sensors

MDPI

Article

ADS-B Crowd-Sensor Network and Two-Step Kalman Filter for GNSS and ADS-B Cyber-Attack Detection

Mauro Leonardi * **and Gheorghe Sirbu**

Department of Electronic Engineering, Tor Vergata University of Rome, 00133 Rome, Italy; gheorghe.sirbu@uniroma2.it
* Correspondence: mauro.leonardi@uniroma2.it

Abstract: Automatic Dependent Surveillance-Broadcast is an Air Traffic Control system in which aircraft transmit their own information (identity, position, velocity, etc.) to ground sensors for surveillance purposes. This system has many advantages compared to the classical surveillance radars: easy and low-cost implementation, high accuracy of data, and low renewal time, but also limitations: dependency on the Global Navigation Satellite System, a simple unencrypted and unauthenticated protocol. For these reasons, the system is exposed to attacks like jamming/spoofing of the on-board GNSS receiver or false ADS-B messages' injection. After a mathematical model derivation of different types of attacks, we propose the use of a crowd sensor network capable of estimating the Time Difference Of Arrival of the ADS-B messages together with a two-step Kalman filter to detect these attacks (on-board GNSS/ADS-B tampering, false ADS-B message injection, GNSS Spoofing/Jamming). Tests with real data and simulations showed that the algorithm can detect all these attacks with a very high probability of detection and low probability of false alarm.

Keywords: ADS-B; GNSS; security; intrusion detection; spoofing; jamming; crowd sourced network; localization; EKF

Citation: Leonardi, M.; Sirbu, G. ADS-B Crowd-Sensor Network and Two-Step Kalman Filter for GNSS and ADS-B Cyber-Attack Detection. *Sensors* **2021**, *21*, 4992. https://doi.org/10.3390/s21154992

Academic Editor: Maorong Ge

Received: 28 June 2021
Accepted: 20 July 2021
Published: 22 July 2021

1. Introduction

The Automatic Dependent Surveillance Broadcast (ADS-B) system is considered to be the backbone of the future air traffic control system [1,2]. Today, more than 80% of commercial aircraft are currently equipped with ADS-B hardware [3]. It is a dependent and cooperative surveillance system in which the aircraft has an ADS-B transponder mounted on-board and continually broadcasts its state vector obtained from the Global Navigation Satellite System (GNSS) positioning equipment to anyone equipped with an ADS-B receiver [4]. The transponder uses the radar Mode S protocol to broadcast this information through the digital data link on the shared L-band channel. The Mode S protocol foresees 120 µs messages that contain a data block which is 112 bits long (112 µs), and an additional 8 µs preamble for synchronization. The messages use the Pulse Position Modulation (PPM), with a pulse length of 0.5 µs and the channel has a maximum speed of 1 Mbit/s. In nominal conditions, the ADS-B messages are received by the ground-based receivers and used to generate traffic images on the controller's display.

Figure 1 shows the ADS-B system architecture: the aircraft computes its position exploiting the GNSS and broadcasts messages containing the state information which are received by other aircraft, and by the ADS-B ground station for ATC operations. Possible attackers are highlighted in red; they could jam or spoof the GNSS signals, tamper the on-board GNSS receiver or the ADS-B transponder, or, finally, directly inject false ADS-B messages in the system.

The ADS-B system has many advantages compared to the classical surveillance radars; for example, the ground stations can be installed in almost any location, resolving the problem of black spots in remote areas where a radar station cannot be installed; it has an easy and low-cost implementation, and increased accuracy of location data allows for

smaller minimum aircraft separations, and therefore higher capacity. It has also some important limitations such as: the dependency on the GNSS (which suffers from Jamming and Spoofing that could corrupt, damage or interfere with the positioning information), and the very simple protocol that is not encrypted and without any authentication.

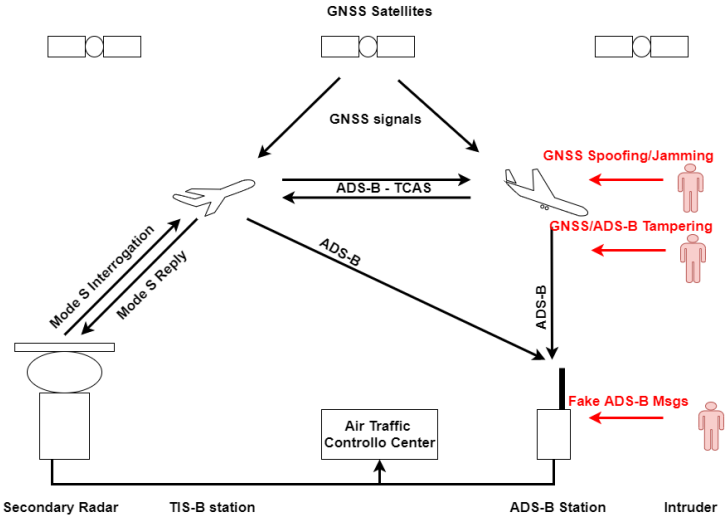

Figure 1. ADS-B system architecture. Possible attacks are in red.

Due to these limitations, different cyber-attacks can be used against the ADS-B system, and they can be classified as follows [5]:

- ADS-B Eavesdropping, i.e., listening to the transmission of the broadcasted messages since there is a lack of encryption: it is impossible to prevent without applying encryption and, of course, it is impossible to be detected;
- ADS-B channel Jamming, i.e., transmitting intentionally signals with a jammer in the RF channel in order to deny the communication: this type of attack may create denial-of-service (DoS) problems;
- ADS-B message injection (or spoofing), i.e., transmitting malicious signals, with a power slightly higher than a legitimate ADS-B signal, which contain misleading information, for example transmitting a sequence of messages representing a fake aircraft on a realistic trajectory;
- ADS-B Message deletion by SSR reply Garbling: deletion of some or all the information contained in a message by exploiting constructive or destructive signal interference;
- ADS-B Message modification, i.e., modifying messages of legitimate nodes by over-shadowing, bit flipping or with a combination of deletion and injection;
- GNSS Spoofing/Jamming, i.e., transmitting high power noise or signal on the GNSS channel producing false or wrong position information or reducing the GNSS availability;
- Aircraft ADS-B transponder or GNSS receiver tampering that is not authorized access to the on-board device that, in principle, allows different types of attacks—for example, the injection of false position in the navigation system or the manipulation and transmission of ADS-B message containing false information.

To mitigate some of these ADS-B related risks, various techniques were proposed in the last few years. As described, ADS-B messages are unencrypted and unauthenticated, and this leads to the possibility for an attacker to modify messages or inject fake messages. Encryption and authentication on the ADS-B protocol were proposed to overcome eavesdropping and message injection, like in [5–8], but they need a protocol modification. Authentication by RF and Low Level fingerprinting, without protocol modification, are proposed in [9–13]. In [14], the authors also propose a method to improve the ADS-B system security by introducing a physical layer protocol evolution for the introduction of an authentication scheme fully compliant with the current standard and exploiting the phase modulation of the signals. In [15], the tracking of the different sensor clocks is

proposed, by the use of Time Difference of Arrival (TDOA), of ADS-B messages to check the veracity of the position information contained in the ADS-B messages and to prevent false ADS-B data injection. Many other works in the past proposed the use of TDOA and Multilateration (MLAT) to verify the veracity of the ADS-B data starting from [16]. ADS-B jamming and message deletion vulnerabilities cannot be reduced with encryption or data verification and are closely related to the ADS-B receiver hardware; they require anti-jamming techniques—see, for example, [11,17,18], or [19,20] where the authors investigate network-wide countermeasures based on redundant coverage. Concerning the GNSS spoofing, there are different types of attacks, as discussed in [21], that threaten the actors that exploit the GNSS. Methods against spoofing attacks include authentication of the GPS signal [22,23], spatial processing aiming to nullify the signal coming from the direction of the incoming attack [24,25], and other methods that include machine learning based techniques for the detection of the spoofing attack [26,27]. These methods are applied on the GNSS receiver and are out of the scope of this work. Refs. [16,28,29] report some methods that exploit multilateration (MLAT), for the integrity check of GNSS derived information that can be used in ADS-B sensors' networks. MLAT provides an independent position information through hyperbolic localization, allowing for the detection of GNSS spoofing attacks.

More recent works also demonstrate that is possible to apply the MLAT algorithm for detecting malicious ADS-B transmitters [30,31]; they also propose to improve the MLAT performance by optimizing the network geometry (using genetic algorithms) and smoothing the measurements by the use of Kalman filters. Finally, in [32], it was shown that it is possible to achieve precise TDOA estimation also using low-cost ADS-B receivers in the MLAT sensor network.

The main disadvantages of MLAT are that it requires a minimum of four ground stations to calculate the position to be verified, and the system must invert a strong-not-linear and ill-posed system that produces numerical instability in the solution [33,34].

Finally, tampering the on-board GNSS receiver or the ADS-B transponder to inject false information has the same effect of GNSS spoofing and can be mitigated in the same way as before, using position consistency check.

Fortunately, nowadays, there are different types of ADS-B sensors and sensor networks that can be utilized for ADS-B message information checking. For example, there are open crowd-sourced networks, like *FlightRadar24* [35] or *OpenSky Network* [36] that are becoming more and more used in the ATC community. In the following, we propose the use of these networks to detect the most important threats on the ADS-B and GNSS channels, in particular:

- we analyze the effects on the ADS-B message information and on the ADS-B sensor network of the different types of threats, developing mathematical models to represent the following attack types: ADS-B message injection, GNSS jamming, GNSS spoofing, and on-board device tampering;
- we propose a method that, exploiting the network measurements, is able to detect these types of attack, without solving the MLAT problem and also taking into account the information about the expected kinematic state of each aircraft.

The proposed method exploits synchronized ADS-B sensors capable of measuring the TDOA of the ADS-B messages, and it was evaluated with real data coming from the OpenSky Network. For any ADS-B message, two different sources of information related to the aircraft position are available in the network: the TDOA measurements and the GNSS estimated position encoded on the ADS-B message. Exploiting a Kalman Filter [37,38], the aircraft kinematic model can be derived and any type of measurements can be integrated to have a better estimation of the aircraft position. Moreover, the Kalman filter has the ability to forecast the expected measurements and, comparing these with the incoming ones, it is possible to check the consistency between the aircraft estimated state and the measurements coming from the GNSS and the station network.

With this approach, it is not necessary to solve the MLAT problem, as done in the previously mentioned works, because the test was done directly in the measurement domain. This allows for performing the test also in case of bad geometry or with less than four stations in view from the aircraft.

In particular, here, we propose a two-step Extended Kalman Filter (EKF), with two consecutive updating phases and two different consistency checks (on the track kinematic and on the emitter position).

Simulations and trials show that the combination of the two tests is able to detect a small deviation from the aircraft predicted trajectory and also to detect false tracks injected by GNSS or ADS-B spoofers that have realistic but fake trajectory.

Last, but not least, considering that, in the last few years, GNSS attacks (in particular the spoofing attack) are increasing, the proposed method that uses the fighting aircraft together with the ground based ADS-B network as a large and pervasive opportunity sensor network to monitor and detect GNSS attacks can improve the general GNSS security also in other fields of application.

In the following sections, the different types of threats are described and modeled, the proposed detection method is derived and evaluated with simulations, using real data coming from the OpenSky Network, and, finally, some conclusions are reported.

2. Threat Models

As mentioned before, different types of attacks can affect the elements of the ADS-B system. In this work, we will focus on the following four threats:

- GNSS jamming;
- GNSS spoofing;
- ADS-B spoofing with fake messages injection;
- On-board ADS-B transponder or GNSS receiver tampering.

In this section, we describe the main threats and discuss the effects on the ADS-B system and on the sensor network; finally, we develop a mathematical model to represent the effect of each threat on the ADS-B system.

2.1. GNSS Jamming Attack

A jamming attack is used against the GNSS receiver to reduce ADS-B aircraft localization performance or to totally deny the localization service. The jammer transmits high power signals in the band of the GNSS to reduce as much as possible the sensitivity of the receiver, improving the noise floor and reducing the performance of the receiver. Moreover, if the jammer is very close to the receiver under attack, the signal-to-noise ratio becomes so small (or the receivers amplifiers go in their saturation zone) that the receiver is not able to decode the GNSS signals, with a total denial of the service.

In this paper, we assume that this second condition doesn't happen: considering flying objects, the receiver is assumed far enough from the jammer to avoid the saturation zone of its components. Consequently, we propose here a model to represent only the position accuracy degradation of the receiver when it is not close to its saturation. The derivation of a more complex model, taking into account nonlinear effects that are dependent on the receiver hardware and on the base-band processing of the different types of GNSS receivers, is out of the scope of this work.

The GNSS jamming effect on the ADS-B system can be modeled with an improvement of the error on the position encoded in the ADS-B messages. Calling $\mathbf{x} = (x, y, z)^T$ the vector containing the true aircraft position, the ADS-B aircraft position is:

$$\mathbf{x}_{ADS-B} = \mathbf{x} + \mathbf{n}_{ADS-B} \tag{1}$$

where $\mathbf{n}_{ADS-B}$ is the three elements ADS-B error vector representing the 3D error on the ADS-B position due to the GNSS localization. In a nominal condition, for the sake of simplicity, this error can be assumed with zero mean and covariance matrix given by:

$$\mathbf{Q}_{ADS-B} = \begin{bmatrix} \sigma_x^2 & 0 & 0 \\ 0 & \sigma_y^2 & 0 \\ 0 & 0 & \sigma_z^2 \end{bmatrix} = \sigma_{ADS-B}^2 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{2}$$

where we have assumed that the noise components are uncorrelated with each other, and, in the second equality, that the error has the same distribution for the three components.

By fixing the σ_{ADS-B} value, it is possible to over-bound the position error for a GNSS receiver on-board. Moreover, the position errors in GNSS systems depend on two factors [39]: the geometry of the GNSS satellite during the measurements (usually referred as Dilution Of Precision—DOP) and the User Equivalent Range Error (UERE) that takes into account the measurement error of the receiver:

$$\sigma_{x,y,z} = f(UERE) \tag{3}$$

Under common conditions, the function f that takes into account the system geometry is considered linear, and this relationship can be simplified in $\sigma_{x,y,z} = DOP_{x,y,z} \cdot UERE$.

The UERE is the sum of the GNSS pseudorange measurements' error contributions—for example, the sum of errors due to the ionosphere, the troposphere, and the measurement process in the receiver:

$$UERE = \sigma_{iono} + \sigma_{tropo} + \ldots + \sigma_{rx} \tag{4}$$

Usually, the GNSS receiver noise (σ_{rx}) is smaller than the other contributions, but, in case of jamming, it increases and can become higher than the others. Let us suppose to have a jammer with a given transmitter power (P_J) and a given antenna gain (G_J). Using the Friis equation [40,41], it is possible to compute the corresponding received power (P_j^r):

$$P_j^r = G_J G_r(\theta_J, \phi_J) \left(\frac{\lambda}{4\pi R_J} \right)^2 P_J \tag{5}$$

where R_J is the jammer–aircraft range, and $G_r(\theta_J, \phi_J)$ is the receiver antenna gain in the direction of the jammer. If P_j^r is higher than the receiver amplifier saturation threshold, P_{sat}, the reception of the GNSS signal is inhibited, and no navigation solution is carried out from the receiver. As mentioned before, if the jammer received power is also lower than the saturation level, the receiver performances are reduced. Fixing the received power for the signals coming from the satellites, P_T^r, the signal-to-interference-plus-noise ratio (SINR) becomes:

$$SINR = \frac{P_T^r}{N + P_J^r} = \frac{P_T^r}{N + G_J G_r(\theta_J, \phi_J) \left(\frac{\lambda}{4\pi R_J} \right)^2 P_J} \simeq k R_J^2. \tag{6}$$

The last equality is valid in case $N \ll P_J^r$; under this condition, the relationship between the jammer distance and the SINR is quadratic (apart from a constant factor k). Recalling that σ_{rx} depends on the SINR with the following relationship [42]:

$$\sigma_{rx}(SINR) \cong \frac{1}{\beta \sqrt{2 SINR}}. \tag{7}$$

During a jamming attack, this term becomes bigger than the other contributions in the UERE budget Equation (4) and using Equations (3) and (7), it is possible to infer a value to over-bound the GNSS position error in case of a jammer at a given distance R_J:

$$\sigma_{ADS-B}(SINR) = f(\cdot(const + \sigma(SINR))) = a + \frac{1}{\beta_2\sqrt{2kR_J^2}} = a + b/R_J \tag{8}$$

where a is a constant that takes into account all the other error effects, and b gives the linear relationship between the distance of the jammer and the GNSS error magnitude (it depends on the jammer parameters, such as the transmitted power, type of transmitted signal, etc.). In the last equality, as stated before, it is assumed that the f function is a linear function as is usually assumed for the computation of the Dilution of Precision in the GNSS system [39]. It follows that, for a GNSS jamming attack, we can assume that the ADS-B message will contain position data with errors on the three components ($\mathbf{n}_{ADS-B}$) that are still with zero mean but with higher standard deviations that decrease linearly with the jammer distance, Equation (2) becomes:

$$\mathbf{Q}_{ADS-B}^{Jamming} = \left(\sigma_{ADS-B}^2 + \overbrace{(a + b/R_J)^2}^{\sigma_{Jamming}^2}\right) \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{9}$$

2.2. GNSS Spoofing Attack

GNSS spoofing is the transmission of fake GNSS signals containing false information. The effect on the receiver is more dangerous compared with the jamming for at least two reasons: it is more difficult to detect by the user, and the receiver uses the fake signals carrying out wrong positions that can have huge biases and can also follow a fake trajectory [43,44].

On the ADS-B system, GNSS spoofing means the ability for an attacker to introduce fake positions in the aircraft under attack. This effect can be modeled adding a bias on the aircraft position, maintaining the same standard deviation for positional error:

$$\mathbf{x}_{ADS-B} = \mathbf{x}_{fake} + \mathbf{n}_{ADS-B} = \mathbf{x} + \mathbf{b}_{GNSS} + \mathbf{n}_{ADS-B} \tag{10}$$

where $\mathbf{b}_{GNSS}$ represents the bias due to the spoofing, i.e., the vector representing the different between the real and the fake position.

2.3. ADS-B Spoofing

ADS-B spoofing includes different possible attacks; in this work, we refer to the most dangerous case: the injection in the Mode S channel of legacy formatted ADS-B messages containing false information. These messages are received from the ADS-B station and are not distinguishable from the correct ones. This can produce two main effects on the ADS-B system:

- the appearing of "ghost" aircraft, in case of fake messages containing data of airplanes not yet present in the coverage area of the ADS-B station;
- the appearing of wrong ADS-B position data incoherent with the other position coming from the real messages, if the aircraft is present in the coverage of the ADS-B system.

In any case, the injection of fake ADS-B messages with wrong positional data can be seen as the introduction of a bias on the ADS-B position, as already done in the case of GNSS spoofing:

$$\mathbf{x}_{ADS-B} = \mathbf{x}_{fake} = \mathbf{x} + \mathbf{b}_{ADS-B} \tag{11}$$

The difference with GNSS spoofing is that, unlike GNSS spoofing that affects only the aircraft close to the spoofer, ADS-B message injection affects only the station under attack and can introduce any number of fake airplanes in any possible position.

2.4. On-Board Tampering Attack

On-Board tampering consists of the replacement, or the manumission, of the on-board hardware or software to inject false information in the on-board devices; for example, replacing the GNSS unit with an emulator that carries out false position or hacking of the ADS-B transponder to transmit fake ADS-B messages. In any case, this threat can be modeled as the previous threats, introducing a bias in the position transmitted by the ADS-B transponder:

$$\mathbf{x}_{ADS-B} = \mathbf{x}_{fake} = \mathbf{x} + \mathbf{b}_{tamp} \tag{12}$$

2.5. Discussion on the Threats Models

The introduced models are used in the following section to emulate the possible attacks on the ADS-B system. The first model (GNSS spoofing) is the only one that introduces additive noise on the ADS-B position. This noise produces more noisy tracks for the aircraft close to the jammer. This effect can be seen in the same moment on one or more aircraft and for the whole duration of the attack. The mathematical model for the other three threats is the same, but the effects on the whole ADS-B system are different:

- in case of GNSS spoofing, the bias appears only for the aircraft close to, or in the coverage of, the spoofer, typically changing the position of the aircraft with a fake one. Moreover, the fake position is the same for all the attacked aircraft. Observing the whole traffic, under this attack, aircraft close to each other and near the spoofer instantly change their positions to a new fake one, equal for all the airplanes. Note that GNSS Spoofing can be very dangerous because the on-board navigation systems also use the GNSS; it means that both the pilot and the controller are deceived, this may cause the total loss of the control of the aircraft;
- in case of ADS-B spoofing, one or more ghost aircraft, having false positions, can appear in any place in the world, and not necessarily near the ADS-B stations that receive the signals; in general, there is no correlation between the ADS-B spoofer and the ghost airplanes' position. Moreover, the fake aircraft can have realistic trajectory. If the injected airplanes are already present and tracked by the ADS-B sensor network, this attack produces outliers or big steps in the airplane tracks. If the injected airplanes are not yet tracked, totally new (and fake) tracks appear in the ADS-B system;
- in case of on-board device tampering, only the aircraft under attack transmits fake positions. This attack can produce steps on the airplane track or, if well-designed, can slightly change the airplane positions to produce a false track, without unexpected steps (for example, the aircraft can change its real trajectory continuing transmitting the expected one to hide a hijacking).

Finally, concerning the GNSS spoofing and jamming, it is important to note that they are used for many reasons in different fields, usually to inhibit its uses; this means that the aircraft can be a secondary victim of an attack designed for other scopes. On the other hand, the aircraft and the ADS-B system can be seen as a detector for any GNSS spoofing and jamming attack also if it is designed for other scopes.

3. Attack Detection Algorithm

As mentioned before, we propose to monitor the ADS-B data exploiting a crowd-sensor network able to perform TDOA estimation of the received ADS-B messages: the idea is to combine the network measurements with the incoming ADS-B data to perform some conformance tests.

Recently, the OpenSky Network released some data-sets containing the TOA of the ADS-B messages. Moreover, many of these stations are GPS synchronized, allowing the TDOA localization of the aircraft [45]. Here, we propose to use TDOA measurements of ADS-B messages not to have an independent estimation of the aircraft position but to verify the consistency of the two sources of information without solving the MLAT problem. This allows for checking the ADS-B data also when less than four stations are present and without solving the MLAT problem that many times can be ill-conditioned.

Moreover, we propose to also test the consistency of the incoming measurements with the historical information and the expected kinematic model for the aircraft. In fact, exploiting Kalman filters, it is possible to use the aircraft expected kinematic model, the statistical knowledge of the measurements and the past measurements to predict the future target position and to predict the expected measurements to be compared with the incoming ones to verify their consistency.

In the following sections, we will derive, firstly, the model and the statistics to test the TDOAs and ADS-B position consistency, and then we extend these models to be used into an EKF.

3.1. Position Check by the Use of TDOAs

Assuming to have M synchronized stations able to measure the TOA of the messages, for each received message, it is possible to write the following equation:

$$TOA_i^k = \frac{\|\mathbf{x}_i - \mathbf{x}^k\|}{c} + t_0^k + n_i \tag{13}$$

where $\mathbf{x}_i$ represents the position of the station i, and $\mathbf{x}^k$ represents the position of the aircraft k, c is the speed of light, t_0^K is the time of transmission of the message, and n_i represents the TOA measurement errors of the station i. Forming the differences between two stations, it is possible to cancel the unknown t_0^k:

$$TDOA_{i,j}^k = \frac{\|\mathbf{x}_i - \mathbf{x}^k\| - \|\mathbf{x}_j - \mathbf{x}^k\|}{c} + n_i - n_j \tag{14}$$

Now, fixing a reference station, $(M-1)$ independent TDOAs can be computed and, using the matrix notation, we have:

$$\boldsymbol{TDOA}^k = \mathbf{f}(\mathbf{x}_1, \ldots, \mathbf{x}_M, \mathbf{x}^k) + \mathbf{n}_{TDOA} \tag{15}$$

where $\boldsymbol{TDOA}^k$ is the vector containing the $(M-1)$ measurement, $\mathbf{n}_{TDOA}$ is the $M-1$ measurements error vector, having zero mean and covariance matrix:

$$\mathbf{Q}_{TDOA} = \begin{bmatrix} \sigma_1^2 + \sigma_M^2 & \sigma_M^2 & \cdots & \sigma_M^2 \\ & & \cdots & \\ \sigma_M^2 & \cdots & \sigma_i^2 + \sigma_M^2 & \sigma_M^2 \\ & & \cdots & \\ \sigma_M^2 & \cdots & \sigma_M^2 & \sigma_{M-1}^2 + \sigma_M^2 \end{bmatrix} \tag{16}$$

where $\sigma_1^2, \ldots, \sigma_M^2$ are the TOA measurement variances for each station.
For the same aircraft, at the same instant, the GNSS derived aircraft position is encoded in the ADS-B message and available in the ADS-B ground station: it can be denoted with $\mathbf{x}_{ADS-B}^k$, as defined in Equation (1). The ADS-B position corresponding to the expected TDOA measurement vector can be computed exploiting Equation (14) and Equation (15):

$$\boldsymbol{TDOA}_{ADS-B}^k = \mathbf{f}(\mathbf{x}_1, \ldots, \mathbf{x}_M, \mathbf{x}_{ADS-B}^k) = \mathbf{f}(\mathbf{x}_1, \ldots, \mathbf{x}_M, \mathbf{x}^k + n_{ADS-B}) \tag{17}$$

and linearizing near the real target position, $\mathbf{x}^k$, it is possible to obtain:

$$\boldsymbol{TDOA}_{ADS-B}^k = \mathbf{f}(\mathbf{x}_1, \ldots, \mathbf{x}_M, \mathbf{x}^k) + \frac{\partial \mathbf{f}(\mathbf{x}_1, \ldots, \mathbf{x}_M, \mathbf{x}^k)}{\partial \mathbf{x}}\Big|_{(\mathbf{x}=\mathbf{x}^k)} \cdot \mathbf{n}_{ADS-B}^k \tag{18}$$

Finally, forming the difference between Equation (18) and Equation (15), we obtain a vector representing the difference between the ADS-B expected **TDOA** and the measured **TDOA**:

$$\boldsymbol{\epsilon} = \boldsymbol{TDOA}^k_{ADS-B} - \boldsymbol{TDOA}^k = \frac{\partial \mathbf{f}(\mathbf{x}_1, \ldots, \mathbf{x}_M, \mathbf{x})}{\partial \mathbf{x}}\Big|_{(\mathbf{x}=\mathbf{x}^k)} \cdot \mathbf{n}^k_{ADS-B} - \mathbf{n}_{TDOA} \tag{19}$$

Calling **F** the Jacobian of **f**, we have:

$$\boldsymbol{\epsilon} = \mathbf{F} \cdot \mathbf{n}^k_{ADS-B} - \mathbf{n}_{TDOA} \tag{20}$$

It follows that, in an ideal case, without measurement noises and ADS-B position errors, $\boldsymbol{\epsilon}$ is an $(M-1)$ vector composed of zeros. In the presence of noises and position errors, $\boldsymbol{\epsilon}$ is a random vector that depends only on the measurement noises, the ADS-B errors, and on the matrix **F**.

Assuming Gaussian distributed noises and errors, the entries of $\boldsymbol{\epsilon}$ will be linear combinations of Gaussian variables, still Gaussian distributed with covariance matrix given from the following equation:

$$\mathbf{Q} = \mathbf{F}\mathbf{Q}_{ADS-B}\mathbf{F}^T + \mathbf{Q}_{TDOA} \tag{21}$$

Finally, the normalized norm of $\boldsymbol{\epsilon}$, $w = \boldsymbol{\epsilon}^t \mathbf{Q}^{-1} \boldsymbol{\epsilon}$ can be used to test the consistency of the ADS-B position and TDOA measurements. In nominal conditions (that is absence of any anomalies), called H_0 hypothesis, recalling that the normalized norm is the sum of $(M-1)$ Gaussian random variables, w is chi-square distributed [46]:

$$H_0 : w \sim \chi^2(M-1, 0) \tag{22}$$

In the case of ADS-B spoofing/on-board tampering/GNSS spoofing (H_1 hypothesis), assuming the presence of a bias on the ADS-B position in the messages, Equation (20) becomes:

$$\boldsymbol{\epsilon} = \mathbf{F} \cdot (\mathbf{n}^k_{ADS-B} + \mathbf{b}^{ADS-B/GNSS/tamp}_{ADS-B}) - \mathbf{n}^k_{TDOA} \tag{23}$$

In this case, the distribution for w will be a not central chi-square distribution with $(M-1)$ degrees of freedom with parameters [46]:

$$H_1 : w \sim \chi^2(M-4, \|\mathbf{F} \cdot \mathbf{b}_{ADS-B/GNSS/tamp}\|_2^2) \tag{24}$$

Unfortunately, the vector $\mathbf{b}_{ADS-B/GNSS/tamp}$ is projected into the **TDOA**-space through the matrix **F**, and, if **F** has a null-space that is not null, some biases could be undetectable. In any case, the resulting norm can be reduced by this projection and there is not an easy way to find a lower bound for the non-central parameter of the chi-square distribution. It follows that it is impossible to find a general way to fix the probability of missed detection: it depends on the combination of ADS-B bias (magnitude and direction) and geometrical distribution of the sensor stations used for the test. Finally, in case of GNSS Jamming, the distribution of the parameters will not be a chi-square distribution and cannot be computed explicitly. For these reasons, the algorithm performance in terms of Missed Detection (or Detection Probability) should be evaluated via Monte Carlo simulations for each specific geometrical configuration of the networks.

In any case, the distribution of w in nominal condition (H_0 hypothesis) is always known (knowing the ADS-B position error and the TDOA measurement noise parameters) and can be used to at least fix the Probability of False Alarm of the test, finding a threshold for the w parameter:

$$P_{fa} = \int_{t_{P_{fa}}}^{\infty} \chi^2(M-1, \hat{\lambda}) \tag{25}$$

If that threshold is overcome, the presence of an anomaly can be declared.

3.2. Two Step Detection by the Use of Kalman Filtering

The approach described in the previous section only checks the ADS-B position information with the TDOA measurements, without taking into account the possible kinematic model for the target. In this section, we extend the concept to be implemented in a tracking algorithm, able to also use the kinematic parameters and the past measurements to forecast the expected TDOA for any new incoming message of the airplane.

Assuming an aircraft with a constant velocity in the short time, and exploiting all the statistical knowledge of the observations (ADS-B position error and TDOA measurement noise), it is possible to set a Discrete Time EKF. The aircraft state transition model is:

$$\mathbf{s}^k(t_{n+1}) = \mathbf{G}\mathbf{s}^k(t_n) + \mathbf{w}(t_n) \tag{26}$$

where $\mathbf{s}^k(t_n)$ is the state vector of the aircraft k at time instant t_n, defined as:

$$(\mathbf{s}^k)^T = \begin{bmatrix} x, y, z, v_x, v_y, v_z \end{bmatrix} \tag{27}$$

where x, y, x, v_x, v_y, v_z represents the position and velocity components of the aircraft; the transition matrix, $\mathbf{G}$, is defined as:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & T & 0 & 0 \\ 0 & 1 & 0 & 0 & T & 0 \\ 0 & 0 & 1 & 0 & 0 & T \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{28}$$

and $\mathbf{w}(t_n)$ represents the process noise. Considering the measurement models, two measurements must be considered: the use of position encoded on the ADS-B message $\mathbf{x}^k_{ADS-B}(t_n)$, and the TDOAs measurements, $\boldsymbol{TDOA}^k$ (recalling Equation (1) and Equation (15)):

$$\mathbf{x}^k_{ADS-B}(t_n) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \mathbf{s}^k(t_n) + \mathbf{n}_{ADS-B}(t_n) = \mathbf{F}_{ADS-B}\mathbf{s}^k(t_n) + \mathbf{n}_{ADS-B}(t_n) \tag{29}$$

$$\boldsymbol{TDOA}^k(t_n) = \mathbf{f}(\mathbf{s}(t_n)) + \mathbf{n}_{TDOA}(t_n)$$

Remembering Equation (14) and Equation (15), the Jacobian of the function $\mathbf{f}$ can be easily computed for the EKF application:

$$\mathbf{F}_{TDOA} = \frac{\partial \mathbf{f}(\mathbf{s}(t_n))}{\partial \mathbf{s}(t_n)} = \begin{bmatrix} \mathbf{F} & \mathbf{0}_{3x3} \end{bmatrix} \tag{30}$$

where $\mathbf{F}$ is introduced in the previous section. Now, the EKF can be applied to estimate the aircraft position exploiting both the ADS-B encoded position and TDOA measurements; here, we propose to use a two step updating process: the first update is done with the ADS-B data and the second update is done with the TDOA measurements. In this way, two innovations (the difference between the expected measurements and the incoming measurements) are computed (w.r.t. the ADS-B data and w.r.t. TDOAs) and can be used to produce two different conformance checks: one on the conformance of the new ADS-B data with the track information, and the other on the conformance of the track with independent TDOA measurements. The steps of the proposed algorithm are reported in Table 1.

It is important to note that this approach allows, at the same time, to test the data and measurement coming from the ADS-B messages and from the sensor measurement, and to have a more accurate estimation of the target position. In the algorithm, three different thresholds were introduced: th_1 is used to check the ADS-B data/track consistency, using

the normalized norm of the first step innovation, th_2 is used to check the consistency of the TDOA/track consistency using the normalized norm of the second step innovation and th_3 is used to decide whether to update the track states with the TDOA measurements or not. The normalized norms are computed using the innovation vectors and their covariance matrices, in the same way as illustrated in the previous section.

Table 1. Proposed Algorithm.

- **Input:**
  $\mathbf{s}(t_n)$: aircraft state vector at time t_n;
  $\mathbf{S}(t_n)$: state covariance matrix at time t_n;
  $\mathbf{G}$: transition matrix;
  $\mathbf{W}$: process noise covariance matrix;
  $\mathbf{f}(\cdot)$: TDOA formulation, quadratic equations as derived in Equation (15)
  $\mathbf{F}_{ADS-B}$: ADS-B observation matrix as defined in Equation (29);
  $\mathbf{F}_{TDOA}$: TDOA observation matrix as defined in Equation (30);
  $\mathbf{x}_{ADS-B}(t_n)$: ADS-B observation vector at time t_n;
  $\mathbf{TDOA}(t_n)$: TDOA observation vector at time t_n;
  $\mathbf{Q}_{ADS-B}$: covariance matrix of the ADS-B position error;
  $\mathbf{Q}_{ADS-B}$: covariance matrix of the TDOA measurements noise;
  the hat operator $\hat{}$, means prediction for time t_{n+1} using information of time t_n.

- **Output:**
  $\mathbf{s}(t_{n+1})$: aircraft state vector at time t_{n+1};
  $\mathbf{S}(t_{n+1})$: state covariance matrix at time t_{n+1};
  alarms: T1, T2;

1. **Prediction**
   predict the state for the time instant of new measurements: $\hat{\mathbf{s}}(t_{n+1}) = \mathbf{G}\mathbf{s}(t_n)$;
   predicted the state covariance matrix: $\hat{\mathbf{S}}(t_{n+1}) = \mathbf{G}\mathbf{S}(t_n)\mathbf{G}^t + \mathbf{W}$;

2. **ADS-B Innovation test**
   compute the innovation: $\mathbf{y}_{ADS-B}(t_{n+1}) = \mathbf{x}_{ADS-B}(t_{n+1}) - \mathbf{F}_{ADS-B}\hat{\mathbf{s}}(t_{n+1})$;
   compute the innovation covariance matirx: $\mathbf{R}_{ADS-B}(t_{n+1}) = \mathbf{F}_{ADS-B}\hat{\mathbf{S}}(t_{n+1})(\mathbf{F}_{ADS-B})^t + \mathbf{Q}_{ADS-B}$;
   compute the test: $w_{ADS-B} = (\mathbf{y}_{ADS-B}(t_{n+1}))^t\mathbf{R}_{ADS-B}(t_{n+1})\mathbf{y}_{ADS-B}(t_{n+1})$;
   if $w_{ADS-B} > th_1$ then
   rise alarm T1;

3. **Updating with ADS-B data**
   compute Kalman gain: $\mathbf{K}_{ADS-B}(t_{n+1}) = \hat{\mathbf{S}}(t_{n+1})(\mathbf{F}_{ADS-B})^t(\mathbf{R}_{ADS-B}(t_{n+1}))^{-1}$;
   update the aircraft state vector: $\mathbf{s}(t_{n+1}) = \hat{\mathbf{s}}(t_{n+1}) + \mathbf{K}_{ADS-B}(t_{n+1})\mathbf{y}_{ADS-B}(t_{n+1})$;
   update the state covariance matrix: $\mathbf{S}(t_{n+1}) = (\mathbf{I} - \mathbf{K}_{ADS-B}(t_{n+1})\mathbf{F}_{ADS-B})\hat{\mathbf{S}}(t_{n+1})$;

4. **TDOA Innovation test**
   compute the new innovation: $\mathbf{y}_{TDOA}(t_{n+1}))^t = \mathbf{TDOA}(t_{n+1}) - \mathbf{f}(\hat{\mathbf{s}}(t_{n+1}))$;
   compute the innovation covariance Matrix: $\mathbf{R}_{TDOA}(t_{n+1}) = \mathbf{F}_{TDOA}\mathbf{S}(t_{n+1})(\mathbf{F}_{TDOA}(t_{n+1}))^t + \mathbf{Q}_{TDOA}$;
   compute the test: $w_{TDOA} = (\mathbf{y}_{TDOA}(t_{n+1}))^t\mathbf{R}_{TDOA}(t_{n+1})\mathbf{y}_{TDOA}(t_{n+1})$;
   if $w_{TDOA} > th_2$ then
   rise alarm T2;

5. **Updating with TDOA measurements**
   if $w_{TDOA} < th_3$ then
   compute the new Kalman gain: $\mathbf{K}_{TDOA}(t_{n+1}) = \mathbf{S}(t_{n+1})(\mathbf{F}_{TDOA}(t_{n+1}))^t(\mathbf{R}_{TDOA}(t_{n+1}))^{-1}$;
   update the aircraft state vector: $\mathbf{s}(t_{n+1}) = \mathbf{s}(t_{n+1}) + \mathbf{K}_{TDOA}(t_{n+1})\mathbf{y}_{TDOA}(t_{n+1})$;
   update the state covariance matrix: $\mathbf{S}(t_{n+1}) = (\mathbf{I} - \mathbf{K}_{TDOA}(t_{n+1})\mathbf{F}_{TDOA}(t_{n+1}))\mathbf{S}(t_{n+1})$;

The test parameters become:

$$w^k_{ADS-B}(t_n) = (\mathbf{y}^k_{ADS-B}(t_n))^t \mathbf{R}_{ADS-B}(t_n)\mathbf{y}^k_{ADS-B}(t_n)$$
$$w_{TDOA} = (\mathbf{y}^k_{TDOA}(t_n))^t \mathbf{R}_{TDOA}(t_n)\mathbf{y}^k_{TDOA}(t_n) \quad (31)$$

where $\mathbf{y}^k_{ADS-B}(t_n)$ is the ADS-B position innovation for the aircraft k at time t_n, and $\mathbf{y}^k_{TDOA}(t_n)$ is the TDOA innovation for the same aircraft and time instant, having covariance matrix (computed by the EKF) $\mathbf{R}_{ADS-B}(t_n)$ and $\mathbf{R}_{TDOA}$, respectively (see Table 1 for their definitions).

Distributions for the H_0 hypothesis, to fix the Probability of False Alarm, can be still computed as described in the previous section, and becomes:

$$H_0 : w_{ADS_B} \sim \chi^2(3,0)$$
$$w_{TDOA} \sim \chi^2(M-1,0) \quad (32)$$

It is easy to understand that w_{ADS-B} is suitable to detect any attack that introduces a step in the trajectory (e.g., GNSS spoofing when switched on, GNSS Jamming, ADS-B spoofing of aircraft already present in the coverage area, simple ADS-B spoofing producing a step in the trajectory, simple tampering producing a step in the trajectory, etc.). Smarter attacks, e.g., ADS-B spoofing with realistic false track injection, or tampering with the introduction of a fake trajectory with a smooth transition from the real one, cannot be detected. In this second case, the w_{TDOA} test is still able to detect the aircraft deviation from the declared trajectory (on board tampering or false aircraft injection; in general smooth but growing deviation of ADS-B positions from the real one) using independent TDOA measurements.

Moreover, as mentioned before, observing all of the traffic, it is possible to distinguish between on-board tampering, GNSS attacks, and ADS-B attacks.

4. Evaluation with Real Data

The OpenSky Network is one of the biggest crowd sourced ADS-B networks able to measure and store TOA of each received message, and, in this work, we use the Localization Reference Data Set [45] to evaluate the proposed algorithm performances. A sub-set of the data was selected from the entire data-set and, in particular, only the data coming from five GPS synchronized stations in Portugal/Spain near Lisbon are selected. The recording is one hour long and contains 264,799 ADS-B position messages coming from 163 different aircraft. Figure 2 shows the tracks used for the simulation and the station positions. Note that, in the figure, blue represents positions where more than three stations are in view, red represents positions where less than four stations are in view: for most of the coverage area, the MLAT approach cannot be used to localize the aircraft or to check their ADS-B data with independent localization.

Due to different types of sensors that use different algorithms for TOA computation (for example, some types of receivers refer to the message starting time and others to the message ending time), there is an instrumental delay that must be corrected to compute the TDOA measurements. The whole data-set is used to estimate the covariance matrix $\mathbf{Q}_{TDOA}$ and the fixed instrumental delay of each combination of stations (computing the standard deviation, and the mean of all the $TDOA_{i,j}$ pairs). The $\mathbf{Q}_{TDOA}$ was computed with Equation (16) setting $\sigma_1 = \ldots = \sigma_M = c \cdot 0.7 \cdot 5 \cdot 10^{-7}$ s (the coefficient 0.7 is used to refer to TOA instead of TDOA, assuming the measurements error for the two stations have the same distribution). Examples of calculated TDOA distributions (Station #1 versus the others) are reported in Figure 3. Finally, the ADS-B position error covariance matrix was fixed setting $\sigma_x = \sigma_y = \sigma_z = 40$ m.

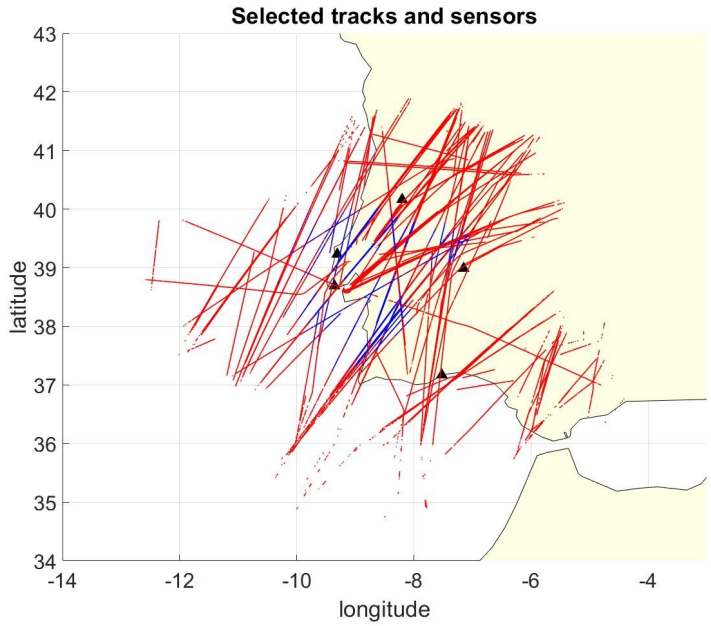

Figure 2. ADS-B tracked routes and selected stations. In the red position, it is not possible to apply the classic MLAT localization algorithm ($M < 4$).

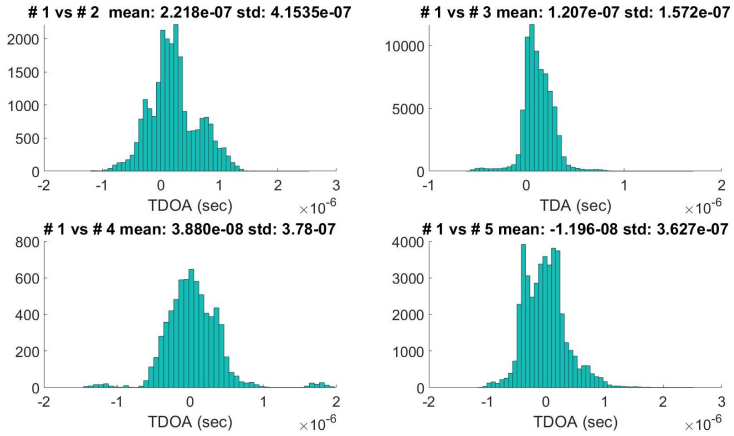

Figure 3. TDOAs means and standard deviations computed for the five stations.

The following sections report the evaluations for the proposed algorithm in case of:

- GNSS/ADS-B/tampering attack that introduces a bias in the ADS-B position;
- ADS-B spoofing that injects fake aircraft following fake but realistic trajectory;
- GNSS jamming introducing additional errors in the ADS-B position information.

In any case, the OpenSky database was intended as the nominal case, and the attacks were simulated applying the models described before.

4.1. Gnss/ADS-B/Tampering Attacks

In this section, the algorithm performances for all the attacks that can be emulated adding a bias on the ADS-B position are evaluated. The attack was simulated introducing a bias having a given magnitude and random direction at a given time for each aircraft in the database. For each airplane, after the track initialization phase of the EKF, for every incoming message, a bias with a random direction was generated, and the tests were performed. Then, the track was updated considering the ADS-B positional data without the bias (in this way, the next step can still be used to perform a new test). This simulation tested the ability of the proposed algorithm to detect a step of the ADS-B/TDOA incoming

data with respect to the aircraft track generated by the EKF.Different values for the bias magnitude (from 400 m to 1000 m) and $th1/th2$ (from 0.5 to 4 times the threshold needed to theoretically fix P_{fa} to 0.001 computed with Equation (25)) are tested, and, for each combination of the parameters, the probability of detection and the probability of false alarm were computed.

Receiver Operating Characteristic (ROC) for different bias values are reported in Figure 4. It is possible to note that the algorithm is able to detect the attack with a high probability of detection and low probability of false alarm also in case of a small bias (400 m) in the ADS-B position; for example, the T1 test (that first test on the innovation) reaches a $P_{fa} = 5 \times 10^{-5}$ with $P_D > 0.95$.

Note also that the second test (the one that use the TDOA) does not introduce performance improvements and, on the contrary, using both the tests (T1 or T2 curves) slightly reduces the P_{fa}. The T2 test performs worse than the T1 test in this class of attack because, recalling its definition from Equation (32) and Table 1, it depends on the TDOA measurement noise covariance matrix and network geometry. In the specific case of a crowd-sourced network, the TDOA measurements usually are very noisy, and the test is not able to detect a small deviation from the aircraft trajectory. It follows that, for this specific set of data, the T2 test becomes unnecessary for this attack, but mandatory for false track injection, as will be shown later. This condition can change in the case of a network of professional receivers with optimized geometry.

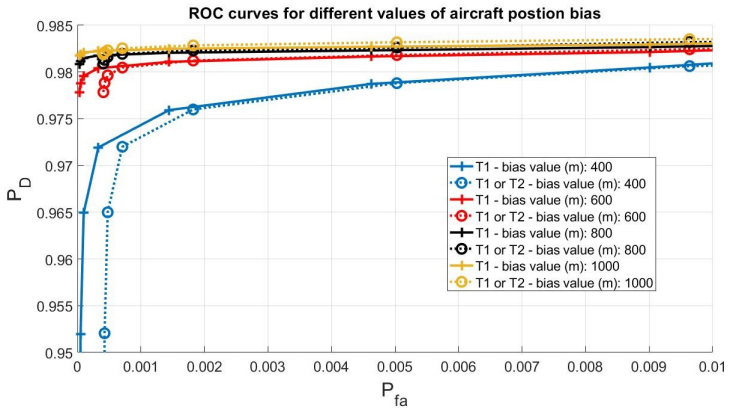

Figure 4. Receiver Operating Characteristic for T1 and T2 different bias values.

4.2. ADS-B Spoofing Attack, Fake Track Injection

In this section, the capability of the algorithms to detect an injection of totally fake tracks is evaluated. The simulation still exploits the previous database but now the ADS-B position of the incoming signal was considered transmitted from an ADS-B spoofer in a given fixed position on the ground. New TDOA measurements consistent with the spoofer position were generated, and the algorithm was applied to track the aircraft. As before, at each step, the ADS-B test (T1) and the TDOA test (T2) were done. In this condition, the test T1, as expected, was not able to detect the attack reaching a maximum P_D of 0.1. This happens because the ADS-B position follows a realistic trajectory, and the track/ADS-B position test is not able to detect the attack. On the contrary, in this condition, the TDOA test (T2) has a $P_D > 0.98$ for any tested threshold value, reaching a probability of false alarm 3×10^{-4}.

Considering the complete algorithm (T1 or T2 to rise an alarm), the probability of detection does not change and the probability of false alarm grows to 4×10^{-4}. Concluding, in any case, if an ADS-B spoofer starts transmitting message with fake positions, the complete algorithm has a high probability to detect it.

4.3. GNSS Jamming Attack

GNSS jamming attack was simulated introducing a jammer in a random position and at a random time instant. Once the jammer was introduced, the Probability of Detection and the Probability of False Alarm were computed.

This time, the attack was considered detected if an alarm was raised within 60 s from the time of introduction of the jammer; otherwise, the attack was considered not detected: all the ADS-B messages received within 60 s were used for the test. The jammer was simulated using Equation (9), fixing a and b so that the additive contribution of to the noise ($\sigma_{Jamming}$) was 200 m for a target closer than 10 km, decreasing linearly until a range of 100 km where it becomes 0 m.

Three different cases for raising an alarm were considered: at least one detection in 60 s, at least two detection in 60 s, and at least three detections in 60 s. This was done to reduce the false alarm rate.

Figure 5 shows the ROC curves computed for the three different cases varying the threshold values of algorithms $th1$ and $th2$. In any case, the alarm was always raised from the first step of the algorithm T1. As shown in the figure, the algorithm is able to assure a good compromise between P_D and P_{fa}. Furthermore, for this type of attack, the Time to Alarm was also evaluated. Figure 6 shows the cumulative distribution function for the time to alarm in the three different cases (one/two/three detections) for the point highlighted with a circle in Figure 5 (the knees of the curves that are, approximately, the best compromise between P_d and P_{fa}): the algorithm assures a time to alarm lower than 15 s in 80% of the cases.

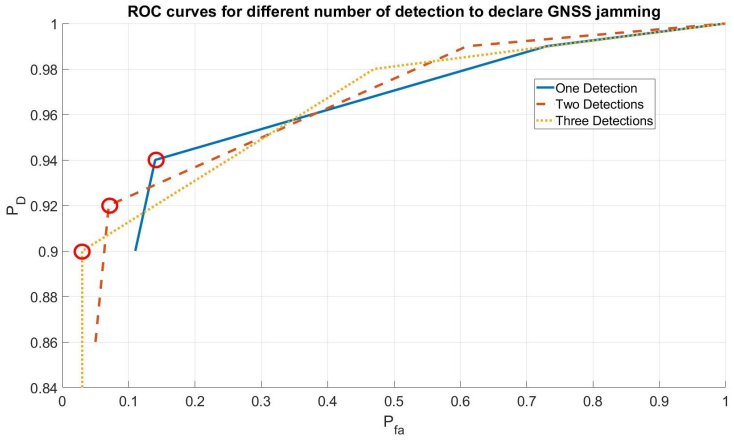

Figure 5. Receiver Operating Characteristic for different numbers of detections.

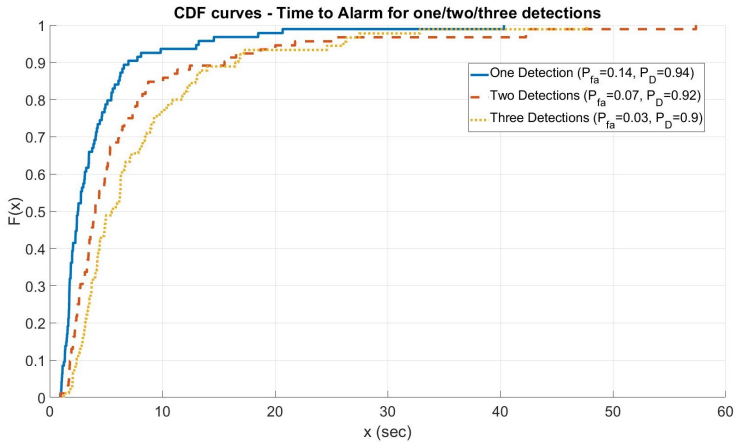

Figure 6. Cumulative Distribution Function for the Time to Alarm in the three different cases.

5. Conclusions

In this work, different models for different types of attacks on the ADS-B and GNSS systems are developed. These models are used to evaluate a two-step EKF algorithm in an ADS-B sensor network to detect cyber-attacks on. The algorithm shows good performances for all the tested conditions and provides alarms for all the cases: the on-board tampering, the ADS-B message injection, GNSS spoofing, and GNSS jamming. This capability was tested with real data coming from the OpenSky Network and simulating the different attacks; we obtained a very high probability of detection and a low probability of false alarm for almost all the cases. In more detail, the proposed algorithm is able to detect, in real time, a small step in the target trajectory also in the case of biases of only 400 m, with a probability of detection higher than 0.97 and a probability of false alarm lower than 3×10^{-4}. The algorithm is also able to detect totally false tracks, not confirmed from TDOA measurements, with a probability of detection higher than 0.98 and the same probability of false alarm as before. Finally, in the case of GNSS jamming, the algorithm shows a probability of detection of the jamming attack of about 0.9 with a probability of false alarm equal to 0.03, detecting the jammer in less than 15 s in 80% of the cases.

Moreover, due to the diffuse and pervasive presence of the ADS-B stations used for the crowd sourced network, the proposed method can be used to monitor both the ADS-B and GNSS systems to detect false ADS-B traffic injection, GNSS spoofing, and jamming without the need for new hardware installation. All the ADS-B equipped aircraft together with the ADS-B ground stations can be considered as a global warning network to detect the cyber-attacks, in particular GNSS attacks.

Last, but non least, alarms generated in this contest can be also used to warn all the other users that use the GNSS for other applications.

Author Contributions: M.L. proposed the idea and gave the theoretical support, conceptualizations, and methodology; implemented the algorithm and contributed to the algorithm evaluation. G.S. revised the models, the paper, and the simulation. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors thank the OpenSky Team for providing the data-set.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. SESAR. Available online: http://www.sesarju.eu/ (accessed on 5 January 2021).
2. NEXTGEN. Available online: https://www.faa.gov/nextgen/ (accessed on 5 January 2021).
3. Strohmeier, M. Large-scale Analysis of Aircraft Transponder Data. *IEEE Aerosp. Electron. Syst. Mag.* **2017**, *32*, 42–44.
4. RTCA Inc. *Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance—Broadcast (ADS-B) and Traffic Information Services Broadcast (TIS-B). DO-260B with Corrigendum 1*; RTCA Inc.: Washington, DC, USA, 2011.
5. Strohmeier, M. Security in Next Generation Air Traffic Communication Networks. Ph.D. Thesis, University of Oxford, Oxford, UK, 2016.
6. Sampigethaya, K.; Poovendran, R. Visualization & assessment of ADS-B security for green ATM. In Proceedings of the 29th Digital Avionics Systems Conference, Salt Lake City, UT, USA, 3–7 October 2010.
7. Alghamdi, F.; Alshhrani, A.; Hamza, N. Effective Security Techniques for Automatic Dependent Surveillance-Broadcast (ADS-B). *Int. J. Comput. Appl.* **2018**, *180*. [CrossRef]
8. Yang, H.; Zhou, Q.; Yao, M.; Lu, R.; Li, H.; Zhang, X. A Practical and Compatible Cryptographic Solution to ADS-B Security. *IEEE Internet Things J.* **2018**. [CrossRef]
9. Leonardi, M.; Gregorio, L.D.; Fausto, D.D. Air Traffic Security: Aircraft Classification Using ADS-B Message's Phase-Pattern. *Aerospace* **2017**, *4*, 51. [CrossRef]

10. Strohmeier, M.; Martinovic, I. On Passive Data Link Layer Fingerprinting of Aircraft Transponders. In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy-CPS-SPC'15, Denver, CO, USA, 16 October 2015. [CrossRef]
11. Leonardi, M.; Piracci, E.; Galati, G. ADS-B jamming mitigation: A solution based on a multichannel receiver. *IEEE Aerosp. Electron. Syst. Mag.* **2017**, *32*, 44–51. [CrossRef]
12. Leonardi, M.; Fausto, D.D. ADS-B Signal Signature Extraction for Intrusion Detection in the Air Traffic Surveillance System. In Proceedings of the 26th European Signal Processing Conference (EUSIPCO), Rome, Italy, 3–7 September 2018. [CrossRef]
13. Leonardi, M.; Gerardi, F. Aircraft Mode S Transponder Fingerprinting for Intrusion Detection. *Aerospace* **2020**, *7*, 30. [CrossRef]
14. Leonardi, M.; Maisano, M. Backward Compatible Physical Layer Protocol Evolution for ADS-B Message Authentication. *IEEE Aerosp. Electron. Syst. Mag.* **2020**, *35*, 16–26. [CrossRef]
15. Leonardi, M. ADS-B Anomalies and Intrusions Detection by Sensor Clocks Tracking. *IEEE Trans. Aerosp. Electron. Syst.* **2018**. [CrossRef]
16. Galati, G.; Leonardi, M.; Paciucci, V. Wide area surveillance using SSR mode S multilateration: Advantages and limitations. In Proceedings of the 2nd European Radar Conference EURAD, Paris, France, 3–8 October 2005; pp. 225–229.
17. Leonardi, M.; Piracci, E.; Galati, G. ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions. In Proceedings of the Tyrrhenian International Workshop on Digital Communications—Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV), Rome, Italy, 15–16 September 2014; pp. 41–46. [CrossRef]
18. Leonardi, M.; Piracci, E.G. ADS-B degarbling and jamming mitigation by the use of Blind Source Separation. In Proceedings of the IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), London, UK, 23–27 September 2018. [CrossRef]
19. Leonardi, M.; Strohmeier, M.; Lenders, V. Jamming/Garbling assessment and possible mitigations in the OpenSky network. In Proceedings of the 7th OpenSky Workshop, Zurich, Switzerland, 21–22 November 2019.
20. Leonardi, M.; Strohmeier, M.; Lenders, V. On Jamming Attacks in Crowdsourced Air Traffic Surveillance. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *36*, 44–54. [CrossRef]
21. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**. [CrossRef]
22. Wesson, K.; Rothlisberger, M.; Humphreys, T. Practical Cryptographic Civil GPS Signal Authentication. *J. Znstitute Navig.* **2012**, *59*. [CrossRef]
23. Kerns, A.J.; Wesson, K.D.; Humphreys, T.E. A blueprint for civil GPS navigation message authentication. In Proceedings of the IEEE/ION Position, Location and Navigation Symposium—PLANS, Monterey, CA, USA, 5–8 May 2014. [CrossRef]
24. Magiera, J.; Katulski, R. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *J. Appl. Res. Technol.* **2015**, *13*. [CrossRef]
25. Konovaltsev, A.; Caizzone, S.; Cuntz, M.; Meurer, M. Autonomous Spoofing Detection and Mitigation with a Miniaturized Adaptive Antenna Array. In Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014), Tampa, FL, USA, 8–12 September 2014. [CrossRef]
26. Panice, G.; Luongo, S.; Gigante, G.; Pascarella, D.; Benedetto, C.D.; Vozella, A.; Pescape, A. A SVM-based detection approach for GPS spoofing attacks to UAV. In Proceedings of the 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017. [CrossRef]
27. Mohsen, R.M.; Kenney, J.; Wen, C.H.; Kumar, V.D.; Kaabouch, N. Detection of GPS Spoofing Attacks on Unmanned Aerial Systems. In Proceedings of the 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019. [CrossRef]
28. Mantilla-Gaviria, I.; Leonardi, M.; Galati, G.; Balbastre-tejodor, J. Localization algorithms for multilateration (MLAT) systems in airport surface surveillance. *Signal Image Video Process.* **2015**, *9*, 1549–1558. [CrossRef]
29. Lenardi, M.; Galati, G.; Gasbarra, M. Multiple faults integrity algorithm for mode s multilateration systems. Tyrrhenian International Workshop on Digital Communications. In Proceedings of the Enhanced Surveillance of Aircraft and Vehicles, TIWDC/ESAV 2008, Capri, Italy, 3–5 September 2008.
30. Monteiro, M.; Barreto, A.; Kacem, T.; Wijesekera, D.; Costa, P. Detecting malicious ADS-B transmitters using a low-bandwidth sensor network. In Proceedings of the 2015 18th International Conference on Information Fusion (Fusion), Washington, DC, USA, 6–9 July 2015; pp. 1696–1701.
31. Monteiro, M.; Barreto, A.; Division, R.; Kacem, T.; Carvalho, J.; Wijesekera, D.; Costa, P. Detecting malicious ADS-B broadcasts using wide area multilateration. In Proceedings of the 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), Prague, Czech Republic, 13–17 September 2015; pp. 4A3–1–4A3–12. [CrossRef]
32. Calvo-Palomino, R.; Ricciato, F.; Repas, B.; Giustiniano, D.; Lenders, V. Nanosecond-Precision Time-of-Arrival Estimation for Aircraft Signals with Low-Cost SDR Receivers. In Proceedings of the 2018 17th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), Porto, Portugal, 11–13 April 2018; pp. 272–277. [CrossRef]
33. Mantilla-Gaviria, I.A.; Leonardi, M.; Galati, G.; Balbastre, J.V. Time-difference-of-arrival regularised location estimator for multilateration systems. *IET Radar Sonar Navig.* **2014**, *8*, 479–489. [CrossRef]
34. Mantilla-Gaviria, I.A.; Leonardi, M.; Balbastre, J.V.; de los Reyes, E. On the application of singular value decomposition and Tikhonov regularization to ill-posed problems in hyperbolic passive location. *Math. Comput. Model.* **2013**, *57*, 1999–2008. [CrossRef]
35. Available online: https://www.flightradar24.com(accessed on 5 January 2021).

36. Available online: https://opensky-network.org/(accessed on 5 January 2021).
37. Kalman, R.E. A New Approach to Linear Filtering and Prediction Problems. *J. Basic Eng.* **1960**, *82*. [CrossRef]
38. Bar-Shalom, Y.; Li, X.R.; Kirubarajan, T. *Estimation with Applications to Tracking Navigation*, 1st ed.; John Wiley & Sons: New York, NY, USA, 2001.
39. Kaplan, E.; Hegarty, C.J. *Understanding GPS/GNSS: Principles and Applications*, 3rd ed.; Artech House, Inc.: Boston, MA, USA, 2017.
40. Friis, H. A Note on a Simple Transmission Formula. *Proc. IRE* **1946**, *34*. [CrossRef]
41. Rappaport, T.S. *Wireless Communications Principles and Practice*, 2nd ed.; Prentice Hall: Englewood, NJ, USA, 2002.
42. Poisel, R. *Electronic Warfare Target Location Methods*, 2nd ed.; Artech House: Boston, MA, USA, 2012.
43. Khan, S.; Mohsin, M.; Iqbal, W. On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions. *PeerJ Comput. Sci.* **2021**, *7*, e507. [CrossRef] [PubMed]
44. Koovic, V.D.; Durdevic, Z. Spoofing in aviation: Security threats on GPS and ADS-B systems. *Vojnoteh. Glas.* **2021**, *69*, 461–485. [CrossRef]
45. Schafer, M.; Strohmeier, M.; Leonardi, M.; Lenders, V. LocaRDS: A Localization Reference Data Set. *arXiv* **2020**, arXiv:abs/2012.00116.
46. Papoulis, A.; Pillai, U. *Probability, Random Variables and Stochastic Processes*, 4th ed.; McGraw-Hill: Boston, MA, USA, 2002.