**2017 9th International Conference on Cyber Conflict**
Defending the Core
H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.)
2017 © NATO CCD COE Publications, Tallinn

# Crowdsourcing Security for Wireless Air Traffic Communications

**Martin Strohmeier**
Department of Computer Science
University of Oxford
Oxford, United Kingdom
martin.strohmeier@cs.ox.ac.uk

**Matt Smith**
Department of Computer Science
University of Oxford
Oxford, United Kingdom
matthew.smith@cs.ox.ac.uk

**Matthias Schäfer**
Department of Computer Science
University of Kaiserslautern
Kaiserslautern, Germany
schaefer@cs.uni-kl.de

**Vincent Lenders**
Cyberspace and Information
armasuisse
Thun, Switzerland
vincent.lenders@armasuisse.ch

**Ivan Martinovic**
Department of Computer Science
University of Oxford
Oxford, United Kingdom
ivan.martinovic@cs.ox.ac.uk

**Abstract:** Protecting the security of the cyber-physical systems that make up the world's critical infrastructures has been a recent hotly debated topic. Legacy wireless communication infrastructure is often an impediment to quickly improving these crucial systems, as cryptographic solutions prove impossible to deploy. In this article, we propose the establishment of a separate verification layer for sensitive wireless data powered by crowdsourced sensors connected to the Internet and apply it to the aviation domain.

We first validate the need for independent data verification in air traffic control networks, where all wireless communication is conducted in the clear and thus subject to manipulation. To counter this threat, we develop a comprehensive model for the verification of wireless communication based on massively distributed data collection and outline how it can be used to immediately improve the security of unprotected air traffic control networks.

By combining several different methods based on the content and the physical characteristics of aircraft signals, our system is able to detect typical injection, modification and jamming attacks. We further develop a trust model to defend against potential insider threats based on compromised sensors.

We illustrate our approach using the crowdsourced sensor network OpenSky, which captures large parts of civil air traffic communication around the globe. We analyse the security of our approach and show that it can quickly, cheaply, and effectively defend against even sophisticated attacks.

**Keywords:** *critical infrastructures, wireless security, air traffic control, crowdsourcing, sensor networks, participatory sensing*

# 1. INTRODUCTION

As modern computer networks become increasingly important for the safe facilitation of travel on the ground, sea and in the air, their cyber security must be ensured. In recent years both the academic community and hacker circles have shown that many vulnerabilities exist in the cyber-physical networks used by core critical infrastructures such as air traffic control (ATC) or vessel traffic services [1]–[3]. Numerous reasons prevent the quick and effective replacement of existing technologies with new and secure ones; because of this, novel methods of protection are required.

In this paper, we propose the crowdsourcing of security to protect core critical infrastructures without the lengthy and costly deployment of new technologies. We present the crowdsourced sensor network OpenSky and outline how it can be used to immediately improve the security of ATC networks.

The idea of crowdsourcing has previously been applied to attempt to solve many large-scale scientific problems such as protein folding [4] and classification of galaxies [5]. Recently, numerous private companies have started to use crowdsourced networks to track the locations of ships and aircraft around the globe. As the networks' data collection infrastructure grows, their services are increasingly requested by large industry players and authorities [6].

Thus, it naturally follows to exploit the data and intelligence gathered by such crowdsourced networks to secure the cyber-physical systems of critical infrastructures. In this work, we present an approach to delivering secure civil ATC using OpenSky, a sensor network for ATC communication consisting of more than 300 crowdsourced sensors, which receive over 100,000 transponder signals per second providing coverage across all continents [7], [8].

Our contributions are:

- We explain how crowdsourced networks can be exploited to act as independent witnesses of attacks such as jamming and spoofing, and to provide a trusted third party opinion.
- We present a system that is able to detect data maliciously injected into the wireless channels used for ATC. By employing several independent verification approaches, we can detect even sophisticated attackers and present a constantly validated picture of the airspace.
- We further analyse the security challenges that arise if malicious sensor owners attempt to compromise the system. We describe the trust models used for newly-connected sensors and how to prevent insider attacks.

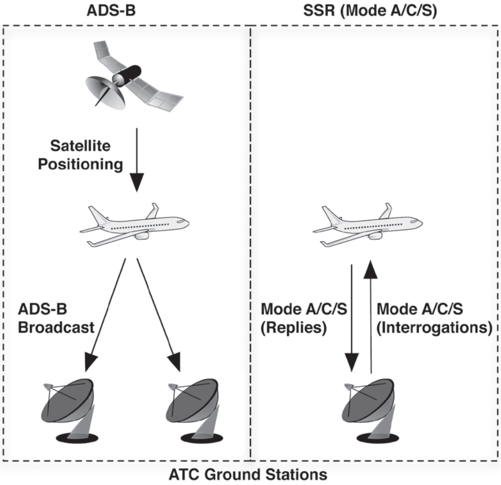
In the remainder of this work, we briefly describe the ATC technologies and their vulnerabilities in Section 2, before considering the related work in Section 3. Section 4 describes the crowdsourced system and the algorithms to detect potential attacks. Section 5 introduces our threat model, while Section 6 explains our countermeasures to wireless ATC threats. Section 7 analyses the security of our system. Section 8 discusses wider application, extensions, and cost. Finally, Section 9 concludes this paper.

## 2. WIRELESS THREATS TO ATC

With the rise of terrorist and organised crime groups interested in cyber attacks on ATC targets, a wide range of vulnerabilities and cyber attack vectors threaten the aviation infrastructure. Such vectors include malware in ATC networks and computers [9] and direct attacks on aircraft onboard networks [10].

In this work, we focus on the attack vectors provided by wireless ATC technologies, which are all inherently insecure by design [1], [2], [11], [12]. We briefly explain the function of two such technologies and the vulnerabilities that we seek to protect against by using a crowdsourced security model. While they act as technical proof-of-concept, the concepts in this paper can be adapted to other wireless technologies used in ATC, such as those used for data links, navigation, or collision avoidance.

**FIGURE 1.** REPRESENTATION OF ADS-B AND MODE S SYSTEMS



## A. Modern ATC Technologies

Secondary Surveillance Radar (SSR) is a cooperative ATC technology currently based on the so-called transponder Modes A, C, and S, which provide digital target information compared to traditional analogue primary radar (PSR) [13]. Aircraft transponders are interrogated on the 1030MHz frequency and reply with the desired information on the 1090MHz channel, as shown in Figure 1.

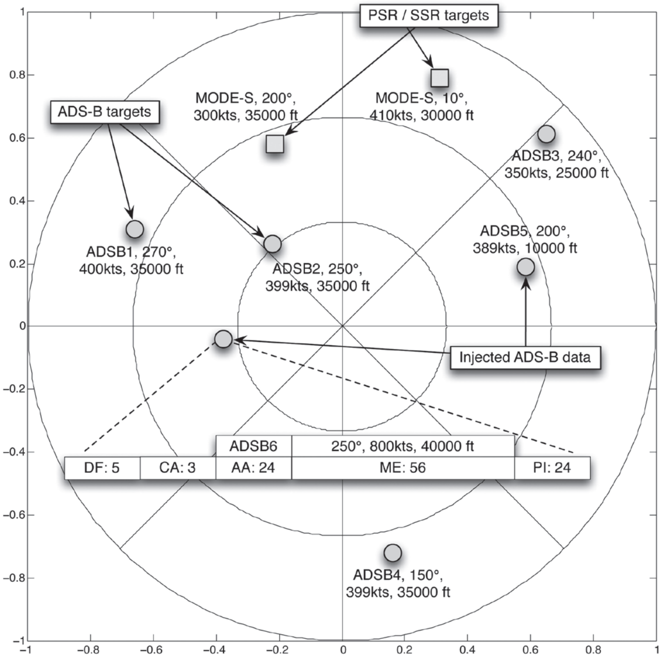
With the newer Automatic Dependent Surveillance-Broadcast (ADS-B) protocol (see Figure 1), aircraft regularly broadcast their own identity, position, velocity and additional information such as intent, status, or emergency codes. These broadcasts do not require interrogation: position and velocity are automatically transmitted twice a second [14].

Unfortunately, security was not part of the design of these systems; neither includes cryptographic protection, which could provide confidentiality, integrity, or authentication for ATC users. Consequently, it is entirely possible to modify any airspace picture based on these technologies, as elaborated in the next section.

## B. Wireless Attack Vectors against ATC Infrastructure

It has been shown that commodity hardware can receive and transmit on the frequencies used by ADS-B and SSR, making them accessible even for unsophisticated threat actors [11]. We consider the following common wireless attack vectors against an ATC receiver system providing data to a radar screen:

**FIGURE 2.** ILLUSTRATION OF AN ATC SCREEN WITH INJECTED ADS-B DATA


PSR / SSR targets
ADS-B targets
MODE-S, 200°, 300kts, 35000 ft
MODE-S, 10°, 410kts, 30000 ft
ADSB3, 240°, 350kts, 25000 ft
ADSB1, 270°, 400kts, 35000 ft
ADSB2, 250°, 399kts, 35000 ft
ADSB5, 200°, 389kts, 10000 ft
Injected ADS-B data
ADSB6
250°, 800kts, 40000 ft
DF: 5
CA: 3
AA: 24
ME: 56
PI: 24
ADSB4, 150°, 399kts, 35000 ft
1
0.8
0.6
0.4
0.2
0
−0.2
−0.4
−0.6
−0.8
−1
−1
−0.8
−0.6
−0.4
−0.2
0
0.2
0.4
0.6
0.8
1

### *1) Injections of Ghost Aircraft*

The first attack injects a new ghost aircraft created from scratch, by creating correctly formatted SSR/ADS-B. We assume that the attacker crafts transponder signals with a legitimate identifier and reasonable flight parameters (e.g., plausible altitude and speed) to create an aircraft that is indistinguishable from a legitimate one for radars relying solely on these technologies (see Figure 2 for a high-level illustration). The requirement to handle this aircraft – or many such aircraft – creates significant additional workload for the controller, which can lead to a loss of situational awareness and decrease the safety of the airspace [12]. Consequences may include the requirement to go procedural and use analogue voice technology for communication and aircraft separation, causing significant decrease in air traffic throughput, or even accidents in the worst case [12].

### *2) Modification of Labels*

More subtle is the modification of data sent by real aircraft and seen on the labels on controllers' radar screens. Among other things, these labels include identity, altitude, velocity, heading, and the flight level the aircraft intends to use. It is obvious that any modification of the wireless messages that provide the data for the display can have severe consequences for the safe control of the airspace [12].

***3) Jamming or Denial of Service***

Lastly, we consider jamming attacks, both targeted and unspecific. In an unspecific attack, the frequency is jammed with noise at the receiver, effectively causing a denial of service (DoS). Targeted attacks destroy only specific packets (e.g. for a single aircraft), which can be done even reactively as the packet is on the wireless channel [15]. Jamming ATC technologies can have severe consequences for the situational awareness of pilots and controllers [12].

# 3. RELATED WORK

We briefly analyse the state-of-the-art security for wireless ATC technologies before discussing the related work on crowdsourced security in other fields.

## *A. Wireless Security Approaches for ATC*

Several academic works and presentations at hacker conferences in recent years have highlighted ATC vulnerabilities and inspired urgently needed research on potential security measures. Generally, the most promising approaches can be divided into two different avenues, depending on whether or not they use cryptography.

Using cryptography enables authentication, integrity and confidentiality for all ATC messages and is thus the preferable option to defeat message injections and modifications. However, due to real-world constraints, both technological and regulatory, any advances in this direction will not see widespread deployment for many years [11].

As a result, much research conducted to secure ADS-B and SSR today has considered the application of *transparent* security measures, which do not require changes to the protocols or certified transponder hardware installed in aircraft and ground stations around the world. These typically focus on non-cryptographic schemes that exploit physical characteristics of the wireless signals broadcast by the aircraft, including ADS-B/SSR. Examples of such characteristics include the time differences of arrival [16], [17], Doppler shift [18], or strength [19] of the received transponder signals.

## *B. Crowdsourcing Security using Participatory Sensing*

Governments and other institutions are no strangers to the idea of exploiting crowdsourced sensor data to improve the security of various systems. In particular, the ubiquity of smartphones as sensing devices has inspired the popular research area of participatory surveillance [20]. For example, the authors in [21] explore the Department of Homeland Security's Cell-All project, which seeks to equip mobile phones with chemical-agent detectors to detect potentially dangerous volatile chemical compounds.

Similar concepts have been developed for many other security-related domains, such as nuclear disaster recovery or emergency evacuations [22]. However, to the best of our knowledge the present work is the first to propose crowdsourced sensing of unprotected critical infrastructure communication in order to develop an attack detection system for civil ATC.

# 4. CROWDSOURCING IN AVIATION

In this section, we discuss the motivations and advantages of a separate crowdsourced sensor network used to verify wireless information in critical infrastructures. As a proof-of-concept we introduce the sensor network OpenSky, its existing capabilities, and how we can exploit them to provide a secure radar picture of the civil airspace.

## *A. Motivation*

Crowdsourced networks provide many benefits to aviation users, from airlines and airports to passengers. Airlines and airports use the services offered by several large companies such as Flightradar24 [23] or FlightAware [24], which exploit crowdsourcing to track the movements of all transponder-equipped aircraft around the globe, both in the past and live. Similarly, private end users use the displayed data to track, for example, the punctuality of particular flights relevant to them or simply enjoy following flights in their region for a host of other reasons [25].

Flightradar24 states that their network alone includes more than 10,000 receivers [26]; as the number of such tracking services based on freely available, volunteer-provided ATC communication grows, they illustrate the potential of crowdsourced sensing. For our work, we focus on the utility of these networks for security purposes.

Our goal is to provide a cheap yet reliable and powerful second view of the airspace, acting as a witness and detecting potential attacks on wireless ATC protocols. In a second step, if possible, false data injected by an attacker is filtered out before it is displayed, providing a clean backup view for verification and validation purposes. Finally, it is desirable to narrow down the origin of any such attack to be able to initiate physical protection measures.

## *B. Advantages of Crowdsourced Networks*

In our proposal, we first consider the viewpoint of air navigation service providers who use potentially vulnerable SSR/ADS-B systems. As safety demands in aviation require long, expensive certification processes, such providers cannot quickly upgrade their infrastructure, which explains why ADS-B has been in development since the late 1990s [27]. Implementing new security features into already deployed technologies is also impractical, as it requires an overhaul of all airspace participants [28].

Consequently, we propose an uncertified system based on crowdsourcing to independently verify received ATC signals and validate the information displayed on certified radar systems. Analogous to intrusion detection systems (IDS) in classical computer networks, it collects the available air traffic communication in its coverage range in a distributed fashion, analysing it for potential wireless attacks.

A crowdsourced network of cheap ATC receivers is low-cost, agile and easily scalable. Many compatible receivers already exist around the world, powered by volunteers who provide the view of their local airspace to several crowdsourced networks simultaneously. While it would be feasible to exclusively use self-deployed ATC sensors for a smaller airspace, the use of crowdsourcing offers low barriers to entry, much lower cost and superior scalability for potentially global reach. Using this wealth of data, it is possible to integrate various different data verification methods; and we can directly deploy security software, which does not need to fulfil the strict safety requirements applied in aviation.

In terms of security properties, the massively redundant, distributed and fluid nature of crowdsourced networks provides the key advantage over certified systems with comparatively few expensive sensors in fixed, long-term locations. For example, a single SSR ground sensor is typically responsible for a radius of 200NM [29]. It is thus comparatively easy to mount a jamming attack on such a sensor, which would cause a denial of service in its airspace.

In contrast, the exact number and location of the many active sensors in a crowdsourced network is unknown at any given time. The high sensor density directly improves system resilience, as there are other receivers with overlapping coverage not impacted by an attack.

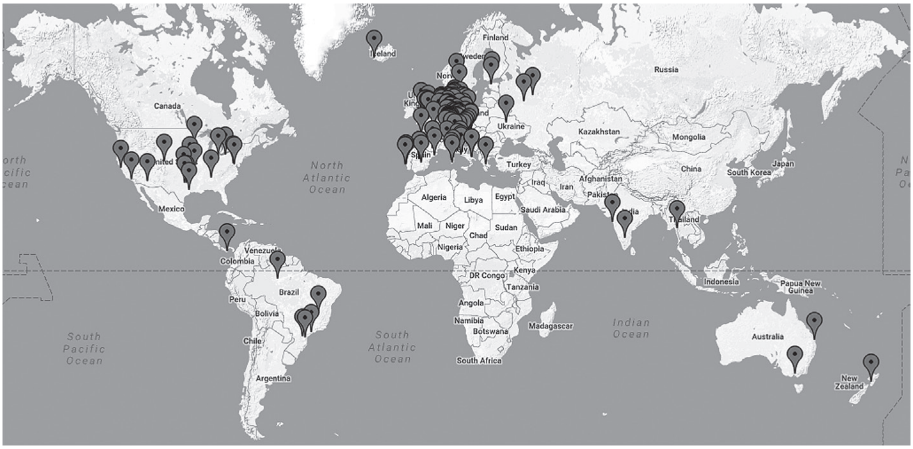
## C. The OpenSky Network

OpenSky is a crowdsourced network used as proof-of-concept for our security approach. In the following we discuss its current deployment and trust model for the integration of new sensors.

### 1) Current Deployment

As of April 2017, the OpenSky Network consists of 260 registered and 300-450 anonymous sensors streaming data to its servers. Registered sensors are those operated by active members of the OpenSky Network community. Their operators are usually known to the administrators, either because the sensor was provided by the network itself or through personal contact. In contrast, the operators of anonymous sensors are unknown. While the exact locations of anonymous sensors are also unknown, they can be approximated based on their coverage and IP address. The locations of registered sensors are known with an accuracy of 10 meters.

**FIGURE 3.** A MAP OF SENSORS REGISTERED TO THE OPENSKY NETWORK (MARCH 2017)



***2) Trust Model***

In general, we consider data from a particular sensor trustworthy if the operator is considered trustworthy. However, the crowdsourcing paradigm prevents the use of classical identity verification methods to build trust in operators. Encryption and authentication are not currently implemented by any of the popular ATC receivers that are used for feeding data flows to the OpenSky Network (e.g., dump1090 [30]). Consequently, securing these flows directly would require the use of a non-standard way of feeding, which would ultimately severely hamper the growth of the network.

The success of a crowdsourced network greatly depends on the simplicity of joining the crowd. Complex approaches such as mandatory passport verification of the operator's identity or setting up PGP keys would discourage operators from feeding data. For this reason, building trust in registered operators is achieved through personal long-term relationships and constant communications with other trusted operators and network administrators.

This method, however, cannot be applied to anonymous sensors, where, except for the exchange of sensor data, there is no communication between the network and the operator. Our method to build trust in these sensors is therefore data-based and trust is constantly re-evaluated. Specifically, we consider an anonymous sensor trustworthy if a considerable fraction of its data can continuously be confirmed by an existing trusted sensor with overlapping coverage. If the number of mismatches in the data between a trusted and an anonymous sensor exceeds a certain threshold, the anonymous sensor is considered untrustworthy and its data is ignored by the network. Anonymous sensors with no common coverage with trusted sensors cannot be verified and their data is therefore considered untrustworthy. However, as Figure 3 shows, there are registered sensors in several parts of the world and the trust of most anonymous sensors in the network can be assessed through the transitivity of our approach.

## 5. THREAT MODEL

We consider two active attackers from a hobbyist to cyber-criminal level as described in [11]. One is an outsider threat, and has the ability to inject, modify or jam transponder signals. The other is an insider threat, and joins the crowdsourcing scheme and attempts to attack it under the guise of being a participant.

We consider the outsider to be moderately-resourced, and capable of performing primarily ground-based attacks. We assume they use off-the-shelf SDRs with readily available transmission equipment. They are capable of attacking from several different positions at once, but without perfect synchronisation.

The insider attacker is also moderately-resourced, and capable of running a number of data feeds at once into the crowdsourcing system. Given the amount of data generated by Mode S, this would be achievable with off-the-shelf computing equipment, though specialist knowledge would be required to synthesise data in such a way that it appears realistic.

The reliable and consistent injection of several matching ATC data feeds with correct timestamps over a long time span (to obtain the necessary trust) exceeds the typical level of sophistication of hobbyists, but it is possible for well-resourced cyber-criminal operations. State actors, which are able to attack network points and modify traffic on the fly, are considered out of our scope.

# 6. CROWDSOURCED SECURITY METHODS FOR ATC

This section presents a crowdsourced security system based on OpenSky. We discuss several independent approaches based on data obtained by a crowdsourced network to detect attacks on ATC protocols, as considered in Section 2.B. We also describe the procedures taken after an attack is detected.

## *A. Crowdsourced Attack Detection*

We use four different detection methods, with varying levels of complexity and sensor requirements summarised in Table 1. The employed methods range from simple plausibility checks based on the content of the received surveillance data to more complex statistical and cyber-physical analysis.

**TABLE 1:** OVERVIEW OF CROWDSOURCED ATTACK DETECTION METHODS

| Method | Number of Receivers | Complexity | Attack Localisation |
|---|---|---|---|
| Plausibility Checks | 1 | Low | No |
| Cross Referencing | 2 or more | Low | No |
| Multilateration | 3 or more | High | Yes |
| Statistical Analysis | 2 or more | Moderate | No |

### *1) Plausibility Checks*

Many attacks can be detected by running comparatively simple checks on the plausibility of the inputs, a method also used by professional radar systems [31]. As a first line of defence, the network uses rules to detect modified flight data. The first set of rules pertains to the communication of an aircraft:

- The position claimed by an aircraft is outside the known recorded range of the receiving sensor, with a safety margin of 50 km;
- An aircraft suddenly appears well within the communication range of a receiver; or
- The required message types (in particular, position, velocity and identity) are not following the technical standards in terms of frequency and order.

The second set of rules is concerned with the technical capabilities of an aircraft, for example:

- The velocity or altitude of an aircraft is outside the possible parameters for the particular class and model;

- The reported velocity of an aircraft and the same aircraft's velocity as derived from its positional data are different (outside of a safety margin of 50 km/h); or
- An aircraft reports an aircraft class/model or capabilities different from its official registration of the network's aircraft database.

***2) Cross Referencing of Data between Sensors***

If we have a redundant coverage of sensors in a given region, we can cross-reference their knowledge about the received aircraft messages. This concerns both the content and the physical characteristics of the messages.

For example, if an aircraft claims to be in an area that is covered by three sensors, when only one of these sensors receives the aircraft's messages, there would be cause for concern. As there is significant frequency overuse on the 1090MHz channel, which causes message loss of 50% or more [32], a single message failing such a cross-reference check is too common to be noteworthy. A sequence of several missed messages which, according to the positional claims are well within a sensor's coverage area, should however be treated as highly suspicious. Similarly, different sensors each receiving different message content from the same aircraft should raise immediate concerns, barring any transponder or decoding errors. Any such instance may indicate a typical message injection, where the threat agent is not close to the claimed position but instead attacks a single ATC receiver location, for example at an airport.

***3) Multilateration and Aircraft Localisation***

Independent localisation of aircraft using the physical characteristics of their communication signals is a popular approach in civil aviation. In areas with sufficient sensor coverage, we can calculate the origin of a signal based on the time differences of arrival at three or more receivers and thus verify an aircraft's location claim. This technique, called multilateration, is used in many modern airspace surveillance systems, but comes at significant costs in installation and maintenance. OpenSky is capable of conducting independent localisation based on the time difference of arrival (TDOA) even with cheap off-the-shelf sensors [33]. While certified systems guarantee higher accuracy and reliability, our crowdsourced approach is sufficient to detect the origins of SSR/ADS-B signals and can easily verify the positions of all civil aircraft. While the requirements for the successful localisation of aircraft signals are high compared to other methods, there is another significant advantage: localising the actual origin of an ATC message will pinpoint the location of the adversary in the event of an attack.

***4) Statistical Analysis***

For areas covered by fewer than three sensors, we can still exploit the time differences of arrival to build a statistical attack detection system based on hard-to-forge physical layer characteristics. By applying hypothesis testing, we can detect potential attackers quickly, even with only two sensors.

We first learn the distribution of errors between the expected and actual time differences between our sensors. In the attack detection phase, we use the non-parametric Wilcoxon rank-sum test to check if the received sample distribution matches the expected distribution. By establishing the proximity to the expected data distribution, we can validate the sender.

## *B. Attack Handling with OpenSky*

If an aircraft track violates one or more of the expectations set out by the detection methods, it is a strong indication of an anomaly, whether deliberately induced or not. To avoid false positives, which strongly detract from the practicality of the system in real-world environments, we combine the knowledge of all available methods, depending on the quality of the sensor data.

If the occurrence is indeed deemed an attack, there are several potential consequences:

- The concerned aircraft tracks are flagged as unreliable, requiring separate handling from the affected controllers;
- The concerned messages are dropped and their content disregarded for the aircraft display on OpenSky's radar view, which is preferable in case of label manipulation or of denial-of-service attacks, whereby the radar screen is flooded with ghost aircraft beyond the controller's handling ability; or
- In cases where sufficient receiver data is available, we can use localisation techniques to narrow down the origin of the attack and follow up with physical containment procedures.

# 7. SECURITY ANALYSIS

In this section, we analyse the potential attacks on a crowdsourced system. We divide these into two categories: insider and outsider attacks. Outsider attacks address issues presented in Section 2, namely the main wireless attack avenues for ATC systems. Insider attacks consider adversaries who attempt to attack the system by subverting the crowdsourced network, here OpenSky. This may provide cover or diversion for other attacks.

## *A. Outsider Attacks on Real-World ATC*

We consider the detection of jamming, injection, and modification attacks separately. Depending on the sophistication of the attacker, all attacks can take different forms [11], as explained in our threat model, we consider attackers below the nation state level, which are moderately resourced and are able to operate from a single location or multiple locations at the same time.

Throughout this section, we consider $n$ sensors (collectively referred to as $S$), which at least partially cover some area $X$. This area is primarily covered by sensor $S_A$, a sensor under attack. $G$ is the set of aircraft currently observable over area $X$ for sensors $S\backslash S_A$, with $G_{S_A}$ being the set of aircraft observable by $S_A$.

### ***1) Jamming Attacks***

We distinguish two different cases of jamming attacks: indiscriminate broadband jamming of the 1090MHz channel leading to the disappearance of all aircraft from radar screens, and targeted jamming of a particular aircraft.

Detecting an indiscriminate jam on a sensor $S_A$ is relatively straightforward as the affected sensor will remain online but cease to report aircraft, which other overlapping sensors may be reporting. Similarly, detection of a targeted jam relies on other sensors with overlapping coverage receiving the data correctly. By cross-referencing the set $G$ with $G_{S_A}$, we can identify any aircraft not detected by $S_A$.

Ultimately, a geographically distributed crowdsourced sensor network limits the potential impact of both. An attacker would have to be sufficiently close to several sensors in order to jam each of their signals. In the case of jamming particular aircraft, time synchronicity of jamming signals at separate sites would have to be tight and require significant resources.

### *2) Injection Attacks*

This section considers an attacker who constructs SSR messages in order to either create a non-existent aircraft or impersonate one not currently in reception range, referred to as a ghost aircraft in [1], [34], [35]. We analyse two cases attempting to inject aircraft $c$: single and multiple location attackers. A single location attacker transmits at a power which either only reaches one sensor or reaches several. If it only reaches a single sensor, $\nexists c : c \in G \cap G_{S_A}$ thus indicating the anomalous aircraft. If messages reach some $s$ in $S$ but not all, comparing each $G_S$ will identify anomalous aircraft. Further steps to identify it as such may be needed though if the majority of $S$ report it to exist. A localisation technique such as TDOA will reveal the true location $Pos_{TDOA}$, for comparison to the claim $Pos_{claim}$. If these differ significantly, an attack is likely. If messages reach all $s \in S$ sensors, the anomalous aircraft will exist in $\exists c : c \in G \cap G_{S_A}$ thus a comparison will not reveal said aircraft; this is the worst case scenario and would rely on localisation such as TDOA to identify an anomalous aircraft.

An attacker using multiple locations to attack multiple sensors will make some positional claim $Pos_{claim}$ using each location to ensure that a number of crowdsourced sensors receive it. This would cause $\exists c : c \in G \cap G_{S_A}$. However, to defeat TDOA, the time synchronisation required is beyond the capability of our attacker model.

Considering that a crowdsourced network such as OpenSky has significant coverage redundancy, an attacker would need to fool many sensors in order to successfully inject messages, even in the unlikely case that they know the exact location of all active sensors. Each additional sensor requires significant further complexity from an attack.

### *3) Modification Attacks*

Modification attacks occur when the attacker changes data transmitted by an aircraft before it is received at a ground station. Based on [2], there are two different approaches to modify a target message; overshadowing and bit-flipping. Overshadowing transmits an entire message at a higher power than the message from the aircraft, whereas bit-flipping transmits a specific part of a message over the aircraft transmission at a higher power. As overshadowing is much easier to perform than bit-flipping, we assume it here.

Again, we consider the cases of an attacker transmitting from a single or multiple locations. We denote the aircraft under attack as  and consider the possible attack intentions to either modify the position/status or identifiers. We first consider each of these for the single-location attacker.

For attackers modifying position, if a single sensor receives modified messages, comparing the position claims of $c \in G$ to $c_{attack} \in G_{S_A}$ will identify the anomalous position, allowing the aircraft in question to be highlighted as anomalous. If modified messages are received by multiple sensors in $S$ then the position claims for $c$ in $\forall\ s \in S: G_s$ must be compared. At this point we cannot know how many members of $S$ are under attack. We can construct $S_{similar}$ by finding $s \in S$ where $c$ in each is making similar position claims. A significant majority of $S$ would need to agree before it could be taken as consensus – otherwise, a multilateration approach would be needed to check the claims for each group of similar sensors. The inaccurate sensors can then be deemed under attack.

Where attackers modify identity, if modified messages are reaching a single sensor, $G \setminus G_{S_A}$ will identify the aircraft $c_{true}$ being attacked, with $G_{S_A} \setminus G$ identifying the modified aircraft $c_{attack}$. Using this, $c_{attack}$ can be highlighted as anomalous. Furthermore, the positions of $c_{true}$ and $c_{attack}$ should be the same. If modified messages are reaching multiple sensors, we compare $c$ in $\forall\ s \in S: G_s$ by positional claims. If sensors $s_1,\ldots,s_n$ report multiple of different identities aircraft $c_1,\ldots,c_m$ with the same position, this indicates an attack. Then, we must perform multilateration on messages from each $c_1,\ldots,c_m$ to identify which aircraft is in the claimed position and is not attacker-generated. From this we can establish which sensors are not under attack and are thus receiving legitimate messages.

In the case of an attacker using multiple locations, this becomes an extended case of a single location attacker transmitting to multiple sensors. We can detect anomalous aircraft by comparing the output of sensors, assuming the attacker is not simultaneously attacking all sensors. Since we assume our attacker does not have the required infrastructure to defeat TDOA, we rely on it to identify aircraft which are claiming to be in positions which they are not, and in the case of attacks on identity, establish which of the claimed aircraft identities for a given position are actually in the air.

## *B. Insider Attacks on OpenSky*

Besides direct attacks on ATC technologies, it is imperative to consider the integral security of our crowdsourced system. Since we do not directly control all sensors used for attack detection, we require a separate trust-based security layer to detect and defeat internal attacks. We consider the manipulation of data by a single rogue sensor and the stronger Sybil attack.

### ***1) Single Sensor Data Manipulation***

First, we consider the case where an attacker manipulates a single sensor, which provides incorrect data to the network. In particular, an attacker may either act benignly for some time to gain trust or hijack a network connection of a trusted sensor. Given the range of a typical SSR sensor, this can result in a significant coverage area being affected.

Sanity checks will defeat more simplistic attacks; for example, should a sensor suddenly change its coverage area or begin to report significantly different numbers of aircraft then this is enough to identify a possible attack and request feedback from the sensor's operator.

Analogous to outsider attacks, coverage redundancy can also be exploited to identify data manipulation. By identifying areas that overlap with other sensors and crosschecking aircraft appearance and properties, rogue sensors can be identified.

#### *2) Sybil Attacks*

Lastly, we consider Sybil attacks, the most sophisticated threat to a crowdsourced sensor network. In a Sybil attack, attackers attempt to integrate multiple sensors under their control (covering their targeted airspace) into the network. In order to hide a real-world ATC attack, these sensors feed false data to OpenSky, similar to the single sensor data manipulation, but this time in a coordinated fashion to outvote legitimate sensors covering the area.

To defend against such attacks, the system monitors new sensors for irregularities. For example, several new sensors in the same region in a short time will require review. However, as [36] proves, despite such defences, Sybil attacks are always possible as long as there is no trusted agency that certifies the identities of entities in a trust network. Other security-related networks such as Tor suffer from the same problem: new actors can behave well for any necessary time period to obtain the desired trust level before attacking.

Hence, the future aim of OpenSky is to individually certify and secure the connections to all sensors. While none of these defences are adequate to defend against the most powerful military or state actors, they are sufficient for our attacker model, from script kiddies to cyber criminals and cyber terrorists.

## 8. DISCUSSION

Finally, we discuss possible applications to other critical infrastructures, future extensions, and the costs of our system.

### *A. Application to other Critical Infrastructures*

The principles introduced in this paper can also be applied to similar wireless systems. The closest example is provided by the automatic identification system (AIS), an automatic tracking system used on ships and other marine traffic [37]. Similar to ADS-B, its use cases include the identification and localisation of vessels through exchanging messages with nearby ships, base stations, and satellites. Like ATC, AIS also foregoes cryptographic measures, providing a large attack surface [38]. While the maritime scenario adds further difficulties such as shortened signal propagation and aggravated deployment of ground stations, these could be overcome, at least near busy traffic hotspots such as shores and straits.

### *B. Possible Future Extensions*

Two natural extensions come to mind to improve the security of OpenSky in the future: the option of cryptographic certification of individual sensors (as discussed above) and the integration of non-stationary receivers.

By integrating non-stationary, i.e. mobile, receivers such as drones, we can make it harder for an attacker to obtain the exact position of all receivers, which in turn further improves the security of the discussed countermeasures. Related work has shown that a randomly moving mobile substantially increases the difficulty of making false messages appear genuine [39].

### *C. Cost*

The International Civil Aviation Organization (ICAO) specifies the technological cost of using SSR to monitor an en-route airspace (200 NM radius) at $6 million, while a certified ADS-B system is estimated to be significantly cheaper at $380,000 [40]. This estimate assumes more expensive, certified sensors with extremely high availability and technical capabilities (in addition to the cost for the backend system).

As capable commercial off-the-shelf ADS-B receivers priced at around $100 already provide the basis of a highly available and redundant crowdsourced network in most Western airspaces, our system comes in at a fraction of these costs even when taking into account OpenSky's central processing unit and limited maintenance cost. Our best-placed receivers offer a reception radius of up to 600km, thus surveillance of an en-route airspace can be provided even by a single receiver. In practice, 10-50 sensors are sufficient for coverage with high accuracy, redundancy and reliability.

## 9. CONCLUSION

In this paper, we have presented an approach that exploits the concept of crowdsourcing to build a sensor network which acts as a defensive layer for the wireless interfaces of critical infrastructures. Using ATC as a case study, we introduced the crowdsourced sensor network OpenSky and laid out the potential for employing several independent countermeasures against common wireless attacks. Our security analysis shows that we can reliably detect even more sophisticated attackers and present a constantly validated picture of the airspace.

Based on these results, it is our strong belief that crowdsourcing can facilitate a transparent layer of security for many legacy wireless technologies that cannot be upgraded with cryptographic primitives in the short or medium term. The use of physical security primitives and a massively-distributed infrastructure provide a good defence against all but the most sophisticated military and nation-state attackers. Combined with attractive cost characteristics and agile deployment, crowdsourced networks pose a serious solution for the wireless security vulnerabilities that threaten many critical infrastructures today.

## REFERENCES

[1] A. Costin and A. Francillon, 'Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices,' in *Black Hat USA*, 2012, pp. 1-10.

[2] M. Schäfer, V. Lenders, and I. Martinovic, 'Experimental analysis of attacks on next generation air traffic communication,' *Lect. Notes Comput. Sci*., 2013, vol. 7954 LNCS, pp. 253-271.

[3] M. Balduzzi, A. Pasta, and K. Wilhoit, 'A security evaluation of AIS automated identification system,' in *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014, pp. 436-455.

[4] S. Cooper, F. Khatib, A. Treuille, J. Barbero, J. Lee, M. Beenen, A. Leaver-Fay, D. Baker, Z. Popović, and others, ‘Predicting protein structures with a multiplayer online game,’ *Nature*, 2010, vol. 466, no. 7307, pp. 756-760.

[5] D. Clery, ‘Galaxy Zoo volunteers share pain and glory of research,’ *Science* (80-. ), 2011, vol. 333, no. 6039, pp. 173-175.

[6] Flightradar24.com, ‘Successfully Testing Satellite-based ADS-B Tracking,’ Jul. 2016.

[7] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm, ‘Bringing up OpenSky: A large-scale ADS-B sensor network for research,’ *IPSN 2014 - Proc. 13th Int. Symp. Inf. Process. Sens. Networks (Part CPS Week)*, 2014, pp. 83-94.

[8] M. Schäfer, M. Strohmeier, M. Smith, M. Fuchs, R. Pinheiro, V. Lenders, and I. Martinovic, ‘OpenSky’s Report 2016: Facts, Figures and Trends in Wireless ATC Communication Systems,’ in *35th Digital Avionics Systems Conference - Proceedings*, 2016.

[9] C. W. Johnson, ‘Cyber security and the future of safety-critical air traffic management: identifying the challenges under NextGen and SESAR,’ in *IET Conference Proceedings*, 2015.

[10] K. Zetter, ‘Feds Say That Banned Researcher Commandeered a Plane,’ *Wired*, May 2015.

[11] M. Strohmeier, M. Schäfer, M. Smith, V. Lenders, and I. Martinovic, ‘Assessing the impact of aviation security on cyber power,’ in *Cyber Conflict (CyCon), 2016 8th International Conference on*, 2016, pp. 223-241.

[12] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, ‘On Perception and Reality in Wireless Air Traffic Communications Security,’ *IEEE Transactions on Intelligent Transportation Systems*, October 2016.

[13] C. R. Spitzer, U. Ferrell, and T. Ferrell, *Digital Avionics Handbook*, 3rd ed. CRC Press, 2014.

[14] RTCA Inc., ‘Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B).’ Dec-2006.

[15] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, ‘Short Paper : Reactive Jamming in Wireless Networks – How Realistic is the Threat,’ *Proc. fourth ACM Conf. Wirel. Netw. Secur. (WiSec ’11)*, 2011, pp. 47-52.

[16] M. Schäfer, V. Lenders, and J. Schmitt, ‘Secure Track Verification,’ in *IEEE Symposium on Security and Privacy*, 2015, pp. 199-213.

[17] N. Xu, R. Cassell, and C. Evers, ‘Performance assessment of multilateration systems - a solution to NextGen surveillance,’ in *Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2010, pp. 2-9.

[18] M. Schäfer, P. Leu, V. Lenders, and J. Schmitt, ‘Secure Motion Verification using the Doppler Effect,’ in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2016, pp. 135-145.

[19] M. Strohmeier, V. Lenders, and I. Martinovic, ‘Intrusion Detection for Airborne Communication using PHY-Layer Information,’ in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, 2015, pp. 67-77.

[20] A. Malatras and L. Beslay, ‘A generic framework to support participatory surveillance through crowdsensing,’ in *2015 Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2015, pp. 1135-1146.

[21] T. Monahan and J. T. Mokos, ‘Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks,’ *Geoforum*, 2013, vol. 49, pp. 279-288.

[22] T. Ludwig, C. Reuter, T. Siebigteroth, and V. Pipek, ‘Crowdmonitor: mobile crowd sensing for assessing physical and digital activities of citizens during emergencies,’ in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 4083-4092.

[23] Flightradar24 AB, ‘Flightradar24,’ 2017. [Online]. Available: https://www.flightradar24.com. [Accessed: 06-Mar-2017].

[24] FlightAware, ‘FlightAware,’ 2017. [Online]. Available: https://www.flightaware.com/. [Accessed: 06-Mar-2017].

[25] S. Edwards, ‘Inside the World of People Who Track Flights for No Reason,’ *Vice*, Oct. 2015.

[26] Flightradar24 AB, ‘About Flightradar24,’ 2017.

[27] J. Scardina, ‘Overview of the FAA ADS-B link decision,’ Jun. 2002.

[28] K. D. Wesson, T. E. Humphreys, and B. L. Evans, ‘Can cryptography secure next generation air traffic surveillance?’ *IEEE Secur. Priv. Mag.*, 2014.

[29] M. Schäfer, M. Strohmeier, M. Smith, M. Fuchs, R. Pinheiro, V. Lenders, and I. Martinovic, ‘OpenSky’s Report 2016: Facts, Figures and Trends in Wireless ATC Communication Systems,’ in *35th Digital Avionics Systems Conference*, 2016.

[30] M. Robb, 'Dump1090,' *GitHub*, 2017. [Online]. Available: https://github.com/MalcolmRobb/dump1090. [Accessed: 12-Feb-2017].

[31] K. Pourvoyeur and R. Heidger, 'Secure ADS-B usage in ATC tracking,' in *2014 Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)*, 2014, pp. 35-40.

[32] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, 'Realities and challenges of NextGen air traffic management: the case of ADS-B,' *IEEE Commun. Mag.*, 2014, vol. 52, no. 5.

[33] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm, 'Bringing up OpenSky: A large-scale ADS-B sensor network for research,' *Proc. 13th Int. Symp. Inf. Process. Sens. Networks*, 2014, pp. 83-94.

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

[35] M. Schäfer, V. Lenders, and I. Martinovic, 'Experimental analysis of attacks on next generation air traffic communication,' in *International Conference on Applied Cryptography and Network Security (ACNS)*, 2013, pp. 253-71.

[36] J. R. Douceur, 'The sybil attack,' in *International Workshop on Peer-to-Peer Systems*, 2002, pp. 251-260.

[37] B. Tetreault, 'Automatic Identification System,' *Proc. Mar. Saf. Secur. Counc.*, vol. 63, no. 3, 2006.

[38] M. Balduzzi, A. Pasta, and K. Wilhoit, 'A security evaluation of AIS automated identification system,' in *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014, pp. 436-445.

[39] R. Baker and I. Martinovic, 'Secure Location Verification with a Mobile Receiver,' in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, 2016, pp. 35-46.

[40] International Civil Aviation Organization (ICAO), 'Guidance Material: Security issues associated with ADS-B,' Montreal, QC, Canada, 2014.