sensors

MDPI

Article

Distributed Consensus Estimation for Networked Multi-Sensor Systems under Hybrid Attacks and Missing Measurements

Zhijian Cheng, Lan Yang, Qunyao Yuan, Yinren Long and Hongru Ren *

School of Automation, Guangdong-Hong Kong Joint Laboratory for Intelligent Decision and Cooperative Control, and Guangdong Provincial Key Laboratory for Intelligent Decision and Cooperative Control, Guangdong University of Technology, Guangzhou 510006, China; chengzhijian2019@163.com (Z.C.); yanglan202304@163.com (L.Y.); yuanqunyao2000@163.com (Q.Y.); longyinren2022@163.com (Y.L.)
* Correspondence: renhongru2019@gdut.edu.cn

Abstract: Cyber-security research on networked multi-sensor systems is crucial due to the vulnerability to various types of cyberattacks. For the development of effective defense measures, attention is required to gain insight into the complex characteristics and behaviors of cyber attacks from the attacker's perspective. This paper aims to tackle the problem of distributed consensus estimation for networked multi-sensor systems subject to hybrid attacks and missing measurements. To account for both random denial of service (DoS) attacks and false data injection (FDI) attacks, a hybrid attack model on the estimator-to-estimator communication channel is presented. The characteristics of missing measurements are defined by random variables that satisfy the Bernoulli distribution. Then a modified consensus-based distributed estimator, integrated with the characteristics of hybrid attacks and missing measurements, is presented. For reducing the computational complexity of the optimal distributed estimation method, a scalable suboptimal distributed consensus estimator is designed. Sufficient conditions are further provided for guaranteeing the stability of the proposed suboptimal distributed estimator. Finally, a simulation experiment on aircraft tracking is executed to validate the effectiveness and feasibility of the proposed algorithm.

Keywords: networked multi-sensor systems; distributed consensus estimation; hybrid attacks; missing measurements

check for updates

Citation: Cheng, Z.; Yang, L.; Yuan, Q.; Long, Y.; Ren, H. Distributed Consensus Estimation for Networked Multi-Sensor Systems under Hybrid Attacks and Missing Measurements. *Sensors* **2024**, *24*, 4071. https://doi.org/10.3390/s24134071

Academic Editors: Sofiène Affes and Wei Yi

Received: 7 May 2024
Revised: 30 May 2024
Accepted: 20 June 2024
Published: 22 June 2024

1. Introduction

With the advancement of communication technologies, networked multi-sensor systems have garnered significant interest in recent decades [1,2]. Networked multi-sensor systems contain components connected via a shared network, thus reducing unnecessary wired connections, lowering installation costs, and increasing system scalability [3–5]. It is because of such benefits that networked multi-sensor systems are extensively applied in smart grids, autonomous driving, robotics, and satellite navigation [6–8]. However, due to the data transmitted over open and shared communication links, networked multi-sensor systems are vulnerable to malicious cyber attacks, which can pose a huge threat to life and property security [9]. As a result, it is of utmost importance to enhance the security of networked multi-sensor systems to ensure their normal operation. This issue has attracted widespread attention in recent years [10–12].

There are two main categories into which typical attack models in networked multi-sensor systems fall: denial of service (DoS) attacks and deception attacks [13]. As all individuals know, false data injection (FDI) attacks, which are regarded as a typical deception attack, seek to manipulate the transmitted data by injecting some faked data [14]. DoS attacks attempt to prevent legitimate users from accessing the server by sending a great deal of false information, thereby blocking the communication channel [15]. Obviously, both types of cyber attacks can have profound negative impacts on networked multi-sensor systems. This problem has also aroused considerable interest among researchers, especially regarding the estimation and control issues under FDI and DoS attacks. For instance, based on prior research in [14], the author proposed a power system state estimation algorithm under imperfect FDI attacks. The FDI attack model in [14] aimed at compromising defenseless sensors to corrupt measurement information, focusing on the stealthiness of the attack strategy. By utilizing the event-triggered mechanism, a modified secure remote estimator under DoS attacks was designed for cyber-physical systems [16], in which DoS attacks occurring on the sensor-estimator communication channel considered noise and interference. It is common to find only a single type of attack considered in estimation for sensor networks. However, in practical systems, to increase the possibility of success of attacks, adversaries often alternately launch different types of attacks with a certain probability [13]. Such hybrid attacks not only have a greater negative impact on estimation and control algorithms, but also pose challenges to existing attack detection mechanisms [17]. Therefore, this has aroused the interest of researchers to address the estimation and control issues of networked multi-sensor systems under hybrid attacks.

As mentioned before, previous work focused more on centralised multi-sensor systems or single sensor systems, rather than on distributed systems. With the all-round development of computation and communication capabilities in sensor networks, distributed estimation is widely applied in networked multi-sensor systems due to its high robustness, scalability and flexibility [9,18]. However, since information sharing and data transmission are constrained by the inherent coupling relationship between different nodes, distributed sensor networks are more vulnerable to various cyber attacks [19,20]. As a result, it is a critically important yet complicated topic to investigate the security issues of distributed multi-sensor systems. In most existing research, some results such as [21–23] primarily addressed the distributed estimation problem under malicious cyber attacks on communication links connecting sensors, and only considering a single type of attack. To our knowledge, however, few research have addressed the distributed consensus estimation problem under hybrid attacks that occur between estimators, where data transmitted over wireless networks between nodes may be tampered with by attackers.

Note that distributed consensus estimation is formed by integrating multi-agent consensus theory into the standard Kalman filter, so it also faces the challenge of missing measurement issues in traditional state estimation. This challenge has spawned a large amount of related research [24–26]. For instance, a novel locally optimal distributed consensus estimator was presented in [25] for stochastic systems with missing measurements, where the missing measurement phenomena are represented by a set of random variables with Bernoulli distribution. However, reviewing the literature on distributed estimation from the past few years, it is rare to find that issues regarding cyber attacks and network communication such as missing measurements are taken into account simultaneously. This is mainly because the superimposed effect of missing measurements and cyber attacks will accelerate the degradation of distributed estimation performance, eventually leading to system instability.

Drawing from the aforementioned discussions, this paper focuses on distributed consensus estimation issues for networked multi-sensor systems subject to the dual impact of hybrid attacks and missing measurements. The following three points highlight the difficulties encountered in this paper: (1) how to construct a hybrid attack model targeting the estimator–estimator communication channel to account for the joint impact of FDI and DoS attacks? (2) how can the optimal filter gain matrix be determined under the influence of multi-random variables? (3) how to construct suitable sufficient conditions to ensure the convergence of the estimation error under the dual impact of hybrid attacks and missing measurements?

In light of these difficulties, the following is a summary of the main contributions in this paper:

1. Governed by multi-random variables with Bernoulli distribution, a unified hybrid attack model considering the joint impact of random FDI and DoS attacks is proposed. Different from cyber attacks on the sensor-to-estimator communication chan-

nel in [13,18], the proposed hybrid attack disrupts the data transmission between neighboring estimators in the distributed consensus estimation.

2. This paper is the first attempt to provide a modified distributed consensus estimation algorithm for networked multi-sensor systems subject to hybrid attacks and missing measurements. A suboptimal distributed estimation algorithm, simplified by an approximation method, is devised to circumvent the computation of the cross-covariance matrix, thereby reducing the computational complexity.
3. A co-design scheme of consensus gain coefficients, hybrid attack parameters, missing measurement probabilities and model parameters based on Lyapunov stability analysis is proposed. It is theoretically proved that the stability of the proposed distributed consensus estimator can be guaranteed by constructing a sufficient condition.

The following is how the rest of the paper is structured. System models under missing measurements, hybrid attack models, and problem descriptions on the distributed consensus estimation are covered in Section 2. The optimal/suboptimal distributed consensus estimation algorithms are presented in Section 3, respectively. A formal stability analysis procedure is performed in Section 4. A simulation experiment is executed in Section 5, and conclusions are provided in Section 6.

Notation 1. *Throughout the paper, the notations are absolutely standard.* $\mathbb{R}^m$ *means the m-dimensional Euclidean space.* A^T *denotes the transpose of the variable A, and* B^{-1} *represents the inverse matrix of an invertible* $n \times n$ *matrix B. In addition,* $tr(C)$ *is the trace of the matrix C.* $\mathbb{E}\{D\}$ *expresses the expectation of the random variable D. diag{•} is a diagonal matrix, and the random variable X has a probability density function denoted by* $\mathbb{P}\{X\}$. $N(\mu, R)$ *denotes the Gaussian stochastic process with* μ *and R representing the corresponding mean value and covariance matrix, respectively.*

2. Problem Statement

2.1. System Description

This paper considers a class of linear time-invariant systems as

$$x_{k+1} = Ax_k + w_k \tag{1}$$

$$y_{i,k} = H_i x_k + v_{i,k}, \quad i = 1, 2, \cdots, \mathcal{M} \tag{2}$$

where $x_k \in \mathbb{R}^N$ and $y_{i,k} \in \mathbb{R}^M$ are the state vector and measurement vector of the i-th sensor at time instant k, respectively. A and H_i denote the system and measurement matrices, respectively. In addition, the random variables w_k and $v_{i,k}$ are the system noise and the measurement noise respectively, which are assumed to be mutually independent, and satisfy $w_k \sim N(0, Q_k)$ and $v_{i,k} \sim N(0, R_{i,k})$.

In practical applications, due to sensor failure, unsuccessful measurement, or network congestion, etc., the measurement values from sensors are not always consecutive and may be randomly lost [27]. Therefore, the missing measurement model in this paper is described as follows:

$$z_{i,k} = \ \gamma_{i,k} H_i x_k + v_{i,k} \tag{3}$$

where the random variable $\gamma_{i,k}$ that satisfies the Bernoulli distribution is used to describe the missing measurement phenomenon, which is assumed to be uncorrelated with all noise signals. Furthermore, the probability density function of $\gamma_{i,k}$ is

$$\mathbb{P}\{\gamma_{i,k} = 0\} = 1 - \lambda_i$$
$$\mathbb{P}\{\gamma_{i,k} = 1\} = \lambda_i$$

where λ_i represents the probability that the measurement information of the i-th sensor successfully arrives.

2.2. Hybrid Attack Model

To characterize the communication topology of the above sensor network in Equations (1) and (2), consider a fixed undirected graph $G = (V_x, E_x)$ with a set of nodes $V_x = \{v_1, v_2, \cdots, v_n\}$ and a set of edges $E_x \subseteq V_x \times V_x$. In this sensor network, the neighbor set of node i is defined as $N_i = \{j|(i,j) \in E_x\}$, where the total number of neighbors of node i, also called its degree, is expressed as $d_i = |N_i|$.

Derived from previous works in [28], a distributed consensus estimation algorithm is introduced for the above sensor network:

$$\hat{x}_{i,k+1} = A\hat{x}_{i,k} + K_{i,k}(y_{i,k} - H_i\hat{x}_{i,k}) + \epsilon A \sum_{j\in N_i} (\hat{x}_{j,k} - \hat{x}_{i,k}) \tag{4}$$

where $\hat{x}_{i,k}$ is the estimate of the state x_k for node i at time instant k. $K_{i,k}$ is the filter gain matrix to be determined, and ϵ is the consensus gain coefficient. Referring to existing works [29,30], it is noted that $\epsilon \in (0, \frac{1}{\delta})$ with $\delta = \max_i d_i$.

When executing the state estimation process under the distributed consensus estimation in (4), it can be found that not only the innovation of node i itself is utilized, but also the estimation information from node j needs to be integrated. This prompts us to investigate the security of the estimation information transmitted between nodes i and j since the information may be subject to various malicious cyber attacks. Therefore, in order to describe the actual cyber attack characteristics more realistically in this paper, the following hybrid attack model is constructed as

$$\hat{x}^a_{j,k} = \alpha_{ij,k}(\hat{x}_{j,k} + q_{ij,k}b_{ij,k}) + (1 - \alpha_{ij,k})A\hat{x}^a_{j,k-1} \tag{5}$$

where $\hat{x}^a_{j,k}$ denotes the state estimation for node j under hybrid attacks. The random variable $\alpha_{ij,k}$ is used to characterize the occurrence of DoS attacks, which satisfies the Bernoulli distribution. In other words, $\alpha_{ij,k} = 0$ means that the estimation information $\hat{x}_{j,k}$ is subject to DoS attacks and cannot be successfully transmitted; $\alpha_{ij,k} = 1$ indicates otherwise. Furthermore, in the case of DoS attacks, this paper introduces the compensation strategy in [31,32] to improve the loss of transmitted data. $q_{ij,k}$ indicates whether the estimation information transmitted between nodes i and j is subject to FDI attacks, taking values of 0 or 1. The random variable $b_{ij,k} \sim N(0, B_{ij,k})$ is used to model FDI attacks, which is also assumed to be uncorrelated with all noise signals.

2.3. Problem Statement

In terms of that, this paper considers the issues of missing measurements in (3) and hybrid attacks in (5), so the distributed consensus estimation algorithm in (4) is redesigned as

$$\hat{x}_{i,k+1} = A\hat{x}_{i,k} + K_{i,k}(z_{i,k} - \lambda_i H_i\hat{x}_{i,k}) + \epsilon A \sum_{j\in N_i} (\hat{x}^a_{j,k} - \hat{x}_{i,k}) \tag{6}$$

The main goal of this paper, as indicated by the discussion above, is to derive a suitable distributed consensus estimator to estimate the system states under the dual impact of missing measurements and hybrid attacks, and then seek sufficient conditions to ensure the stability of the proposed distributed estimator.

3. Distributed Consensus Estimator

In this section, a suitable Kalman filter gain matrix and error covariance matrix are derived to obtain the state estimates.

For the convenience of presentation, first define

$$\begin{aligned} e_{i,k} &= x_k - \hat{x}_{i,k}, \quad e^a_{j,k} = x_k - \hat{x}^a_{j,k} \\ P_{ij,k} &= \mathbb{E}\{e_{i,k}e^{\mathrm{T}}_{j,k}\}, \quad \hat{P}_{ij,k} = \mathbb{E}\{e^a_{i,k}e^{\mathrm{T}}_{j,k}\} \\ \check{P}_{ij,k} &= \mathbb{E}\{e_{i,k}(e^a_{j,k})^{\mathrm{T}}\}, \quad P^a_{ij,k} = \mathbb{E}\{e^a_{i,k}(e^a_{j,k})^{\mathrm{T}}\} \end{aligned}$$

Theorem 1. *Consider the linear time-invariant system in* (1) *and* (2) *under missing measurements in* (3) *and hybrid attacks in* (5)*. Then, the distributed consensus estimation algorithm designed in* (6) *has the optimal filter gain as follows:*

$$K_{i,k} = \lambda_i A[P_{i,k} + \epsilon \sum_{r\in N_i} (\hat{P}_{ri,k} - P_{i,k})]H_i^T G^{-1}_{i,k}$$

where $G_{i,k} = \lambda_i^2 H_i P_{i,k} H_i^T + \tilde{\lambda}_i H_i \Lambda_k H_i^T + R_{i,k}$*.*

Proof of Theorem 1. According to the above definition, it can be known

$$\begin{aligned} e_{i,k+1} &= x_{k+1} - \hat{x}_{i,k+1} \\ &= (A - \lambda_i K_{i,k} H_i)e_{i,k} - K_{i,k}(\gamma_{i,k} - \lambda_i)H_i x_k \\ &\quad + \epsilon A \sum_{j\in N_i} (e^a_{j,k} - e_{i,k}) + w_k - K_{i,k}v_{i,k} \end{aligned} \tag{7}$$

where

$$\begin{aligned} e^a_{j,k} &= x_k - \hat{x}^a_{j,k} \\ &= \alpha_{ij,k}e_{j,k} - \alpha_{ij,k}q_{ij,k}b_{ij,k} + (1 - \alpha_{ij,k})Ae^a_{j,k-1} \\ &\quad + (1 - \alpha_{ij,k})w_{k-1} \end{aligned} \tag{8}$$

Naturally, we can easily obtain the error covariance matrix

$$\begin{aligned} P_{ij,k+1} &= \mathbb{E}\{e_{i,k+1}e^{\mathrm{T}}_{j,k+1}\} \\ &= (A - \lambda_i K_{i,k} H_i)P_{ij,k}(A - \lambda_j K_{j,k} H_j)^{\mathrm{T}} + K_{i,k}H_i \\ &\quad \times \mathbb{E}\{(\gamma_{i,k} - \lambda_i)(\gamma_{j,k} - \lambda_j)x_k x_k^{\mathrm{T}}\}H_j^{\mathrm{T}} K^{\mathrm{T}}_{j,k} + \epsilon^2 \\ &\quad \times A \sum_{r\in N_i} \sum_{s\in N_j} (P^a_{rs,k} - \hat{P}_{rj,k} - \check{P}_{is,k} + P_{ij,k})A^{\mathrm{T}} \\ &\quad + \epsilon(A - \lambda_i K_{i,k} H_i) \sum_{s\in N_j} (\check{P}_{is,k} - P_{ij,k})A^{\mathrm{T}} \\ &\quad + \epsilon A \sum_{r\in N_i} (\hat{P}_{rj,k} - P_{ij,k})(A - \lambda_j K_{j,k} H_j)^{\mathrm{T}} \\ &\quad + K_{i,k}\mathbb{E}\{v_{i,k}v^{\mathrm{T}}_{j,k}\}K^{\mathrm{T}}_{j,k} + Q_k \end{aligned} \tag{9}$$

When $i = j$, it yields

$$\begin{aligned} P_{i,k+1} &= (A - \lambda_i K_{i,k} H_i)P_{i,k}(A - \lambda_i K_{i,k} H_i)^{\mathrm{T}} + \tilde{\lambda}_i K_{i,k} \\ &\quad \times H_i \Lambda_k H_i^{\mathrm{T}} K^{\mathrm{T}}_{i,k} + \epsilon^2 A \sum_{r\in N_i} \sum_{s\in N_i} (P^a_{rs,k} - \hat{P}_{ri,k} \\ &\quad - \check{P}_{is,k} + P_{i,k})A^{\mathrm{T}} + K_{i,k}R_{i,k}K^{\mathrm{T}}_{i,k} + Q_k \\ &\quad + \epsilon(A - \lambda_i K_{i,k} H_i) \sum_{s\in N_i} (\check{P}_{is,k} - P_{i,k})A^{\mathrm{T}} \\ &\quad + \epsilon A \sum_{r\in N_i} (\hat{P}_{ri,k} - P_{i,k})(A - \lambda_i K_{i,k} H_i)^{\mathrm{T}} \end{aligned} \tag{10}$$

where $\tilde{\lambda}_i = \mathbb{E}\{(\gamma_{i,k} - \lambda_i)(\gamma_{i,k} - \lambda_i)\} = \lambda_i(1 - \lambda_i)$, and $\Lambda_k = \mathbb{E}\{x_k x_k^{\mathrm{T}}\} = A\Lambda_{k-1}A^{\mathrm{T}} + Q_{k-1}$.

In addition, it has

$$\begin{aligned}\hat{P}_{ri,k} = {}& \mathbb{E}\{e^a_{r,k} e^{\mathrm{T}}_{i,k}\} \\ ={}& \alpha_i P_{ri,k} + (1 - \alpha_i)[A\hat{P}_{ri,k-1}(A - \lambda_i K_{i,k-1} H_i)^{\mathrm{T}} \\ & + \epsilon A \sum_{s \in N_i} (P^a_{rs,k-1} - \hat{P}_{ri,k-1})A^{\mathrm{T}} + Q_{k-1}]\end{aligned} \tag{11}$$

$$\begin{aligned}\check{P}_{is,k} = {}& \mathbb{E}\{e_{i,k}(e^a_{s,k})^{\mathrm{T}}\} \\ ={}& \alpha_i P_{is,k} + (1 - \alpha_i)[(A - \lambda_i K_{i,k-1} H_i)\check{P}_{is,k-1}A^{\mathrm{T}} \\ & + \epsilon A \sum_{r \in N_i} (P^a_{rs,k-1} - \check{P}_{is,k-1})A^{\mathrm{T}} + Q_{k-1}]\end{aligned} \tag{12}$$

where $\alpha_i = \mathbb{P}\{\alpha_{ij,k} = 1\}$.

From the definition of $P^a_{ij,k}$, it follows that

$$\begin{aligned}P^a_{rs,k} ={}& \mathbb{E}\{e^a_{r,k}(e^a_{s,k})^{\mathrm{T}}\} \\ ={}& \alpha_i^2 P_{rs,k} + \alpha_i(\check{P}_{rs,k} - \alpha_i P_{rs,k}) + \alpha_i(\hat{P}_{rs,k} - \alpha_i P_{rs,k}) \\ & + (1 - \alpha_i)^2(AP^a_{rs,k-1}A^{\mathrm{T}} + Q_{k-1}) + \alpha_i q_{ir,k} B_{ir,k}\end{aligned} \tag{13}$$

Note that the total estimation error for all nodes is expressed as $\sum_{i=1}^{\mathcal{M}} \mathbb{E}\{\|x_k - \hat{x}_{i,k}\|^2\}$, which is equivalent to $\sum_{i=1}^{\mathcal{M}} \mathrm{tr}(P_{i,k})$. Based on this, the optimal filter gain matrix $K_{i,k}$ can be obtained by solving the equation $\partial \mathrm{tr}(P_{i,k+1})/\partial K_{i,k} = 0$.

Thus, applying the matrix calculus operation theory yields

$$\begin{aligned}\frac{\partial \mathrm{tr}(P_{i,k+1})}{\partial K_{i,k}} ={}& 2(A - \lambda_i K_{i,k} H_i)P_{i,k}(-\lambda_i H_i)^{\mathrm{T}} \\ & + 2\tilde{\lambda}_i K_{i,k} H_i \Lambda_k H_i^{\mathrm{T}} + 2K_{i,k} R_{i,k} \\ & + \epsilon A \sum_{s \in N_i} (\check{P}_{is,k} - P_{i,k})^{\mathrm{T}}(-\lambda_i H_i)^{\mathrm{T}} \\ & + \epsilon A \sum_{r \in N_i} (\hat{P}_{ri,k} - P_{i,k})(-\lambda_i H_i)^{\mathrm{T}} = 0\end{aligned} \tag{14}$$

From Equation (14), we have

$$K_{i,k} = \lambda_i A[P_{i,k} + \epsilon \sum_{r \in N_i} (\hat{P}_{ri,k} - P_{i,k})]H_i^{\mathrm{T}} G_{i,k}^{-1} \tag{15}$$

where $G_{i,k} = \lambda_i^2 H_i P_{i,k} H_i^{\mathrm{T}} + \tilde{\lambda}_i H_i \Lambda_k H_i^{\mathrm{T}} + R_{i,k}$. This finishes the proof of Theorem 1. □

4. A Scalable Estimation Algorithm and Stability Analysis

Note that the derived error covariance matrix in (10) for the proposed distributed consensus estimation algorithm is not scalable in the number of nodes, making it unsuitable for large-scale systems such as smart grids and mobile communication networks [33]. In order to compensate for this weakness, this paper derives the following suboptimal estimation method:

$$\begin{aligned}
\hat{x}_{i,k+1} &= A\hat{x}_{i,k} + K_{i,k}(z_{i,k} - \lambda_i H_i \hat{x}_{i,k}) + \epsilon A \sum_{j\in N_i} (\hat{x}^a_{j,k} - \hat{x}_{i,k}) \\
\hat{x}^a_{j,k} &= \alpha_{ij,k}(\hat{x}_{j,k} + q_{ij,k} b_{ij,k}) + (1 - \alpha_{ij,k}) A \hat{x}^a_{j,k-1} \\
K_{i,k} &= \lambda_i A P_{i,k} H_i^{\mathrm{T}} (\lambda_i^2 H_i P_{i,k} H_i^{\mathrm{T}} + \tilde{\lambda}_i H_i \Lambda_k H_i^{\mathrm{T}} + R_{i,k})^{-1} \\
P_{i,k+1} &= (A - \lambda_i K_{i,k} H_i) P_{i,k} (A - \lambda_i K_{i,k} H_i)^{\mathrm{T}} + \tilde{\lambda}_i K_{i,k} \\
&\quad \times H_i \Lambda_k H_i^{\mathrm{T}} K_{i,k}^{\mathrm{T}} + K_{i,k} R_{i,k} K_{i,k}^{\mathrm{T}} + Q_k
\end{aligned} \tag{16}$$

Remark 1. *Such an assumption is achieved by eliminating the influence of the cross-covariance matrices in the proposed distributed consensus estimation algorithm. Instead, by setting $\epsilon = 0$ in solving Equations (10) and (15) in this paper, a scalable estimator in (16) is obtained. Meanwhile, it can be easily known that the designed estimator is suboptimal due to the missing terms.*

In the following, a formal stability analysis for the suboptimal distributed consensus estimator constructed as (16) is presented. The following assumptions and lemmas are first given as

Assumption 1. *For some positive numbers, the following inequalities are satisfied*

$$\begin{aligned}
\underline{f} \leq &\|A\| \leq \overline{f}, \quad \underline{h}_i \leq \|H_i\| \leq \overline{h}_i \\
\underline{q} I \leq &Q_k \leq \overline{q} I, \quad \underline{r}_i I \leq R_{i,k} \leq \overline{r}_i I \\
&\underline{p}_i I \leq P_{i,k} \leq \overline{p}_i I
\end{aligned}$$

Lemma 1 ([34])**.** *There are real numbers $\overline{v}, \underline{v}, v > 0$ and $0 < \sigma \leq 1$ such that the stochastic process $\mathcal{V}_k(\xi_k)$ satisfies the following inequalities*

$$\underline{v}\|\xi_k\|^2 \leq \mathcal{V}_k(\xi_k) \leq \overline{v}\|\xi_k\|^2 \tag{17}$$

and

$$\mathbb{E}\{\mathcal{V}_{k+1}(\xi_{k+1})|\xi_k\} - \mathcal{V}_k(\xi_k) \leq v - \sigma \mathcal{V}_k(\xi_k) \tag{18}$$

which means that the stochastic process $\mathcal{V}_k(\xi_k)$ is exponentially bounded in mean square, and is bounded with probability one.

Then, the following will present the main results of the stability analysis.

Theorem 2. *For the linear time-invariant system in (1) and (2), consider missing measurements in (3) and hybrid attacks in (5) and the suboptimal distributed consensus estimation algorithm proposed in (16). Under Assumption 1 and setting the following condition*

$$\sum_{j\in N_i} (\hat{x}^a_{j,k} - \hat{x}_{i,k})^T (\hat{x}^a_{j,k} - \hat{x}_{i,k}) \leq \varsigma_i$$

where $\varsigma_i > 0, i = 1, 2, \cdots, n$, the estimation error $e_{i,k}$ is exponentially bounded in mean square and is bounded with probability one.

Proof of Theorem 2. In order to satisfy the conditions of Lemma 1, first construct the augmented estimation error as $e_k = [e^{\mathrm{T}}_{1,k}, e^{\mathrm{T}}_{2,k}, \cdots, e^{\mathrm{T}}_{n,k}]$ and the augmented estimation error covariance as $P_k = \mathrm{diag}\{P_{1,k}, P_{2,k}, \cdots, P_{n,k}\}$, and then define a suitable Lyapunov function as follows

$$\mathcal{V}_k(e_k) = e_k^{\mathrm{T}} P_k^{-1} e_k = \sum_{i=1}^{n} e_{i,k}^{\mathrm{T}} P_{i,k}^{-1} e_{i,k} \tag{19}$$

By Assumption 1, it can be easily obtained

$$\frac{1}{\overline{p}}\|e_k\|^2 \leq \mathcal{V}_k(e_k) \leq \frac{1}{\underline{p}}\|e_k\|^2 \tag{20}$$

which proves that the first condition (17) of Lemma 1 is satisfied with $\underline{\nu} = \frac{1}{\overline{p}}$ and $\overline{\nu} = \frac{1}{\underline{p}}$. Here, $\overline{p} = \max\{\overline{p}_1, \overline{p}_2, \cdots, \overline{p}_n\}$ and $\underline{p} = \min\{\underline{p}_1, \underline{p}_2, \cdots, \underline{p}_n\}$.

To further meet the second requirement for Lemma 1, Equation (19) needs to be extended. Combining Equation (7), the following expression is obtained:

$$\begin{aligned}
\mathbb{E}\{V_{k+1}(e_{k+1})\} = & \sum_{i=1}^{n} \mathbb{E}\{e_{i,k}^{\mathrm{T}}(A - \lambda_i K_{i,k} H_i)^{\mathrm{T}} P_{i,k+1}^{-1}(A - \lambda_i K_{i,k} H_i) \\
& \times e_{i,k}\} + \sum_{i=1}^{n} \mathbb{E}\{\tilde{\lambda}_i x_k^{\mathrm{T}} H_i^{\mathrm{T}} K_{i,k}^{\mathrm{T}} P_{i,k+1}^{-1} K_{i,k} H_i x_k\} \\
& + \epsilon^2 \sum_{i=1}^{n} \mathbb{E}\{\sum_{j \in N_i}(e_{j,k}^{a} - e_{i,k})^{\mathrm{T}} A^{\mathrm{T}} P_{i,k+1}^{-1} A \sum_{j \in N_i}(e_{j,k}^{a} \\
& - e_{i,k})\} + 2\epsilon \sum_{i=1}^{n} \mathbb{E}\{e_{i,k}^{\mathrm{T}}(A - \lambda_i K_{i,k} H_i)^{\mathrm{T}} P_{i,k+1}^{-1} \\
& \times A \sum_{j \in N_i}(e_{j,k}^{a} - e_{i,k})\} + \sum_{i=1}^{n} \mathbb{E}\{w_k^{\mathrm{T}} P_{i,k+1}^{-1} w_k\} \\
& + \sum_{i=1}^{n} \mathbb{E}\{v_{i,k}^{\mathrm{T}} K_{i,k}^{\mathrm{T}} P_{i,k+1}^{-1} K_{i,k} v_{i,k}\}
\end{aligned} \tag{21}$$

According to the definition, $\tilde{\lambda}_i \geq 0$ is horizontally established. Therefore, it follows from Equation (16) and Assumption 1 that

$$\|K_{i,k}\| = \|\lambda_i A P_{i,k} H_i^{\mathrm{T}} (\lambda_i^2 H_i P_{i,k} H_i^{\mathrm{T}} + \tilde{\lambda}_i H_i \Lambda_k H_i^{\mathrm{T}} + R_{i,k})^{-1}\| \leq \frac{\overline{f}\,\overline{p}_i \overline{h}_i}{\lambda_i \underline{h}_i^2 \underline{p}_i} \tag{22}$$

Similarly, according to (16) and (22), we obtain

$$\begin{aligned}
P_{i,k+1} \geq & (A - \lambda_i K_{i,k} H_i) P_{i,k} (A - \lambda_i K_{i,k} H_i)^{\mathrm{T}} + Q_k \\
\geq & (A - \lambda_i K_{i,k} H_i)[P_{i,k} + \frac{\underline{q}}{(\overline{f} + \frac{\overline{f}\,\overline{p}_i \overline{h}_i^2}{\underline{h}_i^2 \underline{p}_i})^2}](A - \lambda_i K_{i,k} H_i)^{\mathrm{T}}
\end{aligned} \tag{23}$$

Then, it can be further obtained, as from inequality (23),

$$(A - \lambda_i K_{i,k} H_i)^{\mathrm{T}} P_{i,k+1}^{-1} (A - \lambda_i K_{i,k} H_i) \leq [1 + \frac{\underline{q}}{\overline{p}_i(\overline{f} + \frac{\overline{f}\,\overline{p}_i \overline{h}_i^2}{\underline{h}_i^2 \underline{p}_i})^2}]^{-1} P_{i,k}^{-1}$$

Therefore, the first term on the right-hand side of Equation (21) can be scaled as

$$\sum_{i=1}^{n}\mathbb{E}\{e_{i,k}^{\mathrm{T}}(A-\lambda_i K_{i,k}H_i)^{\mathrm{T}}P_{i,k+1}^{-1}(A-\lambda_i K_{i,k}H_i)e_{i,k}\} \\ \leq [1+\frac{\underline{q}}{\overline{p}_i(\overline{f}+\frac{\overline{f}\,\overline{p}_i\overline{h}_i^2}{\underline{h}_i^2\underline{p}_i})^2}]^{-1}\mathbb{E}\{V_k(e_k)\} \tag{24}$$

In addition, from (16), we have

$$P_{i,k+1}\geq\tilde{\lambda}_i K_{i,k}H_i\Lambda_k H_i^{\mathrm{T}}K_{i,k}^{\mathrm{T}}$$

Then we have

$$\sum_{i=1}^{n}\mathbb{E}\{\tilde{\lambda}_i x_k^{\mathrm{T}}H_i^{\mathrm{T}}K_{i,k}^{\mathrm{T}}P_{i,k+1}^{-1}K_{i,k}H_i x_k\}\leq\sum_{i=1}^{n}\mathbb{E}\{x_k^{\mathrm{T}}\Lambda_k^{-1}x_k\}=n \tag{25}$$

Further, we proceed to deal with the other terms in (21). Under Assumption 1, we have

$$\epsilon^2\sum_{i=1}^{n}\mathbb{E}\{\sum_{j\in N_i}(e_{j,k}^{a}-e_{i,k})^{\mathrm{T}}A^{\mathrm{T}}P_{i,k+1}^{-1}A\sum_{j\in N_i}(e_{j,k}^{a}-e_{i,k})\} \\ \leq\frac{\epsilon^2\overline{f}^2}{\underline{p}_i}\sum_{i=1}^{n}\sum_{j\in N_i}(e_{j,k}^{a}-e_{i,k})^{\mathrm{T}}(e_{j,k}^{a}-e_{i,k}) \\ =\frac{\epsilon^2\overline{f}^2}{\underline{p}_i}\sum_{i=1}^{n}\sum_{j\in N_i}(\hat{x}_{j,k}^{a}-\hat{x}_{i,k})^{\mathrm{T}}(\hat{x}_{j,k}^{a}-\hat{x}_{i,k}) \tag{26}$$

Choose a condition as

$$\sum_{j\in N_i}(\hat{x}_{j,k}^{a}-\hat{x}_{i,k})^{\mathrm{T}}(\hat{x}_{j,k}^{a}-\hat{x}_{i,k})\leq\varsigma_i \tag{27}$$

where $\varsigma_i>0, i=1,2,\cdots,n$ is a real number. After that, (26) can be scaled as

$$\epsilon^2\sum_{i=1}^{n}\mathbb{E}\{\sum_{j\in N_i}(e_{j,k}^{a}-e_{i,k})^{\mathrm{T}}A^{\mathrm{T}}P_{i,k+1}^{-1}A\sum_{j\in N_i}(e_{j,k}^{a}-e_{i,k})\}\leq\frac{\epsilon^2\overline{f}^2}{\underline{p}_i}\sum_{i=1}^{n}\varsigma_i \tag{28}$$

In terms of the elementary inequality $x^{\mathrm{T}}y+xy^{\mathrm{T}}\leq x^{\mathrm{T}}x+y^{\mathrm{T}}y$, it naturally follows that

$$2\epsilon\sum_{i=1}^{n}\mathbb{E}\{e_{i,k}^{\mathrm{T}}(A-\lambda_i K_{i,k}H_i)^{\mathrm{T}}P_{i,k+1}^{-1}A\sum_{j\in N_i}(e_{j,k}^{a}-e_{i,k})\} \\ \leq\epsilon\sum_{i=1}^{n}\mathbb{E}\{e_{i,k}^{\mathrm{T}}(A-\lambda_i K_{i,k}H_i)^{\mathrm{T}}P_{i,k+1}^{-1}(A-\lambda_i K_{i,k}H_i)e_{i,k}\} \\ +\epsilon\sum_{i=1}^{n}\sum_{j\in N_i}\mathbb{E}\{(e_{j,k}^{a}-e_{i,k})^{\mathrm{T}}P_{i,k+1}^{-1}(e_{j,k}^{a}-e_{i,k})\} \\ \leq\epsilon[1+\frac{\underline{q}}{\overline{p}_i(\overline{f}+\frac{\overline{f}\,\overline{p}_i\overline{h}_i^2}{\underline{h}_i^2\underline{p}_i})^2}]^{-1}\mathbb{E}\{V_k(e_k)\}+\epsilon\sum_{i=1}^{n}\varsigma_i \tag{29}$$

The remaining noise terms will be processed next, and we have

$$\sum_{i=1}^{n}\mathbb{E}\{w_k^{\mathrm{T}}P_{i,k+1}^{-1}w_k\}\leq\frac{1}{\underline{p}_i}\sum_{i=1}^{n}\mathbb{E}\{\mathrm{tr}(w_k w_k^{\mathrm{T}})\}\leq\frac{\overline{q}Nn}{\underline{p}_i} \tag{30}$$

and

$$\sum_{i=1}^{n}\mathbb{E}\{v_{i,k}^{\mathrm{T}}K_{i,k}^{\mathrm{T}}P_{i,k+1}^{-1}K_{i,k}v_{i,k}\} \leq \frac{\overline{f}^2\overline{p}_i^2\overline{h}_i^2}{\lambda_i^2\underline{h}_i^4\underline{p}_i^3}\sum_{i=1}^{n}\mathbb{E}\{\mathrm{tr}(v_{i,k}v_{i,k}^{\mathrm{T}})\} \leq \frac{\overline{f}^2\overline{p}_i^2\overline{h}_i^2\overline{r}_iMn}{\lambda_i^2\underline{h}_i^4\underline{p}_i^3} \tag{31}$$

According to Equations (21), (24), (25) and (28)–(31) can be further scaled as

$$\mathbb{E}\{V_{k+1}(e_{k+1})\} \leq v + (1-\sigma)\mathbb{E}\{V_k(e_k)\} \tag{32}$$

where

$$\begin{aligned}\sigma =& 1-(1+\epsilon)[1+\frac{\underline{q}}{\overline{p}_i(\overline{f}+\frac{\overline{f}\,\overline{p}_i\overline{h}_i^2}{\underline{h}_i^2\underline{p}_i})^2}]^{-1}\\ \epsilon =& (\frac{\epsilon^2\overline{f}^2}{\underline{p}_i}+\epsilon)\sum_{i=1}^{n}\varsigma_i+n+\frac{\overline{q}Nn}{\underline{p}_i}+\frac{\overline{f}^2\overline{p}_i^2\overline{h}_i^2\overline{r}_iMn}{\lambda_i^2\underline{h}_i^4\underline{p}_i^3}\end{aligned}$$

It can be found that the second condition (18) of Lemma 1 is satisfied when $\epsilon < \underline{q}/\overline{p}_i(\overline{f}+\frac{\overline{f}\,\overline{p}_i\overline{h}_i^2}{\underline{h}_i^2\underline{p}_i})^2$. Finally, it can be concluded that the estimation error is bounded with probability one and exponentially bounded in mean square, which completes the proof of Theorem 2. □

5. Simulation Results

In this section, a simulation example of the aircraft tracking problem moving in two-dimensional horizontal plane is presented. The state vector is defined as $x_k = [\zeta_k, \dot{\zeta}_k, \eta_k, \dot{\eta}_k]^{\mathrm{T}}$, which consists of position (ζ_k, η_k) and velocity $(\dot{\zeta}_k, \dot{\eta}_k)$. The tracking system considered in this section is as described in (1) and (2), where the relevant parameters are defined as follows:

$$A = \begin{bmatrix} 1 & T & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & T \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad T = 1$$

$$Q_k = 0.04\begin{bmatrix} T^4/4 & T^3/2 & 0 & 0 \\ T^3/2 & T^2 & 0 & 0 \\ 0 & 0 & T^4/4 & T^3/2 \\ 0 & 0 & T^3/2 & T^2 \end{bmatrix}$$

To track the target aircraft, ten distributed sensors with the topology shown in Figure 1 are utilized, where each sensor interacts with only a matched estimator. The target position is generated as the sensor measurement

$$y_{i,k} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} x_k + v_{i,k}, \quad i = 1, 2, \cdots, \mathcal{M}$$

where the measurement noise covariance is set to $R_{i,k} = i * R_0$ with $R_0 = \mathrm{diag}\{0.2^2, 0.2^2\}$. Further, the initial state is set to $x_0 = [10, 1.5, 10, 1.2]^{\mathrm{T}}$.

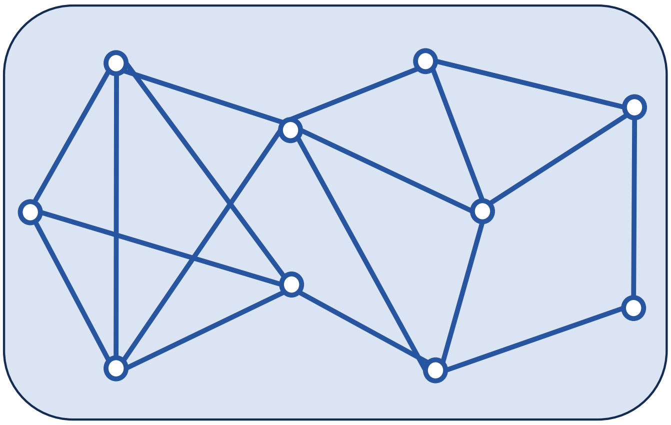

Figure 1. Network topology with $\mathcal{M} = 10$.

In addition, the root-mean-square errors (RMSEs) are introduced to more precisely assess the estimation performance. The RMSEs on position and velocity over all sensors are respectively defined as

$$\mathrm{RMSE}_k^p = \sqrt{\frac{1}{M}\sum_{t=1}^{M}\left[\left(\zeta_k - \hat{\zeta}_{t,k}\right)^2 + \left(\eta_k - \hat{\eta}_{t,k}\right)^2\right]}$$

$$\mathrm{RMSE}_k^v = \sqrt{\frac{1}{M}\sum_{t=1}^{M}\left[\left(\dot{\zeta}_k - \hat{\dot{\zeta}}_{t,k}\right)^2 + \left(\dot{\eta}_k - \hat{\dot{\eta}}_{t,k}\right)^2\right]}$$

where $M = 100$ represents 100 Monte Carlo runs over 10 targets. $\hat{\zeta}_{t,k}$, $\hat{\eta}_{t,k}$, $\hat{\dot{\zeta}}_{t,k}$, and $\hat{\dot{\eta}}_{t,k}$ are the estimates of position and velocity at time k from the i-th run, respectively.

The performance of the proposed distributed consensus estimation algorithm under hybrid attacks and missing measurements is shown in Figure 2, where the measurement arrival probability λ_i is set to 0.9 and the consensus gain is chosen as 0.05. It is assumed that the hybrid attack considered in (5) only occurs between two targets, where the relevant parameters are set to $\alpha_i = 0.5$ and $B_{ij,k} = 0.04I$. It can be found that the distributed consensus estimator still has good tracking performance in position and velocity under hybrid attacks and missing measurements. In addition, the RMSEs in position for ten estimators are presented in Figure 3. It can be seen that all the curves fluctuate around the horizontal axis 0, which also proves the effectiveness of the proposed algorithm in (16). Further, RMSEs in position with different consensus gains $\epsilon = 0.05, 0.1, 0.15, 0.2$ are plotted in Figure 4. It can be seen that when $\epsilon = 0.05, 0.1, 0.15$, the curves still fluctuate near the horizontal axis 0, but when $\epsilon = 0.2$, the curve rises rapidly. Thus, it can be found that the consensus parameter in this paper has an upper bound. Once this upper bound is exceeded, the estimator lacks stability, which also proves the correctness of Theorem 2. It is worth noting that the consensus parameters need to be chosen very carefully to make a tradeoff between tracking performance and stability.

On the other hand, the performance of the proposed distributed consensus estimation algorithm under hybrid attacks, FDI attacks in [30] and DoS attacks, as well as without attacks in [35] are compared in Figure 5. For examining the impact of different attack scenarios on the proposed distributed estimation algorithm, it is first necessary to exclude the interference of the missing measurement, so the measurement arrival probability λ_i is set to 1 in this comparison experiment. As shown in Figure 5, RMSEs under hybrid attacks are significantly higher than those under other attack scenarios, while RMSEs under only DoS attacks are almost the same as those without attacks. This proves that hybrid attacks have a greater impact on the proposed distributed estimator than only one single type of attack. In addition, this paper introduces a compensation strategy for DoS attacks. Thus, only DoS attacks have little impact on the estimation performance of the proposed distributed estimator, which is clearly demonstrated in Figure 6. As shown in Figure 6, RMSEs in position do not change significantly as the DoS attack probability increases, strongly proving the effectiveness of the compensation strategy. Further, RMSEs in position under different FDI attack intensities are plotted in Figure 7. In order to better characterize the FDI attack intensity, the standard deviation ς of the random attack variable $b_{ij,k}$ is introduced. It is clear that the proposed distributed consensus estimator has certain resistance to FDI attacks when ς is small. Finally, it is noted that hybrid attacks will degrade the estimation performance in Figure 5, but the distributed estimator proposed in this paper can still remain stable, which is a major advantage of this algorithm.

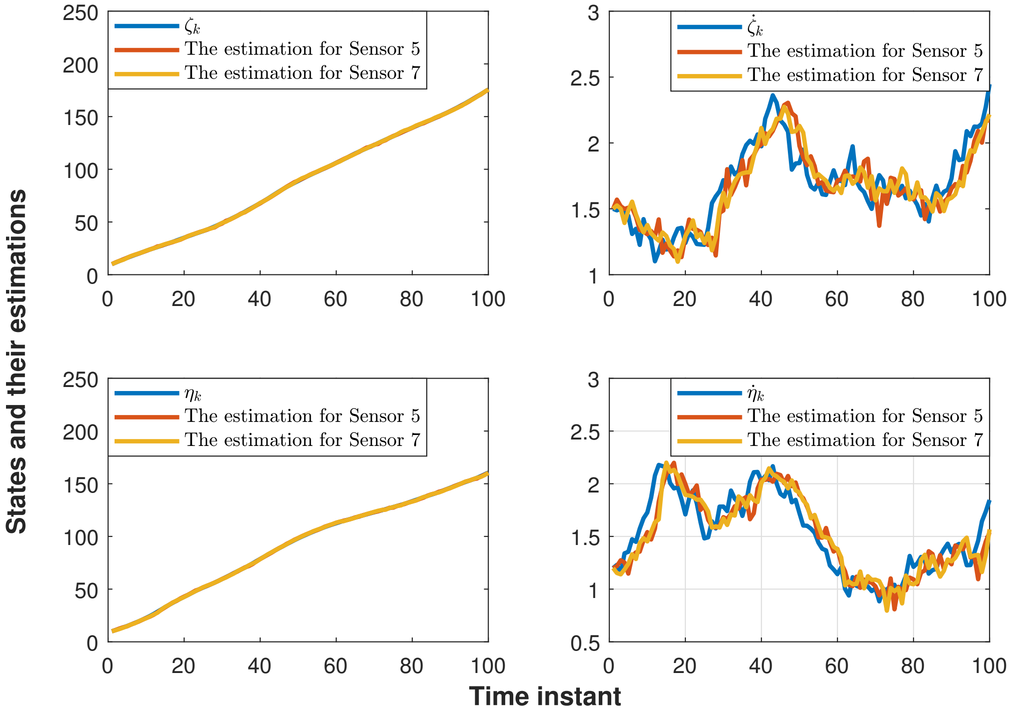

Figure 2. States and their estimations for sensors 5 and 7.

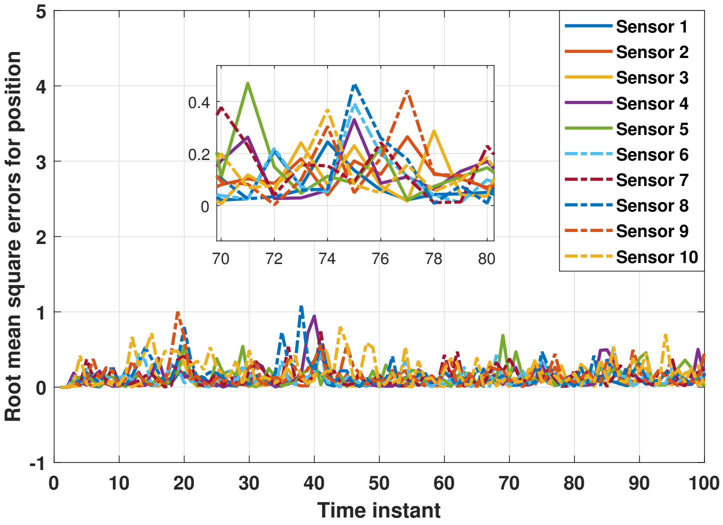

Figure 3. RMSEs in position for ten estimators.

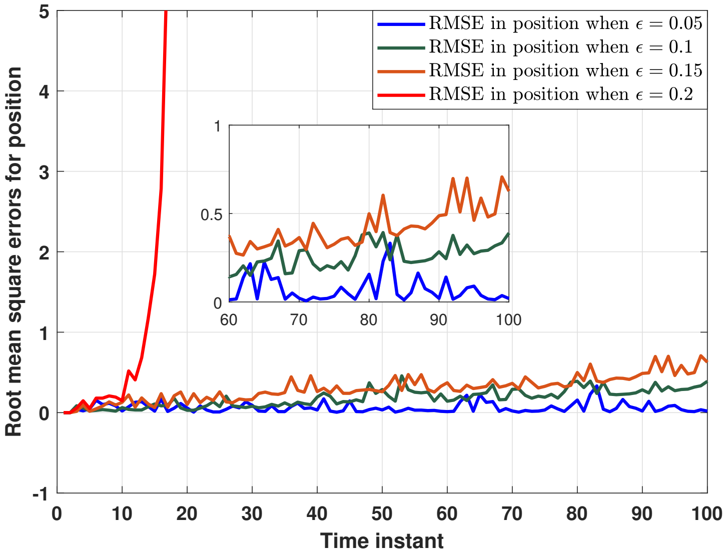

Figure 4. RMSEs in position with different consensus parameter.

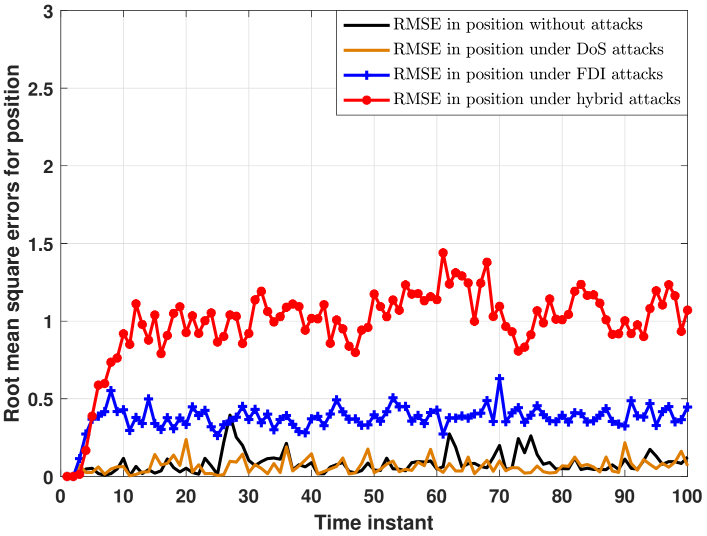

Figure 5. RMSEs in position under hybrid attacks, FDI attacks and DoS attacks as well without attacks.

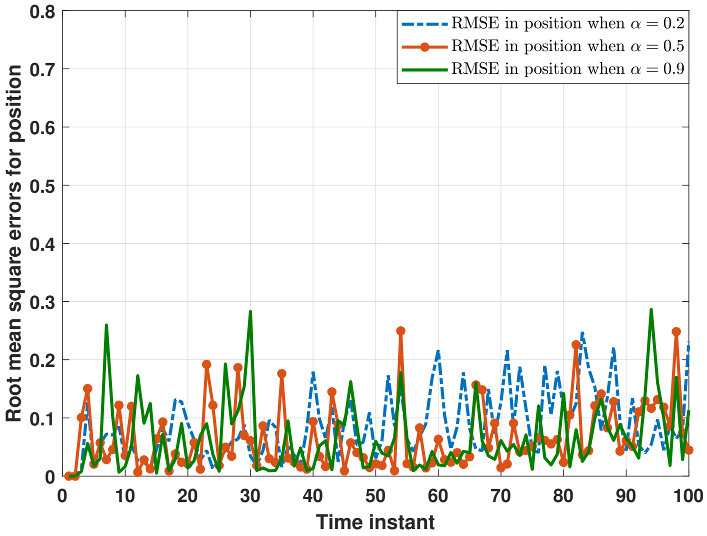

Figure 6. RMSEs in position under different DoS attack probabilities.

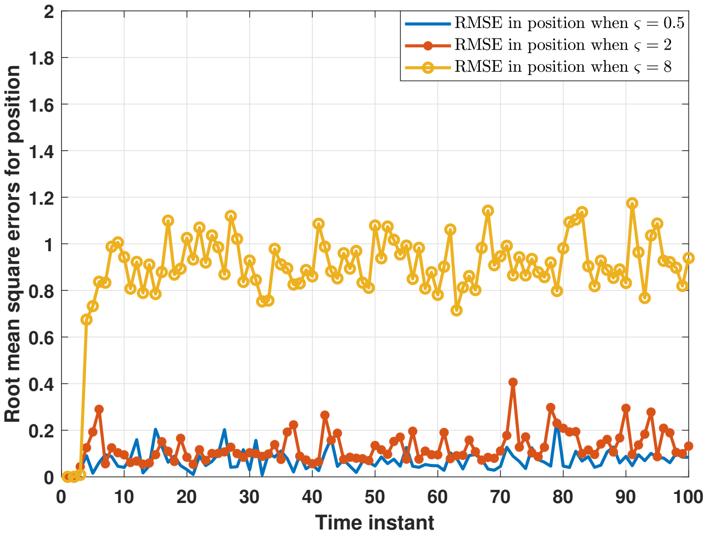

Figure 7. RMSEs in position under different FDI attack intensities.

6. Conclusions

In this paper, a modified distributed consensus estimation algorithm has been provided for networked multi-sensor systems subject to hybrid attacks and missing measurements. A random variable satisfying the Bernoulli distribution has been applied to account for the missing measurement phenomenon. From the viewpoint of the attacker, a unified hybrid attack model has been constructed to disrupt the data transmission between neighboring estimators, which takes into account the characteristics and behaviors of both random FDI and DoS attacks. Starting from optimality and scalability, optimal/suboptimal distributed consensus estimators have been proposed, respectively. Furthermore, sufficient conditions for convergence of the proposed distributed suboptimal estimator have been obtained. It has been explicitly established that there are correlations between the convergence and hybrid attack model as well as missing measurement parameters. Future works will focus on extending linear multi-sensor systems to nonlinear systems.

Author Contributions: Conceptualization, Z.C. and H.R.; methodology, Z.C.; software, L.Y. and Q.Y.; validation, Z.C., L.Y. and Q.Y.; formal analysis, Z.C.; investigation, Z.C.; resources, L.Y.; data curation, L.Y. and Q.Y.; writing—original draft preparation, Z.C.; writing—review and editing, Z.C.; visualization, Y.L.; supervision, H.R.; project administration, Y.L.; funding acquisition, Z.C. and H.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by the National Natural Science Foundation of China under Grants 62303121, 62121004, U23A20341, 62303125, and 62373111, the China Postdoctoral Science Foundation under Grants 2023M740750, and in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2022A1515110949 and 2023B1515120010.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

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

Abbreviations

The following abbreviations are used in this manuscript:

FDI	false data injection
DoS	denial of service
RMSEs	root-mean-square errors

References

1. Zhou, H.; Sun, S. Distributed filtering for multi-sensor networked systems with stochastic communication protocol and correlated noises. *Inf. Fusion* **2024**, *104*, 102121. [CrossRef]
2. Zhou, J.; Yang, W.; Zhang, H.; Zheng, W.X.; Xu, Y.; Tang, Y. Security analysis and defense strategy of distributed filtering under false data injection attacks. *Automatica* **2022**, *138*, 110151. [CrossRef]
3. Zha, L.; Guo, Y.; Liu, J.; Xie, X.; Tian, E. Protocol-based distributed security fusion estimation for time-varying uncertain systems over sensor networks: Tackling DoS attacks. *IEEE Trans. Signal Inf. Process. Over Netw.* **2024**, *10*, 119–130. [CrossRef]
4. Ren, H.; Ma, H.; Li, H.; Wang, Z. Adaptive fixed-time control of nonlinear MASs with actuator faults. *IEEE/CAA J. Autom. Sin.* **2023**, *10*, 1252–1262. [CrossRef]
5. Ren, H.; Liu, Z.; Liang, H.; Li, H. Pinning-based neural control for multiagent systems with self-regulation intermediate event-triggered method. *IEEE Trans. Neural Netw. Learn. Syst.* **2024**. [CrossRef] [PubMed]
6. Xu, S.; Ye, D.; Li, G.; Yang, D. Globally stealthy attacks against distributed state estimation in smart grid. *IEEE Trans. Autom. Sci. Eng.* **2024**. [CrossRef]
7. Wang, J.; Liu, J.; Kato, N. Networking and communications in autonomous driving: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1243–1274. [CrossRef]
8. Lee, J.H.; Hashimoto, H. Controlling mobile robots in distributed intelligent sensor network. *IEEE Trans. Ind. Electron.* **2003**, *50*, 890–902. [CrossRef]
9. Huang, J.; Tang, Y.; Yang, W.; Li, F. Resilient consensus-based distributed filtering: Convergence analysis under stealthy attacks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4878–4888. [CrossRef]
10. Niu, M.; Wen, G.; Lv, Y.; Chen, G. Innovation-based stealthy attack against distributed state estimation over sensor networks. *Automatica* **2023**, *152*, 110962. [CrossRef]
11. Chen, Y.; Kar, S.; Moura, J.M. Resilient distributed estimation: Sensor attacks. *IEEE Trans. Autom. Control* **2019**, *64*, 3772–3779. [CrossRef]
12. Han, F.; Wang, Z.; Dong, H.; Alsaadi, F.E.; Alharbi, K.H. A local approach to distributed H_∞-consensus state estimation over sensor networks under hybrid attacks: Dynamic event-triggered scheme. *IEEE Trans. Signal Inf. Process. Over Netw.* **2022**, *8*, 556–570. [CrossRef]
13. Chen, Y.; Meng, X.; Wang, Z.; Dong, H. Event-triggered recursive state estimation for stochastic complex dynamical networks under hybrid attacks. *IEEE Trans. Neural Netw. Learn. Syst.* **2023**, *34*, 1465–1477. [CrossRef] [PubMed]
14. Cheng, Z.; Ren, H.; Qin, J.; Lu, R. Security analysis for dynamic state estimation of power systems with measurement delays. *IEEE Trans. Cybern.* **2023**, *53*, 2087–2096. [CrossRef]
15. Li, T.; Chen, B.; Yu, L.; Zhang, W.A. Active security control approach against DoS attacks in cyber-physical systems. *IEEE Trans. Autom. Control* **2021**, *66*, 4303–4310. [CrossRef]
16. Sun, Y.C.; Yang, G.H. Event-triggered remote state estimation for cyber-physical systems under malicious DoS attacks. *Inf. Sci.* **2022**, *602*, 43–56. [CrossRef]
17. Liu, J.; Wang, Y.; Cao, J.; Yue, D.; Xie, X. Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack. *IEEE Trans. Cybern.* **2021**, *51*, 4000–4010. [CrossRef]
18. Lv, Y.; Lu, J.; Liu, Y.; Lou, J. Resilient distributed state estimation under stealthy attack. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 3254–3263. [CrossRef]
19. Zhou, J.; Yang, W.; Ding, W.; Zheng, W.X.; Xu, Y. Watermarking-based protection strategy against stealthy integrity attack on distributed state estimation. *IEEE Trans. Autom. Control* **2023**, *68*, 628–635. [CrossRef]
20. Li, X.M.; Yao, D.; Li, P.; Meng, W.; Li, H.; Lu, R. Secure finite-horizon consensus control of multiagent systems against cyber attacks. *IEEE Trans. Cybern.* **2022**, *52*, 9230–9239. [CrossRef]
21. An, D.; Zhang, F.; Cui, F.; Yang, Q. Toward data integrity attacks against distributed dynamic state estimation in smart grid. *IEEE Trans. Autom. Sci. Eng.* **2024**, *21*, 881–894. [CrossRef]
22. Lei, X.; Wen, G.; Zheng, W.X.; Fu, J. Security strategy against location-varying sparse attack on distributed state monitoring. *IEEE Trans. Autom. Control* **2024**, *69*, 2514–2521. [CrossRef]
23. Zhang, T.Y.; Ye, D.; Shi, Y. Decentralized false-data injection attacks against state omniscience: Existence and security analysis. *IEEE Trans. Autom. Control* **2023**, *68*, 4634–4649. [CrossRef]
24. Li, W.; Jia, Y.; Du, J. Distributed Kalman consensus filter with intermittent observations. *J. Frankl. Inst.* **2015**, *352*, 3764–3781. [CrossRef]
25. Hu, J.; Wang, Z.; Liu, G.P.; Zhang, H.; Navaratne, R. A prediction-based approach to distributed filtering with missing measurements and communication delays through sensor networks. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 7063–7074. [CrossRef]
26. Jin, H.; Sun, S. Distributed filtering for multi-sensor systems with missing data. *Inf. Fusion* **2022**, *86*, 116–135. [CrossRef]
27. Liang, J.; Wang, Z.; Liu, X. State estimation for coupled uncertain stochastic networks with missing measurements and time-varying delays: The discrete-time case. *IEEE Trans. Neural Netw.* **2009**, *20*, 781–793. [CrossRef]
28. Ren, H.; Cheng, Z.; Qin, J.; Lu, R. Deception attacks on event-triggered distributed consensus estimation for nonlinear systems. *Automatica* **2023**, *154*, 111100. [CrossRef]

29. Yang, W.; Yang, C.; Shi, H.; Shi, L.; Chen, G. Stochastic link activation for distributed filtering under sensor power constraint. *Automatica* **2017**, *75*, 109–118. [CrossRef]
30. Yang, W.; Zhang, Y.; Chen, G.; Yang, C.; Shi, L. Distributed filtering under false data injection attacks. *Automatica* **2019**, *102*, 34–44. [CrossRef]
31. Du, D.; Li, X.; Li, W.; Chen, R.; Fei, M.; Wu, L. ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1698–1711. [CrossRef]
32. Qin, J.; Li, M.; Shi, L.; Yu, X. Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks. *IEEE Trans. Autom. Control* **2018**, *63*, 1648–1663. [CrossRef]
33. Cheng, Z.; Ren, H.; Zhang, B.; Lu, R. Distributed Kalman filter for large-scale power systems with state inequality constraints. *IEEE Trans. Ind. Electron.* **2021**, *68*, 6238–6247. [CrossRef]
34. Reif, K.; Gunther, S.; Yaz, E.; Unbehauen, R. Stochastic stability of the discrete-time extended Kalman filter. *IEEE Trans. Autom. Control* **1999**, *44*, 714–728. [CrossRef]
35. Li, W.; Wang, Z.; Ho, D.W.; Wei, G. On boundedness of error covariances for Kalman consensus filtering problems. *IEEE Trans. Autom. Control* **2019**, *65*, 2654–2661. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.