applied sciences

MDPI

Article

Consensus-Based Distributed Target Tracking with False Data Injection Attacks over Radar Network

Yongtao Shui [1], Yu Wang [1,*], Yu Li [2], Yongzhi Shan [3], Naigang Cui [1] and Baojun Pang [1]

[1] Harbin Institute of Technology, Harbin 150001, China; syt_hit@126.com (Y.S.); Cui_naigang@163.com (N.C.); pangbj@hit.edu.cn (B.P.)
[2] Beijing Aerospace Technology Institute, Beijing 100000, China; yuli_happy@126.com
[3] Harbin Jiancheng Group Co. Ltd., Harbin 150001, China; syz_hit@163.com
* Correspondence: wangyu_hitsa@hit.edu.cn

Abstract: For target tracking in radar network, any anomaly in a part of the system can quickly spread over the network and lead to tracking failures. False data injection (FDI) attacks can damage the state estimation mechanism by modifying the radar measurements with unknown and time-varying attack variables, therefore making traditional filters inapplicable. To tackle this problem, we propose a novel consensus-based distributed state estimation (DSE) method for target tracking with FDI attacks, which is effective even when all radars are under FDI attacks. First, a real-time residual-based detector is introduced to the DSE framework, which can effectively detect FDI attacks by analyzing the statistical properties of the residual. Secondly, a simple yet effective attack parameter estimation method is proposed to provide attack parameter estimation based on a pseudo-measurement equation, which has the advantage of decoupled estimation of state and attack parameters compared with augmented state filters. Finally, for timely attack mitigation and global consistency achievement, a novel hybrid consensus method is proposed which can compensate for the estimation error caused by FDI attacks and provide estimation accuracy improvement. The simulation results show that the proposed solution is effective and superior to the traditional DSE method for target tracking in the presence of FDI attacks.

Keywords: false data injection; hybrid consensus; distributed state estimation; radar network; target tracking

Citation: Shui, Y.; Wang, Y.; Li, Y.; Shan, Y.; Cui, N.; Pang, B. Consensus-Based Distributed Target Tracking with False Data Injection Attacks over Radar Network. *Appl. Sci.* **2021**, *11*, 4564. https://doi.org/10.3390/app11104564

Academic Editor: Jérôme Morio

Received: 6 April 2021
Accepted: 14 May 2021
Published: 17 May 2021

1. Introduction

In recent years, radar networks have been widely applied in many fields, including indoor tracking [1], air traffic control [2], surveillance [3,4] and autonomous vehicles [5] because of its capability of achieving better performance than conventional radars by utilizing spatial diversity. State estimation over a radar network, if performed in a centralized manner, can achieve optimal estimation results but suffers from heavy communication and computation load, considering the increasing network size. An alternative solution is a distributed scheme [6–16], where a peer-to-peer communication scheme is used instead of collecting raw measurements from every single sensor in the network to a fusion center. Each sensor only exchanges information with its local neighbors. However, there are two main challenges in target tracking using a radar network.

First, the radar network is vulnerable to cyberattacks because the networks between radars can be maliciously compromised [17], therefore bringing the risk of security threats to the systems. Common cyberattacks launched in radar networks include electronic countermeasure jamming [18], false data injection [19], denial-of-service attacks [20], replay attacks [21] and so on. Electronic countermeasure jamming is a way to interfere with radar echoes between a radar and its targets. For the denial-of-service attack, the attacker sends a large amount of fake data to block the communication channel between radars. In the replay attack case, the attacker records and replays radar data to degrade the system's

performance. Different from the cyberattacks mentioned before, false data injection (FDI) is a specific type of deception attack [19] which can deteriorate the estimation accuracy of the radar network by modifying the measurements of the attacked radars with unknown and time-varying attack variables. Most existing works about FDI attacks concentrate on the detector's design. Several effective detectors, such as χ^2 detectors, summation detectors [22] and cumulative sum-based detectors [23], have been proposed to detect this kind of attack. The easiest way to deal with the attacked measurements is to discard them so that they will not affect the radar tracking system. Obviously, discarding the measurements leads to information loss, and it will suffer from filter divergence when the attack lasts for a long time. An alternative is to estimate the attack parameter and eliminate its effect. For attack parameter estimation, an augmented state Kalman filter (ASKF) may be used to produce the optimal state estimate, in which the stack vector technique is used by augmenting the attack parameter into the state. However, the computational burden of the ASKF increases dramatically with the augmented state dimension, especially in a large-scale network. Several studies considered distributed state estimation (DSE) with FDI attacks. In [24], a trust-based combination strategy was developed to classify sensors in a network into two clusters: the trusted one and the untrusted one. The sensor measurements in the untrusted cluster are discarded, which is obviously a waste of information. Moreover, the method can only deal with a case where less than half of the sensors are under attack. In [17], a confident covariance intersection-based fusion method was proposed, where the confidence factor is used to weight the estimate confidences of all radars, thus reducing the fusion weights of the injected data. The weight of the injected data is decreased, but the effect of it is not eliminated.

The second challenge in target tracking using radar networks is how to achieve global consistency over the radar network. For DSE, consensus estimation is an effective tool for state estimation in sensor networks that are not fully connected to achieve global consistency. Consensus-based methods can be categorized based on the exchanged quantities among neighboring sensors. For example, sensors can exchange local state estimates (consensus on estimates method (CE)) [11,14], local measurements and innovation covariances (consensus on measurements method (CM)) [10,16] and information vectors and matrices (consensus on information method (CI)) [9,15]. The CE does not exchange error covariance matrices, which makes it suffer from poor performance [12]. The CM can achieve the same accuracy as the centralized method only when the number of consensus steps trends toward infinity. The CI guarantees stability for any number of consensus steps, but its performance can be hampered because of the assumption that the correlations between the estimates from different sensors are completely unknown. Recently, a consensus method named Hybrid CMCI (HCMCI) [12,13] has been proposed, which has the advantages of both the CM and CI methods. The stability analysis of the HCMCI in the case of linear systems has been given, and the effectiveness of the HCMCI has been shown in [12]. For the nonlinear case, Taylor expansion is used. However, to the best of our knowledge, there have been few results concerning consensus-based DSE with FDI attacks, which serves as the main motivation of this paper.

In this paper, we aim to combat FDI attacks on radar networks. The contributions of this paper are summarized as follows:

1. A novel, consensus-based DSE algorithm is proposed to enhance the resilience of radar networks against FDI attacks. Only local information exchange is needed in the proposed method. Different from the existing works, a real-time, residual-based detector is introduced to the DSE framework to detect FDI attacks effectively by analyzing the statistical properties of the residual. The proposed method eliminates the hypothesis in [24]; that is, less than half of the sensors are attacked. Note that even if half of the sensors are under an FDI attack, the proposed method is also effective.
2. To estimate the FDI attack parameters, a simple yet effective attack parameter estimation method is proposed based on a pseudo-measurement equation, which has the

advantage of decoupled estimation of the state and attack parameters compared with augmented state filters.

3. To mitigate the FDI attack and achieve global consistency in a timely manner, a novel hybrid consensus method is proposed by combining the CM and CI methods, which can provide estimation accuracy improvement when the number of consensus iterations is moderate.

The paper is outlined as follows. Section 2 formulates the problem. Moreover, the topology structure, target dynamics and radar measurement model are introduced. Section 3 derives the novel DSE algorithm with FDI attacks. In Section 4, the effectiveness of the proposed consensus-based DSE method is demonstrated via simulation. In Section 5, the conclusions are given.

2. Problem Formulation

Assume that a communication-limited network of N radars tracks a common target. The radar network is under malicious FDI attacks, which deteriorate the target estimation by injecting unknown and time-varying attack variables into the radar's measurements. In this paper, we propose a novel DSE method that can combat FDI attacks for radar networks and provide high accuracy target tracking results. In this section, we introduce the topology structure, target dynamics and radar measurement model.

2.1. Topology Structure

Define an undirected graph $G = (V, E)$ to describe the radar network, where $V = [1, 2, \ldots, N]$ denotes the radar set. The symbol $E \subseteq V \times V$ denotes the set of radar connections in the network. The pair (m, n) is a member of set E, where radar m and radar n can exchange information between each other. If two radars can exchange information, they are called neighbors. The set of radar m and its neighbors is denoted by E_m. The degree d_m of radar m means the number of its neighbors. Define the adjacency matrix $A(G)_{mn}$ as

$$A(G)_{mn} = \begin{cases} 1, \ if(m,n) \in E \\ 0, \ otherwise \end{cases} \tag{1}$$

2.2. Target Dynamics and Radar Measurement Model

Consider that the target dynamic is modeled as follows:

$$\boldsymbol{x}(k) = \boldsymbol{F}(k-1)\boldsymbol{x}(k-1) + \boldsymbol{w}(k-1) \tag{2}$$

where $\boldsymbol{x}(k) \in \mathbb{R}^n$ denotes the state at time k, $\boldsymbol{x} = \begin{bmatrix} x & y & z & \dot{x} & \dot{y} & \dot{z} \end{bmatrix}^T$; $\boldsymbol{F}$ is the transition matrix; $\boldsymbol{w}(k-1)$ is the zero-mean Gaussian process noise; and the process noise covariance is $\boldsymbol{Q}(k-1)$.

We consider the ground-based active radars used to track the target, where the measured values are generally in spherical coordinates. Therefore, the sensing model of the ith radar under an FDI attack is described in spherical coordinates as follows [25,26]:

$$\boldsymbol{y}_i^s(k) = \begin{bmatrix} \widetilde{r}_i(k) \\ \widetilde{\theta}_i(k) \\ \widetilde{\varphi}_i(k) \end{bmatrix} = \begin{bmatrix} r_i(k) + r_i^a(k) + v_i^r(k) \\ \theta_i(k) + \theta_i^a(k) + v_i^\theta(k) \\ \varphi_i(k) + \varphi_i^a(k) + v_i^\varphi(k) \end{bmatrix} \tag{3}$$

where $\widetilde{r}_i(k)$, $\widetilde{\theta}_i(k)$ and $\widetilde{\varphi}_i(k)$ are the range, elevation and azimuth measurements in spherical coordinates, respectively, and $r_i(k)$, $\theta_i(k)$ and $\varphi_i(k)$ are true measurements, which are simulated as follows (subscript i is omitted for simplicity):

$$\begin{bmatrix} r(k) \\ \theta(k) \\ \varphi(k) \end{bmatrix} = \begin{bmatrix} \sqrt{x_r^2 + y_r^2 + z_r^2} \\ \arcsin\frac{z_r}{d} \\ \text{arctan2}(y_r, x_r) \end{bmatrix} \tag{4}$$

where $[x_r, y_r, z_r]^T$ is the position of the target in the sensor coordinate system and

$$\begin{bmatrix} x_r \\ y_r \\ z_r \end{bmatrix} = \boldsymbol{C}_i^r \begin{bmatrix} x - x_s \\ y - y_s \\ z - z_s \end{bmatrix} \tag{5}$$

where $\boldsymbol{C}_i^r$ is the coordinate transform matrix from the Earth-centered inertial coordinate system to the sensor coordinate system and $[x_s, y_s, z_s]^T$ is the position of the sensor in the Earth-centered inertial coordinate system.

In Equation (3), $r_i^a(k)$, $\theta_i^a(k)$ and $\varphi_i^a(k)$ are unknown attack variables designed by the attacker, and $v_i^r(k)$, $v_i^\theta(k)$ and $v_i^\varphi(k)$ are zero-mean measurement noises in the range, elevation and azimuth with corresponding variances σ_{ir}^2, $\sigma_{i\theta}^2$ and $\sigma_{i\varphi}^2$, respectively. The measurement noises are assumed to be mutually independent.

There are three main attack methods for false data injection: (1) the attack variable is a time-varying signal and converges to a constant value gradually; (2) the attack variable is a Gaussian random process; and (3) the attack variable is an arbitrary random variable. In practical application, the second attack is easy to implement and the most widely used. Therefore, in this chapter, the attack variable is modeled as a Gaussian random process, and the attack variable is assumed to be irrelevant to the measurement noise and the state. The false data injection variable is as follows:

$$\boldsymbol{a}(k+1) = \boldsymbol{a}(k) + \boldsymbol{\omega}(k) \tag{6}$$

where $\boldsymbol{a}(k)$ denotes the attack variable vector and $\boldsymbol{\omega}(k)$ is the zero-mean Gaussian noise.

Since the motion equations of the targets are better modeled in Cartesian coordinates [25], we converted the 3D spherical measurements in Equation (3) into Cartesian coordinates. By transforming the measurements into Cartesian coordinates, we could perform the target state estimation within a completely linear framework.

Denote $\boldsymbol{y}_i(k) = \begin{bmatrix} \widetilde{x}_i(k) & \widetilde{y}_i(k) & \widetilde{z}_i(k) \end{bmatrix}^T$ as the measurements in Cartesian coordinates. The measurement model can be written as

$$\begin{aligned} \widetilde{x}_i(k) &= \widetilde{r}_i(k) \cos\widetilde{\theta}_i(k) \cos\widetilde{\varphi}_i(k) \\ \widetilde{y}_i(k) &= \widetilde{r}_i(k) \cos\widetilde{\theta}_i(k) \sin\widetilde{\varphi}_i(k) \\ \widetilde{z}_i(k) &= \widetilde{r}_i(k) \sin\widetilde{\theta}_i(k) \end{aligned} \tag{7}$$

Substitute Equation (3) into Equation (7), and by using a first order approximation, we can obtain

$$\boldsymbol{y}_i(k) = \boldsymbol{H}(k)\boldsymbol{x}_i(k) + \boldsymbol{A}_i(k)\boldsymbol{a}_i(k) + \boldsymbol{v}_i(k) \tag{8}$$

where $\boldsymbol{H}(k) = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$ is the measurement matrix and $\boldsymbol{a}_i(k) = [r_i^a(k) \quad \theta_i^a k \quad \varphi_i^a(k)]^T$ is the attack parameter.

In the following, the subscript i and symbol k of the true measurements in the spherical coordinates are omitted for simplicity, and $\boldsymbol{A}_i(k)$ is defined as

$$\boldsymbol{A}_i(k) = \begin{bmatrix} \cos\theta\cos\varphi & -r\sin\theta\cos\varphi & -r\cos\theta\sin\varphi \\ \cos\theta\sin\varphi & -r\sin\theta\sin\varphi & r\cos\theta\cos\varphi \\ \sin\theta & r\cos\theta & 0 \end{bmatrix} \tag{9}$$

where $v_i(k)$ is the measurement noise in the Cartesian coordinates with covariance $\boldsymbol{R}_i(k)$, such that

$$\begin{aligned}
\boldsymbol{R}_i^{11}(k) &= \sigma_{ir}^2 \cos^2\theta \cos^2\varphi + \sigma_{i\theta}^2 r^2 \sin^2\theta \cos^2\varphi + \sigma_{i\varphi}^2 r^2 \cos^2\theta \sin^2\varphi \\
\boldsymbol{R}_i^{22}(k) &= \sigma_{ir}^2 \cos^2\theta \sin^2\varphi + \sigma_{i\theta}^2 r^2 \sin^2\theta \sin^2\varphi + \sigma_{i\varphi}^2 r^2 \cos^2\theta \cos^2\varphi \\
\boldsymbol{R}_i^{33}(k) &= \sigma_{ir}^2 \sin^2\theta + \sigma_{i\theta}^2 r^2 \cos^2\theta \\
\boldsymbol{R}_i^{12}(k) &= \boldsymbol{R}_i^{21}(k) = \sigma_{ir}^2 \cos^2\theta \cos\varphi \sin\varphi + \sigma_{i\theta}^2 r^2 \sin^2\theta \sin\varphi \cos\varphi \\
&\quad -\sigma_{i\varphi}^2 r^2 \cos^2\theta \sin\varphi \cos\varphi \\
\boldsymbol{R}_i^{13}(k) &= \boldsymbol{R}_i^{31}(k) = \sigma_{ir}^2 \sin\theta \cos\theta \cos\varphi - \sigma_{i\theta}^2 r^2 \sin\theta \cos\theta \cos\varphi \\
\boldsymbol{R}_i^{23}(k) &= \boldsymbol{R}_i^{32}(k) = \sigma_{ir}^2 \sin\theta \cos\theta \sin\varphi - \sigma_{i\theta}^2 r^2 \sin\theta \cos\theta \sin\varphi
\end{aligned} \tag{10}$$

where $\boldsymbol{R}_i^{bc}(k)$ denotes the bth row and the cth column of $\boldsymbol{R}_i(k)$.

3. Distributed State Estimation Algorithm with False Data Injection Attacks

In this section, a novel DSE algorithm is proposed to deal with the FDI attacks in radar networks. The algorithm consists of three main parts: injected data detection, attack parameter estimation and hybrid consensus. To estimate the attack parameter, every two radars are grouped together in the radar network. The determination for each radar of whether it is attacked is performed by using a real-time, residual-based χ^2 detector. Then, each group runs a simple-yet-effective attack parameter estimation algorithm based on the detection results and pseudo-measurements of both radars. Finally, each group exchanges values with its neighbors and updates its own value by employing a hybrid consensus method to timely mitigate the FDI attack and achieve global consistency.

3.1. Injected Data Detection

In cyber-physical systems, attack detectors based on the analysis of the statistical properties of the residual are developed to detect FDI attacks [22,23,27]. In this paper, we adopt the real-time, residual-based χ^2 detector to determine whether FDI attacks exist in the radar network by analyzing the statistical properties of the residual.

If there are no attacks for radar i, the measurement equation can be expressed as

$$\boldsymbol{y}_i(k) = \boldsymbol{H}(k)\boldsymbol{x}_i(k) + \boldsymbol{v}_i(k) \tag{11}$$

Denote the estimation error as $\boldsymbol{e}_i(k) = \boldsymbol{x}(k) - \hat{\boldsymbol{x}}_i(k)$ and the residual of radar i as $\Delta\boldsymbol{y}_i(k) = \boldsymbol{y}_i(k) - \boldsymbol{H}(k)\boldsymbol{x}_i(k)$. The estimation error satisfies $\boldsymbol{e}_i(k) \sim \mathcal{N}(0, \boldsymbol{P}_{k-1})$ and the residual $\Delta\boldsymbol{y}_i(k) \sim \mathcal{N}\left(0, \boldsymbol{P}_{k|k-1}\right)$, where $\boldsymbol{P}_{k|k-1} = \boldsymbol{H}(k)\boldsymbol{P}_{k-1}\boldsymbol{H}^T(k) + \boldsymbol{R}(k)$.

We adopted the real-time, residual-based detector to determine whether FDI attacks exist, and the detection criterion is given as in [22]:

$$J_i(k) = \Delta\boldsymbol{y}_i^T(k)\boldsymbol{P}_{k|k-1}^{-1}\Delta\boldsymbol{y}_i(k) \leqslant J_{th} \tag{12}$$

Note that since $\Delta\boldsymbol{y}_i(k)$ obeys the Gaussian distribution, $J_i(k)$ obeys χ^2 distribution with the degree of freedom d, where d is the dimension of $\boldsymbol{y}_i(k)$. The threshold value J_{th} is an alarm-triggering threshold. If $J_i(k) > J_{th}$, then it is considered as radar i being under attack, and the detection flag is set to $fl_i = 1$. Otherwise, radar i is not under attack, and the detection flag is set to $fl_i = 0$. Additionally, note that the SUM detector can be used to detect carefully crafted FDI attacks (see [22]).

3.2. Attack Parameter Estimation

Very few papers focus on how to estimate the unknown and time-varying attack parameters and eliminate its effect on tracking performance. Inspired by the sensor bias estimation method proposed in [25], we propose a simple-yet-effective attack parameter estimation solution based on a pseudo-measurement equation. Every two radars in the

network are seen as a group. Taking the radar m,n group as an example, assuming that the radar m is the leader of the group, the detailed derivation is given as follows.

Define the pseudo-measurement as

$$\mathbb{Y}(k) = \boldsymbol{y}_m(k) - \boldsymbol{y}_n(k) \tag{13}$$

where $\boldsymbol{y}_m(k)$ and $\boldsymbol{y}_n(k)$ are the measurements of radars m and n, respectively.

If radar m is attacked, substitute Equation (8) into Equation (13), and we can obtain the pseudo-measurement equation of the attack parameter:

$$\mathbb{Y}(k) = \mathbb{H}(k)\mathbb{A}(k) + \mathbb{V}(k) \tag{14}$$

where the pseudo-measurement matrix is expressed as

$$\mathbb{H}(k) = \boldsymbol{A}_m(k) \tag{15}$$

The attack parameter vector is

$$\mathbb{A}(k) = \boldsymbol{a}_m(k) \tag{16}$$

The pseudo-measurement noise is expressed as

$$\mathbb{V}(k) = \boldsymbol{v}_m(k) - \boldsymbol{v}_n(k) \tag{17}$$

Note that the measurement noise $\boldsymbol{v}_m(k)$ and $\boldsymbol{v}_n(k)$ are zero-mean Gaussian noise. Thus, the pseudo-measurement noise covariance is

$$\mathbb{R}(k) = \boldsymbol{R}_m(k) + \boldsymbol{R}_n(k) \tag{18}$$

The time-varying attack parameter can be modeled as

$$\mathbb{A}(k) = \mathbb{F}(k-1)\mathbb{A}(k-1) + \mathbb{W}(k-1) \tag{19}$$

where $\mathbb{F}(k-1)$ is the transition matrix and $\mathbb{W}(k-1)$ is the process noise of the attack parameter with a zero mean and a variance of $\boldsymbol{Q_a}(k-1)$.

Based on the linear pseudo-measurement equation, the standard Kalman filter can be used to obtain the estimation of the attack parameter. Assume that the attack parameter estimate is $\hat{\mathbb{A}}(k-1|k-1)$ at time $k-1$ and its corresponding covariance $\boldsymbol{P}_a(k-1|k-1)$ is available. The attack parameter can be recursively estimated as follows.

Calculate the predicted attack parameter based on Equation (19):

$$\hat{\mathbb{A}}(k|k-1) = \mathbb{F}(k-1)\hat{\mathbb{A}}(k-1|k-1) \tag{20}$$

Calculate the predicted covariance as follows:

$$\boldsymbol{P}_a(k|k-1) = \mathbb{F}(k-1)\boldsymbol{P}_a(k-1|k-1)\mathbb{F}^T(k-1) + \boldsymbol{Q_a}(k-1) \tag{21}$$

Obtain the measurements from both radars, and calculate the pseudo-measurement $\mathbb{Y}(k)$, the pseudo-measurement matrix $\mathbb{H}(k)$ and the measurement noise covariance $\mathbb{R}(k)$ according to Equations (13), (15) and (18), respectively.

Calculate the predicted measurement based on Equation (14):

$$\hat{\mathbb{Y}}(k) = \mathbb{H}(k)\hat{\mathbb{A}}(k|k-1) \tag{22}$$

Calculate the gain as follows:

$$\boldsymbol{S}(k) = \mathbb{R}(k) + \mathbb{H}(k)\boldsymbol{P}_a(k|k-1)\mathbb{H}^T(k) \tag{23}$$

$$\boldsymbol{K}(k) = \boldsymbol{P}_a(k|k-1)\mathbb{H}^T(k)\boldsymbol{S}^{-1}(k) \tag{24}$$

Update the attack parameter estimation and the associated covariance to be

$$\hat{\mathbb{A}}(k|k) = \hat{\mathbb{A}}(k|k-1) + \boldsymbol{K}(k)\Big(\mathbb{Y}(k) - \hat{\mathbb{Y}}(k)\Big) \tag{25}$$

$$\boldsymbol{P}_a(k|k) = \boldsymbol{P}_a(k|k-1) - \boldsymbol{K}(k)\mathrm{S}(k)\boldsymbol{K}^T(k) \tag{26}$$

Remark 1. *The above derivation is based on the assumption that radar m is under FDI attacks. If the detection result shows that there is no radar under attack, then* $\hat{\mathbb{A}}(k|k)$ *is a zero vector.*

3.3. Time Update for Each Group

Before employing the consensus method, each group carries out the time update simultaneously. The time update consists of two steps, prediction and information calculation, which are given as follows.

Prediction. *Given the state* $\hat{\boldsymbol{x}}_i(k-1|k-1)$ *and the covariance* $\boldsymbol{P}_i(k-1|k-1)$ of group i at time $k-1$*:*

$$\hat{\boldsymbol{x}}_i(k|k-1) = \boldsymbol{F}(k-1)\hat{\boldsymbol{x}}_i(k-1|k-1) \tag{27}$$

$$\boldsymbol{P}_i(k|k-1) = \boldsymbol{F}(k-1)\boldsymbol{P}_i(k-1|k-1)\boldsymbol{F}^T(k-1) + \boldsymbol{Q}(k-1) \tag{28}$$

Information Calculation: The information state $\Omega_i(k|k-1)$ and information matrix $\boldsymbol{Y}_i(k|k-1)$ of group i can be calculated as

$$\Omega_i(k|k-1) = \boldsymbol{P}_i(k|k-1)^{-1}\hat{\boldsymbol{x}}_i(k|k-1) \tag{29}$$

$$\boldsymbol{Y}_i(k|k-1) = \boldsymbol{P}_i(k|k-1)^{-1} \tag{30}$$

3.4. Hybrid Consensus

For DSE, consensus estimation is an effective way for state estimation in a radar network that is not fully connected to achieve global consistency for all radars. Existing consensus methods, including the CE, CM, CI and HCMCI methods, were proposed and applied in [9–16]. However, the above methods do not take into account the occurrence of FDI attacks. To address this problem, a novel hybrid consensus method, which can mitigate the FDI attacks and achieve global consistency in a timely manner, is proposed.

In the proposed hybrid consensus procedure, each group is treated as a whole part. If the detection results show that there is no radar under attack in a group, we call the group as not being under attack; otherwise, we call the group as being under attack. Denote ζ_i as the exchanged information of group i. Each group receives iterative exchange information with its neighbors and updates its own information as follows:

$$\zeta_i(t+1) = \sum_{s \in E_i} \pi^{s,i}\zeta_s(t) \tag{31}$$

where t denotes the iteration number and $\pi^{s,i}$ denotes the consensus weight that is given by the Metropolis weights [28] as

$$\pi^{s,i} = \begin{cases} (1+\max\_d)^{-1} s \in E_i and s \neq i \\ 1 - \sum_{\substack{s \in E_i \\ s \neq i}} \pi^{s,i} s = i \\ 0 otherwise \end{cases} \tag{32}$$

where $\max\_d = \max(d_s, d_i)$.

The novel hybrid consensus method combines the CM and CI methods. The CM method employs the consensus method, namely Equations (31) and (32), for the exchanged $\boldsymbol{i}(k)$ and $\boldsymbol{I}(k)$. The tth iteration of consensus for the CM method can be described as follows:

1. Calculate the information state contribution $\boldsymbol{i}_i(k)$ and information matrix contribution $\boldsymbol{I}_i(k)$.The group under an FDI attack can be expressed as

$$\boldsymbol{i}_i(k) = \boldsymbol{H}^T(k)\boldsymbol{R}_i^{-1}(k)\left(\mathbb{Y}_i(k) - \boldsymbol{A}_i(k)\hat{\mathbb{A}}_i(k|k)\right) \tag{33}$$

$$\boldsymbol{I}_i(k) = \boldsymbol{H}^T(k)\boldsymbol{R}_i^{-1}(k)\boldsymbol{H}(k) \tag{34}$$

The group which is not under an FDI attack can be expressed as

$$\boldsymbol{i}_i(k) = \boldsymbol{H}^T(k)\boldsymbol{R}_i^{-1}(k)\mathbb{Y}_i(k) \tag{35}$$

$$\boldsymbol{I}_i(k) = \boldsymbol{H}^T(k)\boldsymbol{R}_i^{-1}(k)\boldsymbol{H}(k) \tag{36}$$

2. Exchange the information contributions. For example, group i broadcasts $\boldsymbol{i}_i(k)$ and $\boldsymbol{I}_i(k)$ to its neighbors and receives $\boldsymbol{i}_s(k)$ and $\boldsymbol{I}_s(k)$ from its neighbors $s \in E_i$.
3. Measurement consensus can be achieved by

$$\begin{aligned} \boldsymbol{i}_i^{t+1}(k) &= \sum_{s \in E_i} \pi^{s,i} \boldsymbol{i}_s^t(k) \\ \boldsymbol{I}_i^{t+1}(k) &= \sum_{s \in E_i} \pi^{s,i} \boldsymbol{I}_s^t(k) \end{aligned} \tag{37}$$

After T iterations, the information state and information matrix can be updated as

$$\Omega_i(k|k) = \Omega_i(k|k-1) + \rho_i(k)\boldsymbol{i}_i^T(k) \tag{38}$$

$$\boldsymbol{Y}_i(k|k) = \boldsymbol{Y}_i(k|k-1) + \rho_i(k)\boldsymbol{I}_i^T(k) \tag{39}$$

where $\rho_i(k)$ are the scalar weights.

Similarly, the CI method employs the consensus method to $\Omega(k|k)$ and $\boldsymbol{Y}(k|k)$. The tth iteration of consensus for the CI method is given as follows:

1. Calculate the updated information matrix $\boldsymbol{Y}_i(k|k)$ and information state $\Omega_i(k|k)$ based on the predicted information matrix and information state:

$$\Omega_i(k|k) = \Omega_i(k|k-1) + \boldsymbol{i}_i(k) \tag{40}$$

$$\boldsymbol{Y}_i(k|k) = \boldsymbol{Y}_i(k|k-1) + \boldsymbol{I}_i(k) \tag{41}$$

Note that for the group under an FDI attack, $\boldsymbol{i}_i(k)$ is calculated based on Equation (33). For the group which is not under an FDI attack, $\boldsymbol{i}_i(k)$ is calculated based on Equation (35).

2. Exchange information contributions. Each group broadcasts $\Omega_i(k|k)$ and $\boldsymbol{Y}_i(k|k)$ to its neighbors and receives information $\Omega_s(k|k)$ and $\boldsymbol{Y}_s(k|k)$, where $s \in E_i$.
3. The information consensus is as follows:

$$\Omega_i^{t+1}(k|k) = \sum_{s \in E_i} \pi^{s,i} \Omega_s^t(k|k) \tag{42}$$

$$\boldsymbol{Y}_i^{t+1}(k|k) = \sum_{s \in E_i} \pi^{s,i} \boldsymbol{Y}_s^t(k|k) \tag{43}$$

To improve the estimation accuracy, we combined the CM and CI methods to obtain a hybrid consensus algorithm, in which each group broadcasted its information $\{\boldsymbol{i}_i(k), \boldsymbol{I}_i(k)\}$ and $\{\Omega_i(k|k-1), \boldsymbol{Y}_i(k|k-1)\}$ to its neighbors and received information $\{\boldsymbol{i}_s(k), \boldsymbol{I}_s(k)\}$ and $\{\Omega_s(k|k-1), \boldsymbol{Y}_s(k|k-1)\}$ from its neighbors $s \in E_i$. Then, we employed the consensus approach to the exchanged information:

$$\Omega_i^{t+1}(k|k-1) = \sum_{s \in E_i} \pi^{s,i} \Omega_s^t(k|k-1) \tag{44}$$

$$\boldsymbol{Y}_i^{t+1}(k|k-1) = \sum_{s \in E_i} \pi^{s,i} \boldsymbol{Y}_s^t(k|k-1) \tag{45}$$

$$\boldsymbol{i}_i^{t+1}(k) = \sum_{s \in E_i} \pi^{s,i} \boldsymbol{i}_s^t(k) \tag{46}$$

$$\boldsymbol{I}_i^{t+1}(k) = \sum_{s \in E_i} \pi^{s,i} \boldsymbol{I}_s^t(k) \tag{47}$$

Therefore, each group updates its information state and information matrix:

$$\Omega_i(k|k) = \Omega_i^T(k|k-1) + \rho_i(k) \boldsymbol{i}_i^T(k) \tag{48}$$

$$\boldsymbol{Y}_i(k|k) = \boldsymbol{Y}_i^T(k|k-1) + \rho_i(k) \boldsymbol{I}_i^T(k) \tag{49}$$

Remark 2. *Note that Equations (45) and (46) are a combination of the CM and CI methods. The combination of the prior information is maintained to ensure fast consensus, and the consensus on measurements is maintained to alleviate the weight deficiency caused by the CI method. In addition, note that if no attack exists in the system, the novel hybrid consensus method becomes the traditional HCMCI method.*

The complete DSE algorithm with FDI attacks is summarized in Table 1.

Table 1. The proposed DSE algorithm with FDI attacks.

Algorithm 1:
1: **Procedure1: Injected data detection:**
2: **for** each radar $i = 1, \ldots, N$ **do**
3: Calculates $J_i(k)$ using Equation (12).
4: If $J_i(k) > J_{th}$, $fl_i = 1$
5: Else $fl_i = 0$.
6: **Procedure2: Attack parameter estimation:**
7: **for** each group
8: Run the time update steps using Equations (20) and (21).
9: Calculate pseudo-measurement $\mathbb{Y}(k)$ the pseudo-measurement matrix $\mathbb{H}(k)$ and the measurement noise covariance $\mathbb{R}(k)$ using Equations (13), (15) and (18), respectively.
10: Run the measurement update steps using Equations (22)–(26).
11: Procedure3: Time update for each group:
12: Each group carries out the time update using Equations (27)–(30).
13: **Procedure4: Hybrid consensus:**
14: **for** each group
15: Calculates the information state contribution $\boldsymbol{i}_i(k)$ and information matrix contribution $\boldsymbol{I}_i(k)$ using Equations (33–36).
16: Calculates the predicted information matrix $\boldsymbol{Y}_i(k\|k-1)$ and information state $\Omega_i(k\|k-1)$ using Equations (29) and (30).
17: **for** $t = 1, 2, \ldots, T$, **do**
18: Exchange information among the groups.
19: Employ consensus approach to the exchanged information using Equations (41)–(44)
20: Each group updates its information state and information matrix using Equations (45) and (46)
21: **Procedure5: State estimation:**
22: Each group calculate its state estimate $\hat{\boldsymbol{x}}_i(k\|k)$ and covariance $\boldsymbol{P}_i(k\|k)$
$\boldsymbol{P}_i(k\|k) = \boldsymbol{Y}_i(k\|k)^{-1}$
$\hat{\boldsymbol{x}}_i(k\|k) = \boldsymbol{P}_i(k\|k) \cdot \Omega_i(k\|k)$

4. Numerical Simulation

In order to show the effectiveness of the proposed DSE algorithm with FDI attacks, two cases are presented. In Section 4.1, assume there are two radars under FDI attacks in an eight-radar network. A comparison between the traditional hybrid consensus-based DSE method [12] (denoted as DSE) and the proposed DSE algorithm with FDI attacks (denoted as DSE-FDI) was made, which shows that DSE-FDI performed better than DSE method. In Section 4.2, the results are given for when four radars were under FDI attacks in an eight-radar network.

By assuming modeling of the target dynamics by the constant velocity model [29], then the matrix can be given by

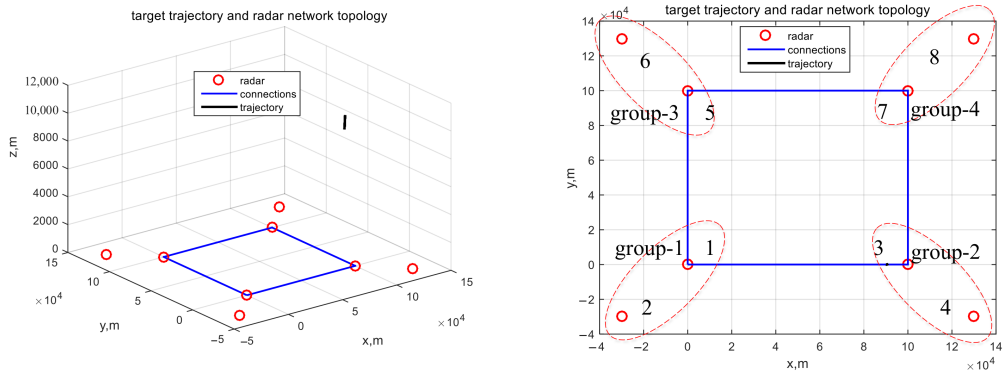
$$\boldsymbol{F}(k-1) = \begin{bmatrix} 1 & 0 & 0 & \Delta t & 0 & 0 \\ 0 & 1 & 0 & 0 & \Delta t & 0 \\ 0 & 0 & 1 & 0 & 0 & \Delta t \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{50}$$

$$\boldsymbol{Q}(k-1) = \sigma_w^2 \begin{bmatrix} \Delta t^3/3 & 0 & 0 & \Delta t^2/2 & 0 & 0 \\ 0 & \Delta t^3/3 & 0 & 0 & \Delta t^2/2 & 0 \\ 0 & 0 & \Delta t^3/3 & 0 & 0 & \Delta t^2/2 \\ \Delta t^2/2 & 0 & 0 & \Delta t & 0 & 0 \\ 0 & \Delta t^2/2 & 0 & 0 & \Delta t & 0 \\ 0 & 0 & \Delta t^2/2 & 0 & 0 & \Delta t \end{bmatrix} \tag{51}$$

where σ_w is the standard deviation of the process noise and Δt is the time step.

In the scenario, the target is tracked by an eight-radar network divided into four groups, as shown in Figure 1. The adjacency matrix of the groups is expressed as

$$A(G) = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \tag{52}$$



(**a**) (**b**)

Figure 1. Simulation scene. (**a**) 3D. (**b**) 2D.

The true initial state of the target is $\boldsymbol{x}_0 = [90{,}000\text{ m } 10{,}000\text{ m } 10{,}000\text{ m } 40\text{ m/s } 40\text{ m/s } 40\text{ m/s}]^{\mathrm{T}}$. The total simulation time is 20 s. The time step is 0.1 s. The standard deviation of the process noise $\sigma_w = 6$. The standard deviation of the measurement noise $\sigma_{ir} = 10$, $\sigma_{i\theta} = \sigma_{i\varphi} = 1 \times 10^{-3}$ for $i = 1, 2, \ldots 8$. The attack sequence is $r_i^a(k) \sim N(20, 0.5)$, $\theta_i^a(k) \sim N\left(5 \times 10^{-3}, 0.2 \times 10^{-3}\right)$, $\varphi_i^a(k) \sim N\left(5 \times 10^{-3}, 0.2 \times 10^{-3}\right)$. The consensus steps of two filters are $T = 1$. The threshold J_{th} is set to be 12.838. The root mean square errors (RMSEs) were used as a metric to compare the performance of different algorithms, defined as

$$RMSE_k = \sqrt{\frac{1}{M}\sum_{i=1}^{M}\left(\hat{\boldsymbol{x}}_k^i - \boldsymbol{x}_k\right)^2} \tag{53}$$

where M denotes the number of Monte Carlo runs, which equals 100 here, $\hat{\boldsymbol{x}}_k^i$ denotes the estimated state at time k in the ith run and $\boldsymbol{x}_k$ denotes the true state at time k.

4.1. Two Radars under Attack

Consider the case that radar 1 and radar 3 are under an FDI attack. The attack begins at time $t = 5$ and ends at time $t = 20$. We first verify the effectiveness of the injected data detection method with DSE-FDI. Figure 2 plots the χ^2 distribution variable $J_i(k)$ over time for radars 1–8. It can be seen that for the attacked radars (radar 1 and radar 3), the alarm triggering condition in Equation (9) was satisfied when an attack existed. For the radars not under attack, $J(k)$ satisfied $0 \le J_i(k) \le J_{th}, i = 2, 4, 5, 6, 7, 8$. In most of the time, with only some false alarms occurring. Note that false alarms will affect the detection flag, resulting in a false trigger of the estimation method. However, as long as the alarm triggering threshold is set properly, the false alarm will not last. Thus, false alarm had little effect on the estimation accuracy. In order to reduce the false alarms, the alarm triggering threshold can be increased appropriately.

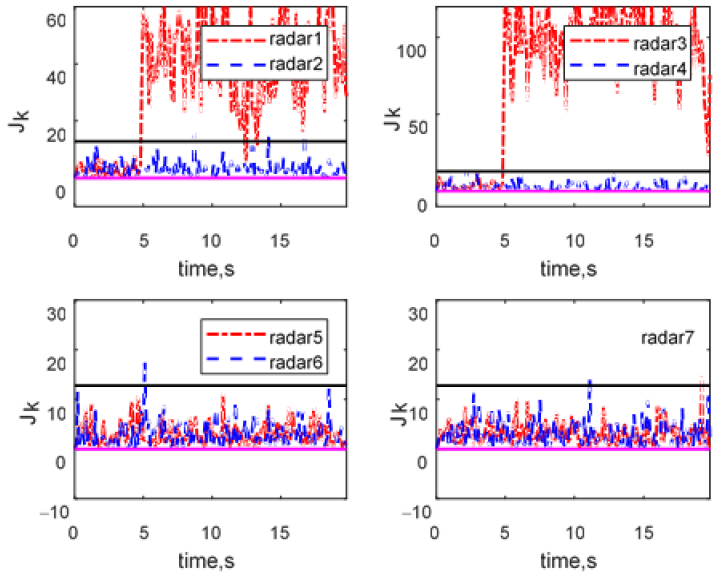


Figure 2. Injected data detection results.

In order to verify the superiority of the proposed attack parameter estimation method in DSE-FDI, the RMSEs of the attack parameter estimations (APE) were obtained by 100 Monte Carlo runs. Figures 3 and 4 plot the RMSE of the estimated range, elevation and azimuth APE for radars 1–4 and radars 5–8 over time, respectively. It can be seen that the APE of all the radars were close to zero during time $t < 5$. The reason for this was that there were no attacks in this time interval. When the simulation time $t > 5$, the attack parameters of radar 1 and radar 3 were estimated, and the RMSEs of the APE converged fast. Note that the RMSEs of APE of other radars were not zero when no attack existed, which was due to the false alarms in the 100 Monte Carlo runs.

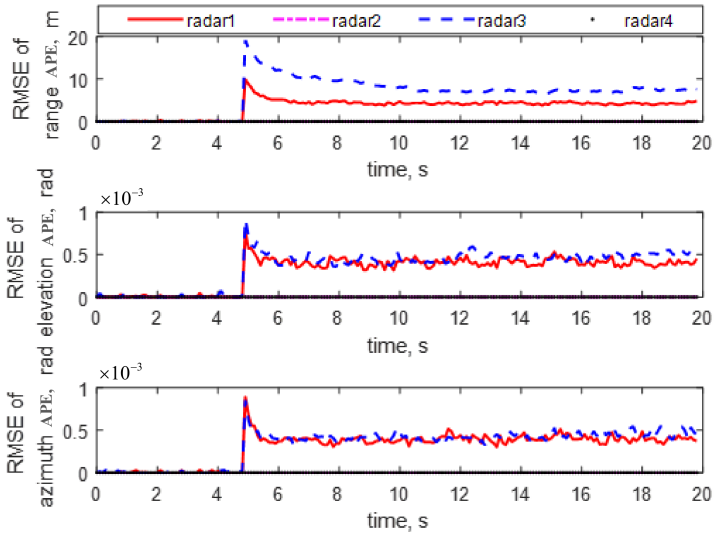


Figure 3. RMSE of the attack parameter estimations for radars 1–4.

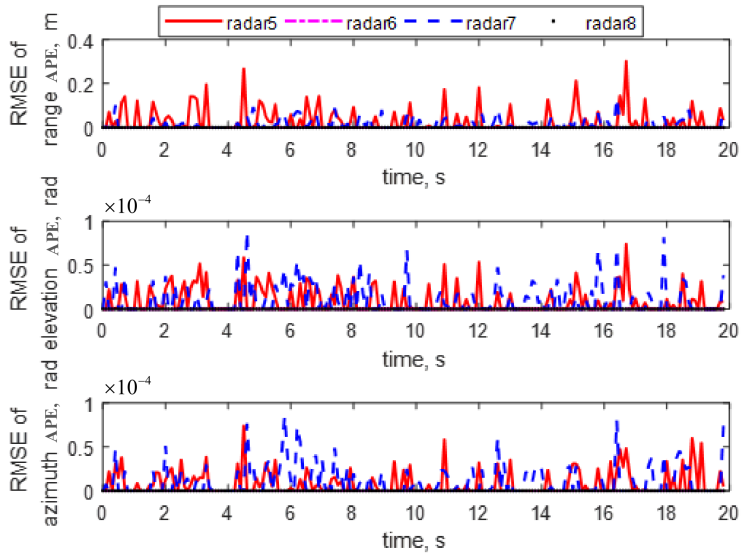


Figure 4. RMSE of the attack parameter estimations for radars 5–8.

After verifying the effectiveness of the proposed injected data detection and attack parameter estimation method, we compared DSE-FDI with the DSE method. Figure 5 plots the RMSE of the estimated position and velocity over time for DSE-FDI and the DSE method. It can be seen that DSE-FDI performed the same as the DSE method when no attack existed, but it performed much better than the DSE method when suffering from an FDI attack.

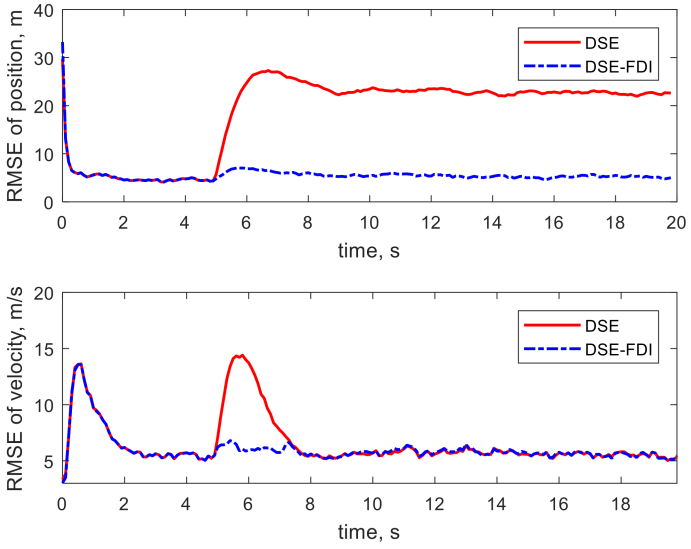


Figure 5. RMSE of the position and velocity over time for different algorithms.

4.2. Four Radars under Attack

In this part scene with four radars under attack was considered to test the estimation accuracy when half the radars in the network were under attack. Radar 1 and radar 3 were attacked starting from simulation time $t = 5$, and radar 5 and radar 7 were attacked starting from simulation time $t = 10$. Figure 6 shows the injected data detection results for all the radars. It can be seen that the attacks could be detected in a timely manner.

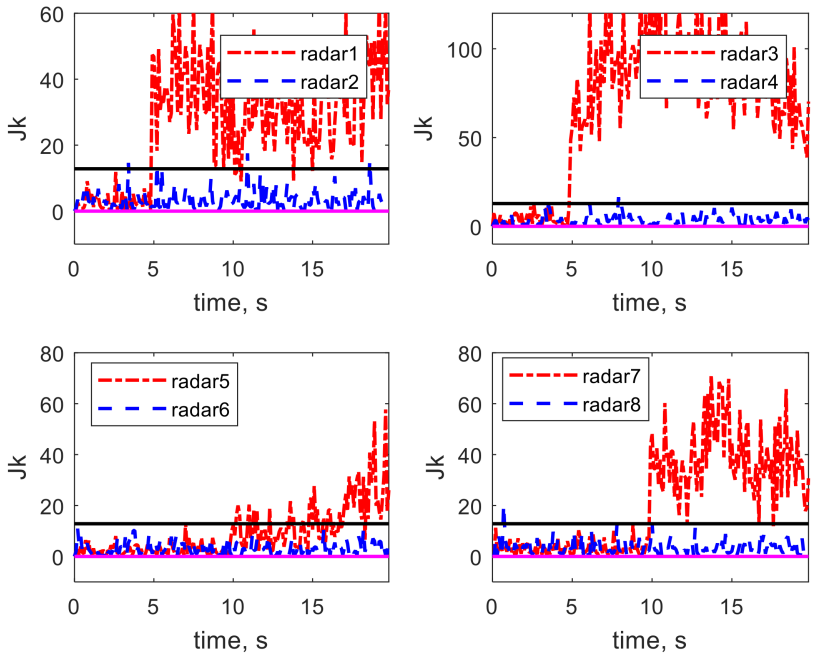


Figure 6. Injected data detection results.

Figures 7 and 8 show the RMSE of the estimated range, elevation and azimuth APE for radars 1–4 and radars 5–8 over time, respectively. It can be seen that the attack parameters could be estimated as soon as the attacks occurred.

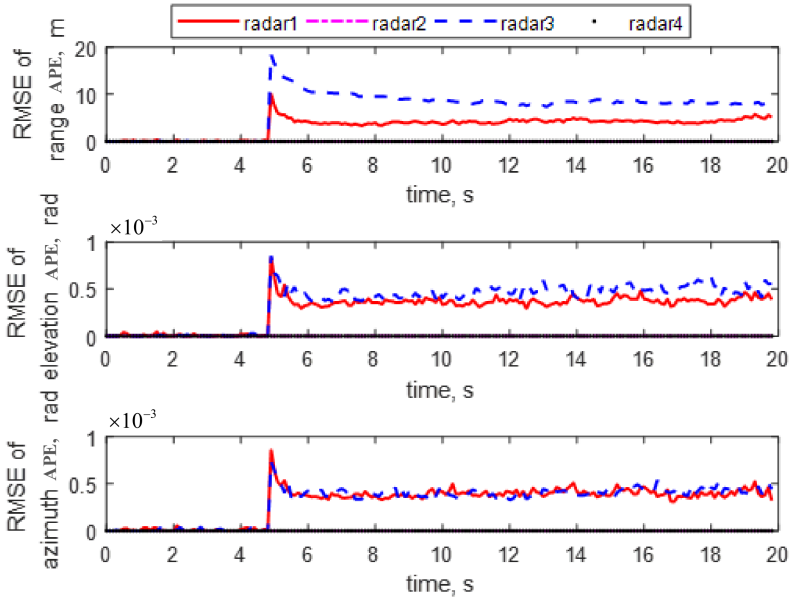


Figure 7. RMSE of the attack parameter estimations for radars 1–4.

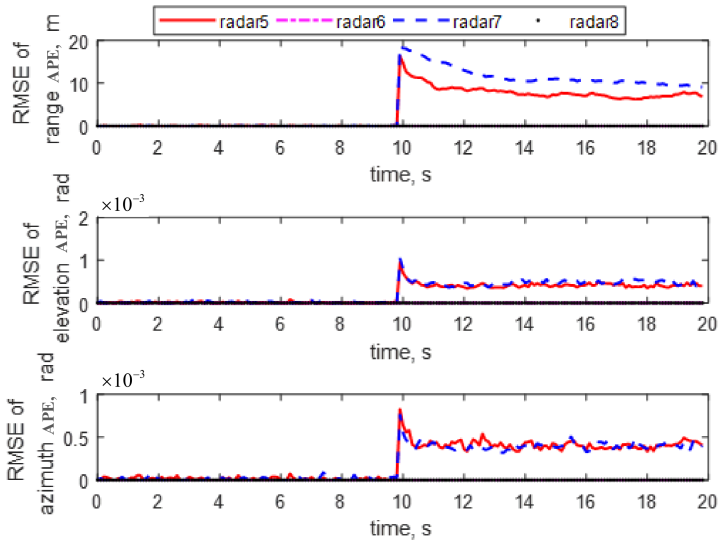


Figure 8. RMSE of the attack parameter estimations for radars 5–8.

To illustrate the superiority of the proposed DSE-FDI method, a comparison with other methods is given. The methods include (1) the traditional hybrid consensus-based DSE method [12] (denoted as DSE); (2) the traditional hybrid consensus-based DSE method with injected data detection, in which the attacked measurements are discarded directly (denoted as DSE-D); and (3) the CM-based method [10] with FDI compensation proposed in this paper (denoted as CM-FDI).

Figure 9 shows that DSE-D diverged as time went on, which was caused by information loss. The performance of DSE decreased as the number of attacked radars increased, and the performance of DSE-FDI was almost unaffected by FDI attacks. Moreover, DSE-FDI performed better than CM-FDI, which verifies the superiority of hybrid consensus over consensus in the measurements.

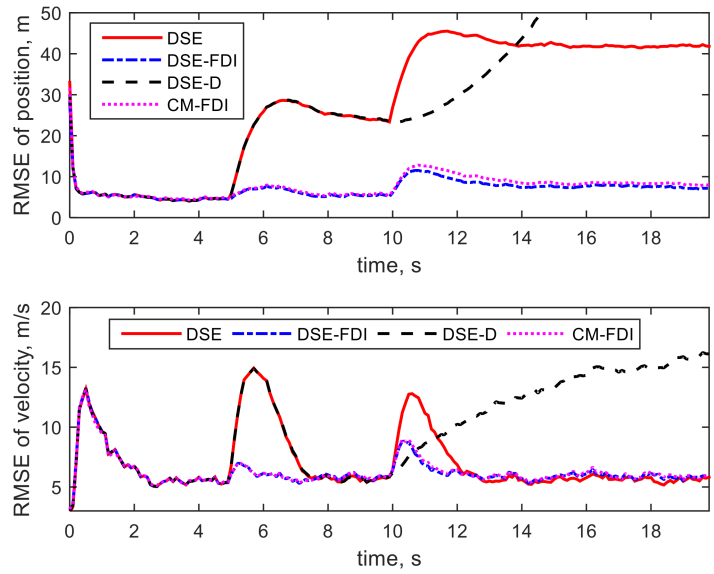


Figure 9. RMSE of the position and velocity over time for different algorithms.

5. Discussion

This paper studied distributed target tracking with FDI attacks. A novel DSE algorithm was proposed to deal with FDI attacks in a radar network which consisted of three main parts: injected data detection, attack parameter estimation and hybrid consensus. In the proposed algorithm, a real time residual-based detector was designed to effectively detect

FDI attacks by analyzing the statistical properties of the residual. A simple yet effective attack parameter estimation method was proposed to estimate the unknown and time-varying attack parameter and state independently. A novel hybrid consensus method was proposed to compensate the estimation error caused by an attack and provide estimation accuracy improvement when the number of consensus iterations was moderate. The simulation results show that the proposed algorithm was superior to other algorithms in the presence of FDI attacks. In the future, we will focus on dealing with other kinds of malicious attacks.

Author Contributions: Conceptualization, Y.S. (Yongtao Shui) and Y.W.; methodology, Y.L. and Y.S. (Yongtao Shui); software, N.C.; validation, Y.S. (Yongzhi Shan), Y.W. and B.P.; formal analysis, N.C.; investigation, Y.L.; resources, Y.S. (Yongtao Shui); data curation, Y.S. (Yongtao Shui) and Y.W.; writing—original draft preparation, Y.W. and Y.L.; writing—review and editing, Y.S. (Yongzhi Shan) and N.C.; visualization, N.C.; supervision, B.P.; project administration, N.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Bartoletti, S.; Conti, A.; Giorgetti, A.; Win, M.Z. Sensor radar networks for indoor tracking. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 157–160.
2. Hessar, F.; Roy, S. Spectrum sharing between a surveillance radar and secondary Wi-Fi networks. *IEEE Trans. Aerosp. Electron. Syst.* **2016**, *52*, 1434–1448. [CrossRef]
3. Hack, D.E.; Patton, L.K.; Himed, B.; Saville, M.A. Detection in Passive MIMO Radar Networks. *IEEE Trans. Signal Process.* **2014**, *62*, 2999–3012. [CrossRef]
4. Deligiannis, A.; Panoui, A.; Lambotharan, S.; Chambers, J.A. Game-Theoretic Power Allocation and the Nash Equilibrium Analysis for a Multistatic MIMO Radar Network. *IEEE Trans. Signal Process.* **2017**, *65*, 6397–6408. [CrossRef]
5. Wang, J.; Liu, J.; Kato, N. Networking and Communications in Autonomous Driving: A Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1243–1274. [CrossRef]
6. Lyu, Y.; Pan, Q.; Lv, J. Unscented Transformation-Based Multi-Robot Collaborative Self-Localization and Distributed Target Tracking. *Appl. Sci.* **2019**, *9*, 903. [CrossRef]
7. Wang, G.; Li, N.; Zhang, Y. Diffusion distributed Kalman filter over sensor networks without exchanging raw measurements. *Signal Process.* **2017**, *132*, 1–7. [CrossRef]
8. Xu, S.; Doğançay, K.; Hmam, H. Distributed pseudolinear estimation and UAV path optimization for 3D AOA target tracking. *Signal Process.* **2017**, *133*, 64–78. [CrossRef]
9. Keshavarz-Mohammadiyan, A.; Khaloozadeh, H. Consensus-based distributed unscented target tracking in wireless sensor networks with state-dependent noise. *Signal Process.* **2018**, *144*, 283–295. [CrossRef]
10. Das, S.; Moura, J.M.F. Distributed Kalman Filtering with Dynamic Observations Consensus. *IEEE Trans. Signal Process.* **2015**, *63*, 4458–4473. [CrossRef]
11. Soatti, G.; Nicoli, M.; Savazzi, S.; Spagnolini, U. Consensus-Based Algorithms for Distributed Network-State Estimation and Localization. *IEEE Trans. Signal Inf. Process. Netw.* **2017**, *3*, 430–444. [CrossRef]
12. Battistelli, G.; Chisci, L.; Mugnai, G.; Farina, A.; Graziano, A. Consensus-Based Linear and Nonlinear Filtering. *IEEE Trans. Automat. Contr.* **2015**, *60*, 1410–1415. [CrossRef]
13. Yu, W.; Xiaogang, W.; Naigang, C. Hybrid consensus-based distributed pseudomeasurement information filter for small UAVs tracking in wireless sensor network. *IET Radar Sonar Navig.* **2019**, *14*, 556–563.
14. Olfati-Saber, R. Kalman-Consensus filter: Optimality, stability, and performance. In Proceedings of the IEEE Conference on Decision and Control, Shanghai, China, 15–18 December 2009.
15. Battistelli, G.; Chisci, L. Kullback-Leibler average, consensus on probability densities, and distributed state estimation with guaranteed stability. *Automatica* **2014**, *50*, 707–718. [CrossRef]
16. Haipeng, W.; You, H.; Yu, L. Squared-root cubature information consensus filter for non-linear decentralised state estimation in sensor networks. *IET Radar Sonar Navig.* **2014**, *8*, 931–938.
17. Yang, C.; Feng, L.; Zhang, H.; He, S.; Shi, Z. A Novel Data Fusion Algorithm to Combat False Data Injection Attacks in Networked Radar Systems. *IEEE Trans. Signal Inf. Process. Netw.* **2018**, *4*, 125–136. [CrossRef]
18. Coluccia, A.; Ricci, G. ABORT-Like Detection Strategies to Combat Possible Deceptive ECM Signals in a Network of Radars. *IEEE Trans. Signal Process.* **2015**, *63*, 2904–2914. [CrossRef]
19. Li, L.; Yang, H.; Xia, Y.; Yang, H. State estimation for linear systems with unknown input and random false data injection attack. *IET Control Theory Appl.* **2019**, *13*, 823–831. [CrossRef]

20. Qin, J.; Li, M.; Shi, L.; Yu, X. Optimal Denial-of-Service Attack Scheduling With Energy Constraint. *IEEE Trans. Automat. Control* **2015**, *60*, 3023–3028.
21. Fei, M.; Pajic, M.; Pappas, G. Stochastic game approach for replay attack detection. In Proceedings of the 52nd IEEE Conference on Decision and Control, Firenze, Italy, 10–13 December 2013.
22. Ye, D.; Zhang, T.-Y. Summation Detector for False Data-Injection Attack in Cyber-Physical Systems. *IEEE Trans. Cybern.* **2019**, *5*, 1–8. [CrossRef]
23. Kurt, M.N.; Yilmaz, Y.; Wang, X. Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 498–513. [CrossRef]
24. Liang, C.; Wen, F.; Wang, Z. Trust-based distributed Kalman filtering for target tracking under malicious cyber attacks. *Inf. Fusion* **2019**, *46*, 44–50. [CrossRef]
25. Taghavi, E.; Tharmarasa, R.; Kirubarajan, T.; Bar-Shalom, Y.; McDonald, M. A practical bias estimation algorithm for multisensor-multitarget tracking. *IEEE Trans. Aerosp. Electron. Syst.* **2016**, *52*, 1–19. [CrossRef]
26. Lin, X.; Bar-Shalom, Y.; Kirubarajan, T. Exact multisensor dynamic bias estimation with local tracks. *IEEE Trans. Aerosp. Electron. Syst.* **2004**, *40*, 576–590.
27. Yu, J.J.Q.; Hou, Y.; Li, V.O.K. Online False Data Injection Attack Detection with Wavelet Transform and Deep Neural Networks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3271–3280. [CrossRef]
28. Qian, C.; Wancheng, W.; Chao, Y.; Xiaoxiang, J.; Jun, Z. Distributed cubature information filtering based on weighted average consensus. *Neurocomputing J.* **2017**, *243*, 115–124.
29. Li, X.R.; Jilkov, V.P. Survey of Maneuvering Target Tracking. Part I: Dynamic Models. *IEEE Trans. Aerosp. Electron. Syst.* **2003**, *39*, 1333–1364.