Hindawi
Security and Communication Networks
Volume 2019, Article ID 8936784, 11 pages
https://doi.org/10.1155/2019/8936784

Research Article

Multidevice False Data Injection Attack Models of ADS-B Multilateration Systems

Fute Shang, Buhong Wang, Fuhu Yan, and Tengyao Li

School of Information and Navigation, Air Force Engineering University, Xi'an, Shanxi, China

Correspondence should be addressed to Buhong Wang; wbhyl@aliyun.com

Received 11 September 2018; Revised 12 December 2018; Accepted 14 January 2019; Published 3 March 2019

Academic Editor: Stefan Katzenbeisser

Location verification is a promising approach among various ADS-B security mechanisms, which can monitor announced positions in ADS-B messages with estimated positions. Based on common assumption that the attacker is equipped with only a single device, this mechanism can estimate the position state through analysis of time measurements of messages using multilateration algorithm. In this paper, we propose the formal model of multidevice false data injection attacks in the ATC system against the location verification. Assuming that attackers equipped with multiple devices can manipulate the ADS-B messages in distributed receivers without any mutual interference, such attacker can efficiently construct attack vectors to change the results of multilateration. The feasibility of a multidevice false data injection attack is demonstrated experimentally. Compared with previous multidevice attacks, the multidevice false data injection attacks can offer lower cost and more covert attacks. The simulation results show that the proposed attack can reduce the attackers' cost by half and achieve better time synchronization to bypass the existing anomaly detection. Finally, we discuss the real-world constraints that limit their effectiveness and the countermeasures of these attacks.

1. Introduction

With the rapid development of air transportation, the surveillance technology of air traffic control is gradually evolving from primary surveillance radar technology to higher precision and lower cost Automatic Dependent Surveillance-Broadcast (ADS-B) [1] technology. ADS-B provides surveillance data to support mission-critical automatic and human decisions in the next generation ATC system to increase safety of air traffic. The aircraft equipped with ADS-B transmitter can broadcast plain text of the aircraft position retrieved from their onboard GPS receiver. The messages then are received by ground or airborne ADS-B receiver and displayed on the screens of controllers and pilots [2]. However, due to the fact that ADS-B technology did not consider the security problem comprehensively [3, 4] at the design stage, it is vulnerable to multiple wireless threats [5]. The false data injection attack can be injected into the monitoring system by low cost software defined radio equipment, which can interfere with the work of the controllers and even cause safety problems.

In order to improve protection against the ADS-B false data injection attack, a variety of location verification schemes have been proposed. At present, multilateration technology [6, 7] has been widely used [8]. The advantage of this technology is that it can reduce the cost of deployment by using the existing secondary surveillance radar and ADS-B systems. Given the precise distance between transmitter and four receivers, it is easy to calculate the position of the transmitter, that is, the position of the aircraft [9]. Finally, by comparing the location of the aircraft and the position information in the ADS-B message, it is possible to verify whether the ADS-B message is legitimate and effectively improves the capability of detecting the false data injection attack.

Existing multilateration techniques can effectively detect attackers using a single transmitter, but did not consider the multidevice attack scenario [10]. In this scenario, the attacker uses multiple transmitters distributed in different geographic locations to transmit a ADS-B message that is constructed ingeniously under a specific time delay, controlling the time of receivers to receive the signal, making the location multilateration calculated the same as the location of the attacker's injection, thus bypassing the multilateration verification and injection of large number of false ADS-B data. We call this new attack pattern multidevice false data injection attack.

Moser et al. [11] first proposed the multidevice false data injection attack of ADS-B multilateration system in ATC surveillance. However, Moser et al. simulate the arrival time of the real transmitter without utilizing the characteristics of the multilateration algorithm. The attacker needs to use the identical number of transmitters and receivers to make the attack success, which increases the cost of an attack. Secondly, as the transmitters are deployed in a large area, it is difficult to realize time synchronization, which makes it possible to be detected by other detection methods based on frequency and phase. Therefore, we consider how to find a better attack scheme, using less attacker transmitters to realize the attack and make the distance between the transmitters within a certain range to effectively realize the time synchronization between the transmitters.

In this paper, we propose a more accurate model of multidevice attacker for multilateration algorithm which utilizes less transmitters and centralized deployment of the antennas to achieve the attack and overcome the shortcomings mentioned earlier. Finally, we propose possible countermeasures for this kind of attack. The main contributions of this article are as follows:

(1) We establish the formal model of ADS-B multilateration system and multidevice false data injection attack.

(2) We proposed the best attack scheme calculation method.

(3) We demonstrate the feasibility of multidevice false data injection attack method.

In Section 2 we introduce the ADS-B system security and multilateration technology. In Section 3 we describe the ADS-B multilateration system and the multidevice false data injection attacker model and find out the requirements of the false data injection attack. In Section 4 we give the implementation of the model and the example validation. Possible countermeasures for this kind of attack are discussed in Section 5 and we conclude in Section 6.

2. Background and Related Work

At present, researchers have proposed a variety of false data injection attacks against ADS-B systems, but most of these attacks can be detected by ADS-B location verification based on multilateration.

2.1. ADS-B Attack Patterns. The ADS-B transmitters emit the ADS-B messages in the signal format specified by the ADS-B protocol standard DO-260 [12], DO-260A [13], and DO-260B [14], and these messages are not encrypted. The characteristics of wireless communication allow attackers easily interference, eavesdrop, and modify, inject, and delete ADS-B messages [15].

2.1.1. Ghost Aircraft Inject. Based on the false data injection attack, the attacker is able to broadcast the ADS-B message generated by the ghost aircraft that does not exist in the surveillance system. The target may be any legitimate ADS-B receiver. When the visibility is low, the ghost aircraft may be confused with legitimate aircraft and the ground air traffic controller may force the aircraft to land or change the track. In the same way, for aircraft targets, the attacker can also make the ADS-B based collision avoidance system generate error instructions. In the case of low visibility, the pilot may perform dangerous operations based on these instructions.

2.1.2. Aircraft Flood Denial. Based on the above ghost aircraft injection attack, the aircraft flood denial attack can inject multiple aircraft simultaneously. The purpose of the attack is to enable the air traffic controller's surveillance system to deny of service. Due to the fact that the air traffic controllers confused real aircraft with ghost aircraft, the surveillance system is defeated.

2.1.3. Virtual Trajectory Modification. The purpose of this attack is to modify the trajectory of real aircraft. First delete all location reports of the target aircraft, and inject modified messages. This attack takes advantage of the low precision of other surveillance technologies, such as the first radar. When the central processing station (CPS) fuses the radar data and ADS-B data, a certain error is allowed. If the distance between the real aircraft position and injected position is very small, the attack will be able to bypass the detection technology and lead to the wrong judgment or response to the collision avoidance system.

2.1.4. False Alarm Inject. Similar to the virtual trajectory modification attack, attackers delete the messages generated by real aircraft and inject false ADS-B messages for alarm. ADS-B provides emergency (such as hijacking) alarm mechanism. False alarm injection attack will lead to an emergency response mechanism, such as a refusal of landing requests. Due to the fact that voice recognition is not reliable in hijacking events, it is difficult to detect such attacks at the physical level.

If an attacker uses a single transmitter to attack, all of the attacks above will result in multilateration results that are not consistent with the ADS-B report location, which will be detected easily.

2.2. Existing Countermeasures. According to the review article by Strohmeier et al. [16], ADS-B protection technology is mainly divided into two categories: secure broadcast authentication [17] and secure location verification [18] technology.

2.2.1. Secure Location Verification Technology. It can identify abnormal ADS-B messages after the attack has launched and then filter them out. Various characteristics of wireless signal are extracted to locate the position of the aircraft, such as receiving signal strength, angle of arrival, frequency of arrival, time of arrival (TOA), and time difference of arrival (TDOA). The location estimation method using angle of arrival is called triangulation, and the one using time of arrival is called multilateration [19].

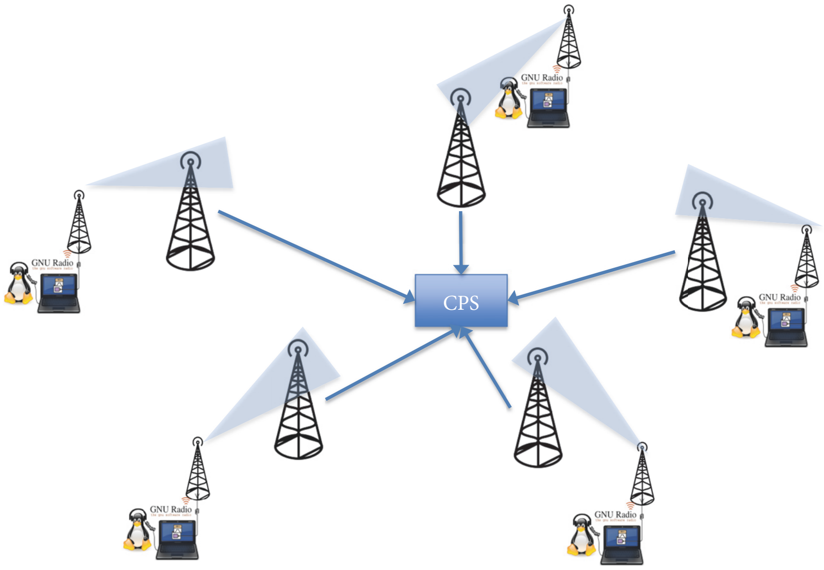


Figure 1: Single-to-single multidevice false data injection attack model.

The advantage of multilateration technology is that it can reuse existing ADS-B devices without any modification to airborne equipment. Multilateration can easily detect the false data injection attack and even locate the position of the attacker transmitter. The central processing station utilizes time difference of arrival of the same messages from different ADS-B receivers to calculate the location of the ADS-B transmitter and compares it with the position information in the ADS-B message. The legitimate ADS-B message with allowed position error will be passed to the Air Traffic Control Center [20] to manage the air traffic.

At present, multilateration technology is widely used in ground location verification. It is used by the ASDE-X system [21] at airports and the Wide Area Multilateration [22, 23]. Although multilateration technology has been widely applied, there are still many problems [24]. For example, it is difficult to estimate altitude information accurately based on ground based receiver. Besides, multilateration technology also needs many receivers to receive the same signal accurately, and all receivers are connected with the central processing station safely.

And we should notice that crowdsourcing is a well-established paradigm in the commercial air traffic tracking domain [25]. Volunteers around the world set up and operate large numbers of receivers for transponder signals and send the live tracking data to a central server via the Internet. This approach has been used to improve the security in GPS [26].

2.2.2. Secure Broadcast Authentication Technology. It is to prevent attacks through the authentication mechanism, which falls into two categories, the noncryptographic schemes on the physical layer and cryptographic schemes. Here we focus on physical layer based technology, which is to find differences between legitimate and nonlegitimate packets based on characteristics of the wireless channel which are hard to replicate.

There are various approaches of physical layer based technology, such as approaches based on received signal strength (RSS, [27, 28]), based on frequency offset caused by imperfections in the transmitters synchronization [11], or based on the carrier phase (e.g., [29]). While these methods can effectively defeat jamming and modification attacks, the inherently lower performance makes them difficult to use in a large-scale system such as ADS-B.

2.3. Multidevice Attack. The above security countermeasures are based on the attacker model of single transmitter, but ignore the scenario of multiple transmitters. With the development of software defined radio equipment, the cost of attackers using multiple transmitters is getting lower and lower. Therefore, the multilateration system with outdated attack models may be unsafe, and a new attack model is needed to study its security [30].

In the multidevice attack proposed by Moser et al., a low-power, small covering radius transmitter is set near each receiver to transmit the signal to ensure that the signal is only injected into the nearest receiver, as shown in Figure 1. Under this configuration, the attacker transmitter can easily control the time delay between transmissions, making the arrival time at each receiver identical to the arrival time generated from the ghost aircraft. As a consequence, the multilateration calculated location is consistent with the position encoded in the malicious ADS-B message, and the attacker bypasses the location verification successfully. However, there are still some shortcomings in this type of attack:

(1) The transponder needs to be near the receiver, once found easy to destroy.

(2) This attacker needs to have the same number of transponders as ADS-B receivers. SDR platforms have different transient phase feature, which is easy to be detect. While high-end arbitrary waveform generators might be able to produce highly accurate signals with little noise in the transient phase, they are by a factor of 20 to 100 times more expensive than today's SDR platforms and would require a prohibitively high budget on the attacker's side since a distributed attack requires at least a couple of such devices.

(3) In practice, it is difficult to synchronize the local oscillators of different devices that are separated over large distance, which make it easy to be detected by frequency based detection methods.

Based on these features, Moser et al. have built ATC intrusion detection system to detect this kind of attack. Therefore, we consider how to find a better attack scheme, using less attacker transmitters to realize the attack and make the distance between the transmitters within a certain range to effectively realize the time synchronization between the transmitters.

3. Multidevice Attack Model of ADS-B Multilateration System

Next, we will establish the mathematical model of the ADS-B multilateration system, find out the requirements to implement the false data injection attack, and finally establish the model of the multidevice false data injection attack.

3.1. ADS-B Multilateration System Model

Definition 1 (ADS-B multilateration system). The ADS-B multilateration system can be defined as a tuple:

$$\mathbf{S} = \left\langle \mathbf{P}^S, \mathbf{X}, \mathbf{Z}^g, \mathbf{Z}^m \right\rangle \tag{1}$$

Suppose we use K ADS-B receivers for multilateration, and the coordinates of these receivers are represented by the $K \times 3$ matrix $\mathbf{P}^S = \{s_{i,j}\}$.

$$\mathbf{P}^S = \begin{bmatrix} s_{11} & s_{12} & s_{13} \\ s_{21} & s_{22} & s_{23} \\ \vdots & \vdots & \vdots \\ s_{K1} & s_{K2} & s_{K3} \end{bmatrix} \tag{2}$$

P_k^S is the position of kth receiver:

$$\mathbf{P}_k^S = \begin{bmatrix} s_{k1} & s_{k2} & s_{k3} \end{bmatrix} \tag{3}$$

$\mathbf{X}$ is the real position of aircraft i, $\mathbf{Z}^g = \{\mathbf{z}_{ij}^g\}$ is the position of aircraft i decoded from the ADS-B message by the receiver j, and $\mathbf{Z}^m = \{\mathbf{z}_{ij}^m\}$ is the time when receiver j received the ADS-B message from aircraft i.

ADS-B multilateration system can estimate transmitter location through multiple receiver's TDOA of the same ADS-B message. Therefore, the receivers need precise time synchronization. The TDOA based multilateration algorithm generally assumes that the error is determined by the Gauss distribution. Given the TDOA of receivers, the least square algorithm is applied to find the optimal estimation of the position of the aircraft.

Definition 2 (location estimation using multilateration algorithm). Given the TOA of certain ADS-B messages $\mathbf{Z}^m$, the corresponding receiver location $\mathbf{P}^S$, and the speed of light v, we can estimate the location of target $\mathbf{x} = (x, y, z)$:

$$\mathsf{est}_{\varepsilon}\left(\mathbf{z}^m, \mathbf{x}\right) \coloneqq \exists \widehat{\mathbf{x}} : \bigwedge_{j \in S} \mathbf{z}_j^m = h_j\left(\widehat{\mathbf{x}}\right) \wedge \left\|\widehat{\mathbf{x}} - \mathbf{x}\right\| < \varepsilon \tag{4}$$

The propagation time $h_i(\mathbf{x})$ from location $\mathbf{x}$ to receiver $\mathbf{P}_j^S$ is given as

$$h_j\left(\mathbf{x}\right) = \frac{\left\|\mathbf{x} - \mathbf{P}_j^S\right\|}{v} \tag{5}$$

The estimation error of target location has upper bound ε, which consists of the time synchronization error and error generated during signal propagation. If the error does not always satisfy the requirement, it is considered that multilateration algorithm can not converge and the location fails.

Definition 3 (bad data detection). The central processing station receives aircraft location encoded in a group of ADS-B messages with the same content and estimates the aircraft location $\mathbf{x}$ using TDOA of these messages. The residue is the difference between them, which is used to monitor the status of the system. If the residue is smaller than the threshold τ, these messages are valid messages; otherwise, they will be filtered out.

$$\mathsf{mon}_{\tau}\left(\mathbf{z}^g, \mathbf{x}\right) \coloneqq \left\|\mathbf{z}^g - \mathbf{x}\right\| < \tau \tag{6}$$

There are different methods to select the threshold τ, such as χ^2 test.

Although these attackers have the ability to inject arbitrary messages, they must follow some rules to make the attack success in the real world. The measurements have to satisfy some constraints to ensure the receivers can accept the messages successfully. We can encode the communication domain specific knowledge in the logic formulas:

$$\begin{aligned} &\mathsf{con}\left(\mathbf{z}^m, \mathbf{z}^g\right) \\ &\quad \coloneqq \left(0 < \mathbf{z}^m < \frac{R}{v}, \mathbf{z}^g \in V, abs\left(\mathbf{z}_i^m - \mathbf{z}_j^m\right) > l_m\right) \end{aligned} \tag{7}$$

where R is maximum propagation distance of ADS-B messages and V is a reasonable area where the aircraft could appear. According to the RTCA DO-260, the time length of the message block with preamble is $l_m = 120\mu sec$. To ensure two messages received by one receiver will not overlap and interfere with each other, the difference of TOAs must be larger than that.

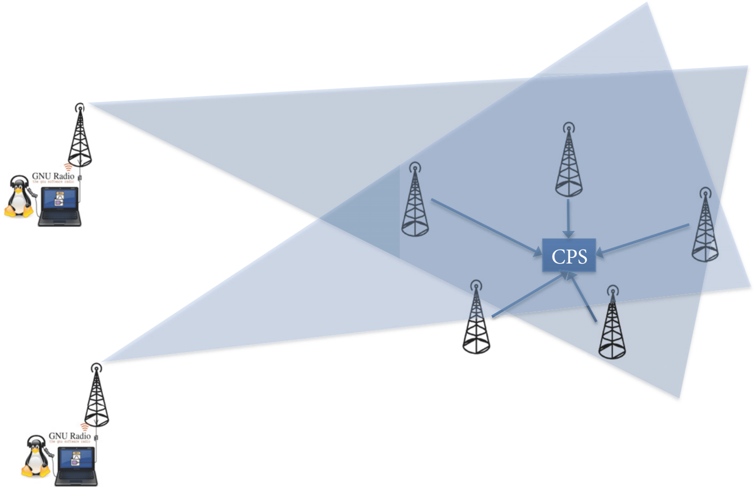


Figure 2: Full connected multidevice false data injection attack model.

3.2. False Data Injection Attack Requirement. Because of the lack of authentication mechanism in ADS-B, attackers can inject false ADS-B messages. Using multilateration mechanism described above, these messages can be labelled as bad data and filter out of the system. In order to realize a false data injection in the ADS-B multilateration system, the following requirements must be satisfied.

Definition 4 (requirement for false data injection attack). Let $\mathbf{S}$ be an ADS-B multilateration system and $\mathsf{est}_\varepsilon(\mathbf{z}^m, \mathbf{x})$ and $\mathsf{mon}_\tau(\mathbf{z}^g, \mathbf{x})$ be as specified above. The requirements of false data inject are defined as follows.

$$\begin{aligned}&\mathsf{fdi}_{\varepsilon,\tau}\left(\mathbf{z}^g, \mathbf{z}^m\right)\\&\quad \coloneqq \exists \mathbf{x} : \left(\mathsf{est}_\varepsilon\left(\mathbf{z}^m, \mathbf{x}\right) \wedge \mathsf{mon}_\tau\left(\mathbf{z}^g, \mathbf{x}\right) \wedge \mathsf{con}\left(\mathbf{z}^g, \mathbf{z}^m\right)\right)\end{aligned} \tag{8}$$

$\mathbf{z}^g$ are the location claimed by attacker in the ADS-B messages and $\mathbf{z}^m$ are the admissible measurement vector constructed by attacker to satisfy the requirements above to bypass the state estimation and monitor process [31].

In order to meet the requirements of the false data injection attack, a formal model of multidevice false data injection attack is proposed. We analyze the requirements of this new attack model and describe the method of implementing this attack.

3.3. Multidevice False Data Injection Attacker Model. In the formal model of multidevice false data injection attack, we use high-power transmitters to implement message injection attacks at a relatively long distance from the receiver, as shown in Figure 2. To simplify the problem, the multidevice attack model proposed in this paper is based on the following assumptions:

(1) Assume that each receiver can receive all transmitter signals. We consider the communication graph is complete. If the transmitter power is large enough, all receivers will be able to receive the message effectively.

(2) Assume that the receiver only takes the receiving time of the first ADS-B message as the arrival time of the actual signal. In practice, the receiver may receive multiple signals because of the multipath effect of signal propagation. If multiple signals are received, the earliest arrival signal is most likely to be the original signal.

If multilateration systems consider receiving multiple ADS-B messages of the same content at the same station as being attacked, attackers may adopt the combination of message deleting attack and message injection attack to remove the additional messages. As the TOA of the duplicated messages can be predicted in advance, the attacker is able to send an interference signal at the right time to cancel these messages.

Definition 5 (multidevice false data injection attack). Let $\mathbf{S}$ be an ADS-B multilateration system, an attacker wants to inject the ADS-B message of single aircraft at position $\mathbf{z}^g$. A attacker model of multidevice false data injection attack is tuple $\mathbf{A} = \langle \mathbf{P}^A, \Delta t \rangle$, which satisfies

$$\mathsf{fdi}_{\varepsilon,\tau}\left(\mathbf{z}^g, \mathbf{z}^m\right) \tag{9}$$

$\mathbf{P}^A = \{\mathbf{P}_i^A, i = 1..N\}$ is the matrix of attacker's transmitters locations and N is the number of the attacker's transmitters. $\Delta t = \{\Delta t_i, i = 1..N\}$ is the time delay of ADS-B messages transmitted by the attacker, assuming $\Delta t_i = 0$. Redefine the measurement $\mathbf{z}_j^m$ of receiver j as follows, which is the time of arrival used in multilateration estimation $\mathsf{est}_\varepsilon(\mathbf{z}^m, \mathbf{x})$.

$$\mathbf{z}_j^m = \min_{i \in N}\left(h_j\left(\mathbf{P}_i^A\right) + \Delta t_i\right) \tag{10}$$

$h_j(\mathbf{P}_i^A)$ is given in formula (10). As we assume that the receiver only takes the receiving time of the first ADS-B message as the arrival time of the actual signal, the receiver j chooses the minimum of arrival time of all transmitters as its measurement. The arrival time of a transmitter includes the signal propagation time from transmitter i to receiver j and the time delay Δt_i of transmitter i.

The attacker model is used to describe the transmitters' location and time delay $\langle \mathbf{P}^A, \Delta t\rangle$ to control the arrival time $\mathbf{z}_j^m$ of ADS-B message, which should satisfy the requirement $\mathsf{fdi}_{\varepsilon,\tau}(\mathbf{z}^g, \mathbf{z}^m)$ defined in Definition 4.

4. Implementation of Multidevice False Data Injection Attack

To implement the multidevice FDI attack, we need to find an optimized configuration of the transmitters' location and the transmission delay of each message. According to the configuration, the injected ADS-B message can bypass the multilateration scheme to influence the ATC center. The core of the problem is how to build an optimization model to calculate the transmitters' location and the transmission delay of each message, so that it satisfies the false data injection attack requirement.

4.1. Optimization Problem Establishment. According to Definition 5, we can establish an optimization model of multidevice false data injection attack for ADS-B multilateration system. Let $\mathbf{S}$ be an ADS-B multilateration system; $\mathbf{z}^g$ is the location that attacker want to inject. $\mathbf{P}_i^A$ is the location of attacker transmitter i and Δt_i is the corresponding time delay, which makes the aircraft location estimated by the multilateration the closest to the desired fake position. The problem can be expressed as the following optimization problem:

$$\min \quad \sum_{i=1}^{M}\sum_{\substack{j=1\\ j\neq i}}^{M}\left(\left\|\mathbf{z}_i^m-\mathbf{z}_j^m\right\|-\left(h_i\left(\mathbf{z}^g\right)-h_j\left(\mathbf{z}^g\right)\right)\right)^2 \tag{11}$$

$$\text{s.t.} \quad \left\|\mathbf{P}_i^A-\mathbf{P}_j^A\right\|\le r, \quad i=1,\dots,N,\ j=1,\dots,N \tag{12a}$$

$$\left\|\mathbf{P}_i^A-\mathbf{P}_j^S\right\|\le R, \quad i=1,\dots,N,\ j=1,\dots,M \tag{12b}$$

$$0<\mathbf{z}^m<\frac{R}{v},\ \mathbf{z}^g\in V,\ abs\left(\mathbf{z}_i^m-\mathbf{z}_j^m\right)>l_m. \tag{12c}$$

where r is the upper bound of the distance between any two transmitters to meet the time synchronization requirement between the transmitters; R indicates the maximum distance between the arbitrary transmitter and the receiver, which is the ADS-B coverage radius. $\|\mathbf{z}_i^m-\mathbf{z}_j^m\|$ is the measured time difference of arrival (TDOA). $h_i(\mathbf{z}^g)-h_j(\mathbf{z}^g)$ shows the TDOA of the signal emitted from the ghost aircraft. If the difference between two TDOA is the least, the position error is the least.

4.2. Solving the Optimization Problem. The optimization problem described in formula (11) is to solve the multidevice false data injection attack scheme. Then we use the optimized result to evaluate the feasibility and attack efficiency of the attack scheme. To simplify the problem, we use two transmitters to achieve the attack as an example.

In order to simplify the optimization problem, the locations of attacker transmitters are selected at the discrete point of two-dimensional space. First choose the location $\mathbf{P}_1^A$ of the first transmitter in a circular area of radius R and the circular center is the geometric mean of all receiver coordinates so that the ADS-B messages can be normally received between the receivers and the transmitters. The area is discretized and the points in the area are enumerated as the location of the first transmitter. Then, the location of the second transmitter location $\mathbf{P}_2^A$ is enumerated among the discrete points in the second circular area of radius r, the center of which is the first transmitter location $\mathbf{P}_1^A$ to make any two transmitters meet the time synchronization requirements. After determining the position of the two transmitters, the unconstrained single variable optimization problem is constructed to find the best time delay, which makes the position error minimized between the coordinates position calculated by the multilateration and the attacker desired position $\mathbf{z}^g$, as is shown in Algorithm 1.

After solving the optimal attack scheme, we verify the attack configuration. First, we implemented the multilateration algorithm, which can estimate the location of the aircraft by the arrival time of the same message received by 5 receivers. Then, given two transmitter locations, the estimated location changes at different time delays Δt_2 are calculated, as shown in Figure 3. The blue curve indicates that the x coordinate change with the delay Δt_2, the orange curve represents the coordinate y change, and the green curve represents the coordinate z change.

It is found from the graph that, with the linear variation of the transmission delay, the locations estimated by the multilateration will change sharply, which gives us a great convenience to inject continuous flight track.

4.3. Simulation Experiments. Given the number of the receivers, we can get a configuration of the multilateration system by generating the receivers positions randomly. These positions are uniformly chosen in a selected area. Given a certain number of receivers, if the position error in the best solution is larger than 500 meters, we should increase the necessary number of attacker's transmitters. Then we can get the necessary number of transmitters in the configuration after simulation as shown in Table 1. As the increasing of number of receivers, the number of transmitters can be reduced by two. Only under the four-receiver configuration, the attacker can achieve high attack efficiency. Under the condition of 6 receivers, the error is reasonable with 4 receivers. However, it is much bigger than other conditions. It is related to the placement of the receivers. We randomly choose the positions of receivers, which makes the error uncertain. The error is acceptable for this level disturbance, so we do not need extra transmitters for this status.

In order to make the attack more practical, we use real-world data from the OpenSky Network. First, we extract ground stations' locations and select 4 stations from them, which are all in coverage of one ADS-B source and have a dense usage.

This is a configuration of the attackers as shown in Figure 4. If transponders send the message at time offset of $(0.00226, 5.63\times10^{-6})$, the multilateration algorithm will

```
input: ADS-B multilateration system $\mathbf{S}$, the location that attacker want to
       inject $\mathbf{z}^g$, the upper bound of the distance between any two
       transmitters $r$, the maximum distance between the arbitrary
       transmitter and the receiver $R$.
output: The location of attacker transmitters $\mathbf{P}^A$, the time delay of the second transmitter $\Delta t$.
$\mathbf{P}_c \longleftarrow (1/K)\sum_i \mathbf{P}_i^S$;
$\epsilon \longleftarrow \infty$;
for $r_1 \longleftarrow 1$ to $R$ do
    for $\theta_1 \longleftarrow 0$ to $2\cdot\pi$ do
        $\mathbf{P}_1^A \longleftarrow \mathbf{P}_c + (r_1\cdot\cos\theta_1, r_1\cdot\sin\theta_1)$;
        for $r_2 \longleftarrow 1$ to $r$ do
            for $\theta_2 \longleftarrow 0$ to $2\cdot\pi$ do
                $\mathbf{P}_2^A \longleftarrow \mathbf{P}_1^A + (r_2\cdot\cos\theta_2, r_2\cdot\sin\theta_2)$;
                $\mathbf{P}^A \longleftarrow (\mathbf{P}_1^A, \mathbf{P}_2^A)$;
                $\Delta\hat{t}, \hat{\epsilon} \longleftarrow \min_{\Delta t}\sum_{i=1}^{M}\sum_{\substack{j=1\\ j\neq i}}^{M}(\|\mathbf{z}_i^m - \mathbf{z}_j^m\| - (h_i(\mathbf{z}^g) - h_j(\mathbf{z}^g)))^2$;
                if $\hat{\epsilon} < \epsilon \wedge \mathrm{con}(\mathbf{z}^m, \mathbf{z}^g)$ then
                    $\epsilon \longleftarrow \hat{\epsilon}$;
                    $\Delta t \longleftarrow \Delta\hat{t}$;
                end
            end
        end
    end
end
return $\mathbf{P}^A, \Delta t$;
```

Algorithm 1: Implementation of the optimization algorithm (discrete enumeration of the locations of transmitters).

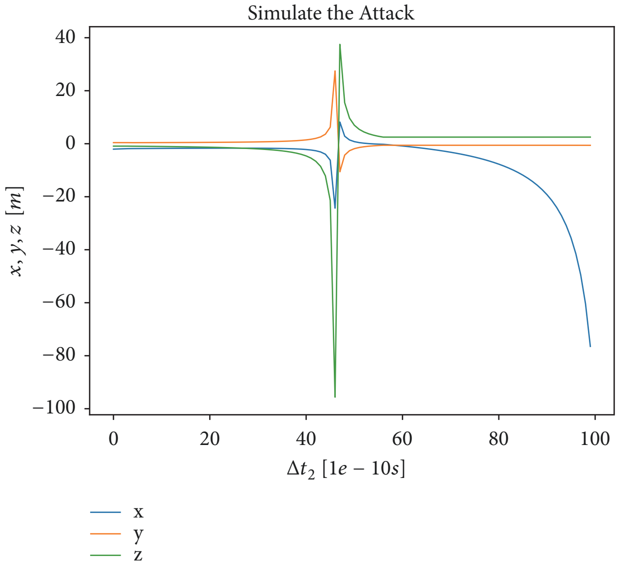


Figure 3: Given the position of attacker's transponder position, the multilateration result variation along with the time delay. The blue curve indicates that the coordinate x change, the orange curve represents the coordinate y change, and the green curve represents the coordinate z change.

estimate the aircraft location at green circle, which is the target of the false message injection. Just ranging the time offset, we can get a trajectory.

Table 1: #Receivers = number of receivers in the ADS-B multilateration system, #Transmitters = number of attacker's transmitters in FDI, and Error = the difference between the target location of ghost aircraft and the estimated location calculated by the multilateration.

#Receivers	#Transmitters	Error $[m]$
4	2	44.3417
5	3	45.6391
6	4	107.9898
7	5	67.2437

To demonstrate the constraints on the trajectory injection, we randomly chose some placements of transmitters and find out what trajectories we can get by changing the time delay between two transmitters. As shown in Figure 5, the trajectories distribute on straight lines, which can be used to inject to the system to interfere with the job of controllers. Figure 5 includes three subfigures. They are chosen from 100 simulations to demonstrate the typical patterns of injected trajectories. To get one subfigure, we first randomly generate the placement of receivers and attackers transmitters. Then we set the time delays of the first transmitter as a sequence of zero, and set the time delays of the second transmitter as an arithmetic sequence start from zero. Given different time delays for different ADS-B messages, the multilateration algorithm can calculate a sequence of estimated targets as shown in the subfigure. However, if the transmitters' location is given, only one possible trajectory could be injected, which is different from the normal trajectory of the aircraft and may be detected by some advanced abnormity detection mechanism. Therefore, attacker model of moving transmitters needs

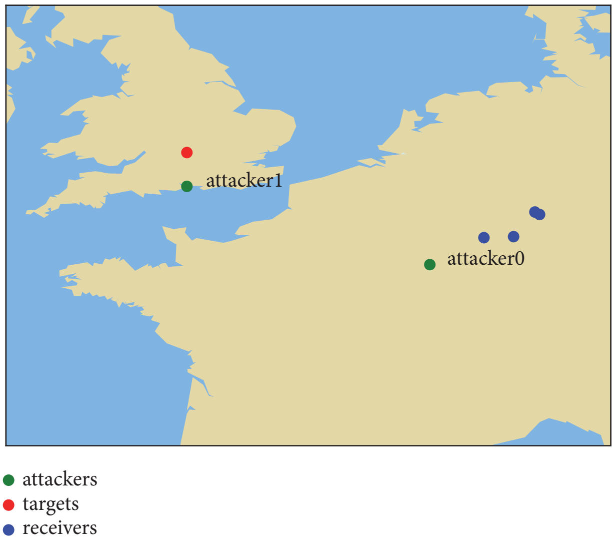


Figure 4: The positions of receivers and attackers. The blue circles are the selected locations of receivers, and the red circles are the locations of attacker's transponders. The green circles are the estimated location of aircraft.

to be studied to construct more realistic trajectories, which has more degrees of freedom.

5. Multidevice False Data Injection Countermeasures

Because the attacker forged the arrival time of the signal, the verification mechanism of the ADS-B multilateration system failed. It is difficult for the existing security mechanisms to detect such attacks effectively. Therefore, we should strengthen the ADS-B multilateration system security. New countermeasures could achieve the goal by hiding the information of locations and operational status.

5.1. Changing Locations. We try to move some of the receivers along a trajectory (by loading them on vehicles) in this countermeasure. They report ADS-B data to the center process station by wireless communication. The multilateration system could get the accurate positions using GNSS on the receive sites. The attackers only have their original information and could not inject false messages at the right time.

To evaluate the effectiveness of the countermeasure, we construct a simplified model of the moving receiver. We assume one of the receivers is moving towards one random direction, and the attacker uses the receiver's original position $\mathbf{P}_i^S$ to place their transmitters. We analyzed the effect of the location offset d of one receiver for values between 0 and $1700m$, which can be caused by the defense mechanism. Figure 6 shows the position error ϵ of multilateration result $\mathbf{x}$ and target position $\mathbf{z}^g$.

With the increasing of the offset, the multilateration result error is increasing. There is a maximum location offset value required for successful false data injection, which can serve as the reference parameter in countermeasures. However, this method needs some vehicles which increase the cost and the moving pattern may also be observed by the attacker easily.

5.2. Changing Operational Status. We can change the operational status of the receive sites randomly, which makes the attackers have a great possibility of injecting the wrong sites and failed to bypass the monitor. The redundant receivers can be added on the basis of the original receiving station, and the central processing station randomly switches the multilateration receivers used to estimate the location. There need to become more than four receivers to cover a target area. All of them pass ADS-B data to the central process station, but only four of them are used for multilateration. After a certain time period, the operational status is changed again. The time period is related to the attackers power to find out the operational status.

To evaluate this countermeasure, we randomly generate the locations of five receivers. Their locations are in the range of one aircraft's ADS-B communication area. We assume the attacker injects messages to four of them but ignores the existence of the other receiver. However, the ignored receiver could still receive them. We evaluate the position error ϵ under different operational status. As shown in Figure 7, the error is undetectable in Status 1. Attackers may inject successfully when the system is operating under this status. But the error cannot be ignored under other status. If we did not detect the attacker at current period, they could be found after the status changing in the next period.

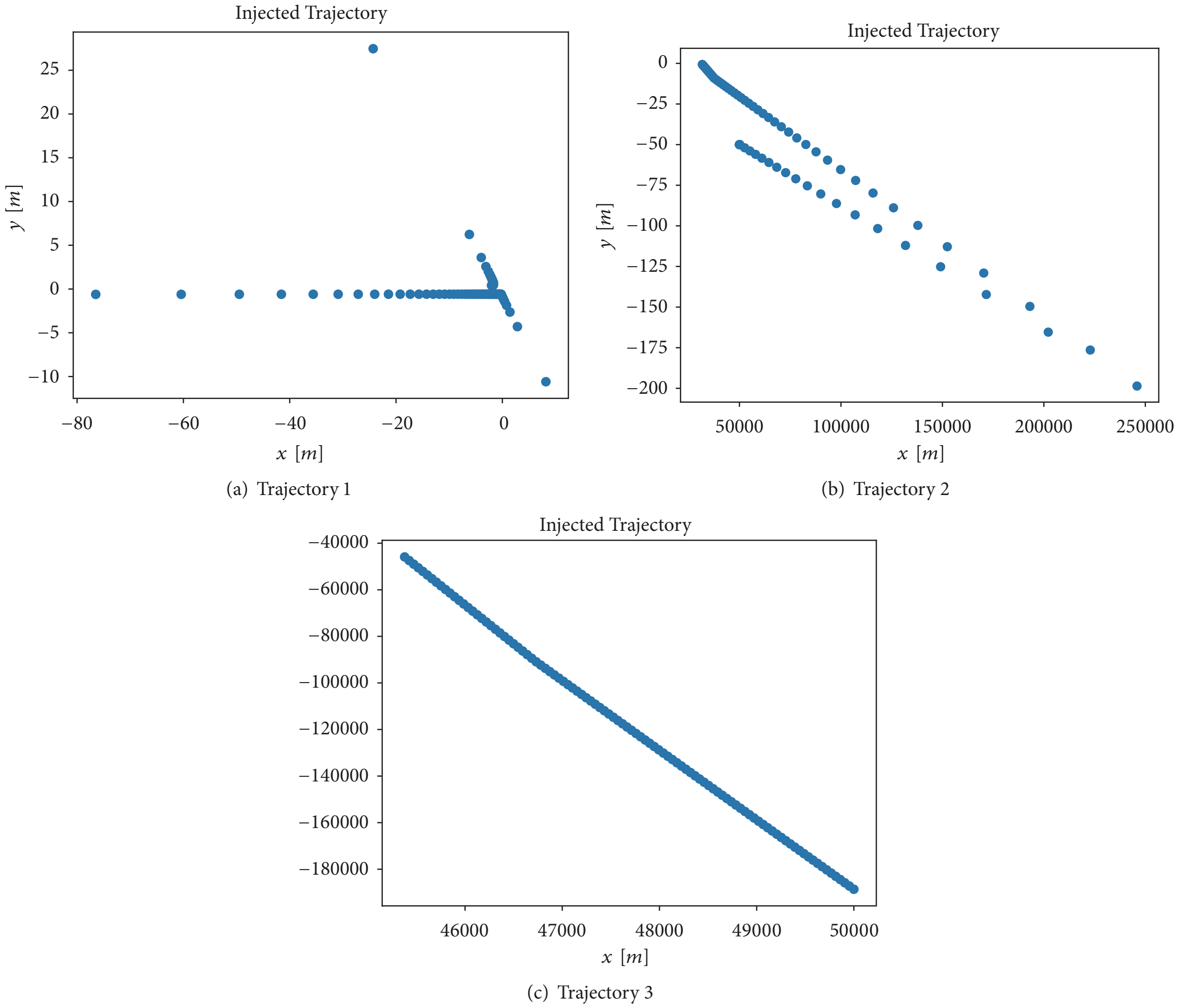
For the defenders, they only need to build 0.25 times more receivers to achieve this. This scheme is much cheaper and stealthier; the attackers have to hack the center process station to get the operational status.

In summary, our countermeasure requires no modifications to the ADS-B signal, the surveillance infrastructure, or the ADS-B receiver; it is resistant against a wide range of attackers, and it can be deployed using multiple standard ADS-B receivers.

6. Conclusions

In this paper, a formal model of the ADS-B multilateration system is established, and a new model of false data injection attack is proposed, which could be used to achieve the optimal attack configuration. This work has shown that a multidevice attacker can inject ghost aircraft with only two transmitters, which makes the cost lower. Finally, we suggest some countermeasures for this attack model. The multidevice false data injection attack model proposed in this paper has a certain generality, which can be applied to other multilateration technology applications. There also exists potential multidevice false data injection threat in the location scenarios based on ZigBee or WiFi technology [32].

In the further study, we will use GNU Radio to perform signal level simulation and try to verify multidevice false data injection attack to bypass the frequency based detection. Second, the above models assume that the location of the attacker's transmitter is fixed. If multiple ghost aircraft tracks are injected, a fixed position attack model may not satisfy the



(a) Trajectory 1

(b) Trajectory 2

(c) Trajectory 3

Figure 5: Spatial analysis of injected trajectories.

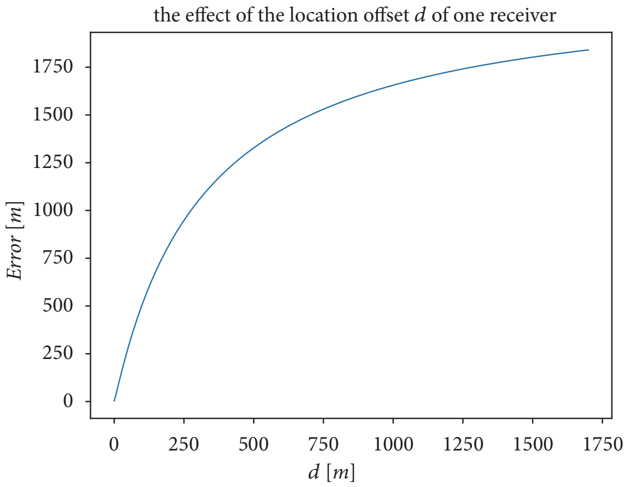


Figure 6: The effect of the location offset d of one receiver.

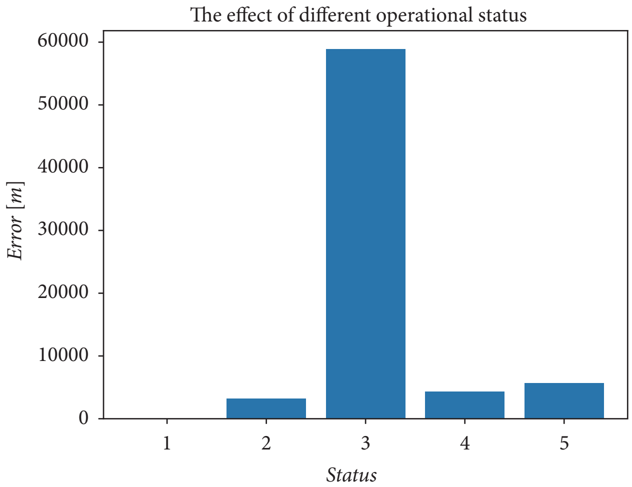


Figure 7: The effect of different operational status.

requirements of false data injection attack, and the attacker's model of moving transmitters is needed to be studied. In addition, we assume the communication graph is complete; i.e., all receivers can receive all transmitted signals. We will study the attack pattern considering the more complicated communication graph. And how to gather information about the ADS-B receivers' locations and operation states to construct the communication graph is also a big question.

Data Availability

The location data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, "Realities and challenges of nextgen air traffic management: the case of ADS-B," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 111–118, 2014.

[2] F. I. Romli, J. D. King, L. Li, and J. P. Clarke, "Impact of automatic dependent surveillance-broadcast (ADS-B) on traffic alert and collision avoidance system (TCAS) performance," in *Proceedings of the AIAA Guidance, Navigation and Control Conference and Exhibit*, p. 6971, USA, August 2008.

[3] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78–87, 2011.

[4] B. S. Ali, "System specifications for developing an automatic dependent surveillance-broadcast (ADS-B) monitoring system," *International Journal of Critical Infrastructure Protection*, vol. 15, pp. 40–46, 2016.

[5] A. Costin and A. Francillon, *Ghost in the Air(Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices*, 2012.

[6] Y. T. Chan and K. C. Ho, "A simple and efficient estimator for hyperbolic location," *IEEE Transactions on Signal Processing*, vol. 42, no. 8, pp. 1905–1915, 1994.

[7] R. O. Schmidt, "A new approach to geometry of range difference location," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-8, no. 6, pp. 821–835, 1972.

[8] J. A. Besada, G. De Miguel, A. M. Bernardos, and J. R. Casar, "Automatic-dependent surveillance-broadcast experimental deployment using system wide information management," *International Journal of Microwave and Wireless Technologies*, vol. 4, no. 2, pp. 187–198, 2012.

[9] M. Monteiro, A. Barreto, R. Division et al., "Detecting malicious ADS-B broadcasts using wide area multilateration," in *Proceedings of the 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, pp. 4A3-1–4A3-12, Prague, Czech Republic, September 2015.

[10] K. Jansen and C. Pöpper, "Advancing attacker models of satellite-based localization systems: the case of multi-device attackers," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '17*, pp. 156–159, ACM Press, Boston, Mass, USA, July 2017.

[11] D. Moser, P. Leu, V. Lenders, A. Ranganathan, F. Ricciato, and S. Capkun, "Investigation of multi-device location spoofing attacks on air traffic control and possible countermeasures," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking - MobiCom '16*, pp. 375–386, ACM Press, New York, NY, USA, October 2016.

[12] R. SC186, "Minimum operational performance standards for 1090 MHz automatic dependent surveillance–broadcast (ADS-B)," RTCA DO-260, 2000.

[13] R. Do, *Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance–Broadcast (Ads-B) and Traffic Information Services–Broadcast (Tis-B)*, vol. 260, Radio Technical Commission for Aeronautics, 2009.

[14] R. DO, *Minimum Operational Performance Standards for 1090Mhz Extended Squitter ADS B and TIS-B*, RTCA, Washington, DC, USA, 2009.

[15] L. Purton, H. Abbass, and S. Alam, "Identification of ADS-B system vulnerabilities and threats," in *Australian Transport Research Forum*, pp. 1–16, Canberra, 2010.

[16] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

[17] J. Baek, E. Hableel, Y.-J. Byon, D. S. Wong, K. Jang, and H. Yeo, "How to protect ADS-B: confidentiality framework and efficient realization based on staged identity-based encryption," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 690–700, 2017.

[18] M. Strohmeier, V. Lenders, and I. Martinovic, "Lightweight location verification in air traffic surveillance networks," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security (CPSS '15)*, pp. 49–60, Singapore, April 2015.

[19] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security (CCS '11)*, pp. 75–86, ACM Press, Chicago, Ill, USA, October 2011.

[20] D. Sriraman, R. K. S. Kumar, and S. V. Subhashini, "Air traffic controller using a new ads-B framework," 2016.

[21] J. Herrero, J. Portas, F. Rodriguez, and J. Corredera, "ASDE and multilateration mode-S data fusion for location and identification on airport surface," in *Proceedings of the 1999 IEEE Radar Conference. Radar into the Next Millennium*, pp. 315–320, Waltham, Mass, USA, 1999.

[22] J. Johnson, H. Neufeldt, and J. Beyer, "Wide area multilateration and ADS-B proves resilient in Afghanistan," in *Proceedings of the 2012 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. A6-1–A6-8, Herndon, Va, USA, April 2012.

[23] L. Gomez and I. T. Sierra, "Implementation of automatic dependent surveillance (ADS-B) in Colombia," in *Proceedings of the 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, pp. 2B2-1–2B2-9, Prague, Czech Republic, 2015.

[24] T. Li and B. Wang, "Sequential collaborative detection strategy on ADS-B data attack," *International Journal of Critical Infrastructure Protection*, vol. 24, pp. 78–99, 2019.

[25] M. Schafer, M. Strohmeicr, M. Smith, M. Fuchs, V. Lenders, and I. Martinovic, "OpenSky report 2018: assessing the integrity of crowdsourced mode S and ADS-B data," in *Proceedings of the 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, pp. 1–9, London, UK, September 2018.

[26] K. Jansen, M. Schafer, D. Moser, V. Lenders, C. Popper, and J. Schmitt, “Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks,” in *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP)*, pp. 1018–1031, San Francisco, Calif, USA, May 2018.

[27] M. Strohmeier, V. Lenders, and I. Martinovic, “Intrusion detection for airborne communication using PHY-layer information,” in *Detection of Intrusions and Malware, and Vulnerability Assessment*, vol. 9148 of *Lecture Notes in Computer Science*, pp. 67–77, Springer International Publishing, Cham, Germany, 2015.

[28] C. Laurendeau and M. Barbeau, “Probabilistic localization and tracking of malicious insiders using hyperbolic position bounding in vehicular networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, Article ID 128679, 13 pages, 2009.

[29] Q. Wang, H. Su, K. Ren, and K. Kim, “Fast and scalable secret key generation exploiting channel phase randomness in wireless networks,” in *Proceedings of the 30th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies (INFOCOM ’11)*, pp. 1422–1430, Shanghai, China, April 2011.

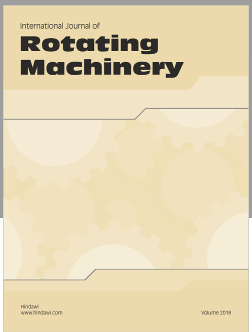
[30] D. Steinmetzer, M. Schulz, and M. Hollick, “Lockpicking physical layer key exchange: weak adversary models invite the thief,” in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec ’15)*, 11, 1 pages, ACM, New York, NY, USA, 2015.

[31] S. Gao, L. Xie, A. Solar-Lezama, D. Serpanos, and H. Shrobe, “Automated vulnerability analysis of AC state estimation under constrained false data injection in electric power systems,” in *Proceedings of the 54th IEEE Conference on Decision and Control, CDC 2015*, pp. 2613–2620, Japan, December 2015.

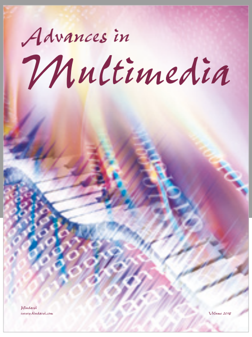
[32] E. Yaksel, H. R. Nielson, F. Nielson, M. Fruth, and M. Kwiatkowska, “Optimizing zigbee security using stochastic model checking,” http://arxiv.org/abs/1205.6675.

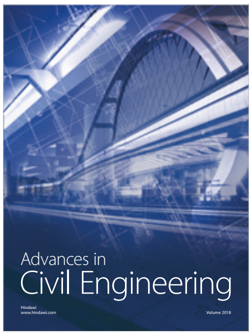
Journal of
Engineering

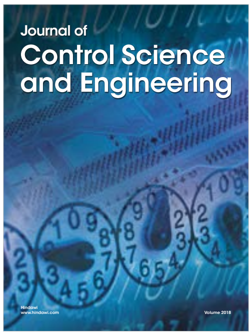
The Scientific
World Journal


International Journal of
Rotating
Machinery

Journal of
Sensors

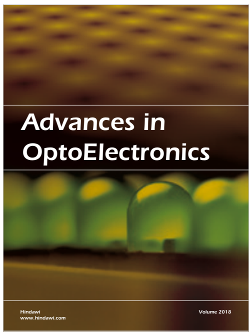

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

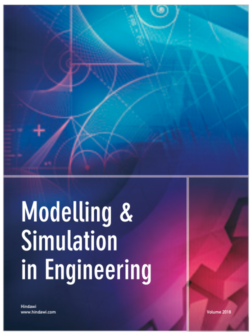
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

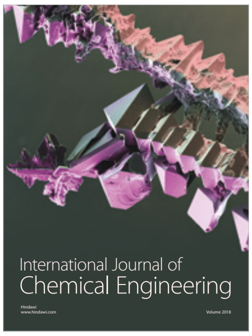

Advances in
OptoElectronics

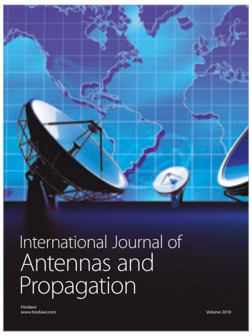
VLSI Design

International Journal of
Navigation and
Observation

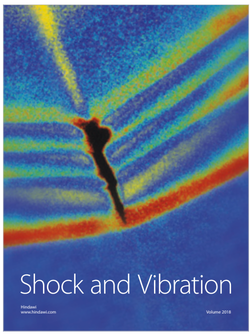

Modelling &
Simulation
in Engineering

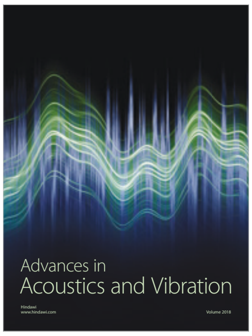
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration