Journal of Advanced Engineering Trends
ISSN : 2682 - 2091

Vol.43, No.1. January 2024

http://jaet.journals.ekb.eg

High Accuracy Next Generation Air Traffic Surveillance System with Potential Cyber-Attacks

Ahmed AbdelWahab Mohamed ElMarady[1] Kamel Hussein Rahouma[2]

[1]Egyptian Civil Aviation Authority, and Faculty of Engineering, Minia University

[2] Professor of Computer Science, Faculty of Engineering, Minia University, Minia, Egypt

**Corresponding author:* ahmedabdelwahab02@yahoo.com

ARTICLE INFO

Article history:
Received:
Accepted:
Online:

Keywords:
Spoofing
Multilateration
Automatic Dependent Surveillance–Broadcast
Cybersecurity
Flight information system

ABSTRACT

Nowadays, there is a crucial need to have an enhanced separation for air traffic to cope with the increase in the flight numbers which requires precise determination of aircraft location. Existing traditional surveillance technologies are not suitable for precise positioning of aircraft, and so, cannot guarantee the requirements for next-generation surveillance systems. Automatic Dependent Surveillance-Broadcast (ADS-B) technology has been used recently to accurately find the position of aircraft. Unfortunately, this new technology suffers from potential cyber-attacks, such as spoofing and jamming. To check the trust of ADS-B data and enhance the position of aircraft, Multilateration /ADS-B data fusion is utilized. Unfortunately, the existing localization verification techniques are not accurately suitable for spoofing detection. Likewise, cryptographic methods that use encryption methods require changing the ADS-B protocol and so, changing the current fleet. In contrast, this paper presents a highly accurate and trusted surveillance framework that accurately detects potential spoofing attacks in ADS-B. Furthermore, the proposed framework uses data fusion of available trusted surveillance sensors, dynamic models of aircraft, and flight information systems to achieve a very accurate surveillance system to be used for next-generation surveillance systems. Our results show that the proposed framework significantly detects the various kinds of spoofing attacks, such as constant/frog-boiling attacks. The localization accuracy of aircraft obtained from our proposed framework is improved by 49% and 49% compared to ADS-B and multilateration, respectively. Furthermore, the detection percentage of constant spoofing and frog-boiling attacks are 97% and 93%, respectively.

1. Introduction

The increasing demand for flights worldwide has recently caused critical air navigation facilities to receive significant attention [1], [2]. To cope with such huge growth in air traffic volume, many concerns have appeared. One of the main concerns is to reduce the minimum separation between aircraft which requires trusted and accurate surveillance systems. To overcome these challenges, the European Union and Federal Aviation Administration have launched Single European Sky Air Traffic Management Research (SESAR) [3] and Next Generation Air Transportation System (NextGen) [4] projects, respectively. In the SESAR and NextGen projects, they use the Automatic Dependent Surveillance–Broadcast (ADS-B) [5] instead of traditional radar surveillance systems, primary and secondary radars [6], [7]. The accuracy in determining aircraft position using ADS-B outperforms primary and secondary radars. Furthermore, the installation and maintenance costs of ADS-B are much lower than traditional radars. ADS-B uses satellite systems and inertial navigation to estimate aircraft position, velocity, and other information followed by broadcasting this information periodically to ground receivers. Unfortunately, ADS-B is exposed to cyber-attacks, such as spoofing and jamming, where security was not considered in the design of the ADS-B system. For example, attackers can modify the trajectory of an aircraft by jamming ADS-B messages and changing them with modified data [1]. By using ADS-B as the main surveillance system with potential cyber-attacks, it may cause a loss of separation between neighboring aircraft and consequently has a catastrophic impact on aviation safety. Many techniques have been proposed to address ADS-B security issues and detect spoofing in ADS-B. Such techniques can be classified into two countermeasures: secure location verification (non-cryptographic) and secure broadcast authentication (cryptographic solutions). In the location verification techniques, the position received from ADS-B is verified with the location received from other independent sources of information. This information could be relevant to Kalman filter [8], distance bounding [9], [10], secondary surveillance radar [11], MLAT [12], Angle of Arrival (AoA) [13], [14], Doppler shift [15], and data fusion of ADS-B, flight model of aircraft, MLAT, and flight information system (FIS) [16]. The aforementioned location verification techniques suffer from problems such as frog-boiling attacks [17], required clock synchronization, or required additional surveillance sensors. Using encryption technologies to detect ADS-B data spoofing should not be applicable where this would violate the original design of ADS-B which includes low-cost design. Additionally, requires changing the avionics of the current fleet. Unlike the existing techniques, our proposed framework aims to have a highly accurate next-generation air traffic surveillance system while mitigating the potential cyber-attacks, such as spoofing and jamming, and without modifying the ADS-B standard. Our proposed framework consists of two components. The first one is the detection of spoofing in ADS-B by comparing the error boundary of aircraft position received from ADS-B and the error boundary of position information received from another independent surveillance sensor. The other independent surveillance sensor could be MLAT, secondary surveillance radar (SSR) or data fusion of MLAT and SSR. MLAT is used mainly in this study as the independent surveillance sensor.

Revised:9 May, 2022, Accepted:25 June , 2022

Tables 1 and 2 show the list of abbreviations and notations used, respectively.

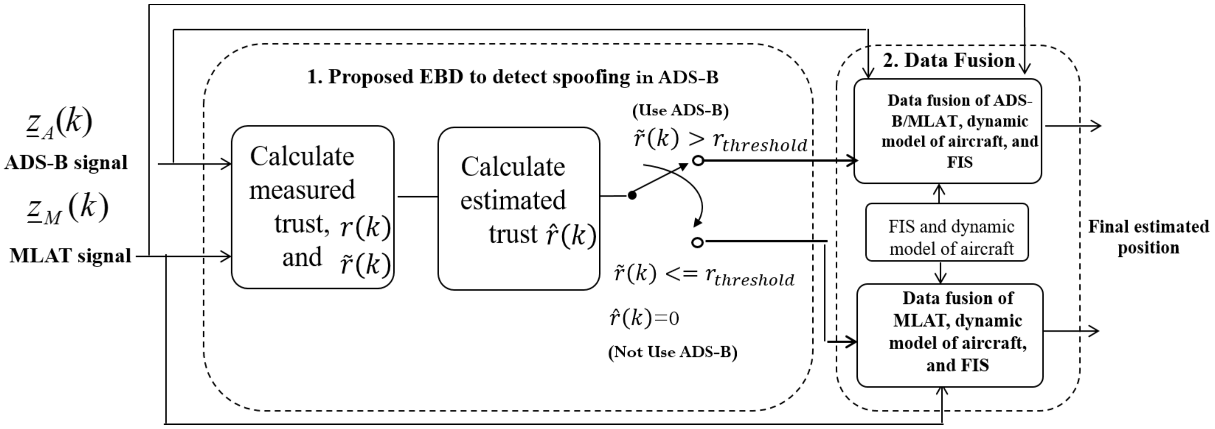

$\underline{z}_A(k)$
ADS-B signal
$\underline{z}_M(k)$
MLAT signal
1. Proposed EBD to detect spoofing in ADS-B
Calculate measured trust, $r(k)$ and $\tilde{r}(k)$
Calculate estimated trust $\hat{r}(k)$
(Use ADS-B)
$\tilde{r}(k) > r_{threshold}$
$\tilde{r}(k) <= r_{threshold}$
$\hat{r}(k)$=0
(Not Use ADS-B)
2. Data Fusion
Data fusion of ADS-B/MLAT, dynamic model of aircraft, and FIS
FIS and dynamic model of aircraft
Data fusion of MLAT, dynamic model of aircraft, and FIS
Final estimated position

Figure 1: Overview of the proposed spoofing detection and data fusion framework.

Table 1. List of abbreviations

Abbreviation	Full term
ADS-B	Automatic Dependent Surveillance–Broadcast
AoA	Angle of Arrival
EBD	Error Boundary Difference
FIS	flight information system
GNSS	global navigation satellite system
IMM	interacting multiple models
MLAT	Multilateration
NextGen	Next Generation Air Transportation System
OWMF	optimal weighting measurement fusion
PSR	primary surveillance radar
SESAR	Single European Sky Air Traffic Management Research
SSR	secondary surveillance radar
TDOA	time difference of arrival
WAM	Wide Area Multilateration

Table 2. Summary of notations used

Symbol	Description
a and b	Weight coefficients
d	The distance between the position determined from ADS-B and MLAT
d'	The distance between the boundaries of error-cubes of ADS-B and MLAT
h_A	The coordinate of the aircraft obtained from ADS-B in the vertical plane
h_M	The coordinate of aircraft obtained from MLAT in the vertical plane
ξ_A	The coordinates of aircraft obtained from ADS-B in horizontal plane
ξ_A	The coordinates of the aircraft obtained from MLAT in the horizontal plane
$\overline{\eta}_A, \overline{\xi}_A, \overline{h}_A$	The exact (error-free) components of aircraft position determined from ADS-B
$\overline{\eta}_M, \overline{\xi}_M, \overline{h}_M$	The exact (error-free) components of aircraft position determined from MLAT
$r(k)$	The calculated trust of ADS-B
$\tilde{r}(k)$	The modified trust of ADS-B
$\hat{r}(k)$	The estimated trust of ADS-B
R_A	Covariance matrix of error obtained from ADS-B
R_M	Covariance matrix of error in MLAT
$r_{threshold}$	the threshold value
σ_A	Standard deviation in the error of ADS-B
σ_M	Standard deviation in the error of MLAT
t	time
$\underline{v}_A$	The noise in the measured position obtained from ADS-B
$\underline{v}_M$	The noise vector of the MLAT
$v_{\eta A}(k), v_{\xi A}(k), v_{hA}(k)$	The noise components of the ADS-B in the three-Cartesian coordinates
$v_{\xi A,max}, v_{\eta A,max}, v_{hA,max}$	The maximum noise components of the ADS-B in the three-Cartesian coordinates
$v_{\eta M}(k), v_{\xi M}(k), v_{hM}(k)$	The noise components of the MLAT in the three-Cartesian coordinates
$v_{\xi M,max}, v_{\eta M,max}, v_{hM,max}$	The maximum noise components of the MLAT in the three-Cartesian coordinates
$\underline{z}_A(k)$	3×1 vector denoting the aircraft position obtained from ADS-B
$\underline{z}_M$	3×1 vector denoting the position of the aircraft obtained from MLAT

The proposed framework can be easily applied to use SSR [33] or other inputs as other independent surveillance sensors. MLAT is commonly used as an explicit surveillance technique or can be established from recently available crowdsourced ADS-B networks, such as FlightRadar24, OpenSky Network, and FlightAware [18]. To detect spoofing, we propose our novel function to check the trust percentage of ADS-B based on Error Boundary Difference (EBD) between ADS-B and MLAT. The percentage of estimated trust of ADS-B ranges from 0 to 100 %, where 100% means that the information obtained from ADS-B is trusted and could be used to further enhance aircraft location, while 0% means that the information obtained from ADS-B is not trusted and could not be used to enhance aircraft location. The second component is the data fusion of the available and trusted surveillance sensors. For the availability of MLAT and ADS-B with no spoofing detected, data fusion of MLAT/ADS-B, flight information, and dynamic model of aircraft is proposed to find the position of aircraft. For availability of MLAT and ADS-B, with spoofing detected in ADS-B, data fusion of dynamic model of aircraft, MLAT, and flight information is proposed to find the position of the aircraft. Fig. 1 shows the overall block diagram of the two components of our proposed framework. The second component, data fusion, is mainly based on our previous work [16] and will not be repeated in this study.

Our results show that our proposed frameworks significantly detect the various types of spoofing attacks, constant and frog-boiling attacks. In addition, our proposed framework can accurately estimate aircraft position with potential jamming or various kinds of spoofing attacks.

The main contributions of this study are as follows:

- Measure the trust percentage of ADS-B data and detect various kinds of spoofing attacks (constant and frog-boiling) using the proposed novel EBD function to check the trust percentage.
- Further enhance aircraft location via the data fusion of the available and trusted surveillance sensors, such that it can be used for next-generation air traffic surveillance system.
- In both spoofing detection and data fusion stages, there is no need to modify ADS-B standard or avionics on aircraft.

The rest of the paper is organized as follows. In Section 2, we present the literature review. In Section 3, we discuss our proposed framework to recognize spoofing in ADS-B. Then, we assess the performance of our proposed frameworks in Section 4, and finally, conclude the paper in Section 5.

2. Literature review

To address cybersecurity in ADS-B, many studies have been proposed. Some methods include cryptographic solutions [19]–[21], while others utilize location verification [14], [15], [22]. Recent techniques have been proposed that use machine learning localization [18], [23]. Cryptographic techniques [19]–[21] utilize encryption algorithms in the communication medium between ADS-B ground sensors and transponders on-board the aircraft. Such methodologies necessitate the participation of an authentication key between the sender and receiver. Unfortunately, the cryptographic techniques require modifying ADS-B protocols and so significant modifications in the aircraft. Location verification techniques can be used to detect spoofing in ADS-B by comparing the position information obtained from ADS-B ground sensors with those determined from other methodologies. The other methodologies could be Kalman filter [8], distance bounding [9], [10], MLAT [12], Angle of Arrival (AoA) [13], [14], Doppler shift [15], and data fusion.

Kalman filter is one of the techniques used to verify the claim received from ADS-B by evaluating the correlation between the ADS-B intent and aircraft flight models [10], [24]. This technique has been proposed mainly to verify the integrity of ADS-B data and not for detecting and mitigating security threats purposes. However, this technique can be used to verify the position claim received by ADS-B. The authors of [8] use the Kalman filter as a correlation technique between aircraft motions and the ADS-B intent. Unfortunately, Kalman filters can be triggered by a so-called frog-boiling attack [17]. In the frog-boiling attack, the attacker jams the original ADS-B data, while continuously sending a light modification in the position of the aircraft. For a gradual and slow change of aircraft position, the Kalman filter will consider the injected information as a valid trajectory of the aircraft.

Another technique used to check the claim received from ADS-B is the distance bounding [9], [10]. In this technique, the position claim received from ADS-B can be correlated with the radiated power and time of flight relevant to the position of the aircraft. This technique uses the fact that electromagnetic waves move at the speed of light. This enables the calculation of a distance on the basis of the time-of-flight between the ADS-B transponder on the aircraft and the ADS-B receiver on the ground. The determined distance is considered an upper bound. When distance-bounding is used by many trusted ADS-B receivers deployed on the ground, it can participate to determine the actual position of the aircraft via trilateration. The authors of [9], [10] use distance bounding to secure multilateration (MLAT) system that can identify false position claims, under ideal assumptions. Furthermore, taking into account received power strength. However, the main concerns in using such techniques in air traffic applications are difficult to resolve. Multilateration is one of the common techniques of cooperative independent surveillance. The aircraft position can be determined if the distance between four or more locations is known. Thus, multilateration requires several receivers in different known locations that receive the same signal from the aircraft transponder at different times. From the time difference of arrival (TDOA), the aircraft position can be determined based on the intersection of the hyperbolas. One of the significant advantages of MLAT is using aircraft avionics that is already in place. In other words, the existing avionics in aircraft will not be changed. The authors of [25], in addition to using MLAT as back-up surveillance, other possible roles for MLAT/WAM were discussed as verification of navigation accuracies such as comparing ADS-B data with multilateration data to verify data accuracy and integrity. Furthermore, it can be used for spoofing detection, where wide-area MLAT systems can be used to identify valid aircraft position reports and the source of spoof transmissions. However, MLAT requires time synchronization and good distribution of ground receivers to achieve good dilution of precision. Some techniques use AoA [13], [14], and Doppler shift [15] to check the trust of ADS-B data. Unfortunately, the proposed techniques that use AoA methods necessitate utilizing sector antennas, while those using Doppler shift depend on the participation of ADS-B sensors on the ground.

Another kind of non-cryptographic method is the data fusion technique. The concept behind using this technique is the best use of the available surveillance sensors, such as primary surveillance radar (PSR), SSR, and MLAT, to check the claim received from ADS-B. The authors of [26] propose the fusion of ADS-B and radar information and indicate that this technique can enhance the tracking quality. The authors of [27] propose a technique to fuse many surveillance techniques, such as PSR, SSR, multilateration, and flight plan information, not mainly for addressing security, but to detect faults generally. Such that this verification technique can be used to know if data received from involved systems operate outside normal parameters. The authors of [28] proposed fusion from multi surveillance sensors, such as ground-based augmentation systems, ADS-B, MLAT, and WAM for improved performance of aircraft position and not for security purposes. Furthermore, the author of [16] proposed the fusion of ADS-B, MLAT, flight information, and dynamic flight model of aircraft for enhancing the accuracy and security of ADS-B using optimal weighting measurement fusion (OWMF) [16], and interacting multiple models (IMM).

Recently, some techniques use machine-learning techniques to estimate the trust of ADS-B data. For example, the authors of [23] proposed a novel machine-learning algorithm that establishes a fingerprint map representing the position of aircraft at each location. Then, it augments the fingerprint map using the previously-stored ADS-B data from the OpenSky network.

3. Proposed methodology to detect spoofing in ADS-B

In this section, the system model is illustrated followed by discussing briefly the surveillance technologies, MLAT [12] and ADS-B [29]. Then, we explain the details of our proposed framework to detect spoofing in ADS-B.

3.1. System Model

In the system model, the ADS-B transponders are equipped on-board aircraft that periodically broadcasts aircraft velocity, position, and other information at frequency 1090 MHZ. The broadcasted information is obtained from the flight management systems deployed on the aircraft using the global navigation satellite system (GNSS) and other on-board sensors. Then, the ADS-B information is received by sensors deployed on the ground which are connected to air traffic monitors to track aircraft. ADS-B information broadcasted from the aircraft transponder to ground receivers is prone to spoofing due to the open nature of ADS-B algorithms. The attacker can intentionally add constant error or gradual increasing error, frog-boiling attack, to the position broadcasted to the ground receivers. Other than ADS-B, multilateration ground sensors are utilized to determine the aircraft's location using the TDOA concept. In the local area of the aerodrome, multilateration is used while Wide Area Multilateration (WAM) is utilized in the en-route phase of flight, as another surveillance technique. MLAT is commonly used as an explicit surveillance technique or can be established from recently available crowdsourced ADS-B networks. ADS-B receivers deployed on the ground can receive ADS-B messages broadcasted from aircraft transponder on the same frequency of MLAT, 1090 MHZ. MLAT is assumed to be more secured than ADS-B where the position of the aircraft is calculated on the ground rather than calculated by other sources. Dynamic flight models of aircraft and flight information systems are used in the data fusion in this study where aircraft typically follow certain routes with specific modes of operation. Furthermore, flight information is typically available in most air navigation systems.

As mentioned before, ADS-B is an accurate surveillance technique that is prone to spoofing due to the open nature of its design. To detect spoofing in the ADS-B sensor, the aircraft position received from ADS-B is verified with the position information received from another independent surveillance sensor. The other independent surveillance sensor could be MLAT, SSR, or data fusion of MLAT and SSR.

3.2. Overview of Multilateration system

MLAT [12] is a surveillance system utilized to determine the aircraft's location by using the TDOA of a signal transmitted out from ADS-B transponders to many ground sensors deployed at various known locations. MLAT system does not require additional avionics where MLAT can participate in using antennas of other systems. The position of aircraft determined from the MLAT system can be written, as follows:

$$\underline{z}_M(k) = [\xi_M(k) \quad \eta_M(k) \quad h_M(k)]^T \qquad (1)$$

where $\underline{z}_M$ is a 3×1 vector denoting the position of the aircraft determined from MLAT. ξ_M and η_M represent the coordinates of aircraft in the horizontal plane; h_M is the coordinate in the vertical plane, at each time step k. Unfortunately, the received location determined from MLAT is prone to noise due to a lack of synchronization among ground MLAT sensors, white noise errors, and propagation effects [30]. Therefore, the position obtained from MLAT is prone to noise, $\underline{v}_M$, where $\underline{v}_M$ is the noise vector of the MLAT which is modeled as Gaussian random noise with zero mean and covariance matrix R_M , i.e., $\underline{v}_M \sim N(0, R_M)$.

3.3. Overview of Automatic Dependent Surveillance–Broadcast system

ADS–B [5] is an aeronautical surveillance system in which an aircraft estimates its location using GNSS and inertial navigation system and then broadcasts this information periodically. Then, the ground receivers received the broadcasted position information. The precision of surveillance using ADS-B is more accurate compared to traditional radars, PSR and SSR, and also the installation cost is much lower than traditional radar systems. The aircraft position received from the ADS-B receiver can be denoted, as follows:

$$\underline{z}_A(k) = [\xi_A(k) \quad \eta(k)_A \quad h_A(k)]^T \qquad (2)$$

where $\underline{z}_A(k)$ is a 3×1 vector denoting the aircraft position obtained from ADS-B. ξ_A, η_A representing the coordinates of the aircraft in the horizontal plane; h_A is the coordinate in the vertical plane, for each time step k.

Unfortunately, the aircraft location determined from ADS-B is prone to noise that can be categorized as unintentional or intentional errors [31]. On one hand, the sources of unintentional errors are GPS jamming, noise in the inertial navigation system, GPS satellite malfunctions, etc. The sources of intentional errors are spoofing, including intentionally transmitting incorrect aircraft data. Therefore, the error in ADS-B is named here as $\underline{v}_A(k)$, where $\underline{v}_A(k)$ is the noise in the measured position in ADS-B which follows Gaussian noise distribution with zero mean and covariance matrix R_A, i.e., $\underline{v}_A(k) \sim N(0, R_A)$.

3.4. Proposed EBD Framework to Detect Spoofing in ADS-B

To detect spoofing in the ADS-B sensor, aircraft position received from ADS-B is judged with the position information received from another independent surveillance sensor. This independent surveillance sensor could be MLAT, SSR, or data fusion of MLAT and SSR. In this paper, MLAT will be used as the surveillance sensor to detect spoofing in ADS-B. MLAT is commonly used as an explicit surveillance technique or can be established from recently available crowdsourced ADS-B networks such as FlightRadar24, FlightAware, and OpenSky Network [18]. Ideally, the position information received from ADS-B is the same as received from the other independent surveillance sensor. Practically speaking, the position information received from ADS-B, SSR, and MLAT suffers from errors, as mentioned earlier. Hence, the position claim received from ADS-B is trusted once the ADS-B position is within the range of the actual position of the other surveillance sensor. In more detail, the position of aircraft received from ADS-B and MLAT can be rewritten in different forms as follow:

$$\eta_A(k) = \overline{\eta}_A(k) + v_{\eta A}(k) \tag{3}$$

$$\xi_A(k) = \overline{\xi}_A(k) + v_{\xi A}(k) \tag{4}$$

$$h_A(k) = \overline{h}_A(k) + v_{hA}(k) \tag{5}$$

$$\eta_M(k) = \overline{\eta}_M(k) + v_{\eta M}(k) \tag{6}$$

$$\xi_M(k) = \overline{\xi}_M(k) + v_{\xi M}(k) \tag{7}$$

$$h_M(k) = \overline{h}_M(k) + v_{hM}(k) \tag{8}$$

where $\overline{\eta}_A$, $\overline{\xi}_A$, $\overline{h}_A$, $\overline{\eta}_M$, $\overline{\xi}_M$ and $\overline{h}_M$ are the exact (error-free) components of aircraft position determined from ADS-B and MLAT sensors, respectively.

To detect spoofing in the ADS-B signal, we consider the worst-case scenario in the comparison between the position determined from ADS-B and MLAT. In the worst-case scenario, we assume maximum error to be used in each dimension for both ADS-B and the other independent surveillance sensor. This error forms an error-cube boundary around the measured position of ADS-B, assuming that the maximum error is the same in each dimension for both ADS-B and MLAT. Fig. 2 shows the measured position of ADS-B and the expected maximum error which forms the error-cube boundary. Also, the same applies to MLAT.

To detect spoofing in ADS-B, we calculate firstly the distance between the position determined from ADS-B and MLAT, d, as follows:

$$d(k) = \sqrt{\left(\xi_A(k) - \xi_M(k)\right)^2 + \left(\eta_A(k) - \eta_M(k)\right)^2 + \left(h_A(k) - h_M(k)\right)^2} \tag{9}$$

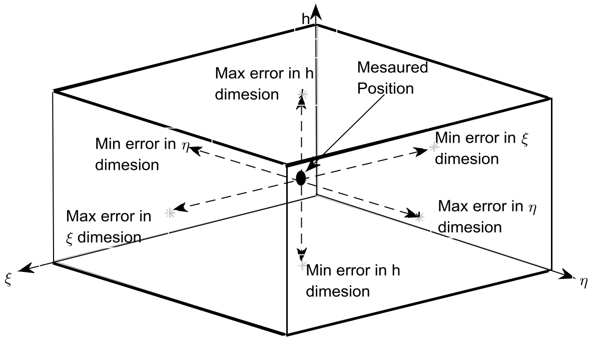


Figure 2: Measured position and it's error-cube envelop.

Secondly, we calculate the distance between the boundaries of error-cubes of ADS-B and MLAT, d'. Then, calculating the relative difference, $\left(d(k) - d'(k)\right)/d(k)$, and percentage of trust of ADS-B, $r(k)$, as follow:

$$r(k) = (1 - \frac{d(k)-d'(k)}{d(k)})X100 \tag{10}$$

For overlapping between error-cubes of ADS-B and MLAT, the relative difference will be a negative value, which means that the ADS-B position is judged to be a trusted source of information. On the other hand, for no overlapping between error-cubes of ADS-B and MLAT, the relative difference will be a positive value. In that case, spoofing is expected in ADS-B. Also, for close boundaries between ADS-B and MLAT, the relative difference will be zero. Where d' is calculated as follows for no-over-lapping between error boundaries:

$$\begin{aligned} d'^2(k) \quad &= \left(\mid \xi_A(k) - \xi_M(k) \mid - \left(v_{\xi A,max} + v_{\xi M,max}\right)\right)^2 \\ &+ \left(\mid \eta_A(k) - \eta_M(k) \mid - \left(v_{\eta A,max} + v_{\eta M,max}\right)\right)^2 \\ &+ \left(\mid h_A(k) - h_M(k) \mid - \left(v_{hA,max} + v_{hM,max}\right)\right)^2 \end{aligned} \tag{11}$$

Where || is the absolute value. Fig. 3 shows an example of three various scenarios of correlation between the positions of ADS-B and MLAT. For more details, Fig. 3a. , Fig. 3b. , and Fig. 3c. show overlapping, no overlapping, and zero overlapping scenarios between the position of ADS-B and MLAT, respectively.

To have a perfect spoofing detection mechanism, the trust percentage should be 100% at normal error levels in ADS-B while 0% at high unexpected error levels in ADS-B. By using the above-mentioned equations to calculate the measured trust of ADS-B, $r(k)$, we can find two issues. The first one is that even if there is a large ADS-B error, the corresponding trust, $r(k)$, is high at some instants. This anomaly in the spoofing detection is due to using the max error boundary in both MLAT and ADS-B. To illustrate this, we insert a high constant error in ADS-B at time t=40 sec with a period of 80 sec, as shown in Fig. 4. Fig. 4 shows the calculated trust, r, with spoofing in ADS-B. As we can see from Fig. 4, around 10% missed in the correct spoofing detection framework while for normal error levels in ADS-B, from time t= 0 to 40 sec, the trust percentage is 100%. To mitigate this issue, we calculate the trust, $\tilde{r}(k)$, based not only on the current values but also using recent history values as follows:

$$\tilde{r}(k) = a[r(k)] + b[r(k-1) + r(k-2) + r(k-3)] \quad (12)$$

Where a and b are weight coefficients. The second issue is that even if there is a high error in ADS-B, the corresponding trust is not zero. In order to have a very low trust at high unexpected error in ADS-B, we apply the following condition to calculate the estimated trust:

$$\hat{r}(k) = \begin{cases} 0 & \tilde{r}(k) <= r_{threshold}, \text{ADS-B is neglected} \\ \tilde{r}(k) & \tilde{r}(k) > r_{threshold}, \text{ADS-B is used} \end{cases}$$
(13)

Where the values of a, b and $r_{threshold}$ will be estimated in the simulation section. Algorithm 1 summarizes the proposed methodology.

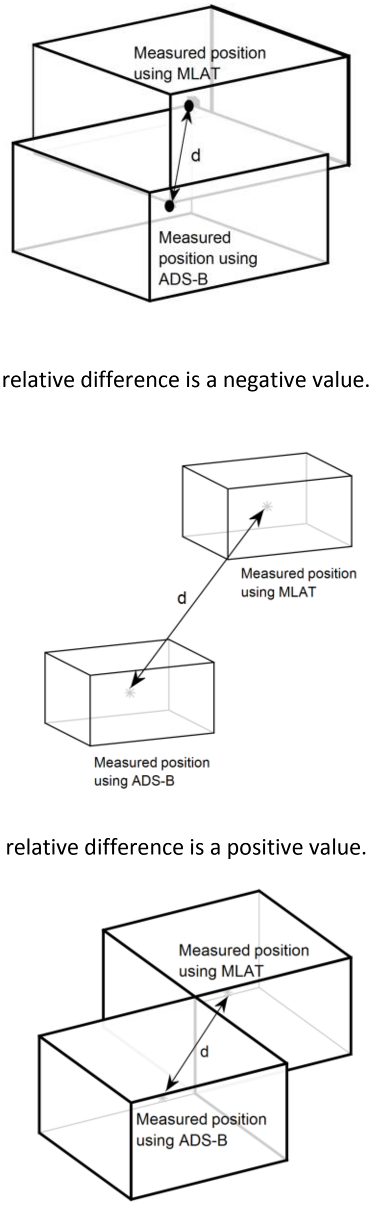
Algorithm 1. Algorithm for the proposed methodology

```
Input position reports received from ADS-B and MLAT, weight coefficients ($a$ and $b$), $r_{threshold}$
For each input report do
    Cal. the distance between the position determined from ADS-B and MLAT, $d$ using eq. 9
    Cal. the distance between the boundaries of error-cubes of ADS-B and MLAT, $d'$ using eq. 11
    Cal. the trust of ADS-B, $r$, given ($d', d$) using eq. 10
    Convert the trust of ADS-B, $r$, into modified trust $\tilde{r}$ given ($a$ and $b$) using eq. 12
    Convert the modified trust of ADS-B, $\tilde{r}$, into estimated trust $\hat{r}$ given ($\tilde{r}$ and $r_{threshold}$) using eq. 13
    If $\hat{r}$ == 0
        ADS-B is not trusted and neglected and the final aircraft position is the output of data fusion of dynamic flight models of aircraft, MLAT, and flight information.
    else
        ADS-B is trusted and the final aircraft position is the output of data fusion of MLAT and ADS-B systems with the integration of the flight information and dynamic flight models of aircraft.
    end if
End for
```

4. Simulation results and analysis

4.1. Simulation Environment

In this section, we evaluate the performance of our proposed framework using Matlab simulations. WAM is utilized in the en-route phase of flights while MLAT is utilized in the local area of the aerodrome [31]. Unlike the positioning accuracy of MLAT which decreases with long distances, the accuracy in determining aircraft position using ADS-B is typically fixed over long distances [27]. Therefore, we follow [28], [31], [32] and consider the ADS-B noise $\underline{v}_A$, modeled as Gaussian distribution with zero mean and standard deviation of 30 m. Furthermore, the error in the position determined from MLAT, $\underline{v}_M$, is modeled as Gaussian distribution with zero mean and standard deviation of 30 m. Position information of aircraft determined by ADS-B is periodically broadcasted every 0.5 sec [33]. For reducing the simulation time and correspond to the update rate of the MLAT which is one second [33], we assume that the update rate of ADS-B is also one second, without loss of generality. The values of $r_{threshold}$, a and b are set to be 99.3%, 0.4 and 0.2 to achieve minimum error. To have a stable estimate of the results, Monte Carlo technique [16] is used in calculating the reported results for 1000 times.

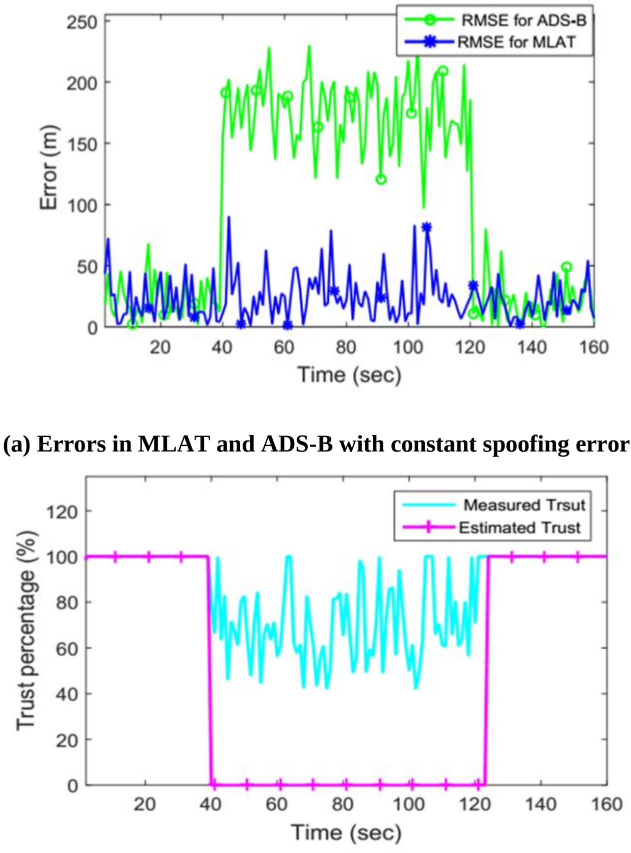

Measured position using MLAT
d
Measured position using ADS-B
Measured position using MLAT
d
Measured position using ADS-B
Measured position using MLAT
d
Measured position using ADS-B

(a) relative difference is a negative value.

(b) relative difference is a positive value.

(c) relative difference is zero.

Figure. 3 Illustration of different values of the relative difference between the error-cubes of ADS-B and MLAT.



(a) Errors in MLAT and ADS-B with constant spoofing error.

(b) Measured and estimated trust.

Figure 4: Illustration of measured and estimated trust of ADS-B.

4.2. The Impact of the Maximum Error Boundary of Surveillance Sensor

As mentioned earlier, for detection of spoofing in ADS-B information, we consider the maximum expected position error in both ADS-B and the other independent surveillance sensor, MLAT in this experiment. In order to set the best maximum error, we simulate our proposed framework at different values of the maximum error with different values of the error in ADS-B for aircraft moving at 100 m/sec. In this experiment, we assume that $\upsilon_{\eta A,max}= 1\sigma_A$, $2\sigma_A$ and $3\sigma_A$ and $\upsilon_{\eta M,max}= 1\sigma_M$, $2\sigma_M$ and $3\sigma_M$. Where σ_A and σ_M are the standard deviation of the noise covariance in ADS-B and MLAT respectively. Fig. 5 shows the trust of ADS-B, r, at different values of the maximum error boundary, as a function of the error in ADS-B. As we can see from Fig. 5, for normal error levels in ADS-B, the trust of ADS-B is 100% at max expected error of $2\sigma_A$ and $3\sigma_A$ while the trust is less than 100% at $1\sigma_A$.

And so, setting the max expected error to $1\,\sigma_A$ is not satisfactory. As the error in ADS-B increases more than the normal error level, the trust of ADS-B decreases at $2\sigma_A$ than $3\sigma_A$. Hence, the best-expected max error is set to be $2\sigma_A$ to have 100% trust at the normal error level in ADS-B and low trust at large error in ADS-B than the normal error levels.

4.3.Impact of the Constant Spoofing Attack in ADS-B on the Performance of our Proposed Framework

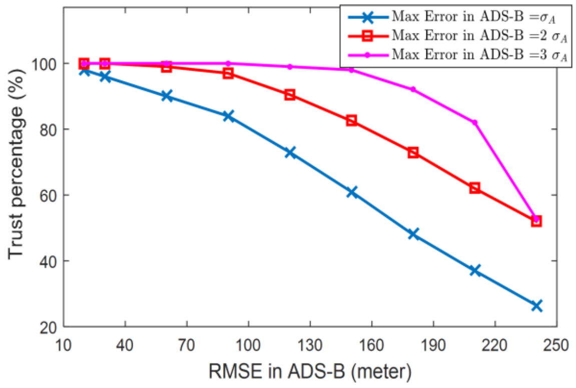
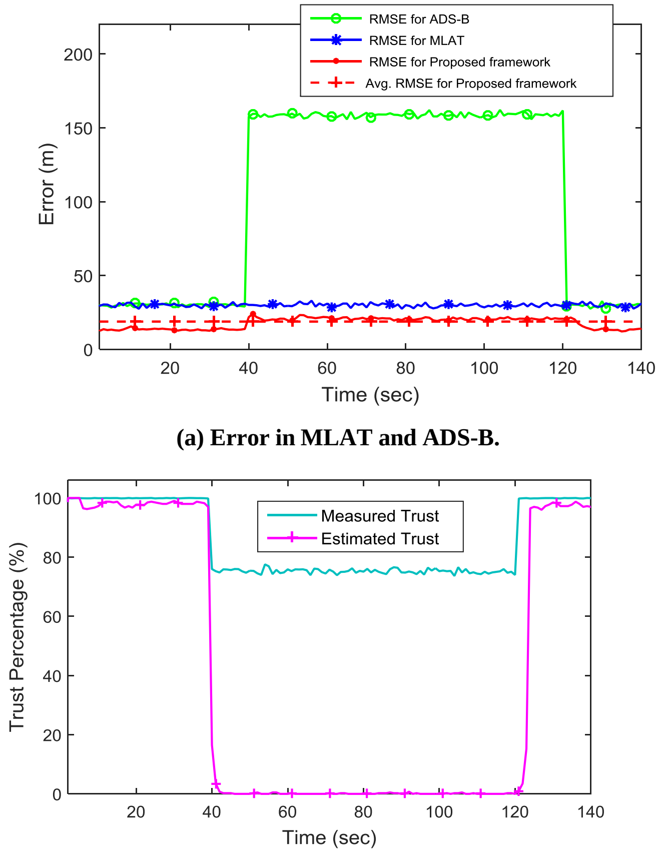


Figure 5: Illustration of trust at various values of maximum error.

In this section, we demonstrate the performance of our proposed spoofing detection framework in the scenario of a constant spoofing attack. In this scenario, we assume that the attacker adding a constant error in the position received from ADS-B. In order to achieve that, we insert a constant error in ADS-B at time t=40 sec with a period of 80 sec. Fig. 6 shows the measured trust, estimated trust, and the error of the estimated position determined from MLAT, and ADS-B. As we can see from Fig. 6, for normal error levels in ADS-B, from time t=0 to 40 sec and from t=120 to 140 sec, there is no spoofing detected in ADS-B and the measured trust is 100% while the estimated trust is slightly less than 100%. Then the estimated position received from our proposed framework is the data fusion of MLAT, ADS-B, dynamic flight models of aircraft, and flight information. In that case, the average RMSE of our proposed data fusion framework is 15.3 meters which improve the aircraft position by 49% and 49% more than MLAT and ADS-B, respectively. On the other hand, the error of the position received from ADS-B from time t=40 sec to 120 sec, is higher than the normal ADS-B error, 160 meters in this experiment. The corresponding measured average trust of ADS-B, r, sharply decreases from 100% to 80% while the average estimated trust sharply decreases from 100% to almost zero. For these very small values of the estimated trust, the position information received from ADS-B is neglected. As shown in Fig. 6, the detection percentage of constant spoofing attacks is 97%. Then the estimated position received from our proposed framework is the data fusion of dynamic flight models of aircraft, MLAT, and flight information. In that case, the average RMSE of our proposed data fusion framework is 20.2 meters which is lower than using MLAT only (30 meters) by 33%.

4.4. Impact of the Frog-Boiling Spoofing Attack in ADS-B on the Performance of our Proposed Framework

In this section, we demonstrate the performance of our proposed spoofing detection framework in the scenario of a frog-boiling attack. In the frog-boiling attack scenario, the attacker continuously adds a small error in the position determined by ADS-B.

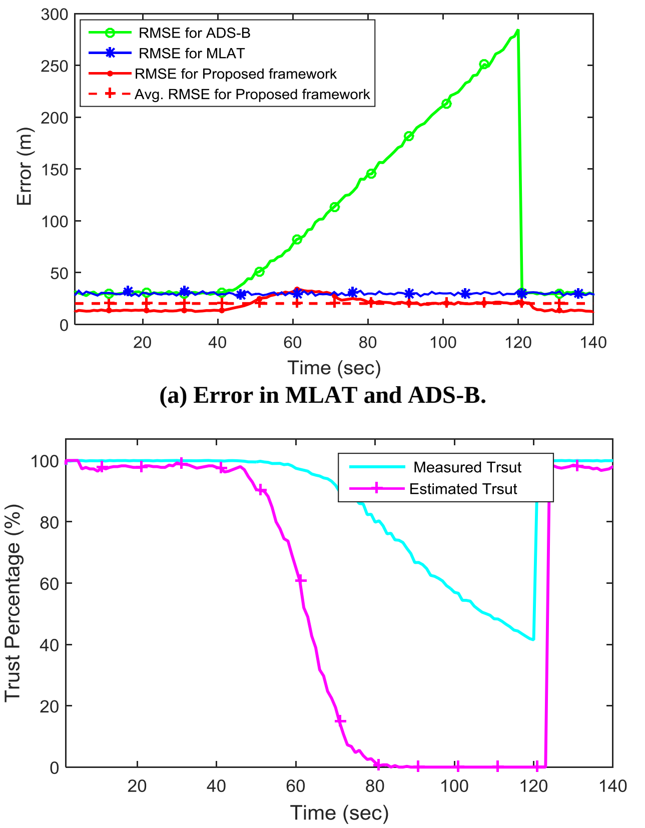


(a) Error in MLAT and ADS-B.

(b) Measured and estimated trust.

Figure 6: Impact of constant spoofing attack in ADS-B

This added error is small enough to detect an anomaly in ADS-B where the measured trust is within the acceptable values. In other words, the attacker disrupts the position information received from ADS-B while consistently operating within the threshold of trust. In order to demonstrate that, we intentionally insert a gradual error in ADS-B from time t=40 sec to time t=120 sec with a step error of 3.34 meters approximately. Fig. 7 shows the measured trust, estimated trust, the error of the calculated position determined from ADS-B and MLAT, and our proposed ADS-B/MLAT framework. As we can see from Fig. 7, the error of the position received from ADS-B is gradually increased from the normal ADS-B error to approximately 280 meters in this experiment. The corresponding average measured trust of ADS-B slowly decreases with the gradual increase in the ADS-B error while the average estimated trust decreases more sharply and then closes to zero at RMES of 140 m. From time t=40 sec to 80 sec, the error in ADS-B is not enough for spoofing to be clearly detected where condition $\tilde{r}(k) > r_{threshold}$ is applied and the position information received from ADS-B is still used. The position error of our data fusion framework increases up to the error level of MLAT. Starting from time t=85 sec to t=120 sec, the estimated trust is zero where condition $\tilde{r}(k) <= r_{threshold}$ is applied and the position information received from ADS-B is neglected. As shown in Fig. 7, the detection percentage of frog-boiling spoofing attacks is 93%.



(a) Error in MLAT and ADS-B.

(b) Measured and estimated trust.

Figure 7: Impact of Frog-Boiling spoofing attack.

Then the estimated position received from our proposed framework is the data fusion of MLAT and flight information. In that case, the RMSE of our proposed data fusion framework is 20.2 meters which is lower than using MLAT only (30 meters) by 33%.

5. Conclusions

In this paper, we proposed a high accurate surveillance framework with potential cyber-attacks in ADS-B. To achieve these targets, we proposed a comprehensive framework to detect spoofing in ADS-B and mitigate the consequences of potential jamming and spoofing attacks. For detection of spoofing in ADS-B, we proposed a novel EBD function via verification of the error boundary of ADS-B with other surveillance sensors. The accuracy of our proposed spoofing detection framework achieved good results in various scenarios of attack like constant and frog-boiling attacks. In more detail:

- For normal error levels in ADS-B reports (trusted ADS-B data), the estimated aircraft position received from our proposed framework data fusion is the data fusion of MLAT and ADS-B systems with the integration of the flight information and dynamic flight models of aircraft. Then, the average RMSE of our proposed data fusion framework is 15.3 meters which improve the aircraft position by 49% and 49% more than MLAT and ADS-B, respectively.

- For constant spoofing attacks, the detection percentage of constant spoofing attacks is 97%. Then the estimated position received from our proposed framework is the data fusion of dynamic flight models of aircraft, MLAT, and flight information. In that case, the average RMSE of our proposed data fusion framework is 20.2 meters which is lower than using MLAT only (30 meters) by 33%.
- For frog-boiling attacks, the detection percentage of attack is 93%. Then the estimated position received from our proposed framework is the data fusion of MLAT and flight information. In that case, the RMSE of our proposed data fusion framework is 20.2 meters which is lower than using MLAT only (30 meters) by 33%.

Therefore, the proposed technique guarantee the specifications of next-generation surveillance systems.

References

[1] A. A. Elmarady and K. Rahouma, Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment, IEEE Access, vol. 9, pp. 143997–144016, 2021, doi: 10.1109/ACCESS.2021.3121230.

[2] "IATA forecasts passenger demand to double over 20 years." www.iata.org/passenger-forecast.

[3] T. Bolić and P. Ravenhill, SESAR: The Past, Present, and Future of European Air Traffic Management Research, Engineering, vol. 7, no. 4, pp. 448–451, 2021, doi: https://doi.org/10.1016/j.eng.2020.08.023.

[4] J. Post, The Next Generation Air Transportation System of the United States: Vision, Accomplishments, and Future Directions, Engineering, vol. 7, no. 4, pp. 427–430, 2021, doi: https://doi.org/10.1016/j.eng.2020.05.026.

[5] J. Sun, X. Olive, M. Strohmeier, M. Schäfer, I. Martinovic, and V. Lenders, OpenSky Report 2021: Insights on ADS-B Mandate and Fleet Deployment in Times of Crisis, in 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), 2021, pp. 1–10, doi: 10.1109/DASC52595.2021.9594361.

[6] G. Minteuan, T. Palade, E. Puschita, P. Dolea, and A. Pastrav, Monopulse Secondary Surveillance Radar Coverage–Determinant Factors, Sensors, vol. 21, no. 12, p. 4198, 2021.

[7] I. Obod, I. Svyd, O. Maltsev, G. Zavolodko, D. Pavlova, and G. Maistrenko, Fusion the coordinate data of airborne objects in the networks of surveillance radar observation systems, in Data-Centric Business and Applications, Springer, 2021, pp. 731–746.

[8] M. Leonardi and G. Sirbu, ADS-B Crowd-Sensor Network and Two-Step Kalman Filter for GNSS and ADS-B Cyber-Attack Detection, Sensors, vol. 21, no. 15, p. 4992, 2021.

[9] J. T. Chiang, J. J. Haas, and Y.-C. Hu, Secure and precise location verification using distance bounding and simultaneous multilateration, in Proceedings of the second ACM conference on Wireless network security, 2009, pp. 181–192.

[10] V. Fox, J. Hightower, L. Liao, D. Schulz, and G. Borriello, Bayesian filtering for location estimation, IEEE Pervasive Comput., vol. 2, no. 3, pp. 24–33, 2003, doi: 10.1109/MPRV.2003.1228524.

[11] J. Ni, L. Chen, S. Yu, and A. Luo, Analysis and Application of Spaceborne Mode S and ADS-B Data Fusion, in 2021 International Conference on Big Data Engineering and Education (BDEE), 2021, pp. 51–55.

[12] P. Zhong, Z. Zhu, and Y. Liu, Coverage Analysis of MLAT Receiver Based on Decoding ADS-B message, in 2021 IEEE 3rd International Conference on Civil Aviation Safety and Information Technology (ICCASIT), 2021, pp. 158–161.

[13] C. Reck, M. S. Reuther, A. Jasch, and L.-P. Schmidt, Verification of ADS-B positioning by direction of arrival estimation, Int. J. Microw. Wirel. Technol. 4.2 S. 181-186. 29.04. 2013, 2012.

[14] J. Naganawa, H. Tajima, H. Miyazaki, T. Koga, and C. Chomel, ADS-B anti-spoofing performance of monopulse technique with sector antennas, in 2017 IEEE Conference on Antenna Measurements & Applications (CAMA), 2017, pp. 87–90.

[15] N. Ghose and L. Lazos, Verifying ADS-B navigation information through Doppler shift measurements, in 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), 2015, pp. 4A2-1.

[16] A. A. W. El Marady, Enhancing accuracy and security of ADS-B via MLAT assisted-flight information system, in 2017 12th International Conference on Computer Engineering and Systems (ICCES), 2017, pp. 182–187.

[17] I. Stylios, A. Skalkos, S. Kokolakis, and M. Karyda, BioPrivacy: Development of a Keystroke Dynamics Continuous Authentication System, in Proceedings of the 5th International Workshop on SECurity and Privacy Requirements Engineering SECPRE, Online, 2021, pp. 4–8.

[18] M. Strohmeier, I. Martinovic, and V. Lenders, A k-NN-based localization approach for crowdsourced air traffic communication networks, IEEE Trans. Aerosp. Electron. Syst., vol. 54, no. 3, pp. 1519–1529, 2018.

[19] K. Jansen, L. Niu, N. Xue, I. Martinovic, and C. Pöpper, Trust the Crowd: Wireless Witnessing to Detect Attacks on ADS-B-Based Air-Traffic Surveillance, in Proceedings of the Network and Distributed System Security Symposium (NDSS), 2021, pp. 21–25.

[20] F. Hasin, T. H. Munia, N. N. Zumu, and K. A. Taher, ADS-B based air traffic management system using ethereum blockchain technology, in 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), 2021, pp. 346–350.

[21] A. Asari, M. R. Alagheband, M. Bayat, and M. R. Asaar, A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems, Comput. Networks, vol. 185, p. 107599, 2021.

[22] M. Schäfer, P. Leu, V. Lenders, and J. Schmitt, Secure motion verification using the doppler effect, in Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 2016, pp. 135–145.

[23] A. A. ELMARADY and K. RAHOUMA, Actual TDoA-based augmentation system for enhancing cybersecurity in ADS-B, Chinese J. Aeronaut., 34(2): 217–228, 2020. doi.org/10.1016/j.cja.2020.05.026.

[24] J. Krozel, D. Andrisani, M. Ayoubi, T. Hoshizaki, and C. Schwalm, Aircraft ADS-B Data Integrity Check. 2004.

[25] A. Smith, R. Cassell, T. Breen, R. Hulstrom, and C. Evers, Methods to Provide System-Wide ADS-B Back-Up, Validation and Security, in 2006 ieee/aiaa 25TH Digital Avionics Systems Conference, 2006, pp. 1–7, doi: 10.1109/DASC.2006.313681.

[26] O. Baud, N. Honore, and O. Taupin, Radar / ADS-B data fusion architecture for experimentation purpose, in 2006 9th International Conference on Information Fusion, 2006, pp. 1–6, doi: 10.1109/ICIF.2006.301555.

[27] W. Liu, J. Wei, M. Liang, Y. Cao, and I. Hwang, Multi-Sensor Fusion and Fault Detection using Hybrid Estimation for Air Traffic Surveillance, IEEE Trans. Aerosp. Electron. Syst., vol. 49, no. 4, pp. 2323–2339, 2013, doi: 10.1109/TAES.2013.6621819.

[28] T. Cho, C. Lee, and S. Choi, Multi-Sensor Fusion with Interacting Multiple Model Filter for Improved Aircraft Position Accuracy, Sensors , vol. 13, no. 4. 2013, doi: 10.3390/s130404122.

[29] J. A. Besada, J. Garcia, G. De Miguel, F. J. Jimenez, G. Gavin, and J. R. Casar, Data fusion algorithms based on radar and ADS measurements for ATC application, in Record of the IEEE 2000 International Radar Conference [Cat. No. 00CH37037], 2000, pp. 98–103, doi: 10.1109/RADAR.2000.851812.

[30] G. de M. Vela, J. B. Portas, and J. G. Herrero, Correction of propagation errors in Wide Area Multilateration systems, in 2009 European Radar Conference (EuRAD), 2009, pp. 81–84.

[31] M. Strohmeier, V. Lenders, and I. Martinovic, On the Security of the Automatic Dependent Surveillance-Broadcast Protocol, IEEE Commun.

Surv. Tutorials, vol. 17, no. 2, pp. 1066–1087, 2015, doi: 10.1109/COMST.2014.2365951.

[32] J. ZHANG, W. LIU, and Y. ZHU, Study of ADS-B Data Evaluation, Chinese J. Aeronaut., vol. 24, no. 4, pp. 461–466, 2011, doi: https://doi.org/10.1016/S1000-9361(11)60053-8.

[33] I. C. A. Organization, Guidance Material on Comparison of Surveillance Technologies (GMST), International Civil Aviation Organization (ICAO). Asia and Pacific Office, Bangkok, Thailand, 2007.