Securing the Air–Ground Link in Aviation

Martin Strohmeier, Ivan Martinovic, Vincent Lenders

Abstract A plethora of wireless communication protocols are used on the air–ground link within aviation, comprising both data links and air traffic control technologies. With the widespread proliferation of modern software-defined radio technology, the threat model for aviation has shifted. Independent security researchers and scientists have shown that the fundamental deficiencies in all of these protocols can be easily exploited with an impact of both the security and the privacy of their users. This article analyzes the current situation of the aviation air–ground link in a comprehensive manner. We collect and classify the known reported security and privacy incidents related to the seven main air–ground technologies. We find that all are considered vulnerable in the literature and many incidents relating to potential breaches and exploits have been made. In the second part of this work, we survey, systematize and discuss the academic research on possible countermeasures. We create a novel taxonomy, based on which we identify gaps in the literature and discuss potential future directions for aviation security research.

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,

Martin Strohmeier, Vincent Lenders
armasuisse W + T, Feuerwerkerstrasse 39, 3603 Thun, Switzerland.
e-mail: martin.strohmeier@armasuisse.ch, vincent.lenders@armasuisse.ch

Ivan Martinovic
Department of Computer Science, University of Oxford. Parks Road, Oxford, OX1 3QD, UK.
e-mail: ivan.martinovic@cs.ox.ac.uk

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 easy accessibility of wireless systems by a wide variety of threat actors [115]. The ubiquitous availability of low-cost SDR (software-defined radio transceiver) 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 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. Following this, we discuss the existing strategies suggested by researchers to address the problems of integrity, authenticity and confidentiality in these technologies. 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 develop recommendations for future aviation security research.

The remainder of this chapter is organised as follows: Section 2 discusses and classifies known vulnerabilities and incidents. Section 3 then outlines the existing research on security before it examines the work on privacy. Section 4 discusses the lessons and recommendations and Section **??** finally concludes this work.

2 Classification of Air–Ground Link Incidents & 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 below provides a short glossary of the surveyed technologies.

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	Voice (Very High Frequency)

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. Additionally, eavesdropping is possible for all considered technologies as none of them uses encryption. However, we do not consider eavesdropping a direct security problem, although it is a possible first stepping stone for active attacks, and thus do not discuss it further in this section. Eavesdropping can have direct consequences for privacy, which is considered in Section 2.2. It is noteworthy that there has been no academic research or public incident reports with regards to TCAS, although its vulnerability is similar to the SSR and ADS-B technologies, whose information TCAS is using.

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. [24]). Later works analyzed the concrete physical circumstances (distance, sending power) required to manipulate the 1090 MHz ADS-B channel and showed concrete laboratory attacks [60, 89]. Since the technology is only mandated by 2020 and not yet widely used operationally, no concrete incidents

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

Technology	Type	Vector	Description	Ref's
ADS-B	Vulnerability	Injection	Analysis of different types of message injection theoretically and in lab	[24, 89]
	Vulnerability	Jamming	Analysis of jamming with SDR in lab	[60]
	Exploit	Injection	Software enabling ADS-B spoofing with SDRs	[25]
SSR	Incident	DoS	Ground-based over-interrogation of aircraft transponders, causing real-world radar failures.	[6]
	Vulnerability	Jamming, Injection	Lab analysis by German Aerospace Center	[80]
PSR	Vulnerability	Jamming	Traditional electronic warfare	[7–9]
MLAT	Vulnerability	Injection	Proof of concept of an attack on MLAT system in lab	[72, 95]
VHF	Incident	Injection	Spoofing of ATC in Turkish airspace and at Melbourne airport	[101, 134]
	Incident	DoS	Regular communication interference from pirate radio stations and other unlicensed transmitters	[102]
ACARS	Vulnerability	Intrusion	Remote intrusion in lab into flight management system	[119]
	Vulnerability	Injection	Analysis of different types of message injection theoretically and in lab	[17, 87, 137]
CPDLC	Incident	Injection	Delayed CPDLC messages received undetected at aircraft hours later	[11, 94]
	Vulnerability	Jamming, Injection, DoS	Lab analyses conducted by several different aviation authorities	[26, 80]

involving ADS-B have been publicly reported until now. However, exploit kits, i.e., tool boxes for SDRs, which enable the spoofing of ADS-B messages are available online (e.g., [25]), 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 the same fundamental protocol characteristics with ADS-B. Thus, sending and exploiting Mode S is trivially possible by adapting existing scripts such as [25] or others. Consequently, the analysis by the German Aerospace Center [80] showed that radio frequency interference is possible, enabling ghost aircraft, jamming, or transponder lockouts. There has been one widely reported real-world incident re-

lated 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 [6]. 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 had a malicious nature. Nevertheless, the consulted cybersecurity experts state that such attacks are possible in principle [6].

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 conducted exclusively based on the reflection of its signals, thus there is no message content that could be injected or modified. Jamming, in contrast, remains fundamentally possible, however it requires much more sophisticated and powerful equipment, available only to the military (see [7–9] for an extended treatment of primary radar jamming and electronic warfare). Due to our focus on civil aviation, and the lack of credible threats and consequently any research on attacking PSR in this context, we will not consider the security of PSR further in this work.

2.1.4 MLAT

Multilateration is by its nature a technology derived from the signals of other wireless protocols, typically SSR or ADS-B. Thus, MLAT is often considered as a verification of unauthenticated wireless links [47]. 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 based on physical layer properties (specifically the propagation speed of electromagnetic waves) which are difficult to manipulate. However, real-world MLAT systems heavily rely on fusing the location obtained from the signals with the message contents to display identification and altitude of the targets, leaving the system as a whole as vulnerable 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 [72].

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 and real-world experiences of outside interference, both malicious and non-malicious [111]. Exemplary incidents in this regard include, but are not limited to, spoofed voice communication, such as the impersonation of air traffic controllers in

Turkish airspace [101] and at Melbourne airport [134], the latter of which caused significant distress. 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 [102].

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 [87]. 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 considered the injection of ACARS messages both in 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 used to compromise ACARS. The German Aerospace Center has recently addressed some vulnerabilities of CPDLC [80], highlighting the ease with which this technology can be spammed and spoofed. While no incidents have been reported publicly related to malicious interference, the robustness of CPDLC against any kind of interference is questionable. To date, several investigations have been launched into duplicate, delayed or lost CPDLC messages as well as logins to unauthenticated ground stations [11, 94]. 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. Besides systematizing these incidents by the technologies concerned, we can broadly classify them into a) tracking-related leaks and b) leaks of (other) personal information via data link technologies. 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.

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	[97, 99]
	Data	Personal data leakage on non-commercial and commercial aircraft	[97, 99, 122]
	Tracking, Data	Weak proprietary cryptography broken	[96]
ADS-B	Tracking	Leak of military operations	[20, 21]
	Tracking	Tracking of personal/governmental assets	[28]
	Tracking	Circumvention of aircraft blocking	[55]
	Tracking	Tracking of business assets	[81]
	Tracking	De-anonymization of transponder IDs	[88]
	Tracking	Fingerprinting of aircraft transponders	[59, 110]
SSR & MLAT	Tracking	Tracking of surveillance drones	[115]
VHF	Tracking	Aircraft tracking using voice recognition	[45]
ATC (general)	Tracking	Correlating CEO vacations with press releases	[132]
	Tracking	Analysis of CEO private aircraft use	[64]
	Tracking	Corporate aircraft movement tracking for merger data	[65, 113]
	Tracking	Large-scale analysis of effects of government and military aircraft tracking	[113, 114]
	Tracking	Use of aircraft blocking to hide merger negotiations	[23]
	Tracking	Analysis of aircraft patterns to uncover surveillance operations	[12]

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 provide easy access to immediate, highly detailed and continuous tracking data. In conjunction with publicly available metadata provided by these sites and many other comprehensive sources (including authoritative ones such as the FAA [32]), tracking of individual users has become feasible for even lowest-resource actors [115]. In the following, we describe the existing incidents and identified vulnerabilities, systematized according to their technologies (those filed under 'ATC general' concern two or more technologies and apply to aircraft tracking in general).

- **ACARS:** ACARS has become a recent target to obtain tracking information about aircraft, caused by its increased popularity for transmission of relevant data such as flight plans and the ease of receiving ACARS data links via novel software-defined radio means. As shown in [96,97,99], ACARS presents a high-value target, as location data sent via satellite can be received far out of the line-

of-sight required for other technologies. Further, data that allow for the identification of aircraft movements and locations are regularly transmitted without effective encryption.

- **ADS-B:** ADS-B has undoubtedly caused the greatest shift in concerns over aircraft tracking and privacy since its conception and even more so since the beginning of the equipage phase, which is mandated to end in 2020. As the authorities in the US, Europe and many other airspaces mandate the use of ADS-B for all flights under instrument flight rules, without practical exceptions for military, government or corporate stakeholders, the effort required to track such potentially sensitive aircraft has decreased substantially. Consequently, reports of sensitive military missions picked up via ADS-B are commonplace (e.g., [21]). Likewise, 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 [28]. Moreover, the private use of corporate aircraft by CEOs has been published, implying reputation and business losses for the firms involved [81]. 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 [55]. Studies on ADS-B have shown that the existing privacy provision in the ADS-B Universal Access Transceiver (UAT) data link is flawed [88] 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 the real transponder ID is unknown [59, 110].
- **SSR/MLAT:** Even if aircraft are not equipped with ADS-B, their presence in the general vicinity is easily derived via 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 [115].
- **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 [45].
- **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 pub-

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

lication of these data led to accusations of under-reported CEO income and increased scrutiny of corporate flight departments [64]. Other authors have used this dataset to establish a correlation between CEOs' holiday schedules and their companies' news announcements to predict stock price volatility [132]. Finally, the data have been used to correlate merger and acquisition activities with corporate flights [65], motivating later research that used ADS-B data to investigate the same issue [113].
Reports indicate that some companies are aware of this vulnerability and therefore attempt to prevent the exposure of their aircraft on public tracking websites [23]. Lastly, aircraft movement data obtained from the ATC system has been used to uncover government and military operations [113, 114] as well as surveillance operations by police entities [12].

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 refers to Internet forums where aviation enthusiasts share potenially sensitive ACARS messages [122]. Very recently, three academic works analyzed the occurrence and impact of misusing unsecured data links for potentially sensitive and confidential data in more systematic ways. The authors in [97, 99] examine the usage of ACARS in Central Europe by analyzing a large amount of messages received via VHF and satellite communication. On both data links, they showed that sensitive information ranging from credit card data and medical records to passenger lists was 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 substitution ciphers in an attempt to protect their communication. Naturally, this approach is highly insecure and leaks both tracking information and personal data.

3 Defensive Research

3.1 Research on Security Countermeasures

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

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

Table 4 Existing research on security for ATC technologies.

Cyber-Physical Security	
Physical Layer	[14,37,53,57,58,60–62,72–74,76,82,91,95,106,118,125,128,133]
Localization	[29, 31, 69, 70, 90, 107, 109]
Watermark/Fingerprinting	[30, 42, 44, 85, 110, 133]
Machine Learning	
Classification	[35, 75, 101, 133]
Anomaly Detection	[35, 41, 57, 58, 62, 106, 108, 116]
Non-technical Measures	
Formal Methods	[17, 68, 71, 78, 117, 120]
Policies/Procedures	[22, 63, 77, 80, 98, 104, 124]
Cryptography	
Cryptographic Measures	[1–3, 10, 13, 16, 18, 33, 34, 36, 38, 40, 46, 48–52, 56, 66, 67, 79, 84, 86, 87, 93, 103, 108, 121, 126, 129–131, 135, 136]

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 are securing the monitoring and controlling of the system. 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 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 achieves 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 [14,72,106], Doppler shifts [37,91], direction of arrival [125], or angle of arrival [73]. Some authors [74,118] further suggest the use of beamforming to detect spoofing attacks. Several works also exploit physical layer characteristics to improve defenses against jamming [60,61,128].

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 [29,69,70] but also using other techniques [90,107,109]. Other approaches have used the angle of arrival to localize aircraft and verify their position claims [31].

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 [30, 42, 44, 85]. 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 [110], another approach uses behavioural differences in the frequencies exhibited by different aircraft transponders [59]. 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 principal 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 [35, 75, 101] use behavioural 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 [35, 101], thereby seeking to detect anomalies with regards to legitimate channel use. In contrast, the authors in [106, 116] 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 the space of states normally occupied by aircraft and detect subsequent diversions from this normal state. Finally, the authors in [41] apply long short-term memory networks to detect spoofed ADS-B location messages in the flight tracks of commercial aircraft.

In general, there are often multiple explanations and causes for abnormal behaviour, making anomaly detection usually only one part of an intrusion detection system. Careful calibration and engineering are required to prevent false positives.

3.1.3 Non-technical Measures

Besides technical approaches, there is significant recent research into non-technical measures to secure the air–ground link. By the term 'non-technical', we refer to approaches that prefer formal and procedural adaptations within 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 and considering potential mitigations [78]. More recently, the authors of [68] 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. Recent work has delivered a complete formal verification of the ACARS Message Security standard ARINC 823 [17]. They confirm the security properties of the protocol, yet their analysis also finds several weaknesses, attacks, and imprecisions in the standard for which they propose potential fixes. Other work proposes the use of ontologies [71], modal logic [120], and dynamic queue networks [117] 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 looked at policies and procedures to improve the security of wireless communications. An overview of security-related initiatives of aviation authorities and the industry can be found in [63].

For example, changes to the education of aviation professionals and air travelers on as regards the security problems of ADS-B are proposed [104], as is the use of flight simulators to simulate cyberattacks [77, 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 [104, 124]. 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 [19]. Finally, it is suggested that the next generation of ATC technology should be designed with cyberattacks and radio frequency interference in mind [80, 105].

3.1.4 Cryptography

Cryptography is the most effective means to realize secure communication in any scenario. Indeed, this is also the single most popular research area regarding the protection of wireless aviation protocols, despite the straightforward obstacles to deployment that have been pointed out by many authors (e.g., [108, 126]). Its main appeal lies in the ability to effectively secure the content of any digital communication, offering integrity, authentication, and confidentiality if required. Confidentiality in particular cannot be offered by any other means, making works on cryptographic security in ATC also a viable starting point for the research on privacy countermeasures, which we discuss in the next chapter. Unfortunately, besides the ARINC 823 standards on ACARS Message Security [2, 3], which have seen no adoption in practice, no currently used aviation standard proposes any implementation of cryptography [97].

Earlier work has analyzed the security problems of unencrypted communication in both ACARS [87], ADS-B [48], and CPDLC [36, 67, 79] and suggested experi-

mental solutions to build on further. Once the security problems of ADS-B came to the fore, many researchers focused on the development of adequate schemes for existing and potentially future protocols. New proposals include identity-based encryption [40, 43, 121, 129, 130], format preserving encryption [10, 33, 34, 46] and retro-active key publication [16, 93, 108]. There has been renewed research on public key infrastructures in the aviation context [56, 136] and the application of blockchains towards the problem [13, 86]. While much work has addressed the downsides of cryptographic countermeasures and their incompatibility with current systems [1, 93, 131], to the best of our knowledge these studies have not yet been considered in detail by aviation authority committees.

3.2 Research on 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. We also discuss the aviation industry's attempts to strengthen privacy and the related measures proposed.

3.2.1 Countermeasures against Tracking

Recent works have analysed industry proposals to mitigate the problem of tracking sensitive private and public aircraft and found them largely ineffective against realistic threat models [113]. The examined countermeasures can be divided into technical and non-technical countermeasures.

Technical Measures

- **Turn position broadcasting off:** As ADS-B is not mandated in all airspaces, there are around 30% of all aircraft in recent samples that did not yet support it and consequently do not broadcast their position [92]. However, this is only a short-term solution until 2020 in Western airspaces, and moreover much recent research has shown that aircraft can easily be tracked using other means.
- **Pseudonymous Identifiers:** The only ATC technology offering pseudonymous identifiers by design, is the UAT data link 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 to avoid third-party tracking [5]. Unfortunately, this approach is both limited to general aviation aircraft in the US and ineffective as the aircraft's real identifiers can be recovered [88]. Furthermore, the FAA warns that using this feature may have serious negative consequences [4]:

> 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 entities offer solutions which enlist an aircraft into an anonymous "DOTCOM" airline [123], thus effectively anonymizing their call sign. While this approach has potential benefits compared to other blocking solutions, aircraft still broadcast their real transponder IDs, such that the solution is ineffective to all but the weakest attacker models.

- **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 Section 3.1.4) may also be effective. In practice, the problem of compatibility and quick implementation remain, in particular as regards the need to prevent data leaks on all wireless technologies used by an aircraft, i.e., separate solutions for SSR, ADS-B, ACARS, CPDLC and even VHF would be required.

Non-Technical Measures

- **Web tracker blocking:** Many stakeholders seek to prevent the live and public display of their aircraft on websites such as *Flightradar24* using block lists. For a history and legal analysis of the FAA's blocking program in the USA, see [39]. The effectiveness of any such approach has however been strongly disputed recently [113], as alternative data sources such as personal SDR receivers or non-complying websites trivially circumvent such obscuration.
- **Ownership obscuration:** Similarly to the blocking of flight data, 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 avoid the described type of privacy concerns is provided by not using designated aircraft, regardless of whether they are operated by the government, military or privately, and instead rely on more anonymous, non-exclusive transport means. As such radical measures may compromise the security or privacy of the user, they may not be feasible in many cases.

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

Recommendations

The literature has further discussed potential directions in aviation privacy: In the short term, regulation could provide one possible avenue in mitigating 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 [113]. 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 [27]. 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.

Hence, the only way to effectively create the short-term opportunity for privacy in ATC systems is through the combination of technical and regulatory measures [113]. Regulatory measures can cover data generated by state entities but technical measures are needed to prevent entities from collecting significant amounts of data.

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 some of the worst misuses reported.

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 voiced as early as 1998 [83, 127]. For example, a Swiss pilot has documented a case study where sensitive credit card data transmitted by plain-text ACARS messages were intercepted [122]. 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 [2, 3, 103], 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, which have not been independently verified. Instead, researchers

have shown examples where these schemes can be broken quickly and trivially [96]. While recent proposals for novel data link technology, such as L-DACS and Aero-MACS, do consider encryption as a standard measure (e.g., [66]), they do not entail readily available solution since the technology 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 between its fee-paying members. However, a free global platform that shares and integrates data among all relevant 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 provides not only physical, but also 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 [100]. While extensive development, testing and certification cycles boosted flight safety performance to record levels, those 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 [54].

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 [15, 112]. 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 industry.

In the meantime, it is finally worth noting that there has been no research into short-term, transparent, quickly applicable solutions for the data link protocols ACARS and CPDLC. 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 as the non-existing uptake of the ACARS Message Security standard and the many flawed proprietary attempts to encrypt ACARS illustrate [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 are unsuited to 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 [115]. 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. ADS-B authentication compliant with Mode-S extended squitter using PSK modulation
2. DataLink Security, Part 1 - ACARS Message Security. Tech. Rep. 823P1, ARINC (2007)
3. DataLink Security, Part 2 - Key Management. Tech. Rep. 823P2, ARINC (2008)
4. Airworthiness Approval of Automatic Dependent Surveillance - Broadcast (ADS-B) Out Systems. Tech. Rep. 20-165, Federal Aviation Administration (2010)
5. Minimum operational performance standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance – Broadcast. Tech. Rep. DO-282B, RTCA, Inc (2011)
6. 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)
7. Adamy, D.: EW 101: A first course in electronic warfare. Artech (2001)
8. Adamy, D.: EW 102: A second course in electronic warfare. Artech (2004)
9. Adamy, D.: EW 103: Tactical battlefield communications electronic warfare. Artech (2008)

10. 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 (2014)
11. Airways New Zealand: FANS1/A Problem Reporting (2018). URL http://www.fans-cra.com/report/de-identified/list/
12. Aldhous, P.: BuzzFeed News trained a computer to search for hidden spy planes. This is what we found. Buzzfeed News (2017). URL https://www.buzzfeed.com/peteraldhous/hidden-spy-planes
13. 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 (2019)
14. 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 (2016)
15. Berges, P.M.: Exploring the Vulnerabilities of Traffic Collision Avoidance Systems (TCAS) Through Software Defined Radio (SDR) Exploitation. Ph.D. thesis, Virginia Tech (2019)
16. Berthier, P., Fernandez, J.M., Robert, J.M.: Sat: Security in the air using tesla. In: 36th Digital Avionics Systems Conference. IEEE (2017)
17. Blanchet, B.: Symbolic and Computational Mechanized Verification of the ARINC823 Avionic Protocols. In: 30th Computer Security Foundations Symposium. IEEE (2017)
18. 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 (2018)
19. Carey, B.: FAA No Longer Expected To Retire Radars. Aviation Week (2018). URL https://aviationweek.com/awincommercial/faa-no-longer-expected-retire-radars
20. Cenciotti, D.: Forget any security concern and welcome Air Force One on Flightradar24! The Aviationist (2011). URL https://theaviationist.com/2011/11/24/af1-adsb
21. Cenciotti, D.: Online flight tracking provides interesting details about Russian air bridge to Syria. The Aviationist (2015). URL https://theaviationist.com/2015/09/11/ads-b-exposes-russian-air-bridge-to-syria/
22. Chivers, H.: Control consistency as a management tool: the identification of systematic security control weaknesses in air traffic management. International Journal of Critical Computer-Based Systems **6**(3), 229–245 (2016)
23. City A.M.: Drugs giant AbbVie flicks privacy switch on corporate jet (2014). URL http://www.cityam.com/1405384925/drugs-giant-abbvie-flicks-privacy-switch-corporate-jet
24. 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)
25. crescenvenus: Wireless Attack Launch Box (WALB) (2018). URL https://github.com/crescentvenus/WALB
26. Di Marco, D., Manzo, A., Ivaldi, M., Hird, J.: Security testing with controller-pilot data link communications. In: Availability, Reliability and Security (ARES), 2016 11th International Conference on, pp. 526–531. IEEE (2016)
27. Directorate of Air Traffic Management: Automatic Dependent Surveillance-Broadcast (ADS-B). Tech. rep., Airports Authority of India, New Delhi, India (2014)
28. Dupraz-Dobias, P.: Swiss officials just seized 11 of the world's most expensive cars from this African president's son. Quartz (2016). URL https://goo.gl/rR34aP
29. El Marady, A.A.W.: Enhancing accuracy and security of ads-b via mlat assisted-flight information system. In: Computer Engineering and Systems (ICCES), 2017 12th International Conference on, pp. 182–187. IEEE (2017)
30. Fantacci, R., Menci, S., Micciullo, L., Pierucci, L.: A secure radio communication system based on an efficient speech watermarking approach. Security and Communication Networks **2**(4), 305–314 (2009)

31. 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)
32. Federal Aviation Administration: Aircraft Registry (2017). URL {https://www.faa.gov/licenses_certificates/aircraft_certification/aircraft_registry/}
33. Finke, C., Butts, J., Mills, R.: ADS-B encryption: confidentiality in the friendly skies. 8th Annual Cyber Security and Information Intelligence Research Workshop (2013)
34. Finke, C., Butts, J., Mills, R., Grimaila, M.: Enhancing the security of aircraft surveillance in the next generation air traffic control system. International Journal of Critical Infrastructure Protection **6**(1), 3–11 (2013)
35. Finke, M., Stelkens-Kobsch, T.H.: A practical example for validation of atm security prototypes. CEAS Aeronautical Journal pp. 1–14 (2018)
36. Getachew, D., Griner Jr, J.H.: An elliptic curve based authentication protocol for controller-pilot data link communications. In: Integrated CNS Conference & Workshop (2005)
37. Ghose, N., Lazos, L.: Verifying ADS-B navigation information through Doppler shift measurements. In: 34th IEEE/AIAA Digital Avionics Systems Conference (DASC) (2015)
38. Gurtov, A., Polishchuk, T., Wernberg, M.: Controller–pilot data link communication security. Sensors **18**(5), 1636 (2018)
39. 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)
40. 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)
41. Habler, E., Shabtai, A.: Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages. arXiv preprint arXiv:1711.10192 (2017)
42. Hagmuller, M., Hering, H., Kropfl, A., Kubin, G.: Speech watermarking for air traffic control. In: IEEE European Signal Processing Conference (2004)
43. 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 Transactions on Information Forensics and Security **12**(2), 454–464 (2017)
44. 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)
45. Hoffman, D., Rezchikov, S.: Busting the BARR: Tracking "Untrackable" Private Aircraft for Fun & Profit. In: DEF CON 20. Las Vegas (2012)
46. 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)
47. International Civil Aviation Organization (ICAO): Guidance Material: Security issues associated with ADS-B. Tech. rep., Montreal, QC, Canada (2014)
48. Jochum, J.R.: Encrypted Mode Select ADS-B tactical military situational awareness. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA (2001)
49. Kacem, T., Wijesekera, D., Costa, P.: Integrity and authenticity of ADS-B broadcasts. In: IEEE Aerospace Conference (2015)
50. Kacem, T., Wijesekera, D., Costa, P.: Key distribution scheme for aircraft equipped with secure ads-b in. In: Intelligent Transportation Systems (ITSC), 2017 IEEE 20th International Conference on, pp. 1–6. IEEE (2017)
51. 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)
52. Kenney, L., Dietrich, J., Woodall, J.: Secure ATC surveillance for military applications. In: IEEE Military Communications Conference (MILCOM), pp. 1–6. IEEE (2008)
53. Kim, Y., Jo, J.Y., Lee, S.: ADS-B vulnerabilities and a security solution with a timestamp. IEEE Aerospace and Electronic Systems Magazine **32**(11), 52–61 (2017)

54. 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 Acocuntability Office (2018)
55. Laboda, A.: Unencrypted ADS-B OUT Confounds Aircraft Blocking. NBAA Convention News (2015)
56. 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 (2015)
57. Leonardi, M.: ADS-B anomalies and intrusions detection by sensor clocks tracking. IEEE Transactions on Aerospace and Electronic Systems (2018)
58. 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 (2018)
59. 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)
60. 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 (2014)
61. Leonardi, M., Piracci, E., Galati, G.: ADS-B jamming mitigation: a solution based on a multichannel receiver. IEEE Aerospace and Electronic Systems Magazine **32**(11), 44–51 (2017)
62. Li, T., Wang, B.: Sequential collaborative detection strategy on ads-b data attack. International Journal of Critical Infrastructure Protection **24**, 78–99 (2019)
63. Mahmoud, M., Pirovano, A., Larrieu, N.: Aeronautical communication transition from analog to digital data: A network security survey. Elsevier Computer Science Review **11** (2014)
64. Maremont, M., McGinty, T.: Corporate jet set: Leisure vs. business. The Wall Street Journal (2011). URL `https://www.wsj.com/articles/SB10001424052748703551304576260871791710428`
65. Maremont, M., McGinty, T.: Ready for departure: M&A airlines. The Wall Street Journal (2011). URL `https://www.wsj.com/articles/SB10001424052702303499204576389923856575528`
66. Mäurer, N., Bilzhause, A.: A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS). In: Digital Avionics Systems Conference. IEEE (2018)
67. McParland, T., Patel, V., Hughes, W.J.: Securing air-ground communications. In: 20th IEEE/AIAA Digital Avionics Systems Conference (DASC), vol. 2 (2001)
68. Montefusco, P., Casar, R., Stelkens-Kobsch, T.H., Koelle, R.: Addressing security in the ATM environment (2016)
69. 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)
70. 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)
71. Morel, L.P.: Using ontologies to detect anomalies in the sky. Ph.D. thesis, École Polytechnique de Montréal (2017)
72. 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)
73. Murphy, T., Harris, W.: Device, System and Methods Using Angle of Arrival Measurements for ADS-B Authentication and Navigation (2014). URL `https://www.google.com/patents/US20140327581`. US Patent App. 13/875,749

74. Naganawa, J., Tajima, H., Miyazaki, H., Koga, T., Chomel, C.: ADS-B anti-spoofing performance of monopulse technique with sector antennas. In: Antenna Measurements & Applications (CAMA), 2017 IEEE Conference on, pp. 87–90. IEEE (2017)
75. Neffe, M., Van Pham, T., Hering, H., Kubin, G.: Speaker segmentation for air traffic control. In: Speaker Classification II. Springer (2007)
76. Nguyen, A.Q., Amrhar, A., Zambrano, J., Brown, G., Landry Jr, R., Yeste, O.: Application of phase modulation enabling secure automatic dependent surveillance-broadcast. Journal of Air Transportation **26**(4), 157–170 (2018)
77. Nguyen, D., Shelton, J.W., Mitchell, T.M.: System and method for evaluating cyber-attacks on aircraft (2017). US Patent 9,836,990
78. Nuseibeh, B., Haley, C.B., Foster, C.: Securing the skies: In requirements we trust. IEEE Computer **42**(9), 64–72 (2009)
79. 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)
80. Osechas, O., Mostafa, M., Graupl, T., Meurer, M.: Addressing vulnerabilities of the CNS infrastructure to targeted radio interference. IEEE Aerospace and Electronic Systems Magazine **32**(11), 34–42 (2017)
81. Palan, D., Boldt, K.: Abflug in höhere Sphären. Manager Magazin (2012). URL `http://www.manager-magazin.de/lifestyle/reise/a-827947-6.html`
82. Park, P., Khadilkar, H., Balakrishnan, H., Tomlin, C.J.: High confidence networked control for next generation air transportation systems. IEEE Transactions on Automatic Control **59**(12), 3357–3372 (2014)
83. Pascoe, K.: ACARS and Error Checking (2015). URL `http://www.flight.org/acars-and-error-checking`
84. Patel, V.: ICAO air-ground security standards strategy. In: IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS) (2015)
85. Prinz, J., Sajatovic, M., Haindl, B.: S/sup 2/EV-safety and security enhanced ATC voice system. In: IEEE Aerospace Conference (2005)
86. Reisman, R.: Blockchain serverless public/private key infrastructure for ADS-B security, authentication, and privacy. In: AIAA Scitech 2019 Forum, p. 2203 (2019)
87. 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)
88. Sampigethaya, K., Taylor, S., Poovendran, R.: Flight privacy in the nextgen: Challenges and opportunities. In: Integrated Communications, Navigation and Surveillance Conf. (2013)
89. 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 (2013)
90. Schäfer, M., Lenders, V., Schmitt, J.: Secure Track Verification. In: IEEE Symposium on Security and Privacy (S&P), pp. 199–213. IEEE (2015)
91. 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 (2016)
92. 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)
93. 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 (2018)
94. Selleck, D.: Iridium fault prompts ban by Oceanic ATC. Flight Service Bureau (2017). URL `ttp://flightservicebureau.org/iridium-fault/`
95. Shang, F., Wang, B., Yan, F., Li, T.: Multidevice false data injection attack models of ADS-B multilateration systems. Security and Communication Networks **2019**, 1–11 (2019)

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. arXiv preprint arXiv:1905.08039 (2019)
99. Smith, M., Strohmeier, M., Lenders, V., Martinovic, I.: On the security and privacy of ACARS. IEEE Integrated Communications, Navigation and Surveillance Conference (2016)
100. Stavridou, V., Dutertre, B.: From security to safety and back. In: Computer Security, Dependability and Assurance: From Needs to Solutions, pp. 182–195. IEEE (1998)
101. Stelkens-Kobsch, T., Hasselberg, A., Mühlhausen, T., Carstengerdes, N.: Towards a more secure ATC voice communications system. In: Digital Avionics Systems Conference (2015)
102. Stewart, J.: Meet the NATS pirate hunters. NATS Blog (2015). URL `https://nats.aero/blog/2015/05/meet-the-nats-pirate-hunters/`
103. Storck, P.: Benefits of commercial data link security. In: IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS) (2013)
104. Strand, D.A.: Automatic dependent surveillance - broadcast (ADS-B) vulnerabilities. Ph.D. thesis, Utica College (2017)
105. Strohmeier, M.: Security in next generation air traffic communication networks. Ph.D. thesis, University of Oxford (2016)
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 (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 (2015)
108. Strohmeier, M., Lenders, V., Martinovic, I.: On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. IEEE Communications Surveys & Tutorials **17**(2) (2015)
109. Strohmeier, M., Lenders, V., Martinovic, I.: A k-nn-based localization approach for crowdsourced air traffic communication networks. IEEE Transactions on Aerospace and Electronic Systems **56**(1) (2018)
110. 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 (2015)
111. 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 (2018)
112. Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V., Martinovic, I.: On perception and reality in wireless air traffic communication security. IEEE Transactions on Intelligent Transportation Systems **18**(6), 1338–1357 (2017)
113. 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)
114. 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)
115. 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)
116. 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)

117. Tamimi, A., Hahn, A., Roy, S.: Cyber threat impact analysis to air traffic flows through dynamic queue networks. arXiv preprint arXiv:1810.07514 (2018)
118. Tart, A., Trump, T.: Addressing security issues in ADS-B with robust two dimensional generalized sidelobe canceller. In: Digital Signal Processing (DSP), 2017 22nd International Conference on, pp. 1–5. IEEE (2017)
119. Teso, H.: Aircraft hacking: Practical aero series. Fourth Annual Hack in the Box Security Conference (2013)
120. Thudimilla, A., McMillin, B.: Multiple security domain nondeducibility air traffic surveillance systems. In: High Assurance Systems Engineering (HASE), 2017 IEEE 18th International Symposium on, pp. 136–139. IEEE (2017)
121. 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 Transactions on Aerospace and Electronic Systems (2019)
122. Tilly, Peter: Die verpasste Chance. AEROPERS Rundschau (2013). URL https://www.aeropers.ch/index.php/der-verband/rundschau1/archiv/rundschau-archiv-rundschau-archiv-2013-1/638-rundschau-2-2013-1/file
123. Trautvetter, C.: FltPlan flight privacy program exposes tangled FAA policy. AIN Online (2011). URL https://www.ainonline.com/aviation-news/aviation-international-news/2011-08-31/fltplan-flight-privacy-program-exposes-tangled-faa-policy
124. 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)
125. 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)
126. Wesson, K.D., Humphreys, T.E., Evans, B.L.: Can cryptography secure next generation air traffic surveillance? IEEE Security and Privacy Magazine (2014)
127. Wolper, J.: Security risks of laptops in airline cockpits (1998). URL http://catless.ncl.ac.uk/Risks/20/12
128. 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)
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 Transactions on Services Computing **10**(2), 165–175 (2015)
130. 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 Chinese Journal of Aeronautics **27**(3), 688–696 (2014)
131. Yang, H., Zhou, Q., Yao, M., Lu, R., Li, H., Zhang, X.: A Practical and Compatible Cryptographic Solution to ADS-B Security. IEEE Internet of Things Journal (2018)
132. Yermack, D.: Tailspotting: Identifying and profiting from CEO vacation trips. Journal of Financial Economics **113**(2), 252–269 (2014)
133. Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L., Poovendran, R.: Detecting ADS-B spoofing attacks using deep neural networks. arXiv preprint arXiv:1904.09969. (2019)
134. Younger, E.: Melbourne Airport hoax caller Paul Sant pleads guilty to making fake flight calls, aborting Virgin landing. ABC News (2017). URL 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: M.S. Musa, Z. Wu (eds.) Aeronautical telecommunications network: Advances, challenges, and modeling. CRC Press (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, FL (2014)