114], since such obscuration can be circumvented by alternative data sources (e.g., personal SDR receivers or non-compliant websites).

Ownership Obscuration Some stakeholders use third-party entities to register their aircraft and conceal the real owner from public records. Popular methods include the use of offshore shell companies, special aircraft registration services, wealth management companies and trusts. This approach can help obscure the movements of their owners, however, a single slip of operational security can permanently destroy this advantage.[3]

Commercial Air Transport The most straightforward and effective approach to neutralize the above privacy concerns is to forego the use of designated aircraft. Instead, more anonymous and non-exclusive means of transport could be used. As such radical measures may compromise the security or privacy of the user, they may not be feasible in many cases.

Recommendations

The literature has further discussed potential directions in aviation privacy: In the short term, regulation may mitigate the privacy impact of large-scale tracking. Governments may legally restrict and regulate entities (such as web trackers) which share data about aircraft movements.

In this respect, more dedicated efforts are required that may, for example, introduce mandatory requirements or enforce significant penalties[114]. Still, as legal norms differ internationally, and as aircraft data can be freely accessed on the Internet, the international enforcement of such regulation remains difficult. Thus, in the longer term, technical solutions should be developed to provide privacy guarantees; a robust pseudonym system could limit the tracking of aircraft over time. There is no critical technical or procedural need to have a consistent, publicly known identifier for any aircraft. On the contrary, there is evidence that authorities have assigned alternative identifiers to aircraft deployed in sensitive (e.g., military) flights [24]. Hence, a more flexible identification and assignment policy could disentangle aircraft identification from flights patterns. This measure alone would greatly reduce the security risk of ATC-based flight tracking.

Only the combination of technical and regulatory measures will create effective privacy solutions for ATC systems [114]. While regulatory measures may address data collection by state agencies, technical measures are still required to prevent data collection by unauthorized third parties.

3.2.2 Privacy for Data Links

In the long term, encryption is the sensible, mature and effective solution to achieve confidentiality in wireless networks. In the short term, as there may be no suitable implementations available, changes in procedures and awareness can at least mitigate the most significant concerns.

Such short-term measures should focus on educating avionics users to not use ACARS or CPDLC to send sensitive information. In fact, this requirement has been

[3] Examples of such slips include pictures and reports by traditional planespotters upon landing, investigative journalism, or posts on social media.

voiced as early as 1998 [81, 126]. For example, a Swiss pilot has documented a case study where sensitive credit card data transmitted by plain-text ACARS messages were intercepted [121]. The author subsequently suggests not to use ACARS free-text messages to send credit card information or names of passengers and crew. The article also suggests to prefer telephone lines on the ground and satellite links over VHF. However, a recent study has found that this suggestion is ineffective [97].

While cryptographic solutions are desirable in the long term, the deployment of related technology and protocols is in its infancy. Besides the ARINC 823 standards on ACARS Message Security [21, 22, 102], which have seen no adoption in practice, no currently used aviation standard proposes cryptographic measures. This leads to a proliferation of several proprietary encryption standards to protect ACARS and/or CPDLC, none of which has been independently verified. Instead, researchers have shown that these standards can be easily compromized [96]. While recent proposals for novel data link technology, such as L-DACS and AeroMACS, do consider encryption as a standard measure (e.g., [63]), the technology required to build such solutions is still in its early development phase.

4 Research Agenda

Our survey suggests that the reporting and data sharing on security vulnerabilities and incidents should be improved. A number of contemporary initiatives are already responding to this call. In Europe, the European Air Safety Agency (EASA) has created the European Centre for Cyber Security in Aviation (ECCSA); while the US-based Aviation Information Sharing & Analysis Center (A-ISAC) aims to distribute crucial cybersecurity information among members. However, a free global platform that integrates and shares such data among all stakeholders has not yet been realized.

Second, we suggest that the aviation industry should reconsider its approach to aviation security. Just as technology firms have evolved from producers of consumer goods to providers of global IT infrastructure, airlines and operators should embrace cooperation with academic research to transform the industry such that it can provide effective cybersecurity.

Third, many authors have pointed out that security is not safety, hence the production of effective security solutions requires a different mindset. Some intersections between these field have been identified early on [99]. While extensive development, testing and certification cycles boosted flight safety performance to record levels, measures traditionally deployed for physical flight safety (e.g., redundancy) are ineffective against malicious actors in the radio and cyber spheres. Indeed, the available (consumer) technology significantly outpaced aviation communication systems, leaving the latter dangerously vulnerable [51]. As a result, there are some fundamental gaps in the literature, which we propose should be addressed by the following agenda.

4.1 Security

There is very little research that focuses on the security of the collision avoidance system TCAS. While there are also no explicit (public) reports on security incidents related to TCAS, the system uses both SSR and ADS-B to communicate, hence, it is exposed to all physical and cyber-related vulnerabilities these technologies entail [10, 110]. In light of the safety criticality of the system, active steps to secure it should be strongly considered.

Further, the application of formal methods to verify security claims in aviation protocols should considered. Such verification procedures can help minimize the risk of technology development failure as novel technology such as L-DACS is deployed throughout the aviation industry. To date, we are not aware of any study that has proposed short-term, transparent, and readily applicable solutions for the ACARS and CPDLC protocols. While there are many proposed approaches based on cyber-physical security or machine learning for all ATC technologies, there have been no attempts to transfer such research in order to protect the integrity of data transmitted on the data link. While cryptographic solutions are desirable in the long term, short-term solutions should focus on alternative technological approaches since the ACARS message security standard has not been adopted to date, and since early attempts to encrypt ACARS messaging were found to be flawed [96].

4.2 Privacy

Privacy research has shown that both innocent and malicious actors can compromise aircraft and passenger privacy by correlating publicly available or leaked data and metadata. This problem is due to the simple fact that the data links used to transmit information cannot consider even basic privacy requirements. To date, little academic work has focused on mitigating these disadvantages. While many studies attempt to improve the integrity and authenticity of ATC systems, few have explicitly looked at the confidentiality of ATC data or the anonymity of its users. To date, the aviation industry still prefers open systems in an attempt to maximize safety by maximizing global compatibility [109]. As a result, this compatibility focus is at odds with demands for more privacy and security. Privacy leaks may be less obvious, but they still compromise the safety of aircraft users. As the number of reported cyber- and radio-related incidents of data interception and manipulation increases, a shift of the research focus towards privacy issues seems desirable.

References

1. Adamy, D.: EW 101: A First Course in Electronic Warfare. Artech, Norwood (2001)
2. Adamy, D.: EW 102: A Second Course in Electronic Warfare. Artech, Norwood (2004)

3. Adamy, D.: EW 103: Tactical Battlefield Communications Electronic Warfare. Artech, Norwood (2008)
4. 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, pp. 245–261. Springer, Heidelberg (2014)
5. Airways New Zealand: FANS1/A Problem Reporting (2018). http://www.fans-cra.com/report/de-identified/list/
6. Airworthiness Approval of Automatic Dependent Surveillance - Broadcast (ADS-B) Out Systems. Tech. Rep. 20-165, Federal Aviation Administration (2010)
7. Aldhous, P.: BuzzFeed News trained a computer to search for hidden spy planes. This is what we found. Buzzfeed News (2017). https://www.buzzfeed.com/peteraldhous/hidden-spy-planes
8. Arora, A., Yadav, S.K.: Batman: Blockchain-based aircraft transmission mobile ad hoc network. In: Proceedings of 2nd International Conference on Communication, Computing and Networking, pp. 233–240. Springer, Singapore (2019)
9. 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, pp. 35–46. ACM, New York (2016)
10. Berges, P.M.: Exploring the vulnerabilities of traffic collision avoidance systems (TCAS) through software defined radio (SDR) exploitation. Ph.D. thesis, Virginia Tech (2019)
11. Berthier, P., Fernandez, J.M., Robert, J.M.: Sat: Security in the air using tesla. In: 36th Digital Avionics Systems Conference. IEEE, Piscataway (2017)
12. Blanchet, B.: Symbolic and computational mechanized verification of the ARINC823 avionic protocols. In: 30th Computer Security Foundations Symposium. IEEE, Piscataway (2017)
13. Bresteau, C., Guigui, S., Berthier, P., Fernandez, J.M.: On the security of aeronautical datalink communications: problems and solutions. In: 2018 Integrated Communications, Navigation, Surveillance Conference (ICNS), pp. 1A4–1. IEEE, Piscataway (2018)
14. Carey, B.: FAA no longer expected to retire radars. Aviation Week (2018). https://aviationweek.com/awincommercial/faa-no-longer-expected-retire-radars
15. Cenciotti, D.: Forget any security concern and welcome Air Force One on Flightradar24! The Aviationist (2011). https://theaviationist.com/2011/11/24/af1-adsb
16. Cenciotti, D.: Online flight tracking provides interesting details about Russian air bridge to Syria. The Aviationist (2015). https://theaviationist.com/2015/09/11/ads-b-exposes-russian-air-bridge-to-syria/
17. Chivers, H.: Control consistency as a management tool: the identification of systematic security control weaknesses in air traffic management. Int. J. Crit. Comput. Based Syst. **6**(3), 229–245 (2016)
18. City, A.M.: Drugs giant AbbVie flicks privacy switch on corporate jet (2014). http://www.cityam.com/1405384925/drugs-giant-abbvie-flicks-privacy-switch-corporate-jet
19. Costin, A., Francillon, A.: Ghost is in the air(traffic): on insecurity of ADS-B protocol and practical attacks on ADS-B devices. In: Black Hat USA, pp. 1–12 (2012)
20. Crescentvenus: Wireless Attack Launch Box (WALB) (2018). https://github.com/crescentvenus/WALB
21. DataLink Security, Part 1 - ACARS Message Security. Tech. Rep. 823P1, ARINC (2007)
22. DataLink Security, Part 2 - Key Management. Tech. Rep. 823P2, ARINC (2008)
23. 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), pp. 526–531. IEEE, Piscataway (2016)
24. Directorate of Air Traffic Management: Automatic Dependent Surveillance-Broadcast (ADS-B). Tech. rep., Airports Authority of India, New Delhi (2014)
25. Dupraz-Dobias, P.: Swiss officials just seized 11 of the world's most expensive cars from this African president's son. Quartz (2016). https://goo.gl/rR34aP

26. El Marady, A.A.W.: Enhancing accuracy and security of ADS-B via MLAT assisted-flight information system. In: 2017 12th International Conference on Computer Engineering and Systems (ICCES), pp. 182–187. IEEE, Piscataway (2017)
27. Fantacci, R., Menci, S., Micciullo, L., Pierucci, L.: A secure radio communication system based on an efficient speech watermarking approach. Secur. Commun. Netw. **2**(4), 305–314 (2009)
28. Faragher, R., et al.: Spoofing mitigation, robust collision avoidance, and opportunistic receiver localisation using a new signal processing scheme for ADS-B or AIS. In: 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (2014)
29. Federal Aviation Administration: Aircraft Registry (2017). https://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/
30. Finke, M., Stelkens-Kobsch, T.H.: A practical example for validation of ATM security prototypes. CEAS Aeronaut. J. 1–14 (2018). https://doi.org/10.1007/s13272-017-0275-y
31. Finke, C., Butts, J., Mills, R.: ADS-B encryption: confidentiality in the friendly skies. 8th Annual Cyber Security and Information Intelligence Research Workshop (2013)
32. Finke, C., Butts, J., Mills, R., Grimaila, M.: Enhancing the security of aircraft surveillance in the next generation air traffic control system. Int. J. Crit. Infrastruct. Prot. **6**(1), 3–11 (2013)
33. Getachew, D., Griner, J.H. Jr.: An elliptic curve based authentication protocol for controller-pilot data link communications. In: Integrated CNS Conference & Workshop (2005)
34. Ghose, N., Lazos, L.: Verifying ADS-B navigation information through Doppler shift measurements. In: 34th IEEE/AIAA Digital Avionics Systems Conference (DASC) (2015)
35. Gurtov, A., Polishchuk, T., Wernberg, M.: Controller–pilot data link communication security. Sensors **18**(5), 1636 (2018)
36. Gurtovaya, O.: Maintaining privacy in a world of technological transparency: The barr program's ups and downs in changing times. J. Air L. Com. **77**, 569 (2012)
37. Hableel, E., Baek, J., Byon, Y.J., Wong, D.S.: How to protect ADS-B: confidentiality framework for future air traffic communication. In: Computer Communications Workshops (2015)
38. Habler, E., Shabtai, A.: Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages. Preprint (2017). arXiv:1711.10192
39. Hagmuller, M., Hering, H., Kropfl, A., Kubin, G.: Speech watermarking for air traffic control. In: IEEE European Signal Processing Conference (2004)
40. He, D., Kumar, N., Choo, K.K.R., Wu, W.: Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system. IEEE Trans. Inf. Forensics Secur. **12**(2), 454–464 (2017)
41. Hering, H., Hagmüller, M., Kubin, G.: Safety and security increase for air traffic management through unnoticeable watermark aircraft identification tag transmitted with the VHF voice communication. In: 22nd IEEE/AIAA Digital Avionics Systems Conference (DASC) (2003)
42. Hoffman, D., Rezchikov, S.: Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit. In: DEF CON 20, Las Vegas (2012)
43. Huang, R.S., Yang, H.M., Wu, H.G.: Enabling confidentiality for ADS-B broadcast messages based on format-preserving encryption. In: Applied Mechanics and Materials, vol. 543, pp. 2032–2035. Trans Tech Publ (2014)
44. International Civil Aviation Organization (ICAO): Guidance material: security issues associated with ADS-B. Tech. rep., Montreal (2014)
45. Jochum, J.R.: Encrypted Mode Select ADS-B tactical military situational awareness. Master's thesis, Massachusetts Institute of Technology, Cambridge (2001)
46. Kacem, T., Wijesekera, D., Costa, P.: Integrity and authenticity of ADS-B broadcasts. In: IEEE Aerospace Conference (2015)
47. Kacem, T., Wijesekera, D., Costa, P.: Key distribution scheme for aircraft equipped with secure ADS-B in. In: 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), pp. 1–6. IEEE, Piscataway (2017)

48. Kacem, T., Wijesekera, D., Costa, P., Carvalho, J., Monteiro, M., Barreto, A.: Key distribution mechanism in secure ADS-B networks. In: IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS) (2015)
49. Kenney, L., Dietrich, J., Woodall, J.: Secure ATC surveillance for military applications. In: IEEE Military Communications Conference (MILCOM), pp. 1–6. IEEE, Piscataway (2008)
50. Kim, Y., Jo, J.Y., Lee, S.: ADS-B vulnerabilities and a security solution with a timestamp. IEEE Aerosp. Electron. Syst. Mag. **32**(11), 52–61 (2017)
51. Kirschbaum, J.: Urgent need for DOD and FAA to address risks and improve planning for technology that tracks military aircraft. Tech. Rep. GAO-18-177, United States Government Accountability Office (2018)
52. Laboda, A.: Unencrypted ADS-B OUT confounds aircraft blocking. NBAA Convention News (2015)
53. Lee, S.H., Han, J.W., Lee, D.G.: The ADS-B protection method for next-generation air traffic management system. In: Ubiquitous Computing Application and Wireless Sensor. Springer, Dordrecht (2015)
54. Leonardi, M.: ADS-B anomalies and intrusions detection by sensor clocks tracking. IEEE Transactions on Aerospace and Electronic Systems (2018)
55. Leonardi, M., Di Fausto, D.: ADS-B signal signature extraction for intrusion detection in the air traffic surveillance system. In: 2018 26th European Signal Processing Conference (EUSIPCO), pp. 2564–2568. IEEE, Piscataway (2018)
56. Leonardi, M., Piracci, E., Galati, G.: ADS-B vulnerability to low cost jammers: risk assessment and possible solutions. In: IEEE Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV), pp. 41–46. IEEE, Piscataway (2014)
57. Leonardi, M., Di Gregorio, L., Di Fausto, D.: Air traffic security: aircraft classification using ADS-B message's phase-pattern. Aerospace **4**(4), 51 (2017)
58. Leonardi, M., Piracci, E., Galati, G.: ADS-B jamming mitigation: a solution based on a multichannel receiver. IEEE Aerosp. Electron. Syst. Mag. **32**(11), 44–51 (2017)
59. Li, T., Wang, B.: Sequential collaborative detection strategy on ADS-B data attack. Int. J. Crit. Infrastruct. Prot. **24**, 78–99 (2019)
60. Mahmoud, M., Pirovano, A., Larrieu, N.: Aeronautical communication transition from analog to digital data: a network security survey. Elsevier Comput. Sci. Rev. **11**, 1–29 (2014)
61. Maremont, M., McGinty, T.: Corporate jet set: leisure vs. business. Wall Street J. (2011). https://www.wsj.com/articles/SB10001424052748703551304576260871791710428
62. Maremont, M., McGinty, T.: Ready for departure: M&A airlines. Wall Street J. (2011). https://www.wsj.com/articles/SB10001424052702303499204576389923856575528
63. Mäurer, N., Bilzhause, A.: A cybersecurity architecture for the L-band digital aeronautical communications system (LDACS). In: Digital Avionics Systems Conference. IEEE, Piscataway (2018)
64. McParland, T., Patel, V., Hughes, W.J.: Securing air-ground communications. In: 20th IEEE/AIAA Digital Avionics Systems Conference (DASC), vol. 2 (2001)
65. Minimum operational performance standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance – Broadcast. Tech. Rep. DO-282B, RTCA, Inc (2011)
66. Montefusco, P., Casar, R., Koelle, R., Stelkens-Kobsch, T.H.,: 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: 11th International Conference on Availability, Reliability and Security (ARES), pp. 532–541. IEEE (2016)
67. Monteiro, M., Barreto, A., Division, R., Kacem, T., Carvalho, J., Wijesekera, D., Costa, P.: Detecting malicious ADS-B broadcasts using wide area multilateration. In: 34th IEEE/AIAA Digital Avionics Systems Conference (DASC) (2015)
68. Monteiro, M., Barreto, A., Kacem, T., Wijesekera, D., Costa, P.: Detecting malicious ADS-B transmitters using a low-bandwidth sensor network. In: IEEE International Conference on Information Fusion (Fusion) (2015)

69. Morel, L.P.: Using ontologies to detect anomalies in the sky. Ph.D. thesis, École Polytechnique de Montréal (2017)
70. Moser, D., Leu, P., Lenders, V., Ranganathan, A., Ricciato, F., Capkun, S.: Investigation of multi-device location spoofing attacks on air traffic control and possible countermeasures. In: 22nd Annual International Conference on Mobile Computing and Networking (MobiCom) (2016)
71. Murphy, T., Harris, W.: Device, system and methods using angle of arrival measurements for ADS-B authentication and navigation (2014). https://www.google.com/patents/US20140327581. US Patent App. 13/875,749
72. Naganawa, J., Tajima, H., Miyazaki, H., Koga, T., Chomel, C.: ADS-B anti-spoofing performance of monopulse technique with sector antennas. In: 2017 IEEE Conference on Antenna Measurements & Applications (CAMA), pp. 87–90. IEEE, Piscataway (2017)
73. Neffe, M., Van Pham, T., Hering, H., Kubin, G.: Speaker segmentation for air traffic control. In: Speaker Classification II. Springer, Berlin (2007)
74. Nguyen, D., Shelton, J.W., Mitchell, T.M.: System and method for evaluating cyber-attacks on aircraft (2017). US Patent 9,836,990
75. Nguyen, A.Q., Amrhar, A., Zambrano, J., Brown, G., Landry, R. Jr., Yeste, O.: Application of phase modulation enabling secure automatic dependent surveillance-broadcast. J. Air Transp. Manag. **26**(4), 157–170 (2018)
76. Nuseibeh, B., Haley, C.B., Foster, C.: Securing the skies: in requirements we trust. IEEE Comput. **42**(9), 64–72 (2009)
77. Olive, M.L.: Efficient datalink security in a bandwidth-limited mobile environment-an overview of the Aeronautical Telecommunications Network (ATN) security concept. In: 20th IEEE/AIAA Digital Avionics Systems Conference (DASC), vol. 2, pp. 1–10 (2001)
78. Osechas, O., Mostafa, M., Graupl, T., Meurer, M.: Addressing vulnerabilities of the CNS infrastructure to targeted radio interference. IEEE Aerosp. Electron. Syst. Mag. **32**(11), 34–42 (2017)
79. Palan, D., Boldt, K.: Abflug in höhere Sphären. Manager Magazin (2012). http://www.manager-magazin.de/lifestyle/reise/a-827947-6.html
80. Park, P., Khadilkar, H., Balakrishnan, H., Tomlin, C.J.: High confidence networked control for next generation air transportation systems. IEEE Trans. Autom. Control **59**(12), 3357–3372 (2014)
81. Pascoe, K.: ACARS and error checking (2015). http://www.flight.org/acars-and-error-checking
82. Patel, V.: ICAO air-ground security standards strategy. In: IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS) (2015)
83. Prinz, J., Sajatovic, M., Haindl, B.: S/sup 2/EV-safety and security enhanced ATC voice system. In: IEEE Aerospace Conference (2005)
84. Reisman, R.: Blockchain serverless public/private key infrastructure for ADS-B security, authentication, and privacy. In: AIAA Scitech 2019 Forum, p. 2203 (2019)
85. Results from EASA technical investigation on the radar detection losses in June 2014 in Central Europe. Tech. Rep. ED0.1-2014-ed04.00, European Aviation Safety Agency (2014)
86. Risley, C., McMath, J., Payne, C.B.: Experimental encryption of aircraft communications addressing and reporting system (ACARS) aeronautical operational control (AOC) messages. In: Digital Avionics Systems Conference (2001)
87. Sampigethaya, K., Taylor, S., Poovendran, R.: Flight privacy in the nextgen: challenges and opportunities. In: Integrated Communications, Navigation and Surveillance Conf. (2013)
88. Schäfer, M., Lenders, V., Martinovic, I.: Experimental analysis of attacks on next generation air traffic communication. In: International Conference on Applied Cryptography and Network Security (ACNS), pp. 253–271. Springer, Berlin (2013)
89. Schäfer, M., Lenders, V., Schmitt, J.: Secure track verification. In: IEEE Symposium on Security and Privacy (S&P), pp. 199–213. IEEE, Piscataway (2015)
90. 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, pp. 135–145. ACM, New York (2016)

91. Schäfer, M., Strohmeier, M., Smith, M., Fuchs, M., Pinheiro, R., Lenders, V., Martinovic, I.: OpenSky Report 2016: facts and figures on SSR mode S and ADS-B usage. In: 35th IEEE/AIAA Digital Avionics Systems Conference (DASC) (2016)
92. Sciancalepore, S., Di Pietro, R.: SOS - securing open skies. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, pp. 15–32. Springer, Berlin (2018)
93. Selleck, D.: Iridium fault prompts ban by Oceanic ATC. Flight Service Bureau (2017). http://flightservicebureau.org/iridium-fault/
94. Shang, F., Wang, B., Yan, F., Li, T.: Multidevice false data injection attack models of ADS-B multilateration systems. Secur. Commun. Netw. **2019**, 1–11 (2019)
95. Smith, M., Strohmeier, M., Lenders, V., Martinovic, I.: On the security and privacy of ACARS. In: IEEE Integrated Communications, Navigation and Surveillance Conference (2016)
96. Smith, M., Moser, D., Strohmeier, M., Lenders, V., Martinovic, I.: Economy class crypto: exploring weak cipher usage in avionic communications via ACARS. In: International Conference on Financial Cryptography and Data Security (2017)
97. Smith, M., Moser, D., Strohmeier, M., Martinovic, I., Lenders, V.: Undermining privacy in the aircraft communications addressing and reporting system (ACARS). In: 18th Privacy Enhancing Technologies Symposium (PETS 2018) (2018)
98. Smith, M., Strohmeier, M., Harman, J., Lenders, V., Martinovic, I.: Safety vs. security: attacking avionic systems with humans in the loop. Preprint (2019). arXiv:1905.08039
99. Stavridou, V., Dutertre, B.: From security to safety and back. In: Computer Security, Dependability and Assurance: From Needs to Solutions, pp. 182–195. IEEE, Piscataway (1998)
100. Stelkens-Kobsch, T., Hasselberg, A., Mühlhausen, T., Carstengerdes, N.: Towards a more secure ATC voice communications system. In: Digital Avionics Systems Conference (2015)
101. Stewart, J.: Meet the NATS pirate hunters. NATS Blog (2015). https://nats.aero/blog/2015/05/meet-the-nats-pirate-hunters/
102. Storck, P.: Benefits of commercial data link security. In: IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS) (2013)
103. Strand, D.A.: Automatic dependent surveillance - broadcast (ADS-B) vulnerabilities. Ph.D. thesis, Utica College (2017)
104. Strohmeier, M.: Security in next generation air traffic communication networks. Ph.D. thesis, University of Oxford (2016)
105. 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 (CPS-SPC), pp. 1–9. ACM, New York (2015)
106. Strohmeier, M., Lenders, V., Martinovic, I.: Intrusion detection for airborne communication using PHY-layer information. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), pp. 67–77. Springer, Berlin (2015)
107. Strohmeier, M., Lenders, V., Martinovic, I.: Lightweight location verification in air traffic surveillance networks. In: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security (CPSS), pp. 49–60. ACM, New York (2015)
108. Strohmeier, M., Lenders, V., Martinovic, I.: On the security of the automatic dependent surveillance-broadcast protocol. IEEE Commun. Surv. Tutorials **17**(2), 1066–1087 (2015)
109. Strohmeier, M., Smith, M., Schäfer, M., Lenders, V., Martinovic, I.: Assessing the impact of aviation security on cyber power. In: 8th International Conference on Cyber Conflict (CyCon), pp. 223–241 (2016)
110. Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V., Martinovic, I.: On perception and reality in wireless air traffic communication security. IEEE Trans. Intell. Transp. Syst. **18**(6), 1338–1357 (2017)
111. Strohmeier, M., Smith, M., Schäfer, M., Lenders, V., Martinovic, I.: Crowdsourcing security for wireless air traffic communications. In: 9th International Conference on Cyber Conflict (CyCon), pp. 1–18 (2017)

112. Strohmeier, M., Lenders, V., Martinovic, I.: A k-NN-based localization approach for crowdsourced air traffic communication networks. IEEE Trans. Aerosp. Electron. Syst. **54**(3), 1519–1529 (2018)
113. Strohmeier, M., Niedbala, A.K., Schäfer, M., Lenders, V., Martinovic, I.: Surveying aviation professionals on the security of the air traffic control system. In: Security and Safety Interplay of Intelligent Software Systems, pp. 135–152. Springer, Berlin (2018)
114. Strohmeier, M., Smith, M., Lenders, V., Martinovic, I.: The real first class? Inferring confidential corporate mergers and government relations from air traffic communication. In: IEEE European Symposium on Security and Privacy (EuroS&P) (2018)
115. Strohmeier, M., Smith, M., Moser, D., Schäfer, M., Lenders, V., Martinovic, I.: Utilizing air traffic communications for OSINT on state and government aircraft. In: 10th International Conference on Cyber Conflict (CyCon) (2018)
116. Tamimi, A., Hahn, A., Roy, S.: Cyber threat impact analysis to air traffic flows through dynamic queue networks. Preprint (2018). arXiv:1810.07514
117. Tart, A., Trump, T.: Addressing security issues in ADS-B with robust two dimensional generalized sidelobe canceller. In: 2017 22nd International Conference on Digital Signal Processing (DSP), pp. 1–5. IEEE, Piscataway (2017)
118. Teso, H.: Aircraft hacking: Practical aero series. In: Fourth Annual Hack in the Box Security Conference (2013)
119. Thudimilla, A., McMillin, B.: Multiple security domain nondeducibility air traffic surveillance systems. In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 136–139. IEEE, Piscataway (2017)
120. Thumbur, G., Gayathri, N., Reddy, P.V., Rahman, M.Z.U., Lay-Ekuakille, A.: Efficient pairing-free identity-based ADS-B authentication scheme with batch verification. IEEE Trans. Aerosp. Electron. Syst. (2019). https://doi.org/10.1109/TAES.2018.2890354
121. Tilly, P.: Die verpasste Chance. AEROPERS Rundschau (2013). https://www.aeropers.ch/index.php/der-verband/rundschau1/archiv/rundschau-archiv-rundschau-archiv-2013-1/638-rundschau-2-2013-1/file
122. Trautvetter, C.: FltPlan flight privacy program exposes tangled FAA policy. AIN Online (2011). https://www.ainonline.com/aviation-news/aviation-international-news/2011-08-31/fltplan-flight-privacy-program-exposes-tangled-faa-policy
123. Viveros, C.A.P.: Analysis of the cyber attacks against ADS-B perspective of aviation experts. Ph.D. thesis, Master's Thesis, University of Tartu, Institute of Computer Science (2016)
124. Wang, W., Chen, G., Wu, R., Lu, D., Wang, L.: A low-complexity spoofing detection and suppression approach for ADS-B. In: IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS) (2015)
125. Wesson, K.D., Humphreys, T.E., Evans, B.L.: Can cryptography secure next generation air traffic surveillance? IEEE Security and Privacy Magazine (2014)
126. Wolper, J.: Security risks of laptops in airline cockpits (1998). http://catless.ncl.ac.uk/Risks/20/12
127. Wu, R., Chen, G., Wang, W., Lu, D., Wang, L.: Jamming suppression for ADS-B based on a cross-antenna array. In: IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS) (2015)
128. Yang, H., Huang, R., Wang, X., Deng, J., Chen, R.: EBAA: an efficient broadcast authentication scheme for ADS-B communication based on IBS-MR. Elsevier Chin. J. Aeronaut. **27**(3), 688–696 (2014)
129. Yang, A., Tan, X., Baek, J., Wong, D.S.: A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification. IEEE Trans. Serv. Comput. **10**(2), 165–175 (2015)
130. Yang, H., Zhou, Q., Yao, M., Lu, R., Li, H., Zhang, X.: A practical and compatible cryptographic solution to ADS-B security. IEEE Internet Things J. (2018). https://doi.org/10.1109/JIOT.2018.2882633
131. Yermack, D.: Tailspotting: identifying and profiting from CEO vacation trips. J. Financ. Econ. **113**(2), 252–269 (2014)

132. Yeste-Ojeda, O., Landry, R.: ADS-B authentication compliant with Mode-S extended squitter using PSK modulation. In: IEEE 18th International Conference on Intelligent Transportation Systems (ITSC), pp. 1773–1778 (2015)
133. Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L., Poovendran, R.: Detecting ADS-B spoofing attacks using deep neural networks. Preprint (2019). arXiv:1904.09969
134. Younger, E.: Melbourne Airport hoax caller Paul Sant pleads guilty to making fake flight calls, aborting Virgin landing. ABC News (2017). http://www.abc.net.au/news/2017-09-05/melbourne-airport-hoax-caller-paul-sant-pleads-guilty/8873984
135. Yue, M.: Security of VHF data link in ATM. In: Musa, M.S., Wu, Z. (eds.) Aeronautical Telecommunications Network: Advances, Challenges, and Modeling. CRC Press, Boca Raton (2015)
136. Yue, M., Wu, X.: The approach of ACARS data encryption and authentication. In: International Conference on Computational Intelligence and Security (CIS) (2010)
137. Zhang, R., Liu, G., Liu, J., Nees, J.P.: Analysis of message attacks in aviation data-link communication. IEEE Access **6**, 455–463 (2018)
138. Zhou, X., Song, L., Zhang, Y.: Physical Layer Security in Wireless Communications. CRC Press, Boca Raton (2014)