Feature Article:

DOI. No. 10.1109/MAES.2021.3054681

# On Jamming Attacks in Crowdsourced Air Traffic Surveillance

***Mauro Leonardi,*** **Tor Vergata University of Rome, 00133 Rome, Italy**
***Martin Strohmeier and Vincent Lenders,*** **armasuisse Science and Technology, 3603 Thun, Switzerland**

## INTRODUCTION

In recent years, the subject of wireless availability has gained significant attention within the communities securing critical infrastructures, such as air traffic control (ATC). As pointed out in several studies, the frequencies used by those technologies responsible for broadcasting aircraft's positions to other aircraft and the ground suffer from high saturation due to crowded airspaces with long-range transmissions of up to 500 km [1], [2]. Being that legacy technologies are geared toward simplicity, these protocols offer no medium access control, resulting in significant message loss rates ranging from 50% to 90%.

In such a wireless environment, malicious jamming attacks can be highly effective using little means. Several academic works (e.g., [3], [4]) in recent years have shown jamming in this context to be feasible with cheap software-defined radios (SDR) and blueprints for such interference attacks have happened in the wild, leading to significant radar losses [5]. In conjunction with the high profile of aviation security, this inherent vulnerability makes ATC communication an attractive target for many types of adversaries and necessitates finding effective countermeasures.

Crowdsourced projects are a form of 'citizen science' whereby members of the public can join larger scientific efforts by contributing to smaller tasks; since SDRs have become readily available and affordable over the past decade, many users can now take part in wireless projects, such as crowdsourced sensor networks (CSN) with little cost. Such participatory CSNs constitute a step change; large networks exist for monitoring wireless communication of aircraft, ships, satellite, or cars. In this article, we use the OpenSky Network, a large-scale CSN, to conduct experiments and design a system that can mitigate jamming attacks on ATC ground receivers, specifically those using the Automatic Dependent Surveillance–Broadcast (ADS–B) technology.

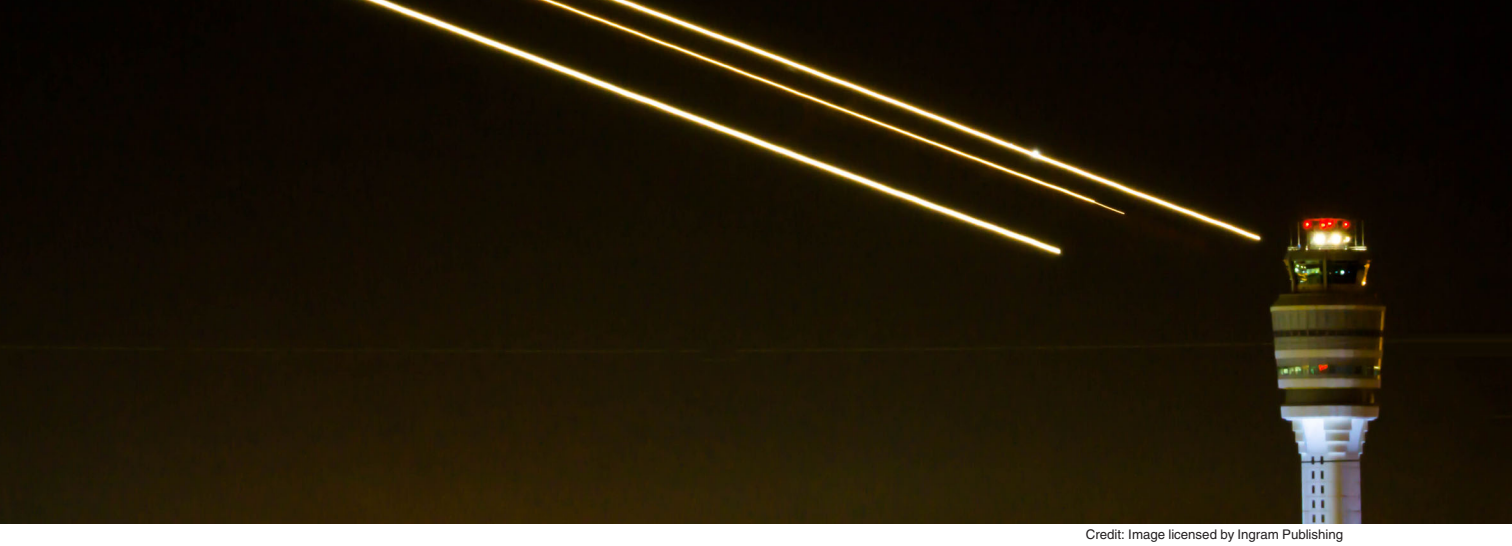
Some preliminary aspects of the paradigm proposed in this article were previously presented at the OpenSky Workshop 2019 [6], where we discussed ideas around the generalized problem of garbling mitigation in CSNs.

Concretely, we make the following contributions.

- We develop realistic jamming threat models for ADS–B communication and analyze the impact of jamming on OpenSky Network and on its most used receiver (also with laboratory tests).
- We propose several mitigation techniques to maximize reception with a crowdsourced network during a jamming incident.
- We design, implement, and test two of these techniques using software-defined radios and low-cost hardware, making them accessible for resource-constraint organizations.

The remainder of this article is organized as follows. The section "Background" provides the necessary background, whereas "Threat Model" discusses our threat model and provides an assessment of the impact of jamming attacks on ADS–B systems. The section "Jamming Mitigation in Crowdsourced Sensor Networks" outlines our proposed solution to the problem and the experimental evaluation is described in "Experimental Evaluation." We end this articles with the sections "Discussion" and "Conclusion."

Authors' current addresses: Mauro Leonardi, Department of Electronic Engineering, Tor Vergata University of Rome, 00133 Rome, Italy (e-mail: mauro.leonardi@uniroma2.it). Martin Strohmeier and Vincent Lenders, armasuisse Science and Technology, 3603 Thun, Switzerland (e-mail: Martin.Strohmeier@armasuisse.ch, Vincent.Lenders@armasuisse.ch).
Manuscript received August 12, 2020, revised January 11, 2021; accepted January 12, 2021, and ready for publication January 23, 2021.
Review handled by Mauro De Sanctis.
0885-8985/21/$26.00 © 2021 IEEE



Credit: Image licensed by Ingram Publishing

## BACKGROUND

Rooted in World War II military developments, the Secondary Surveillance Radar (SSR) technology was created to improve on aircraft information collected through traditional Primary Radar (PSR). Whereas PSR delivers only a rough distance and direction, the aircraft transponder Modes A, C, and S provide altitude, identity, and additional information. Recently, these transponder modes have been complemented by the ADS–B protocol, which provides exact navigation satellite-supported positional information and uses the same underlying Mode S legacy technology (for a detailed discussion, see [7]).

Figure 1 provides the structure of a Mode S Extended Squitter message, which forms the basis of the current aircraft-to-aircraft and aircraft-to-ground communication. The protocol uses a random access to the channel and each aircraft uses pulse position modulation for its packets; a message begins with a preamble of four synchronization pulses. The data block is then transmitted in slots of 1 $\mu$s, a bit is indicated by either sending a 0.5-$\mu$s pulse in the first half of the slot (1-b) or in the second half (0-b); the last 24 b of the data block are used for a cyclic redundancy check.

## SECURITY ISSUES

Due to its legacy history, SSR/ADS–B do not include standard security primitives, such as authentication and integrity during this development or deployment [8]. The consequence is that basic wireless attacks are trivially possible, including eavesdropping, jamming, message injection, and message modification. These issues and their potential impact have been covered extensively in the academic literature and several solutions were proposed for spoofing or message injection/modification attacks on ADS–B. A full review of both attacks and countermeasures is provided in [9].

Beyond these issues, which stem from the lack of cryptographic integrity checks, the denial of service (DoS) due to jamming and interference is another real concern in ADS–B systems. Interference in its unintentional form has been a regular occurrence around the world caused by a wide range of transmitters. Besides the collision with other legitimate aircraft messages on the same 1090-MHz frequency (called garbling), additional severe SSR/ADS–B interference has been reported from test stations on the ground. One notable such incident caused all aircraft to vanish from controller's screens and a subsequent part-suspension of airspace services over a large area of Central Europe [5]. Here, the literature has so far focused on measures on the physical layer, improving signal reception under interference using array antennae [10] and adaptive signal processing [11], [12]. Jamming is the intentional transmission of radio frequency signals to interfere with the operation of an electronic device by saturating its receiver with noise or false information and, usually, is much more difficult to counter or mitigate. A good introduction is provided in [13] and several works have also addressed the topic of jamming in the context of ADS–B and SSR. For example, Leonardi *et al.* [3] provide

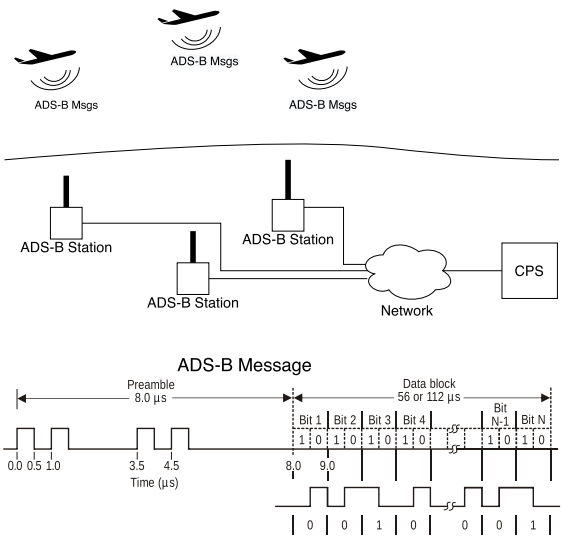



**Figure 1.**
ADS–B system description and Mode S Extended Squitter message structure.

a risk assessment, concluding that jamming is a practical threat even with low-cost receivers. This inspired several works on potential countermeasures, including the use of blind source separation (BSS) [11], digital beamforming (DBF) [12], and multichannel receivers [10], [14].

Our aim is to reduce and mitigate the jamming effect significantly. In this article, we combine and contrast these cited techniques with a novel approach of using widely deployed crowdsourced sensor networks in order to mitigate deliberate wireless jamming attacks against air traffic surveillance systems.

## OPENSKY: A CROWDSOURCED SENSOR NETWORK

The OpenSky Network is a CSN of more than 3000 sensors, which collects ADS–B messages at a large scale and provides these data to researchers for free through several application programming interfaces (live and historical) [15]. The network records the payloads and physical-layer data of all 1090-MHz aircraft messages within its coverage, amounting to more than 23 trillion messages as of August 2020. Due to its free and open nature, it is the ideal evaluation scenario for our jamming work.

## THREAT MODEL

We will focus on the mitigation of noise jamming (i.e., transmission of a high-powered unformatted noise signal in the frequency band under attack). An active noise jammer implies an increase of the noise floor in the receiver and, consequently, a reduction of the signal-to-noise ratio (SNR), or rather, in case of jamming, of the signal-to-jamming ratio (SJR). It follows that the probability to successfully detect and decode any ADS–B message is reduced.

We distinguish between two fundamental attack models, ground-based, and air-based, which is as follows.

- *Ground-based attack*. The jammer is assumed to be placed either in close proximity to the receiver station or on an exposed position such as hill. In the first case, even a low-cost/low-power jammer has the ability to deny the service of the station thanks to the saturation of one or more components at the receiver. On the other hand, it will be very difficult to affect more than one station at a time. In the second case, the low-cost jammer can affect several stations simultaneously but with a lower power, likely causing degradation in SNR only.
- *Air-based attack*. The jammer can be carried by any kind of airborne vehicle, i.e., drones, balloons, airplanes, or helicopters. In the first two cases (drones or balloons), the restricted carrier capacity of the platform limited the available power and, thus, the level of interference. In the other cases (airplanes and helicopters), this restriction vanishes and high-power signals can be emitted from the platform even over a long time period. For all airborne cases, only a reduction of the targets' SNRs is expected, due to the larger distances between the jammer and the stations.

## EVALUATION OF THE THREAT IMPACT

Depending on the scenario, the effect on the receiver can vary significantly. Commercial ADS–B receivers follow the standard defined in [16] and [17]. In practice, this leads to two possible implementations of the receiver: the first implementation is a noncoherent receiver that typically uses a logarithmic receiver that directly converts the RF signal into a voltage level, to be digitized and processed according to the signal specifications and receiver logic; the second implementation uses an intermediate frequency (IF) coherent receiver with a digitizer at the IF. The samples of the received signals are then processed using Hilbert filtering (or equivalent) to extract the I and Q components to be processed further following the standards.

In any case, most of the receiver blocks can be affected negatively by jamming signals in following three fundamental ways.

- Very high power jammers may cause saturation of an amplification stage (or of the limiter). In this case, an analog DoS is experienced because the receiver is not able to make any measurements or detections.
- More generally, jammer signals in the Mode S band affect the SNR/SJR producing false detections (in case of fixed detection threshold), or missed detections (in case of adaptive thresholds).
- Finally, ADS–B receivers usually implement a validation logic (in the digital processing block) (e.g., preamble identification). This logic can be prone to attacks from "smart" jammers, which mimic real Mode S/ADS–B messages.

The first effect, i.e., the analog chain saturation can be mitigated either by improving the receiver's maximum power before it is saturated $P_{\text{sat}}$ (for example, by introducing high dynamic low noise amplifier or logarithmic amplifier) or by introducing an automatic gain control with a passive attenuator before the first amplifier. However, both techniques do not mitigate the other jamming effects, which occur before the saturation level is reached.

To analytically evaluate the impact of the jammer on a receiver (before its saturation), we assume to have a noise

**Table 1.**

| Maximum Coverage of a Jammed Receiver | | | | |
|---|---|---|---|---|
| | Omni-Antenna | | 4 Sectors Antenna | |
| Jammer range | EIRP=100 mW | EIRP=20 W | EIRP=100 mW | EIRP=20 W |
| (km) | (Max. range / reduction) | (Max. range / reduction) | (Reduction) | (Reduction) |
| 0.5 | 17.68 km / 98.80% | 1.25 km / 99.99% | 24.95% | 24.99% |
| 1 | 35.36 km / 99.22% | 2.5 km / 99.99% | 24.80% | 24.99% |
| 10 | 353 km / 21.87% | 25 km / 99.61% | 5.4688% | 24.90% |

*We assume 500-W aircraft transponders, a jammer with 100-mW/20-W peak power, and three jammer/receiver distances. The coverage reduction is obtained considering a nominal range of 400 km. Single receiver with omidirectional antenna and four receivers with four sectors antenna.*

jammer with a given transmitter power $P_J$ and a given antenna gain $G_J$. Using the Friis equation [18], it is possible to compute the corresponding ADS–B station's received power $P_J^r$

$$P_J^r = G_J G_r(\theta_J, \phi_J)\left(\frac{\lambda}{4\pi R_J}\right)^2 P_J \tag{1}$$

where $R_J$ is the jammer-station range and $G_r(\theta_J, \phi_J)$ is the ADS–B station antenna gain in the direction of the jammer. If $P_J^r$ is greater than the saturation threshold of the receiver $P_{\text{sat}}$, the reception of legitimate messages is fully inhibited. If the received jammer power is smaller than the saturation level, the receiver performance is reduced. The concrete value of $P_{\text{sat}}$ is variable, depending on a receiver's hardware.

The received power $P_T^r$ for a legitimate message from an aircraft transponder is computed similarly

$$P_T^r = G_T G_r(\theta_T, \phi_T)\left(\frac{\lambda}{4\pi R_T}\right)^2 P_J \tag{2}$$

where $R_T$ is the transponder–station range and $G_r(\theta_T, \phi_T)$ is the ADS–B station antenna gain in the direction of the transponder. It follows that the SJR is equal to

$$\text{SJR} = \frac{P_T^r}{P_J^r} = \frac{G_T G_r(\theta_T, \phi_T) P_T R_J^2}{G_J G_r(\theta_J, \phi_J) P_J R_T^2}. \tag{3}$$

Finally, by imposing a minimum level for this ratio, for example 6 dB, it is possible to compute the maximum coverage $R_T$ of the receiver under attack (assuming the same receiver gain of the receiver in the directions of the jammer and transponder)

$$R_T = \frac{1}{2}\sqrt{\frac{G_T P_T}{G_J P_J}} R_J = \frac{1}{2}\sqrt{\frac{EIRP_T}{EIRP_J}} R_J. \tag{4}$$

The effective isotropic radiated power of an aircraft transponder $\text{EIRP}_T$ is specified by the International Civil Aviation Organization (ICAO) [17]: the peak (pulsed) EIRP should be 125 W (+21 dBW) to 500 W (+27 dBW) and a lower EIRP limit of 70 W (+18.5 dBW) is further given for aircraft flying below FL150 (15 000 ft).

In Table 1, a theoretical evaluation of the maximum coverage in case of a 500-W transponder jammed by a jammer with 100 mW of peak power (i.e., for example, the peak power of the common Ettus/NI USRP SDR in *L*-band) and in case of 20 W (achieved by adding a power amplifier to the Ettus/NI SDR) is provided. Various jammer/station ranges were considered.

As expected, if the jammer is close to the ADS–B receiver(s), a high coverage reduction is achieved, even if the saturation is not reached. Moreover, ground-based attacks are very effective also with low cost hardware and easy implementation.

In Table 2, a qualitative comparison between the various effects on the receiver for five different scenarios using both threat models is conducted. The effects on the receiver, effects on the system, implementation difficulties, and attack effectiveness are discussed.

In the table, it is clear that the most effective attacks are the ones that are able to be close to the ADS–B station (ground attack), or the one that uses aircraft that are able to carry high-power transmitter. The most dangerous is the ground close attack, also because it can be implemented with very cheap equipment.

To better understand the effect of jammer on a real ADS–B receiver, laboratory tests were conducted on the most common sensor in the OpenSky Network (but also in

**Table 2.**

| Qualitative Comparison of Effects on ADS–B Receivers in Five Different Jamming Scenarios | | | | | |
|---|---|---|---|---|---|
| | **Ground attack** | | **Flight attack** | | |
| | **Close to RX** | **High altitude** | **UAV** | **Balloon** | **Aircraft** |
| Area of Attack | Small (one sensor) | Medium (more sensors) | Large (more sensors) | Large (more sensors) | Large (more sensors) |
| Available maximum power | High | High | Low | Low | High |
| Effect on receiver | Saturation | SNR deg. | SNR deg. | SNR deg. | SNR deg. |
| Effect on station | Full DoS | Coverage cut (high) | Coverage cut (small) | Coverage cut (small) | Coverage cut (high) |
| Implementation difficulty | Low | Low | Medium | Medium | High |
| Cost | Very low | Very low | Low | Low | High |
| Attack probability | Very high | High | Medium | Medium | Low |
| Attack effectiveness | Very high | High | Low | Low | High |

other crowdsourced networks). The RTL-SDR (http://www.rtl-sdr.com) is a commercial off-the-shelf DVB-T dongle modified using software in order to be capable of receiving ADS–B messages on the *L*-band (1090 MHz). It performs a coherent reception and an 8-b analog-to-digital conversion with a sampling rate of 2 Msps. This receiver was connected to an RF-signal generator, which was developed using a Software Defined Radio capable of generating both streams of ADS–B messages and all types of interfering signals. The SDR is a National Instrument device (NI2920; see http://www.ni.com/it-it/support/model.usrp-2920.html) and the baseband signals to be transmitted were generated at 10 Msps and stored in the controller of the device. The SDR up-converts these signals to 1090 MHz and transmits with a transmitter gain (i.e., the output power) that can be software controlled.

Streams of ADS–B packets superimposed with different kinds of jammers were injected into the real receiver using an RF cable and an attenuator. The output of the receiver was recorded on a file in a commercial PC and analyzed by comparing the transmitted stream of messages with the received ones.

Three types of jammers were evaluated (borrowing the most used approach in GNSS and radar jamming): (a) a sequence of Mode S pulses on a carrier wave of 1090 MHz; (b) a continuous sinusoidal waveform at 1090 MHz; (c) a chirp signal with a band of 2 MHz and a repetition time of 100 $\mu$s.

We evaluated the receiver performance under these three jammer types by varying the jammer signal power and the ADS–B message rate. As the target metric, we calculate the probability of a correct message reception (defined as the number of received messages with zero errors over the number of the transmitted messages) in different controlled conditions. The results of these experiments are shown in Figure 2.

As can be seen, different types of interfering signals produce different effects but, in all cases, a large reduction of the receiver performances was obtained (even under high SJR values), confirming the analytically derived results. The worst decoding results are obtained for the chirp jammer: An SJR of around 14 dB was needed to decode the 50% of the transmitted replies. The RTL-SDRs performance fares better against the continuous sinusoidal waveform and the

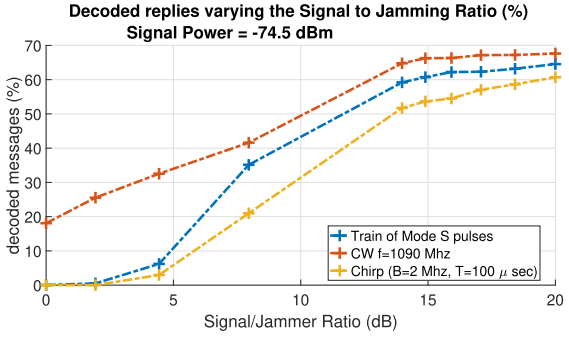



**Figure 2.**
RTL-SDR + dump1090 performance under jamming conditions. Shown is the probability of correct reception based on different SJRs.

pulsed jammer, with an SJR of 12 and 10 dB required to decode half of the messages, respectively.

Finally, it is clear that the RTL-SDR receiver performance has an upper bound of about 70% of error-free decoded messages, even under very high signal-to-jammer ratios. In turn, this means 30% of the messages are never decoded. This limit does not depend on the jamming condition but appears also under normal conditions and is related to the receiver hardware limits (i.e., the relatively low sampling rate of the RTL-SDR).

## JAMMING MITIGATION IN CROWDSOURCED SENSOR NETWORKS

In this section, we analyze and contrast different approaches for jamming mitigation that can be implemented in a crowdsourced ADS–B network, which are as follows.

- *Network-oriented.* By increasing the number of sensors and/or modifying the sensor distribution in a given crowdsourced network, the available redundancy is hypothesized to mitigate some of the jamming effects.
- *Sensor-oriented.* By improving the reception of a single sensor: This can be done either through multichannel signal processing (using omnidirectional antennas and DBF [19] or BSS [20], [21]) or by creating a multichannel receiver using sector antennas.

The first approach requires the installation of more stations using a wide-area network (that is exploiting the crowdsourced network paradigm); the second one requires a more complex receiving station with signal processing capabilities or directive antennas. Mixed solutions are possible, potentially combining the advantages of both approaches.

### NETWORK-BASED MITIGATION

In the network-oriented case, the effect of a jammer mainly depends on the type of attack. If the attack is ground based, the probability to jam more than one station at a time is low. At the same time, the jammer can reduce the coverage of a single station significantly (as shown in Table 1 and Figure 2). However, if every aircraft in the coverage of the jammed station is also in view of, at least, one other unimpaired station, it is intuitive that the effect of the jammer will be cancelled out in full.

If we assume an air-based attack (or more generally attacks from exposed positions), the same jammer can interfere with more stations at the same time, reducing their coverage simultaneously. In this condition, the effectiveness of the attack is dependent on four main factors: the directivity of the jammer, the jammer transmitter power, the geometry of the ADS–B stations, and the distance between stations. Given the multivariate nature of the problem, it is difficult to analytically evaluate the effect of the jammer and it will be done in the following section by the use of simulation and real data for the specific case of OpenSky Network. However, in all cases, we can expect that the likelihood of an effective coverage reduction for several attacked stations is low (due the distance of the jammer).

Finally, it must be noted that it is more difficult to have several stations in view of an airplane if it is on the edge of the crowdsourced network's coverage area. This is, for example, the case near the coasts or in very remote areas, such as deserts, polar regions, and oceans.

### SENSOR-BASED MITIGATION

In the sensor-oriented mitigation approaches, it is simpler to derive a model to forecast the general mitigation performances. First, we consider the sectorization-based countermeasure, followed by the signal processing case. Principally, by splitting a single receiver's coverage into multiple sectors, the jammer is able to interfere only with a single sector/channel at a time (regardless of whether the attack is ground-based or air-based). In this case, only the coverage of the sector under attack will be reduced. The amount of reduction can, hence, be computed with the same approach used for the omnidirectional antenna. The results for different jammer EIRP and distances are reported in Table 1 for the four sectors case.

Moreover, directional antennas increase the SNR of the aircraft messages due to the additional antenna gain. Consequently, the reception probability is increased, also under normal nonjamming conditions. On the other hand, this approach requires directional antennas to generate the different coverage sectors and independent receivers for each sector, increasing the station and set-up cost for their owners. This could be a considerable drawback for crowdsourced networks as it slows global adoption, in particular in less developed regions.

It is possible to exploit the benefits of sectorization without directive antennas through the use of signal processing, i.e., DBF or BSS techniques. Both can provide analog results to the sectorization approach using simpler array of dipole antenna and signal processing. It is intuitive considering that the signal processing can be seen as a way to generate $m$ different antenna beams (for DBF) or $m$ different orthogonal signal spaces (for BSS).

Hence, for both cases, we can assume that jammer power will be projected in $m$ different subspaces, and will interfere with the replies only if its projection will be more powerful than the aircraft signals. Moreover, using

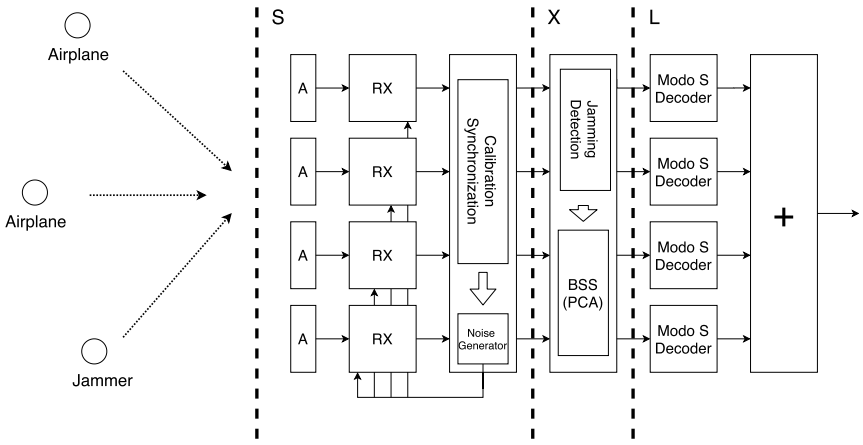



**Figure 3.**
General scheme of a multichannel receiver. Each receiving channel is connected to an antenna element (A). After the analog receiver chain and analog-to-digital converter (RX), a Mode S decoder is present on each channel. In case of sectorization, each antenna element is a directive antenna pointed in a given direction, in case of signal processing, each antenna element is an omnidirectional antenna and the jamming detection and mitigation is applied before the message decoding. The calibration/synchronization is needed only for coherent processing of the channels.

BSS signal processing, it can be possible to find $m$ orthogonal spaces in which a single space fully contains the jammer signal. In this condition, the aircraft signals in the other $m-1$ orthogonal spaces are received without any interference from jamming.

The DBF or BSS approaches have some further advantages compared to physical sectorization. First, the antennas' cost and installation impact is lower. Second, the solution is more agile because it can be adapted to the traffic conditions, for example, it is possible to define multiple beams with optimal directions based on the relative angle of the aircraft in range. Similarly, it would be possible to estimate the angle of arrival of the jammer by exploiting the incoming interference signals.

Many BSS techniques are present in the literature, and some were developed for the ADS–B garbling mitigation also in [11], [14], and [22], For this article, we focus on BSS along with principal component analysis (PCA) [23] as signal-based jamming mitigation technique. This choice allows simple HW and SW implementation in low-cost devices, such as, for example, single-board computer as Raspberry Pi or similar. In that case, in the authors' opinion, it is better choosing a well-known and standard processing technique, such as PCA, that gives the opportunity to use efficient standard library.

As shown in Figure 3, we assume an antenna with $m$ elements connected to an $m$ multichannel receiver and a set of $d$ different sources (aircraft signals and/or jamming signals). The "mixed" signals ($\mathbf{X}$) received by the multichannel receiver can be seen as a linear combination of the individual source signals ($\mathbf{S}$). This combination depends on antenna steering vector and on the signal angles of arrivals. If the number of the sources $d$ is less or equal to the number of the antenna elements $m$, the source signals can be unmixed using algebraic linear manipulation.

Let us consider the received baseband signals after collecting $T$ time samples from the $m$ antenna elements. They can be represented as follows:

$$\mathbf{X} = \mathbf{M} \cdot \mathbf{S} + \mathbf{N} \tag{5}$$

where $\mathbf{X} = [x(1), , x(T)]$ is the $m \times T$ received signal matrix, $\mathbf{S} = [s(1), , s(T)]$ is the $d \times T$ source matrix, $\mathbf{N}$ is the $m \times T$ additive noise matrix and $\mathbf{M}$ is the $m \times d$ mixing matrix that contains the antenna array signatures and the complex gains of the sources. For example, given a $\lambda/2$ uniform linear array of four elements, $\mathbf{M}$ is composed of $d$ column vectors, which can be represented as

$$\mathbf{m}_i = \left[1, e^{j\pi \sin(\theta_i)}, e^{j2\pi \sin(\theta_i)}, e^{j3\pi \sin(\theta_i)}\right]^T \tag{6}$$

where $\theta_i$ is the angle of arrival of the $i$th signals and $i = 1, \ldots, d$.

BSS separates the set of mixed signals $\mathbf{X}$ through the determination of an unmixing matrix $\mathbf{U}$ to recover an approximation of the original signals $\mathbf{S}$. Applying PCA, we can further obtain the two matrices $\mathbf{C}$ and $\mathbf{L}$

$$[\mathbf{C}, \mathbf{L}] = \mathrm{PCA}(\mathbf{X}) \tag{7}$$

where $\mathbf{C}$ is the matrix containing the principal component coefficients, also known as loadings. The $\mathbf{L}$ rows are the representation of the transmitted signals in the principal component space and are ordered by greatest to smallest variance.

Thus, if two or more sources are superimposed and come from different directions, they are considered by the PCA as different and independent sources and projected into different principal components. After successful application, traditional algorithms can then be used to decode the rows of $\mathbf{L}$.

Typically, effective jammer signals are high powered at the receiving station compared to the legitimate aircraft signals. To further improve the jamming effectiveness, they are also transmitted in continuous fashion. Consequently, the jammer signal should be well separated from the other signals as intended and normally be contained in the first principal component.

Before the PCA antijamming processing some preprocessing is also required. After an initial system synchronization and calibration, the signal streams are synchronized with each other. Afterward, we normalize the signal streams to mitigate the effects of different antenna and receiver characteristics. Finally, the data coming from the receiving chains are buffered and consecutive chunks of data of a fixed size are processed sequentially.

After obtaining these data chunks, the independent channels are scanned for ADS–B messages. The message detection is performed on a sliding window larger than a single message of 112 b. The first few elements of the sliding window are used to estimate the floor noise in the signals and to fix a detection threshold.

For the remaining part, we follow the relevant ADS–B/Mode S standards [16], [17] independently for each channel: The Mode S preamble detection verifies if the right sequence of ones and zeros is received. If a preamble is detected, the following samples are considered part of a message and subsequently decoded. Finally, the cyclic redundancy check is applied.

To detect the presence of a jammer, we use a "look through" technique; if a jamming condition is detected on the first samples of every data chunks, the proposed jamming mitigation processing is then performed on the full chunk. The detection mechanism itself uses a mean signal power estimator. If the received mean power is higher than a threshold, the jamming condition is declared and the PCA applied to all the samples of the chunk before the scanning for messages.

This method was selected to have a small impact on the computational load of receiver: If the mean level of the noise floor does not indicate a jamming attack, no additional computation is required and the independent channels are used to receive the ADS–B signals. Moreover, having N channels gives also a statistical improvement in decoding low-power messages: It is enough that the reply is decoded by at least one channel. In case of jamming, the PCA is applied to the data chunks, exploiting the high power, long duration of the jamming signal to force it in one of the principal components (usually the first one).

## EXPERIMENTAL EVALUATION

In this section, the impact of a jammer on an ADS–B receiver and the proposed mitigations are evaluated using real data obtained through the OpenSky crowdsourced sensor network.

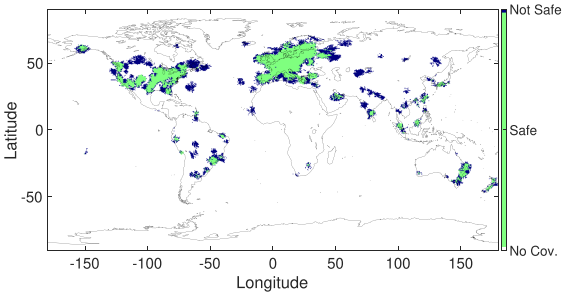



**Figure 4.**
OpenSky Network coverage as of August 24, 2019. Blue regions (49.36%) are covered by a single receiver only and, thus, most susceptible to a DoS attack.

## NETWORK-BASED MITIGATION

To evaluate the impact of a jammer on a crowdsourced receiver network as well as the network-based mitigation model, we used data available through the OpenSky API (https://opensky-network.org/data/apply).

First, we determined the coverage of each receiving station in the OpenSky Network by analyzing 24 h of traffic data. This, in turn, allowed us to calculate the real number of receiving stations in direct line of sight from each point in the network (by superimposing the coverage patterns of all stations).

To evaluate the impact of the different jamming scenarios, a jammer with a given power and a given position was simulated. The reduced coverage of all receivers in range was calculated using (4) and, finally, the new overall coverage of the network was recomputed.

Using this approach, we have first analyzed the concrete network regions most susceptible to a DoS attack by the use of a ground jammer. By calculating which part of the network is covered by a single-receiver station only, it is possible to detect those areas that can be shut down by using a targeted ground jammer. In Figure 4, the full coverage of the OpenSky Network is shown, with the regions susceptible to a ground attack reported in blue.

Overall, we found that almost half (49.36%) of the network only had such 1-coverage. In these regions, a low-cost ground-based transmitter close to an OpenSky receiving station can effectively cause a coverage reduction of up to hundreds of squared kilometers. In total, 14.93% of the network area is covered by two sensors, 9.01% by three, and the remaining 26.7% has at least 4-coverage, making network-based mitigation reasonable.

In case of the more complex aerial attacks (or, in general, any attack that affects more than one station), the jammer impact depends on the relative position within the network. Concretely, it depends primarily on the number of receivers in the line of sight of the jammer and on their geometrical distribution. Large coverage reductions are, under normal circumstances, only experienced by receivers very close to the jammer.

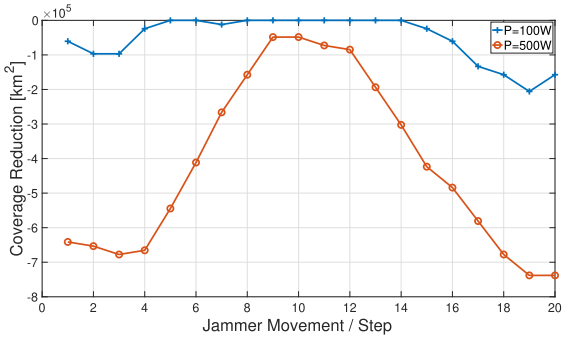



**Figure 5.**
Reduction of the OpenSky Network coverage during aerial jamming between Palermo and Oslo.

An illustration of the effect of an exemplary airborne jammer (with two power settings) that is simulated flying across Europe (from Palermo to Oslo) at 10 000 m altitude is shown in Figure 5. At the beginning and end of the scenario flights (steps 1–4 and 18–20), there are limited ground receivers in the network, leading to coverage losses of up to 700 000 $\mathrm{km}^2$. As there are sufficient in Central Europe during the middle of the flight, the loss is reduced to minimum (steps 9–12).

It is important to note that in the first part of the scenario (over Italy), the area is surrounded by water; hence, the diversity of the receiver geometry on the ground is inherently limited.

From these results, we can see that it is necessary to run a very high-powered transmitter akin to those on a large commercial aircraft to produce any significant impact of an airborne attack on a real-world crowdsourced network as large scale as OpenSky. In reverse, this means that a big reduction of the jammer effect can be obtained purely with the network-based mitigation approach if the network has a sufficient level of coverage redundancy. Moreover, no dedicated actions are needed by either the network or the station owners to obtain this mitigation effect. By simply allowing the naturally occurring organic growth of the community, the network's ability to counter a jamming attack will be improved. Finally, the only drawback of this approach, as mentioned before, is that it cannot be implemented in remote areas with specific geographical constrains. For these specific cases, the signal processing mitigation can be used also in crowdsourced network if suitable for low-cost implementation.

## SENSOR-BASED MITIGATION

The selected underlying hardware for signal processing mitigation trials is the Kerberos-SDR receiver available for less than $200 (https://www.indiegogo.com/projects/kerberossdr-4x-coherent-rtlsdr/). It is based on the RTL-SDR but combines four RTL-SDR channels and the possibility

**Figure 6.**
Picture of the multichannel receiver with four antennas. Kerberos SDR and Raspberry Pi are installed inside the box.

to synchronize and calibrate them using an internal noise generator. We connected this receiver to four omnidirectional antennas, the converted digital signals were then streamed to and recorded by a Raspberry Pi. Figure 6 shows a photograph of our setup, suitable for crowdsourced uses. For our evaluation, the jamming signals are added to the real aircraft signals in the digital section of the receiver. This avoids the (illegal) transmission of a jamming signal in the air. We tested jammers with different power levels.

The obtained performance for all power levels is shown in Figure 7. We calculate and report the number of replies decoded with and without the antijammer processing. For comparison, the baseline performance for our four-channel receiver in a jamming-free environment is also provided.

Our results illustrate the significant performance reduction under jamming, which increases in line with the jamming-to-noise ratio (JNR) and reaches almost 0 at 30 dB. When the PCA-based BSS antijamming processing is applied, the performance remains relatively stable even for increased jamming power values. On

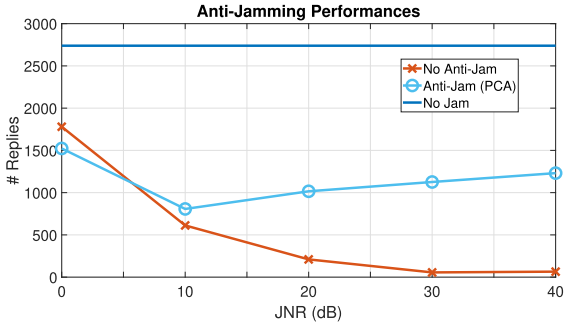



**Figure 7.**
Performance of the PCA-based BSS antijamming approach.

average, we can retrieve roughly 50% of the messages transmitted. At very low-power jamming values, the processing causes a small performance drop compared to doing nothing. However, with an increase in power, this reverses at 10 dB. At higher JNR, the jamming mitigation performance actually improves even in absolute terms, explained due to the easier principal component separation.

## DISCUSSION

Both discussed antijamming paradigms have different strengths and weaknesses. The network-based approach is straight-forward to implement for the network operator, without requiring additional effort from existing and future contributors. Moreover, it allows a strong and effective mitigation against close-up ground-based jamming attacks. Even against powerful airborne jammers with extremely high radiation power, this type of mitigation provides strong results, depending on the geometric distribution of the network.

However, we want to note some of the drawbacks inherent to the network-based mitigation approach. Most notably, the redundant coverage required will increase the network traffic and the server load. While redundant stations are useful in many aviation scenarios (e.g., to conduct multilateration [15]), it will also increase the load in conditions where there are no overall performance or functional improvements. Finally, it cannot be implemented as easily in remote areas due to geographical constraints. In such conditions, and also in situations of very high-powered attacks, the preferred solution should be the improvement of the sensor capabilities, using the multichannel receiver and signal processing.

This approach shows good results in terms of jamming reduction; however, it also enables other possible improvements in the sensor capabilities under normal conditions, including the following.

- Ad-hoc beamforming or BSS improves the reception of low-power messages and, thus, the coverage of the station.
- Null steering can deal with known (nonmalicious) interfering sources.
- The same processing techniques can also be used to separate superimposed legitimate ADS–B messages (garbling), hence improving the channel capacity under normal conditions.
- Multichannel receivers can estimate the angle of arrival [24] of incoming messages, allowing the localization of the airplanes by the central processing server of the network. This may also be fruitful for security issues beyond jamming, such as spoofing and message injections in general [9].

Finally, a combination of both approaches would further increase the antijamming effectiveness. This can happen organically, with a subset of enthusiastic users investing in improved receiver installations. Alternatively, interested parties or providers may be inclined to install a number of multichannel receivers at specific places of high-risk exposure or safety relevance.

Concluding this discussion, we would like to give a nod to the cost and note that all proposed solutions are fundamentally inexpensive. While improving the redundancy means installing more receivers, the most common installations cost less than 100 Euros. In case of the multichannel receiver, the four-channel setup used for this article (Kerberos SDR) costs less than 200 Euros.

## CONCLUSION

In this article, we have analyzed different solutions for jamming mitigation in and with crowdsourced air traffic communication networks. The network-based solution relies on the inherent redundancy of those networks, with their cheap off-the-shelf receivers distributed widely. In contrast, multichannel receivers require additional antennas and processing modifications but can effectively recover up to 50% of the messages compared with nonjammming conditions.

As we have shown, all solutions have different strengths and weaknesses, in particular when taking into account cost and deployment difficulty. Existing crowdsourced networks are already well-equipped to deal with even strong jamming attacks in those areas where they have a lot of redundancy, typically highly developed and densely populated areas. In areas with geographical constraints deploying adaptive receivers could significantly increase robustness against malicious and nonmalicious interference.

## REFERENCES

[1] 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.*, vol. 52, no. 5, pp. 111–118, May 2014.

[2] S. Sciancalepore, S. Alhazbi, and R. Di Pietro, "Reliability of ADS-B communications: Novel insights based on an experimental assessment," in *Proc. 34th ACM/SIGAPP Symp. Appl. Comput.*, 2019, pp. 2414–2421.

[3] M. Leonardi, E. Piracci, and G. Galati, "ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions," in *Proc. Tyrrhenian Int. Workshop Digit. Commun.-Enhanced Surveillance Aircr. Veh.*, 2014, pp. 41–46.

[4] M. Leonardi, E. Piracci, and G. Galati, "ADS-B jamming mitigation: A solution based on a multichannel receiver," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 11, pp. 44–51, Nov. 2017.

[5] "Results from EASA technical investigation on the radar detection losses in June 2014 in central Europe," Eur. Aviation Saf. Agency, Cologne, Germany, Tech. Rep. ED0.1-2014-ed04.00, Jan. 2014.

[6] M. Leonardi, M. Strohmeier, and V. Lenders, "Jamming/garbling assessment and possible mitigations in the OpenSky network," in *Proc. 7th OpenSky Workshop*, vol. 67, pp. 85–96, 2019.

[7] M. Stevens, *Secondary Surveillance Radar*. Norwood, MA, USA: Artech House, 1988.

[8] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *Proc. Int. Conf. Appl. Cryptography Netw. Secur.*, 2013, pp. 253–271.

[9] M. Strohmeier, I. Martinovic, and V. Lenders, "Securing the air-ground link in aviation," in *The Security of Critical Infrastructures*. Cham, Switzerland: Springer, 2020, pp. 131–154.

[10] R. Wu, G. Chen, W. Wang, D. Lu, and L. Wang, "Jamming suppression for ADS-B based on a cross-antenna array," in *Proc. Integr. Commun., Navigation, Surveillance Conf.*, 2015, pp. K3-1–K3-9.

[11] M. Leonardi and E. G. Piracci, "ADS-B degarbling and jamming mitigation by the use of blind source separation," in *Proc. IEEE/AIAA 37th Digit. Avionics Syst. Conf.*, 2018, pp. 1–5.

[12] H. Miyazaki and Y. Kakubari, "Jamming and spoofing protection for ADS-B mode S receiver through array signal processing," in *Proc. Air Traffic Manage. Syst. III: Sel. Papers 5th ENRI Int. Workshop ATM/CNS.*, vol. 555,, pp. 184–204, 2019.

[13] D. Adamy, *EW 101: A First Course in Electronic Warfare*. Norwood, MA, USA: Artech House, 2001.

[14] M. Leonardi, E. Piracci, and G. Galati, "ADS-B jamming mitigation: A solution based on a multichannel receiver," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 11, pp. 44–51, Nov. 2017.

[15] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm, "Bringing up OpenSky: A large-scale ADS-B sensor network for research," in *Proc. 13th Int. Symp. Inf. Process. Sensor Netw.*, 2014, pp. 83–94.

[16] "Minimum operational performance standards for 1090 MHz extended squitter automatic dependent surveillance—Broadcast and traffic information services broadcast," With Corrigendum 1, RTCA Inc., Washington, D.C., USA, RTCA DO-260B, Dec. 2011.

[17] *Annex 10 to the Convention on International Civil Aviation Aeronautical Telecommunication, ICAO*, Montreal, QC, Canada, 1998.

[18] H. T. Friis, "A note on a simple transmission formula," *Proc. IRE*, vol. 34, no. 5, pp. 254–256, May 1946.

[19] J. Litva and T. K. Lo, *Digital Beamforming in Wireless Communications*, 1st ed. Norwood, MA, USA: Artech House, 1996.

[20] G. R. Naik and W. Wang, *Blind Source Separation: Advances in Theory, Algorithms and Applications*, 1st ed. Berlin, Germany: Springer, 2016.

[21] X. Yu, D. Hu, and J. Xu, *Blind Source Separation: Theory and Applications*. Hoboken, NJ, USA: Wiley, 2014.

[22] N. Petrochilos, G. Galati, and E. Piracci, "Separation of SSR signals by array processing in multilateration systems," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 45, no. 3, pp. 965–982, Jul. 2009.

[23] G. R. Naik, *Advances in Principal Component Analysis: Research and Development*, 1st ed. Berlin, Germany: Springer, 2017.

[24] T. E. Tuncer and B. Friedlander, *Classical and Modern Direction-of-Arrival Estimation*. New York, NY, USA: Academic, 2009.