sensors

MDPI

Article

Distributed Optimal and Self-Tuning Filters Based on Compressed Data for Networked Stochastic Uncertain Systems with Deception Attacks

Yimin Ma and Shuli Sun *

School of Electronic Engineering, Heilongjiang University, Harbin 150080, China
* Correspondence: sunsl@hlju.edu.cn; Tel.: +86-136-7468-6865

Abstract: In this study, distributed security estimation problems for networked stochastic uncertain systems subject to stochastic deception attacks are investigated. In sensor networks, the measurement data of sensor nodes may be attacked maliciously in the process of data exchange between sensors. When the attack rates and noise variances for the stochastic deception attack signals are known, many measurement data received from neighbour nodes are compressed by a weighted measurement fusion algorithm based on the least-squares method at each sensor node. A distributed optimal filter in the linear minimum variance criterion is presented based on compressed measurement data. It has the same estimation accuracy as and lower computational cost than that based on uncompressed measurement data. When the attack rates and noise variances of the stochastic deception attack signals are unknown, a correlation function method is employed to identify them. Then, a distributed self-tuning filter is obtained by substituting the identified results into the distributed optimal filtering algorithm. The convergence of the presented algorithms is analyzed. A simulation example verifies the effectiveness of the proposed algorithms.

Keywords: multiplicative noise; weighted measurement fusion; unknown attack rate; identification; distributed self-tuning filter

Citation: Ma, Y.; Sun, S. Distributed Optimal and Self-Tuning Filters Based on Compressed Data for Networked Stochastic Uncertain Systems with Deception Attacks. *Sensors* **2023**, *23*, 335. https://doi.org/10.3390/s23010335

Academic Editor: Raquel Caballero-Aguila

Received: 23 November 2022
Revised: 16 December 2022
Accepted: 19 December 2022
Published: 28 December 2022

1. Introduction

With the development of science and technology, networked systems or sensor networks [1] have been gradually applied to various key infrastructures. The networked systems introduce the network into a control system and realise data sharing among sensors, actuators, and controllers. The networked systems have the characteristics of low cost, simple maintenance, and flexibility. During data exchange between sensor nodes, data may be attacked maliciously by the networks. Methods to address the injected data in the state estimation are of importance. Therefore, the state estimation for systems with network attacks attracts considerable interest in the field of security estimation.

The types of network attacks mainly include deception, DoS, and replay attacks. The deception attack implies that an attacker injects false data into the network channels to affect the performance of the system [2]. The DoS attack implies that the attacker jams network channels to prohibit the transmission of data [3]. The replay attack is a special form of deception attack [4] in which an attacker puts captured historical data back into the channels. The current research on the three types of network attacks has attracted considerable attention. In [5], a deception attack model has been presented against state estimation in electric power grids. In [6], the distributed security filtering problem of wireless sensor networks under network deception attacks has been studied. By introducing an exponential function, a protector has been designed for each sensor node according to an innovation sequence, and an attack protection model is presented. In [7,8], the fusion estimation problem of deception attack signals has been studied for cyberphysical systems.

Under the network DoS attack, the event-triggered security estimation problems of sensor networks have been addressed in [9–11], whereas the distributed dimensional-reduction fusion estimators have been designed in [12,13]. In [14], the optimal DoS attack scheduling problem from the attacker's perspective has been studied. The distributed detection for the DoS attack has also been developed in [15]. In [16], a model with a compensation has been developed to describe the replay attack, and then a recursive distributed estimator is devised in the LMV criterion. In [17], a distributed set membership filter is proposed for linear time-varying systems over sensor networks with limited bandwidths. The discrimination between the replay attack and sensor fault is investigated under an event-triggered transmission mechanism in [18]. In [19], the problem of detection and defence of replay attacks has been studied. In [20–22], the problem of security control and estimation under hybrid attacks has been also investigated.

In networked systems, there are many network-induced stochastic uncertainties in addition to network attacks, such as random delays, packet losses, and multiplicative noises, which affect the performance of the systems [1]. Stochastic uncertain systems have various applications; e.g., parameter errors in system models and fading channels in data transmissions can be depicted by multiplicative noises, and environmental disturbances can be often depicted by additive noises. For multisensor stochastic uncertain systems with random parameters, delays, and packet dropouts, a distributed fusion filter is presented in [23]. For multirate uncertain nonlinear systems with coloured measurement noises, a robust fusion algorithm has been designed in [24]. In the above literature, the statistical characteristics of noises are assumed to be known. Otherwise, adaptive or self-tuning estimation algorithms need to be designed. By using the correlation function method to identify the statistical characteristics of unknown noises, the distributed fusion self-tuning estimators have been proposed for multisensor systems with unknown noise variances in [25,26]. The distributed fusion self-tuning filters have also been developed for multisensor networked systems with unknown model parameters and data loss rates in [27–29]. For nonlinear systems, a fuzzy energy-to-peak filter [30] and distributed fusion filters [31] have also been studied. However, network attacks in networked systems are not involved in the above literature.

Compared to the centralised fusion estimation where the data of all nodes are transmitted to a fusion centre, the distributed fusion estimation based on the network topology has an advantage of resource sharing among sensor nodes. Each node acts as a local fusion centre. Each node can fuse the information from itself and its neighbours to improve the performance of the system. However, as a large amount of data from neighbour nodes is processed, an augmentation method will impose a costly computational overhead. To reduce the computational cost of the filter, the augmented measurement data received at each sensor node can be compressed to a dimensionality reduction measurement before being used for filtering. In addition, the data exchanged between sensor nodes may be subject to malicious attacks from the network. Therefore, it is vital to investigate the distributed security estimation problem of sensor networks based on data compression.

There have been few studies on the network security estimation of mixed uncertain systems subject to multiplicative noises, additive noises, including both state-dependent and noise-dependent multiplication and stochastic deception attacks. In this study, from the perspective of a defender, the distributed security estimation based on data compression is investigated for sensor networks. In contrast to [5–12], which only consider network attacks, and [23–29], which consider uncertainties of system model parameters and noise covariance, this study considers stochastic uncertainties of multiplicative noises, additive noises, and stochastic deception attacks. In contrast to the results on distributed estimation for multisensor systems in the above literature, where a large amount of data are not compressed and directly used by filters, data are first compressed and then used by filters in this study, which can reduce the computational burden of the filter. In contrast to the results on distributed estimation for systems with deception attacks in [32], where attack rates and noise variances of deception attack signals are assumed to be known, distributed

self-tuning filters with unknown attack rates and noise variances of deception attack signals is designed in this study. However, attack rates and noise variances of deception attack signals are often unknown in practical applications.

The contributions of this paper are presented as follows.

(a) In the studied systems, mixed uncertainties of multiplicative noises, additive noises, and stochastic deception attacks are comprehensively considered, which can better reflect some practical systems.

(b) Under the known attack rates and noise variances of stochastic deception attack signals, a weighted measurement fusion algorithm in the least squares is used to compress the measurements of the sensor and its neighbours at each node, and then a distributed optimal filter is presented in the LMV. It has the same accuracy as that based on uncompressed data. Moreover, it has a lower computational cost than that based on uncompressed data.

(c) Under the unknown attack rates and noise variances of the stochastic deception attack signals, a correlation function method is employed to identify the attack rates and noise variances of attack signals at each node and then a distributed self-tuning filter is designed. The convergence of the distributed self-tuning filtering algorithm is analyzed; it converges to the distributed optimal filter if the identifications of attack rates and noise variances of attack signals are consistent.

The rest of this paper is organised as follows. The problem formulation is presented in Section 2. The distributed optimal filter is presented based on compressed data in Section 3. In Section 4, the distributed self-tuning filter based on compressed data is presented and its convergence is analyzed. An example is given in Section 5. Finally, conclusions are presented in Section 6.

Notations: R^n represents the n -dimensional Euclidean space, $R^{n\times n}$ is the set of $n \times n$ real matrices, A^{T} and A^{-1} are the transpose and inverse of matrix A, respectively, $\mathrm{E}\{\bullet\}$ is the expectation, $\mathrm{Cov}\{\bullet\}$ is the covariance, $\rho(A)$ is the spectral radius of matrix A, $\|\bullet\|$ is the Euclidean norm of a real vector or spectral norm of a real matrix, $A \otimes B$ is the Kronecker product of matrices A and B, and δ_{tk} is the Kronecker delta function.

2. Problem Formulation

Consider the multisensor, linear, time-invariant stochastic uncertain system,

$$x(t+1) = (A + \sum_{l=1}^{q} \alpha_l(t) A_l)x(t) + (B + \sum_{l=1}^{q} \beta_l(t) B_l)\omega(t), \tag{1}$$

$$y_i(t) = (C_i + \sum_{l=1}^{q} h_{il}(t) C_{il})x(t) + v_i(t), \quad i = 1, 2, \ldots, L, \tag{2}$$

where $x(t) \in R^n$ is the system state, $y_i(t) \in R^{m_i}$ is the measurement of the ith sensor, $\alpha_l(t) \in R$, $\beta_l(t) \in R$, and $h_{il}(t) \in R$, $l = 1, 2, \ldots, q$, are multiplicative noises to depict stochastic uncertainties of model parameters, where q is a positive integer, $\omega(t) \in R^r$ is the process noise, $v_i(t) \in R^{m_i}$ is the measurement noise, and A, B, C_i, A_l, B_l and C_{il} are constant matrices with appropriate dimensions. The subscript i corresponds to the ith sensor, and L is the number of sensors.

Assumption 1. *Multiplicative noises $\alpha_l(t) \in R$, $\beta_l(t) \in R$, and $h_{il}(t) \in R$ are uncorrelated white noises with zero mean and covariance Q_{α_l}, Q_{β_l}, and $Q_{h_{il}}$, respectively; process noise $\omega(t) \in R^r$ and measurement noise $v_i(t)$ are uncorrelated white noises with zero mean and covariance Q_ω and Q_{v_i}. Moreover, multiplicative noises $\alpha_l(t)$, $\beta_l(t)$, and $h_{il}(t)$ are uncorrelated with additive noises $\omega(t)$ and $v_i(t)$.*

Assumption 2. *The initial state value $x(0)$ is uncorrelated with $\omega(t)$, $v_i(t)$, $\alpha_l(t)$, $\beta_l(t)$, and $h_{il}(t)$, with the mean and covariance as*

$$\mathrm{E}\{x(0)\} = \mu_0, \mathrm{E}\Big\{[x(0)-\mu_0][x(0)-\mu_0]^{\mathrm{T}}\Big\} = P_0. \tag{3}$$

Assumption 3. *A is a stable matrix, and $\rho(A \otimes A + \sum_{l=1}^{q} Q_{\alpha_l} A_l \otimes A_l) < 1$.*

Assumption 1 describes the statistical characteristics of noises. Assumption 2 provides the statistical characteristics of the initial state. They are applicable to state estimation problems in general [23,33]. Assumption 3 implies that the studied systems are stable in the mean square sense, which guarantees the existence of the state second moment in the later text [34].

We consider a sensor network consisting of L sensor nodes. Its topology is described by a graph $G = (V, \mathcal{E})$, where $V = \{1, 2, \ldots, L\}$ is the set of sensor nodes, and $\mathcal{E} = \{(i, j) : i, j \in V\} \subset V \times V$ is the edge set formed by the interactive connections between nodes. We denote the set of neighbour nodes of sensor i by $N_i = \{j \in V : (j, i) \in \mathcal{E}\}$, where $(j, i) \in \mathcal{E}$ indicates that the sensor i can receive the data transmitted by its neighbour node j. We denote the number of neighbour nodes of sensor i as d_i.

In the process of data exchange between nodes, the measurement data may be attacked maliciously by the network. We consider the following form of network deception attack signals when the sensor i transmits its measurement data through the network,

$$\vec{y}_i(t) = -y_i(t) + \sigma_i(t), \quad i = 1, 2, \ldots, L, \tag{4}$$

where $\sigma_i(t)$ is a white noise with zero-mean and variance Q_{σ_i}, independent of other random variables.

Considering the limited energy of the attacker and limited network source, the attack does not always exist and may occur randomly. If we assume that the attack signal satisfies Bernoulli distribution in the network, the measurement data of the attacked sensor node i satisfies the following equation,

$$\bar{y}_i(t) = y_i(t) + \gamma_i(t)\vec{y}_i(t), \tag{5}$$

where $\gamma_i(t)$ is a Bernoulli random variable with the following known statistical characteristics $\mathrm{E}\{\gamma_i(t) = 1\} = \bar{\gamma}_i$, $\mathrm{E}\{\gamma_i(t) = 0\} = 1 - \bar{\gamma}_i$, $\mathrm{Cov}\{\gamma_i(t)\} = \bar{\gamma}_i(1 - \bar{\gamma}_i)$, $0 \le \bar{\gamma}_i \le 1$. In the model (5), if $\gamma_i(t) = 0$ implies the absence of an attack, $\gamma_i(t) = 1$ implies a complete attack. Thus, model (5) is more general.

The purpose of this study is to devise a distributed optimal filter in the LMV sense under the known attack rates $\bar{\gamma}_{i_k}$ and noise variances $Q_{\sigma_{i_k}}$, $i_k \in N_i$ of the deception attack signals, and distributed self-tuning filter under the unknown attack rates $\bar{\gamma}_{i_k}$ and noise variances $Q_{\sigma_{i_k}}$, $i_k \in N_i$ of the deception attack signals at each sensor node i, based on its measurement data $y_i(t)$ and measurement data $\bar{y}_{i_k}(t)$, $k = 1, 2, ..., d_i$ received from its neighbour nodes $i_k \in N_i$.

Remark 1. *The studied systems contain uncertainties due to multiplicative and additive noises. Multiplicative noises can be used to describe parameter errors in system modelling and signal transmission fading. Additive noises can be used to describe the background environmental disturbances of the systems.*

3. Distributed Optimal Filter

Before presenting a distributed self-tuning filter, a distributed optimal filter is first presented in this section. By compressing measurement data of sensor itself and neighbor nodes, a distributed optimal filter in the LMV criterion is devised under the condition that the attack rates and noise variances of the deception attack signals are known.

3.1. Model Transformation

At sensor node i, a distributed optimal filter is devised based on the measurements $y_i(t)$ and $\bar{y}_{i_k}(t)$ of it and its neighbour nodes $i_k \in N_i$. However, the received measurement data $\bar{y}_{i_k}(t)$ from its neighbour nodes $i_k \in N_i$ may be subject to deception attacks. Systems (1) and (2) is then transformed as follows:

$$x(t+1) = Ax(t) + \underline{\omega}(t) \tag{6}$$

$$y_i(t) = C_i x(t) + \underline{v}_i(t) \tag{7}$$

$$\bar{y}_{i_k}(t) = \bar{C}_{i_k} x(t) + \bar{v}_{i_k}(t), \quad i_k \in N_i \tag{8}$$

where

$$\bar{C}_{i_k} = (1 - \bar{\gamma}_{i_k}) C_{i_k} \tag{9}$$

$$\underline{\omega}(t) = \sum_{l=1}^{q} \alpha_l(t) A_l x(t) + B\omega(t) + \sum_{l=1}^{q} \beta_l(t) B_l \omega(t) \tag{10}$$

$$\underline{v}_i(t) = v_i(t) + \sum_{l=1}^{q} h_{il}(t) C_{il} x(t) \tag{11}$$

$$\bar{v}_{i_k}(t) = [\bar{\gamma}_{i_k} - \gamma_{i_k}(t)] C_{i_k} x(t) + [1 - \gamma_{i_k}(t)] \sum_{l=1}^{q} h_{i_k l}(t) C_{i_k l} x(t) + \gamma_{i_k}(t) \sigma_{i_k}(t) + [1 - \gamma_{i_k}(t)] v_{i_k}(t). \tag{12}$$

$\bar{y}_{i_k}(t), i_k \in N_i, k = 1, 2, \cdots, d_i$ are the measurements of the neighbour nodes of sensor node i. $\underline{\omega}(t)$ is the new process noise, $\underline{v}_i(t)$ is the new measurement noise of the transformed systems (6) and (7), and $\bar{v}_{i_k}(t)$, $i_k \in N_i$ are the measurement noises of the neighbour nodes of sensor node i. $\underline{\omega}(t)$, $\underline{v}_i(t)$, and $\bar{v}_{i_k}(t)$ are still white noises of zero-mean and covariance matrices $Q_{\underline{\omega}}(t) = \mathrm{E}\{\underline{\omega}(t)\underline{\omega}^{\mathrm{T}}(t)\}$, $Q_{\underline{v}_i}(t) = \mathrm{E}\{\underline{v}_i(t)\underline{v}_i^{\mathrm{T}}(t)\}$, $Q_{\bar{v}_{i_k}}(t) = \mathrm{E}\{\bar{v}_{i_k}(t)\bar{v}_{i_k}^{\mathrm{T}}(t)\}$:

$$Q_{\underline{\omega}}(t) = \sum_{l=1}^{q} Q_{\alpha_l} A_l X(t) A_l^{\mathrm{T}} + B Q_\omega B^{\mathrm{T}} + \sum_{l=1}^{q} Q_{\beta_l} B_l Q_\omega B_l^{\mathrm{T}} \tag{13}$$

$$Q_{\underline{v}_i}(t) = Q_{v_i} + \sum_{l=1}^{q} Q_{h_{il}} C_{il} X(t) C_{il}^{\mathrm{T}} \tag{14}$$

$$Q_{\bar{v}_{i_k}}(t) = \bar{\gamma}_{i_k}(1 - \bar{\gamma}_{i_k}) C_{i_k} X(t) C_{i_k}^{\mathrm{T}} + (1 - \bar{\gamma}_{i_k}) \sum_{l=1}^{q} Q_{h_{i_k l}} C_{i_k l} X(t) C_{i_k l}^{\mathrm{T}} + \bar{\gamma}_{i_k} Q_{\sigma_{i_k}} + (1 - \bar{\gamma}_{i_k}) Q_{v_{i_k}}. \tag{15}$$

According to (1), the state second moment $X(t) = \mathrm{E}\{x(t)x^{\mathrm{T}}(t)\}$ can be recursively calculated as

$$X(t+1) = AX(t)A^{\mathrm{T}} + \sum_{l=1}^{q} Q_{\alpha_l} A_l X(t) A_l^{\mathrm{T}} + B Q_\omega B^{\mathrm{T}} + \sum_{l=1}^{q} Q_{\beta_l} B_l Q_\omega B_l^{\mathrm{T}}, \tag{16}$$

with an initial of value $X(0) = \mu_0 \mu_0^{\mathrm{T}} + P_0$.

Under Assumption 3, the state second moment $X(t)$ is bounded [34]. Thus, $Q_{\underline{\omega}}(t)$ in (13), $Q_{\underline{v}_i}(t)$ in (14), and $Q_{\bar{v}_{i_k}}(t)$ in (15) are also bounded, which is necessary for the filter design.

Based on the measurements (7) and (8), each node augments its measurement $y_i(t)$ and receives measurements $\bar{y}_{i_k}(t)$ of its neighbour nodes. The augmented measurement equation is

$$Y_i^{(\mathrm{a})}(t) = C_i^{(\mathrm{a})} x(t) + V_i^{(\mathrm{a})}(t), \tag{17}$$

where $Y_i^{(a)}(t) = [y_i^T(t), \bar{y}_{i_1}^T(t), \cdots, \bar{y}_{i_{d_i}}^T(t)]^T$, $C_i^{(a)} = [C_i^T, \bar{C}_{i_1}^T, \cdots, \bar{C}_{i_{d_i}}^T]^T$, $V_i^{(a)}(t) = [\underline{v}_i^T(t), \bar{V}_i^T(t)]^T$ and $\bar{V}_i(t) = \left[\bar{v}_{i_1}^T(t), \cdots, \bar{v}_{i_{d_i}}^T(t)\right]$. The superscript (a) denotes the augmentation.

The statistical characteristic of the noise $V_i^{(a)}(t)$ is

$$Q_{V_i^{(a)}}(t) = \mathrm{E}\left\{ V_i^{(a)}(t)(V_i^{(a)}(t))^T \right\} = \mathrm{diag}[Q_{\underline{v}_i}(t), Q_{\bar{V}_i}(t)],$$

where $Q_{\bar{V}_i}(t) = \mathrm{E}\{\bar{V}_i(t)\bar{V}_i^T(t)\} = \mathrm{diag}[Q_{\bar{v}_{i_1}}(t), Q_{\bar{v}_{i_2}}(t), \cdots, Q_{\bar{v}_{i_{d_i}}}(t)]$.

For the state Equation (6) and augmented measurement (17), the standard Kalman filtering algorithm [35] can be applied to obtain the distributed filter at each sensor node. However, the distributed filter based on the augmented measurement (17) has a heavy computational cost due to the high dimension of the augmented measurement, where the gain matrix requires the inverse of a high-dimensional matrix. To overcome this shortcoming, the augmented high-dimensional measurement can be compressed to a low-dimensional measurement, and then the filter is designed based on the compressed data, reducing the computational burden.

3.2. DOFCD

An augmented measurement is compressed to a dimensionality reduction measurement using a weighted least-squares algorithm [36] in this subsection.

For the augmented measurement Equation (17), if $\mathrm{rank}\{C_i^{(a)}\} = r_i \leqslant \min\{n, \bar{m}_i\}$, where $\bar{m}_i = m_i + \sum_{k=1}^{d_i} m_{i_k}$, there is a full rank decomposition:

$$C_i^{(a)} = F_i^{(c)} C_i^{(c)}, \tag{18}$$

where $F_i^{(c)} \in R^{\bar{m}_i \times r_i}$ is a full column rank matrix and $C_i^{(c)} \in R^{r_i \times n}$ is a full row rank matrix. Let

$$F_i^{(c)} = [F_i^T, F_{i_1}^T, \cdots, F_{i_{d_i}}^T]^T. \tag{19}$$

The augmented measurement (17) can be rewritten as

$$Y_i^{(a)}(t) = F_i^{(c)} C_i^{(c)} x(t) + V_i^{(a)}(t). \tag{20}$$

By applying the weighted least-squares algorithm to compress the measurement, we obtain

$$\begin{aligned} &[F_i^T Q_{\underline{v}_i}^{-1}(t) F_i + \sum_{k=1}^{d_i} F_{i_k}^T Q_{\bar{v}_{i_k}}^{-1}(t) F_{i_k}]^{-1} [F_i^T Q_{\underline{v}_i}^{-1}(t) y_i(t) + \sum_{k=1}^{d_i} F_{i_k}^T Q_{\bar{v}_{i_k}}^{-1}(t) \bar{y}_{i_k}(t)] \\ &= C_i^{(c)} x(t) + [F_i^T Q_{\underline{v}_i}^{-1}(t) F_i + \sum_{k=1}^{d_i} F_{i_k}^T Q_{\bar{v}_{i_k}}^{-1}(t) F_{i_k}]^{-1} [F_i^T Q_{\underline{v}_i}^{-1}(t) \underline{v}_i(t) + \sum_{k=1}^{d_i} F_{i_k}^T Q_{\bar{v}_{i_k}}^{-1}(t) \bar{v}_{i_k}(t)] \end{aligned} \tag{21}$$

Let $Y_i^{(c)}(t) = [F_i^T Q_{\underline{v}_i}^{-1}(t) F_i + \sum_{k=1}^{d_i} F_{i_k}^T Q_{\bar{v}_{i_k}}^{-1}(t) F_{i_k}]^{-1} [F_i^T Q_{\underline{v}_i}^{-1}(t) y_i(t) + \sum_{k=1}^{d_i} F_{i_k}^T Q_{\bar{v}_{i_k}}^{-1}(t) \bar{y}_{i_k}(t)]$ and $V_i^{(c)}(t) = [F_i^T Q_{\underline{v}_i}^{-1}(t) F_i + \sum_{k=1}^{d_i} F_{i_k}^T Q_{\bar{v}_{i_k}}^{-1}(t) F_{i_k}]^{-1} [F_i^T Q_{\underline{v}_i}^{-1}(t) \underline{v}_i(t) + \sum_{k=1}^{d_i} F_{i_k}^T Q_{\bar{v}_{i_k}}^{-1}(t) \bar{v}_{i_k}(t)]$ and the following compressed measurement equation is obtained:

$$Y_i^{(c)}(t) = C_i^{(c)} x(t) + V_i^{(c)}(t), \tag{22}$$

where the superscript (c) denotes compression. The new measurement $Y_i^{(c)}(t)$ has a reduced dimension $r_i \leqslant \min\{n, \bar{m}_i\}$. $V_i^{(c)}(t)$ has a variance matrix of

$$Q_{V_i^{(c)}}(t) = [F_i^{\mathrm{T}} Q_{\underline{v}_i}^{-1}(t) F_i + \sum_{k=1}^{d_i} F_{i_k}^{\mathrm{T}} Q_{\bar{v}_{i_k}}^{-1}(t) F_{i_k}]^{-1}. \tag{23}$$

For state Equation (6) and compressed low-dimensional measurement Equation (22), the following filter is obtained by applying the standard Kalman filtering algorithm [35].

Theorem 1. *For systems (6) and (22), the DOFCD in the LMV criterion is calculated as follows*

$$\hat{x}_i^{(c)}(t+1|t+1) = \hat{x}_i^{(c)}(t+1|t) + K_i^{(c)}(t+1)(Y_i^{(c)}(t+1) - C_i^{(c)}\hat{x}_i^{(c)}(t+1|t)) \tag{24}$$

$$\hat{x}_i^{(c)}(t+1|t) = A\hat{x}_i^{(c)}(t|t) \tag{25}$$

$$K_{fi}^{(c)}(t+1) = P_i^{(c)}(t+1|t) C_i^{(c)\mathrm{T}} [C_i^{(c)} P_i^{(c)}(t+1|t) C_i^{(c)\mathrm{T}} + Q_{V_i^{(c)}}(t+1)]^{-1} \tag{26}$$

$$P_i^{(c)}(t+1|t) = A P_i^{(c)}(t|t) A^{\mathrm{T}} + Q_{\underline{\omega}}(t) \tag{27}$$

$$P_i^{(c)}(t+1|t+1) = [I_n - K_i^{(c)}(t+1) C_i^{(c)}] P_i^{(c)}(t+1|t), \tag{28}$$

where $\hat{x}_i^{(c)}(t+1|t+1)$ and $\hat{x}_i^{(c)}(t+1|t)$ are the filtering and prediction estimates of sensor node i based on the compressed measurement, respectively, $K_{fi}^{(c)}(t+1)$ is the corresponding filtering gain matrix, and $P_i^{(c)}(t+1|t+1)$ and $P_i^{(c)}(t+1|t)$ are the filtering error variance and prediction error variance, respectively. The initial values are $\hat{x}_i^{(c)}(0|0) = \mu_0$ and $P_i^{(c)}(0|0) = P_0$.

Remark 2. *Compared to the distributed optimal filter based on the augmented measurement with the computational complexity $O(\bar{m}_i^3 + n^3)$, the distributed optimal filter based on the compressed measurement in Theorem 1 with the computational complexity $O(n^3)$ has a lower computational cost. In particular, when there are a large number of neighbour sensor nodes, i.e., $n \ll \bar{m}_i$, the distributed filter based on compressed data proposed in Theorem 1 significantly reduce the computational cost. Moreover, they have the same estimation accuracy [36].*

4. Distributed Self-Tuning Filter

In the preceding section, the distributed optimal filter has been designed under the assumption of known attack rates and noise variances of the stochastic deception attack signals. However, the attack rates and noise variances of the stochastic deception attack signals are usually unknown in practical systems. The distributed optimal filter proposed in Section 3 cannot be applied. In this section, we devise a distributed self-tuning filtering algorithm for the case when the attack rates and noise variances of the stochastic deception attack signals are unknown.

4.1. Identification of Attack Rates and Noise Variances of Deception Attack Signals

If the attack rates $\bar{\gamma}_{i_k}$ and noise variances of the stochastic deception attack signals $Q_{\sigma_{i_k}}$, $i_k \in N_i$ are unknown, the unknown attack rates $\bar{\gamma}_{i_k}$ and noise variances $Q_{\sigma_{i_k}}$, $i_k \in N_i$ must be identified first to apply the distributed optimal filtering algorithm in Theorem 1 for state estimation. The real-time identified attack rates $\hat{\bar{\gamma}}_{i_k}(t)$ and noise variances $\hat{Q}_{\sigma_{i_k}}(t)$ are then substituted into Theorem 1 to obtain a distributed self-tuning filter.

The attack rates $\bar{\gamma}_{i_k}$ and noise variances $Q_{\sigma_{i_k}}$, $i_k \in N_i$ are identified by a correlation function method. By using (2), (4), and (5), we obtain

$$\bar{y}_{i_k}(t) = [1-\gamma_{i_k}(t)]C_{i_k}x(t) + [1-\gamma_{i_k}(t)]\sum_{l=1}^{q} h_{i_k l}(t)C_{i_k l}x(t) + [1-\gamma_{i_k}(t)]v_{i_k}(t) + \gamma_{i_k}(t).\sigma_{i_k}(t). \tag{29}$$

The zero-order correlation function of the measurement is calculated as

$$\begin{aligned} R_{i_k}(t,0) &= \mathrm{E}[\bar{y}_{i_k}(t)\bar{y}_{i_k}^{\mathrm{T}}(t)] \\ &= \mathrm{E}\{(1-\gamma_{i_k}(t))^2 C_{i_k}x(t)x^{\mathrm{T}}(t)C_{i_k}^{\mathrm{T}}\} \\ &+\mathrm{E}\{(1-\gamma_{i_k}(t))^2 \sum_{l=1}^{q} h_{i_k l}(t)C_{i_k l}x(t)x^{\mathrm{T}}(t)\sum_{l=1}^{q} C_{i_k l}^{\mathrm{T}}h_{i_k l}^{\mathrm{T}}(t)\} \\ &+\mathrm{E}\{(1-\gamma_{i_k}(t))^2 v_{i_k}(t)v_{i_k}^{\mathrm{T}}(t)\} + \mathrm{E}\{[\gamma_{i_k}(t)]^2\sigma_{i_k}(t)\sigma_{i_k}^{\mathrm{T}}(t)\} \\ &= (1-\bar{\gamma}_{i_k})[C_{i_k}X(t)C_{i_k}^{\mathrm{T}} + \sum_{l=1}^{q} Q_{h_{i_k l}}C_{i_k l}X(t)C_{i_k l}^{\mathrm{T}} + Q_{v_{i_k}}] + \bar{\gamma}_{i_k}Q_{\sigma_{i_k}}. \end{aligned} \tag{30}$$

The first-order correlation function of the measurement is calculated as

$$\begin{aligned} R_{i_k}(t,1) &= \mathrm{E}[\bar{y}_{i_k}(t)\bar{y}_{i_k}^{\mathrm{T}}(t-1)] \\ &= \mathrm{E}\{(1-\gamma_{i_k}(t)(1-\gamma_{i_k}(t-1))C_{i_k}Ax(t-1)x^{\mathrm{T}}(t-1)C_{i_k}^{\mathrm{T}}\} \\ &= (1-\bar{\gamma}_{i_k})^2 C_{i_k}AX(t-1)C_{i_k}^{\mathrm{T}}, \end{aligned} \tag{31}$$

which uses the results $\mathrm{E}\{(1-\gamma_{i_k}(t))^2\} = 1-\bar{\gamma}_{i_k}$. $\mathrm{E}\{[\gamma_{i_k}(t)]^2\} = \bar{\gamma}_{i_k}$, and $\mathrm{E}\{(1-\gamma_{i_k}(t))(1-\gamma_{i_k}(t-1))\} = (1-\bar{\gamma}_{i_k})^2$.

Thus, according to (30) and (31),

$$\hat{\bar{\gamma}}_{i_k}(t) = 1 - (\mathrm{tr}R_{i_k}(t,1)/\mathrm{tr}(C_{i_k}AX(t-1)C_{i_k}^{\mathrm{T}}))^{1/2} \tag{32}$$

$$\hat{Q}_{\sigma_{i_k}}(t) = \hat{\bar{\gamma}}_{i_k}^{-1}(t)\{R_{i_k}(t,0) - (1-\hat{\bar{\gamma}}_{i_k}(t))[C_{i_k}X(t)C_{i_k}^{\mathrm{T}} + \sum_{l=1}^{q} Q_{h_{i_k l}}C_{i_k l}X(t)C_{i_k l}^{\mathrm{T}} + Q_{v_{i_k}}]\}. \tag{33}$$

The correlation functions of the measurement $R_{i_k}(t,0) = \mathrm{E}[\bar{y}_{i_k}(t)\bar{y}_{i_k}^{\mathrm{T}}(t)]$ and $R_{i_k}(t,1) = \mathrm{E}[\bar{y}_{i_k}(t)\bar{y}_{i_k}^{\mathrm{T}}(t-1)]$ can be calculated approximately by the sampled correlation functions [25],

$$\hat{R}_{i_k}(t,0) = \frac{1}{t}\sum_{k=1}^{t} \bar{y}_{i_k}(k)\bar{y}_{i_k}^{\mathrm{T}}(k) \tag{34}$$

$$\hat{R}_{i_k}(t,1) = \frac{1}{t}\sum_{k=1}^{t} \bar{y}_{i_k}(k)\bar{y}_{i_k}^{\mathrm{T}}(k-1), \tag{35}$$

which can be recursively calculated by

$$\hat{R}_{i_k}(t,0) = \hat{R}_{i_k}(t-1,0) + \frac{1}{t}\left[\bar{y}_{i_k}(t)\bar{y}_{i_k}^{\mathrm{T}}(t) - \hat{R}_{i_k}(t-1,0)\right] \tag{36}$$

$$\hat{R}_{i_k}(t,1) = \hat{R}_{i_k}(t-1,1) + \frac{1}{t}\left[\bar{y}_{i_k}(t)\bar{y}_{i_k}^{\mathrm{T}}(t-1) - \hat{R}_{i_k}(t-1,1)\right]. \tag{37}$$

By replacing $R_{i_k}(t,0)$ in (30) by $\hat{R}_{i_k}(t,0)$, and $R_{i_k}(t,1)$ in (31) by $\hat{R}_{i_k}(t,1)$, we can obtain the identified value $\hat{\bar{\gamma}}_{i_k}(t)$ of $\bar{\gamma}_{i_k}$, and $\hat{Q}_{\sigma_{i_k}}(t)$ of $Q_{\sigma_{i_k}}$. As the sampled correlation

function converges to the true correlation function [25], i.e., $\hat{R}_{i_k}(t,0) \to R_{i_k}(t,0)$, $\hat{R}_{i_k}(t,1) \to R_{i_k}(t,1), t \to \infty$, the identified values $\hat{\bar{\gamma}}_{i_k}(t)$ and $\hat{Q}_{\sigma_{i_k}}(t)$ are consistent, i.e.,

$$\hat{\bar{\gamma}}_{i_k}(t) \to \bar{\gamma}_{i_k}, t \to \infty \tag{38}$$

$$\hat{Q}_{\sigma_{i_k}}(t) \to Q_{\sigma_{i_k}}, t \to \infty. \tag{39}$$

Remark 3. *Under no network attacks, the self-tuning estimation problems have been studied for systems with unknown parameters and/or noise variances in the past decade [25–28]. In this paper, only the attack rates and noise variances of the stochastic deception attack signals are unknown. If the model parameters and noise variances of systems are also unknown, the recursive extended least-squares and correlation function can be employed for the identification of unknown model parameters and variances of multiplicative noises, additive noises, and stochastic deception attack signals. This may be more complex, and will be further investigated in future studies.*

4.2. DSTFCD

According to the DOFCD obtained by Theorem 1 in Section 3.2 and identified results of the unknown attack rates and noise variances of the deception attack signals in Section 4.1, we can obtain the following distributed self-tuning filtering algorithm based on compressed data.

Theorem 2. *For systems (6) and (22) with the unknown attack rates and noise variances of deception attack signals, the DSTFCD is calculated as*

$$\hat{x}_i^{(c)}(t+1|t+1) = \hat{x}_i^{(c)}(t+1|t) + \hat{K}_i^{(c)}(t+1)[\hat{Y}_i^{(c)}(t+1) - \hat{C}_i^{(c)}(t)\hat{x}_i^{(c)}(t+1|t)] \tag{40}$$

$$\hat{x}_i^{(c)}(t+1|t) = A\hat{x}_i^{(c)}(t|t) \tag{41}$$

$$\hat{K}_{fi}^{(c)}(t+1) = \hat{P}_i^{(c)}(t+1|t)\hat{C}_i^{(c)\mathrm{T}}(t)[\hat{C}_i^{(c)}(t)\hat{P}_i(t+1|t)\hat{C}_i^{(c)\mathrm{T}}(t) + \hat{Q}_{V_i^{(c)}}(t+1)]^{-1} \tag{42}$$

$$\hat{P}_i^{(c)}(t+1|t) = A\hat{P}_i^{(c)}(t|t)A^{\mathrm{T}} + Q_{\underline{\omega}}(t) \tag{43}$$

$$\hat{P}_i^{(c)}(t+1|t+1) = [I_n - \hat{K}_i^{(c)}(t+1)\hat{C}_i^{(c)}(t)]\hat{P}_i^{(c)}(t+1|t), \tag{44}$$

where $\hat{x}_i^{(c)}(t+1|t+1)$ is the self-tuning filter of sensor node i, $\hat{x}_i^{(c)}(t+1|t)$ is the self-tuning predictor, $\hat{K}_{fi}^{(c)}(t+1)$ is the self-tuning filtering gain, and $\hat{P}_i^{(c)}(t+1|t)$ and $\hat{P}_i^{(c)}(t+1|t+1)$ are the corresponding self-tuning prediction error variance matrix and filtering error variance matrix, respectively. The initial values are $\hat{x}_i^{(c)}(0|0) = \mu_0$ and $\hat{P}_i^{(c)}(0|0) = P_0$.

Proof. By substituting the identified attack rates $\hat{\bar{\gamma}}_{i_k}(t)$ and noise variances $\hat{Q}_{\sigma_{i_k}}(t)$ of the stochastic deception attack signals into the distributed optimal filtering algorithm (24)–(28) in Theorem 1, we obtain (40)–(44). This proof is completed. □

The operation of DSTFCD has been summarized in Algorithm 1.

Algorithm 1: The DSTFCD algorithm.

Initialization:

Set the initial value at each sensor node i with $\hat{x}_i^{(c)}(0|0) = \mu_0$, $\hat{P}_i^{(c)}(0|0) = P_0$, $t = 0$.
Step 1: At each sensor node i, the measurement data of the neighbor node $\bar{y}_{i_k}(t)$ are obtained by (8).
Step 2: Use (30) and (31) to calculate the correlation function $R_{i_k}(t,0)$, $R_{i_k}(t,1)$, use (32) and (33) to calculate the online identified results $\hat{\bar{\gamma}}_{i_k}(t)$, $\hat{Q}_{\sigma_{i_k}}(t)$.
Step 3: Use the identified estimates $\hat{\bar{\gamma}}_{i_k}(t)$, $\hat{Q}_{\sigma_{i_k}}(t)$ to calculate the compressed measurement $\hat{Y}_i^{(c)}(t)$.
Step 4: Substitute the identified estimates $\hat{\bar{\gamma}}_{i_k}(t)$, $\hat{Q}_{\sigma_{i_k}}(t)$ at each time into Equations (40)–(44) in Theorem 2. The DSTFCD Algorithm can be obtained.
Step 5: Set $t = t + 1$, return to step 1.

4.3. Convergence of the Distributed Self-Tuning Filter

Lemma 1 ([35]). *Consider the following equation,*

$$\delta(t) = F(t)\delta(t-1) + u(t), \tag{45}$$

where $\delta(t) \in R^n$, $u(t) \in R^n$. $F(t)$ is uniformly asymptotically stable; i.e., there exist constants $0 < p < 1$ and $c > 0$ such that

$$\|F(t,j)\| \leq cp^{t-j}, \forall t \geq j \geq 0, \tag{46}$$

where $F(t,j) = F(t)F(t-1)\ldots F(j+1)$, $F(t,t) = I_n$. If the input $u(t)$ is bounded, $\delta(t)$ is bounded; furthermore, if $u(t) \to 0$ as $t \to \infty$, $\delta(t) \to 0$ as $t \to \infty$.

Lemma 2 ([35]). *Suppose that the $n \times n$ matrix $\Delta(t)$ satisfies the Lyapunov equation*

$$\Delta(t) = F_1(t)\Delta(t-1)F_2^{\mathrm{T}}(t) + U(t), \tag{47}$$

where $U(t)$ is an $n \times n$ input matrix and $F_1(t)$ and $F_2(t)$ are uniformly asymptotically stable matrices. If $U(t)$ is bounded, $\Delta(t)$ is bounded; furthermore, if $U(t) \to 0$ as $t \to \infty$, $\Delta(t) \to 0$ as $t \to \infty$.

Assumption 4. *Systems (6) and (22) are uniformly completely controllable and observable.*

Based on the DOFCD and DSTFCD, we obtain the following result.

Theorem 3. *The distributed self-tuning prediction and filtering error variances at each sensor node converge to the distributed optimal prediction and filtering error variances with a probability of 1(w.p.1) under any initial values, i.e.,*

$$\lim_{t\to\infty}(\hat{P}_i^{(c)}(t+1|t) - P_i^{(c)}(t+1|t)) = 0, \text{w.p.1} \tag{48}$$

$$\lim_{t\to\infty}(\hat{P}_i^{(c)}(t|t) - P_i^{(c)}(t|t)) = 0, \text{w.p.1}. \tag{49}$$

Proof. See Appendix A. □

Theorem 4. *The distributed self-tuning predictor and filter at each sensor node converge to the corresponding distributed optimal predictor and filter under any initial values, i.e.,*

$$\lim_{t\to\infty}(\hat{\hat{x}}_i^{(c)}(t+1|t) - \hat{x}_i^{(c)}(t+1|t)) = 0, \text{w.p.1} \tag{50}$$

$$\lim_{t\to\infty}(\hat{x}_i^{(c)}(t|t) - \hat{x}_i^{(c)}(t|t)) = 0, \text{w.p.1.} \tag{51}$$

Proof. See Appendix B. □

5. Simulation Example

To verify the effectiveness and applicability of our algorithms, we consider a target tracking system in practical background consisting of five nodes as an example, the system is made up of mixed uncertainties of multiplicative noises, additive noises, and stochastic deception attacks, whereas the communication between nodes may be under network attack, the sensor network topology structure is given in Figure 1.

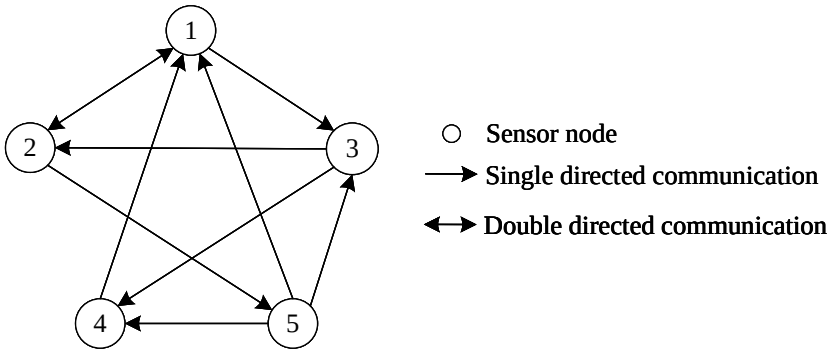

Figure 1. Topology structure of sensor network with five sensors. (authors' own processing).

The discrete-time system is given as follows:

$$x(t+1) = (A + \sum_{l=1}^{2}\alpha_l(t)A_l)x(t) + (B + \sum_{l=1}^{2}\beta_l(t)B_l)\omega(t) \tag{52}$$

$$y_i(t) = (C_i + \sum_{l=1}^{2}h_{il}(t)C_{il})x(t) + v_i(t), \quad i = 1,2,\ldots,5, \tag{53}$$

where the state is $x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}$, $x_1(t)$ and $x_2(t)$ respectively denote the position and velocity of the target. $y_i(t)$ is the measurement of the ith sensor node. In the simulation, $A = \begin{bmatrix} 0.95 & 0.01 \\ 0 & 0.95 \end{bmatrix}$, $A_1 = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.01 \end{bmatrix}$, $A_2 = \begin{bmatrix} 0.2 & 0 \\ 0 & 0.02 \end{bmatrix}$, $B = \begin{bmatrix} 0.8 \\ 0.6 \end{bmatrix}$, $B_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $B_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $C_1 = [\ 1 \quad 0.5\ ]$, $C_2 = [\ 0.9 \quad 1\ ]$, $C_3 = [\ 1 \quad 1\ ]$, $C_4 = [\ 1 \quad 1\ ]$, $C_5 = [\ 1 \quad 1\ ]$, $C_{i1} = [\ 1 \quad 0\ ]$, and $C_{i2} = [\ 0 \quad 1\ ]$, $i = 1,2,\ldots,5$. The process noise $\omega(t)$ and measurement noises $v_i(t)$, $i = 1,2,\ldots,5$ are uncorrelated white noises satisfying the relation $Q_\omega = 0.5$, $Q_{v_1} = 1$, $Q_{v_2} = 1$, $Q_{v_3} = 1$, $Q_{v_4} = 1$, $Q_{v_5} = 1$. Variances of multiplicative noises $\alpha_1(t)$, $\alpha_2(t)$, $\beta_1(t)$, $\beta_2(t)$, $h_{i1}(t)$, and $h_{i2}(t)$, $i = 1,2,\ldots,5$ are set as $Q_{\alpha_1} = Q_{\alpha_2} = 0.16$, $Q_{\beta_1} = Q_{\beta_2} = 0.11$, $Q_{h_{i1}} = 0.21$, and $Q_{h_{i12}} = 0.14$. The variances of the random disturbance noises injected into the attack signals are set as $Q_{\sigma_1} = 9$, $Q_{\sigma_2} = 3.6$, $Q_{\sigma_3} = 16$, $Q_{\sigma_4} = 12$, and $Q_{\sigma_5} = 4$. The distributions of Bernoulli random variables in attack signals $\gamma_i(t)$, $i = 1,\ldots,5$ satisfy $\bar{\gamma}_1 = \mathrm{E}\{\gamma_1(t) = 1\} = 0.2$, $\bar{\gamma}_2 = \mathrm{E}\{\gamma_2(t) = 1\} = 0.4$, $\bar{\gamma}_3 = \mathrm{E}\{\gamma_3(t) = 1\} = 0.6$, $\bar{\gamma}_4 = \mathrm{E}\{\gamma_4(t) = 1\} = 0.8$, $\bar{\gamma}_5 = \mathrm{E}\{\gamma_5(t) = 1\} = 1$. Set the initial values $\mu_0 = 0$ and $P_0 = I_2$.

In this example, our aim is to design DOFCD when the attack rates and noise variances of the stochastic deception attack signals are known, and the DSTFCD when the attack rates and noise variances of the stochastic deception attack signals are unknown.

The performance of DOFCD is depicted in Section 5.1, and the performance of DSTFCD is depicted in Section 5.2.

5.1. The Performance of DOFCD

We simulate 300 Monte Carlo runs. Figure 2 shows the tracking effect of the DOFCD in this paper when the attack rates and noise variances of attack signals are known. From Figure 2, we see that the DOFCD has good tracking accuracy.

In this example, the estimation accuracy is evaluated by MSE and MSD, which are defined as

$$\mathrm{MSE}(t) = \frac{1}{N}\sum_{k=1}^{N}\left(x^{(k)}(t) - \hat{x}_i^{(k)}(t|t)\right)^2,$$

$$\mathrm{MSD}(t) = \frac{1}{L}\sum_{i=1}^{L}\left(\frac{1}{N}\sum_{k=1}^{N}\left(x^{(k)}(t) - \hat{x}_i^{(k)}(t|t)\right)^2\right),$$

where N is the number of Monte Carlo tests. The MSDs of the DOFCD in this paper and DOFUCD in most of the literature are compared in Figure 3. The accuracy of the DOFCD is the same as that of the DOFUCD. However, compared with DOFUCD in most of the literature, the proposed DOFCD has less computational burden than the DOFUCD from Remark 2.

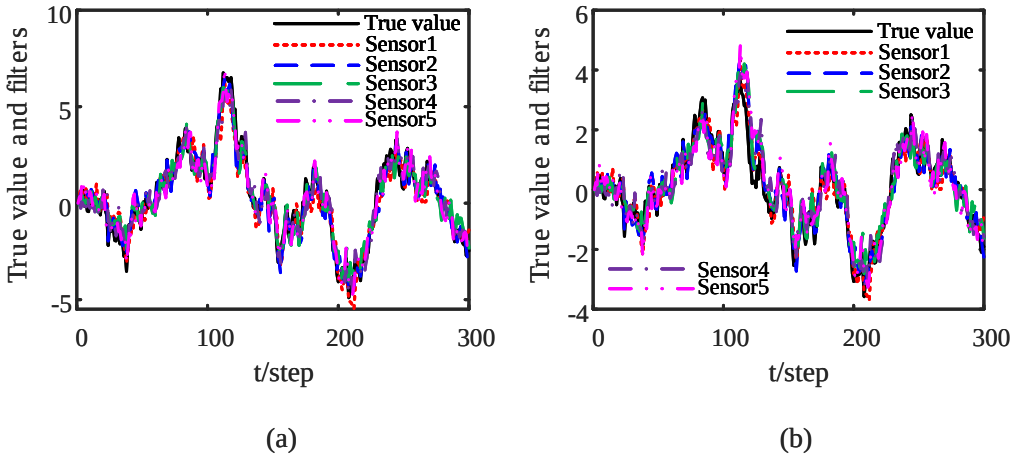

Figure 2. Tracking effects of DOFCDs of five sensor nodes: (**a**) tracking for the position; (**b**) tracking for the velocity (authors' own processing).

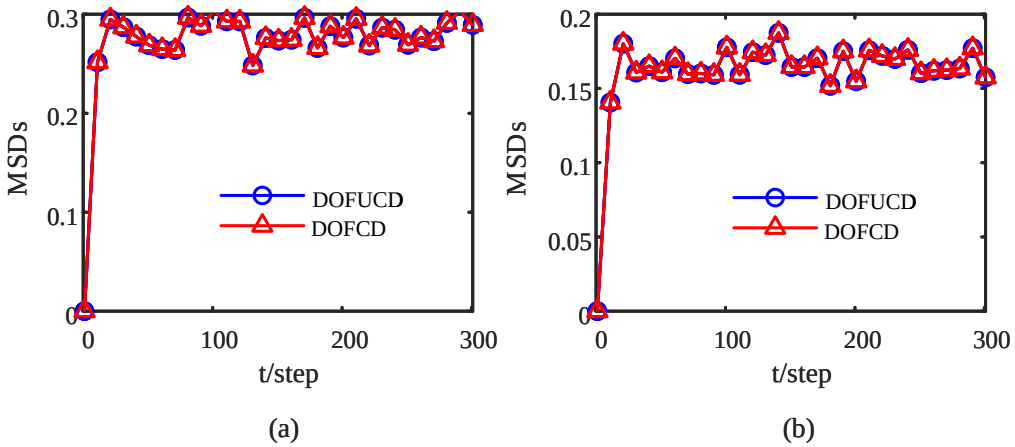

Figure 3. Comparison of MSDs of DOFCD and DOFUCD: (**a**) MSDs of the position filters; (**b**) MSDs of the velocity filters (authors' own processing).

We consider node 1 as an example. Under the different attack rates of attack signals, the impact of the attack signals on the performance of the DOFCD is shown in Figure 4. The probability distributions of the Bernoulli variables $\gamma_i(t)$, $i = 2, 4, 5$ of the attack signals injected to the neighbor nodes of sensor 1 are expressed by five cases as follows:

Case 1: $\bar{\gamma}_2 = 0$, $\bar{\gamma}_4 = 0$, $\bar{\gamma}_5 = 0$;
Case 2: $\bar{\gamma}_2 = 0.2$, $\bar{\gamma}_4 = 0.2$, $\bar{\gamma}_5 = 0.2$;
Case 3: $\bar{\gamma}_2 = 0.5$, $\bar{\gamma}_4 = 0.5$, $\bar{\gamma}_5 = 0.5$;
Case 4: $\bar{\gamma}_2 = 0.8$, $\bar{\gamma}_4 = 0.8$, $\bar{\gamma}_5 = 0.8$;
Case 5: $\bar{\gamma}_2 = 1$, $\bar{\gamma}_4 = 1$, $\bar{\gamma}_5 = 1$.

Figure 4 shows that the MSEs of the DOFCDs increase with the increase in the mean $\bar{\gamma}_i$ of the Bernoulli variables $\gamma_i(t)$, $i = 2, 4, 5$; i.e., the accuracy of the DOFCD in Case 1 outperforms that in Case 2, that in Case 2 outperforms that in Case 3, that in Case 3 outperforms that in Case 4, and that in Case 4 outperforms that in Case 5. Thus, the greater the attack probability of the attack signal corresponds to a worse accuracy of the DOFCD, which is reasonable.

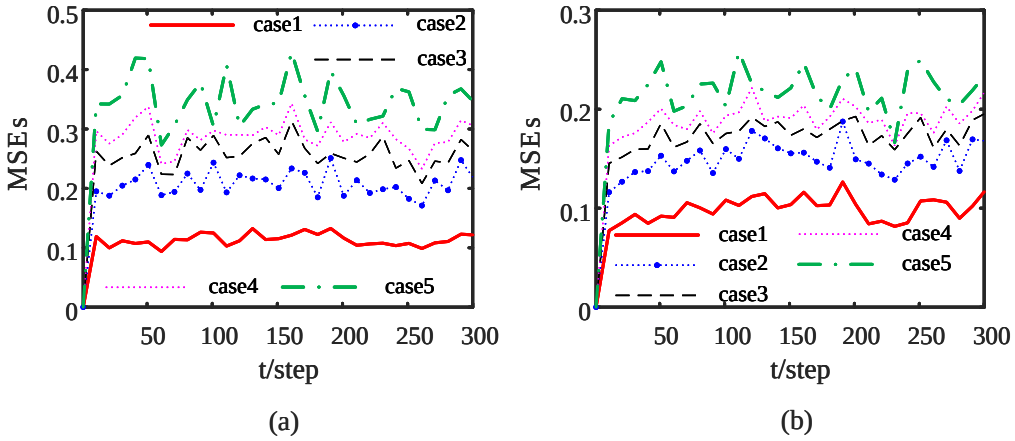

Figure 4. Comparison of MSEs of DOFCDs under different attack rates of the attack signals: (**a**) MSEs of the position filters; (**b**) MSEs of the velocity filters (authors' own processing).

5.2. The Performance of DSTFCD

When the attack rates and noise variances of the deception attack signals are unknown, based on the measurement data of the neighbors of the ith sensor node, from (32) and (33) by the correlation function method, we can obtain the identified $\hat{\bar{\gamma}}_{i_k}(t)$ and $\hat{Q}_{\sigma_{i_k}}(t)$. The identified results are provided in Figures 5 and 6. The identified attack rates and noise variances of the attack signals are consistent. That means that the estimates of the attack rates and noise variances converge to their true values as time increases, i.e., (38) and (39) hold. By using the identified results, the tracking effects of the DSTFCDs of five sensor nodes are shown in Figure 7. Figure 8 compares the MSEs of the DSTFCDs for five sensor nodes. From Figures 7 and 8, the DSTFCDs of all nodes have an effective estimation performance. Figure 9 shows the comparison of MSDs of the DSTFCDs and DSTFUCDs for five sensor nodes. From Figure 9, we can see that the DSTFCDs and DSTFUCDs have the same accuracy. Moreover, comparing Figures 3 and 9, the results in Theorem 3 and Theorem 4 can be verified.

Under the same probability distributions of the Bernoulli variables of the attack signals injected to the neighbour nodes of sensor 1 as those in the above DOFCD, Figure 10 shows the effect of the attack rates of the attack signals on the performance of the DSTFCD. A result consistent with Figure 4 is obtained. All simulation results verify the effectiveness of the proposed algorithms.

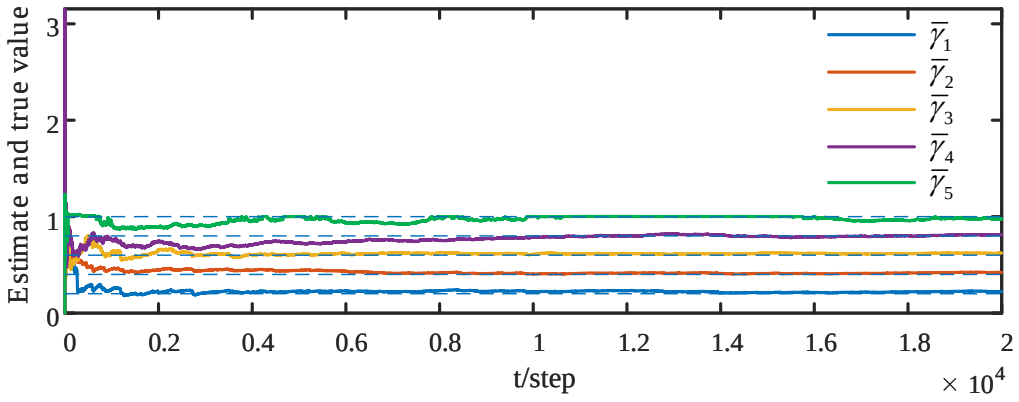

Figure 5. Identified results of unknown attack rates of deception attack signals (authors' own processing).

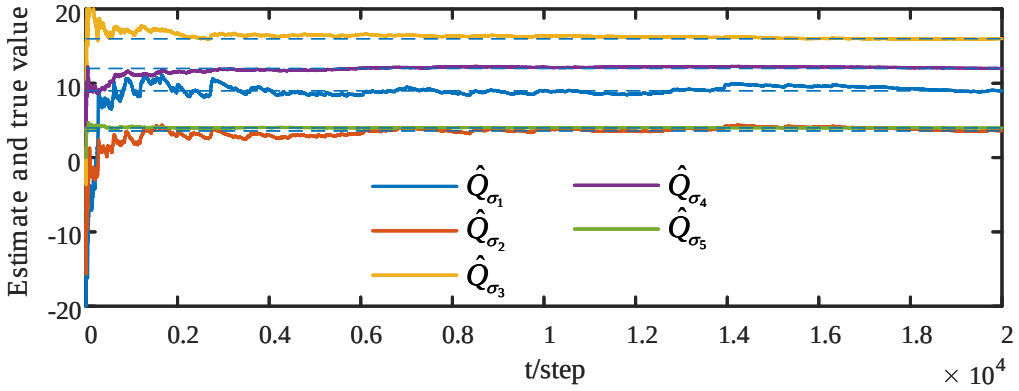

Figure 6. Identified results of unknown noise variances of deception attack signals (authors' own processing).

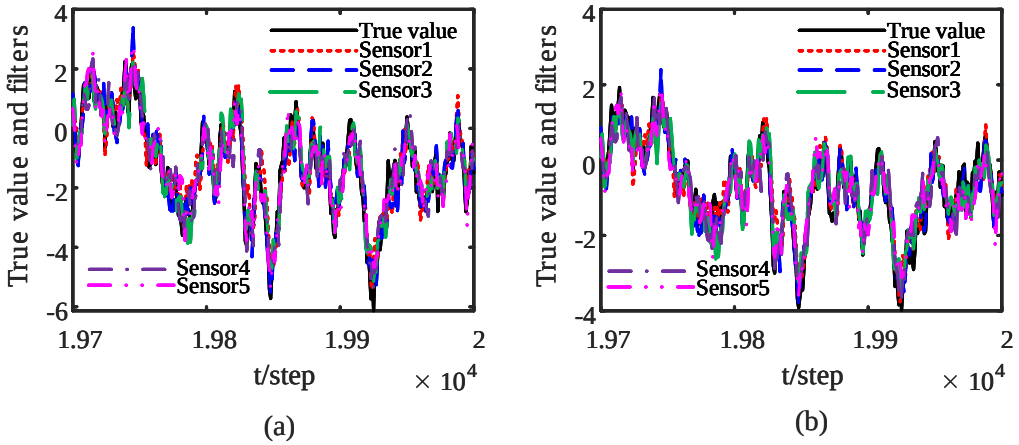

Figure 7. Tracking effects of DSTFCDs of five sensor nodes: (**a**) tracking for the position; (**b**) tracking for the velocity (authors' own processing).

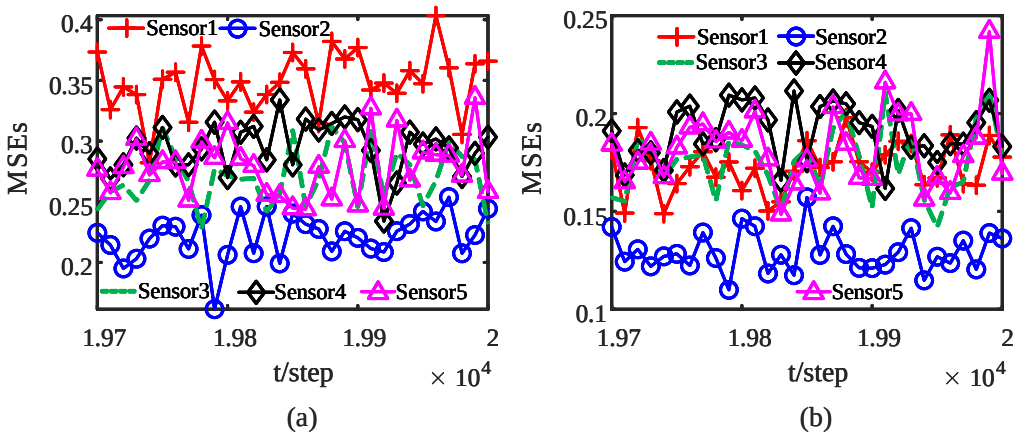

Figure 8. Comparison of MSEs of DSTFCDs of five sensor nodes: (**a**) MSEs of the position filters; (**b**) MSEs of the velocity filters (authors' own processing).

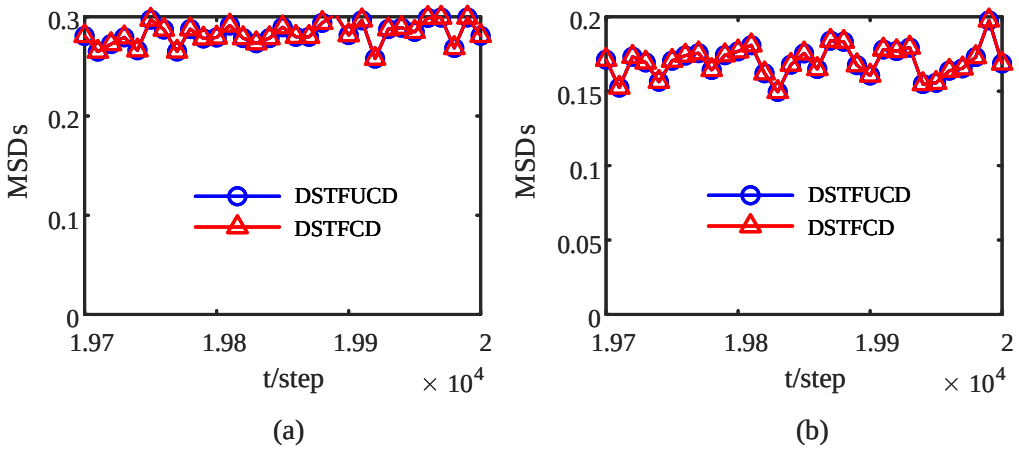

Figure 9. Comparison of MSDs of DSTFCDs and DSTFUCDs of five sensor nodes: (**a**) MSDs of the position filters; (**b**) MSDs of the velocity filters (authors' own processing).

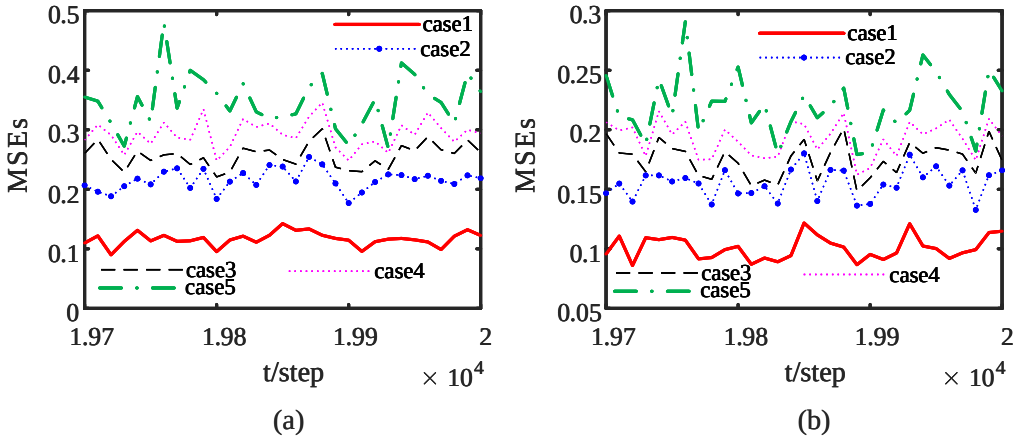

Figure 10. Comparison of MSEs of DSTFCDs with different attack rates of the attack signals: (**a**) MSEs of the position filters; (**b**) MSEs of the velocity filters (authors' own processing).

6. Conclusions

For multisensor networked stochastic uncertain systems with multiplicative noise, the measurement data may be attacked by deception attack signals in the process of data exchange between sensor nodes. When the attack rates and noise variances of the attack signal are known, the received augmented high-dimensional measurement is first compressed to

a low-dimensional measurement based on the weighted least-squares algorithm. Based on the compressed data, a distributed optimal filter in the LMV criterion was achieved, which had the same accuracy and reduced computational burden compared to that based on uncompressed data. Furthermore, a distributed self-tuning filter based on compressed data was designed when the attack rates and noise variances of the attack signals are unknown, where the correlation function method is adopted to identify the unknown attack rates and noise variances. The convergence of the distributed self-tuning filtering algorithm was analyzed.

In future studies, the distributed security estimation problems will be analyzed for networked stochastic uncertain systems with stochastic deception attacks when model parameters and/or noise covariance in systems are unknown. In addition, the systems may be time-varying and/or nonlinear in practical engineering applications, so the security estimation problems for time-varying systems and nonlinear systems with network attacks will be investigated. Moreover, we will investigate practical applications in target tracking and autonomous navigation in smart vehicles.

Author Contributions: Conceptualization, S.S.; methodology, S.S.; software, Y.M.; formal analysis, Y.M.; writing—original draft preparation, Y.M.; writing—review and editing, S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China under Grant No. 61573132, the Key Project of the Natural Science Foundation of Heilongjiang Province, China under Grant No. ZD2021F003.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Computer code could be available on request.

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

Abbreviations

The following abbreviations are used in this manuscript:

LMV	Linear minimum variance
DoS	Denial-of-service
MSEs	Mean square errors
MSDs	Mean square deviations
DOFCD	Distributed optimal filter based on compressed data
DOFUCD	Distributed optimal filter based on uncompressed data
DSTFCD	Distributed self-tuning filter based on compressed data
DSTFUCD	Distributed self-tuning filter based on uncompressed data

Appendix A. The Proof of Theorem 3

When the attack rates $\bar{\gamma}_{i_k}$ and noise variances $Q_{\sigma_{i_k}}$, $i_k \in N_i$ of the stochastic deception attack signals are known, the prediction error covariance of the DOFCD in Theorem 1 satisfies the following optimal time-varying Riccati equation:

$$P_i^{(c)}(t+1|t) = A[I - K_i^{(c)}(t)C_i^{(c)}]P_i^{(c)}(t|t-1)A^{\mathrm{T}} + Q_{\underline{\omega}}(t). \tag{A1}$$

When the attack rates $\bar{\gamma}_{i_k}$ and the variances $Q_{\sigma_{i_k}}$ of the deception attack signals are unknown, we replace $\bar{\gamma}_{i_k}$, $Q_{\sigma_{i_k}}$ in (16), (22), and (23) by $\hat{\bar{\gamma}}_{i_k}(t)$, $\hat{Q}_{\sigma_{i_k}}(t)$. According to the consistency of identification, i.e., $\hat{\bar{\gamma}}_{i_k}(t) \to \bar{\gamma}_{i_k}$, $\hat{Q}_{\sigma_{i_k}}(t) \to Q_{\sigma_{i_k}}$, the following consistency estimates can be obtained:

$$\hat{Y}_i^{(c)}(t) \to Y_i^{(c)}(t), \hat{Q}_{V_i^{(c)}}(t) \to Q_{V_i^{(c)}}(t), t \to \infty, \text{w.p.1.} \tag{A2}$$

The substitution of $\hat{Q}_{V_i^{(c)}}(t)$ into (A1) yields the distributed self-tuning Riccati equation:

$$\hat{P}_i^{(c)}(t+1|t) = A[I_n - \hat{K}_i^{(c)}(t)C_i^{(c)}]\hat{P}_i^{(c)}(t|t-1)A^{\mathrm{T}} + Q_{\underline{\omega}}(t). \tag{A3}$$

The subtraction of (A1) from (A3) yields

$$\begin{aligned}\hat{P}_i^{(c)}(t+1|t) - P_i^{(c)}(t+1|t) = & A[I_n - \hat{K}_i^{(c)}(t)C_i^{(c)}]\hat{P}_i^{(c)}(t|t-1)A^{\mathrm{T}} \\ & - A[I - K_i^{(c)}(t)C_i^{(c)}]P_i^{(c)}(t|t-1)A^{\mathrm{T}}.\end{aligned} \tag{A4}$$

Let $\Delta\hat{P}_i^{(c)}(t+1|t) = \hat{P}_i^{(c)}(t+1|t) - P_i^{(c)}(t+1|t)$, and $\Delta\hat{Q}_{V_i^{(c)}}(t) = \hat{Q}_{V_i^{(c)}}(t) - Q_{V_i^{(c)}}(t)$, according to (A2), and $\Delta\hat{Q}_{V_i^{(c)}}(t) \to 0$. Equation (A4) is further derived as follows:

$$\begin{aligned}\Delta\hat{P}_i^{(c)}(t+1|t) &= A[I_n - \hat{K}_i^{(c)}(t)C_i^{(c)}]\hat{P}_i^{(c)}(t|t-1)A^{\mathrm{T}} - AP_i^{(c)}(t|t-1)[I_n - K_i^{(c)}(t)C_i^{(c)}]^{\mathrm{T}}A^{\mathrm{T}} \\ &= A[I_n - \hat{K}_i^{(c)}(t)C_i^{(c)}][\hat{P}_i^{(c)}(t|t-1) - P_i^{(c)}(t|t-1)][I_n - K_i^{(c)}(t)C_i^{(c)}]^{\mathrm{T}}A^{\mathrm{T}} \\ &\quad + A[I_n - \hat{K}_i^{(c)}(t)C_i^{(c)}]\hat{P}_i^{(c)}(t|t-1)C_i^{(c)\mathrm{T}}(K_i^{(c)}(t))^{\mathrm{T}}A^{\mathrm{T}} \\ &\quad - A\hat{K}_i^{(c)}(t)C_i^{(c)}P_i^{(c)}(t|t-1)[I_n - K_i^{(c)}(t)C_i^{(c)}]^{\mathrm{T}}A^{\mathrm{T}} \\ &= \hat{\Psi}_i^{(c)}(t)\Delta\hat{P}_i^{(c)}(t|t-1)(\Psi_i^{(c)}(t))^{\mathrm{T}} \\ &\quad + A\hat{K}_i^{(c)}(t)\hat{Q}_{V_i^{(c)}}(t)(K_i^{(c)}(t))^{\mathrm{T}}A^{\mathrm{T}} - A\hat{K}_i^{(c)}(t)Q_{V_i^{(c)}}(t)(K_i^{(c)}(t))^{\mathrm{T}}A^{\mathrm{T}} \\ &= \hat{\Psi}_i^{(c)}(t)\Delta\hat{P}_i^{(c)}(t|t-1)(\Psi_i^{(c)}(t))^{\mathrm{T}} + A\hat{K}_i^{(c)}(t)\Delta\hat{Q}_{V_i^{(c)}}(t)(K_i^{(c)}(t))^{\mathrm{T}}A^{\mathrm{T}} \\ &= \hat{\Psi}_i^{(c)}(t)\Delta\hat{P}_i^{(c)}(t|t-1)(\Psi_i^{(c)}(t))^{\mathrm{T}} + U_i(t),\end{aligned} \tag{A5}$$

where $[I - K_i^{(c)}(t)C_i^{(c)}]P_i^{(c)}(t|t-1) = P_i^{(c)}(t|t-1)[I_n - K_i^{(c)}(t)C_i^{(c)}]^{\mathrm{T}}$ has been used in the first equality, $[I_n - \hat{K}_i^{(c)}(t)C_i^{(c)}]\hat{P}_i^{(c)}(t|t-1)C_i^{(c)\mathrm{T}} = \hat{K}_i^{(c)}(t)\hat{Q}_{V_i^{(c)}}(t)$ has been used in the third equality, $\Psi_i^{(c)}(t) = A[I_n - K_i^{(c)}(t)C_i^{(c)}]$, $\hat{\Psi}_i^{(c)}(t) = A[I_n - \hat{K}_i^{(c)}(t)C_i^{(c)}]$, and

$$U_i(t) = A\hat{K}_i^{(c)}(t)\Delta\hat{Q}_{V_i^{(c)}}(t)(K_i^{(c)}(t))^{\mathrm{T}}A^{\mathrm{T}}. \tag{A6}$$

According to [35], $\Psi_i^{(c)}(t)$ and $\hat{\Psi}_i^{(c)}(t)$ are uniformly asymptotically stable matrices under Assumption 4. According to (A2) and (A6), $U_i(t) \to 0, t \to \infty$, w.p.1. From the uniformly asymptotic stability of $\Psi_i^{(c)}(t)$ and $\hat{\Psi}_i^{(c)}(t)$ and Lemma 4, it follows that

$$\Delta\hat{P}_i^{(c)}(t+1|t) \to 0, t \to \infty, \text{w.p.1}. \tag{A7}$$

Thus, (48) is true.

Let $\Delta\hat{P}_i^{(c)}(t|t) = \hat{P}_i^{(c)}(t|t) - P_i^{(c)}(t|t)$, similarly, according to the filtering error variances of (28) and (44),

$$\begin{aligned}\Delta\hat{P}_i^{(c)}(t|t) &= (I_n - \hat{K}_i^{(c)}(t)C_i^{(c)})\hat{P}_i^{(c)}(t|t-1) - (I_n - K_i^{(c)}(t)C_i^{(c)})P_i^{(c)}(t|t-1) \\ &= \hat{P}_i^{(c)}(t|t-1) - P_i^{(c)}(t|t-1) - \hat{K}_i^{(c)}(t)C_i^{(c)}\hat{P}_i^{(c)}(t|t-1) + K_i^{(c)}(t)C_i^{(c)}P_i^{(c)}(t|t-1).\end{aligned} \tag{A8}$$

Let $\Delta\hat{K}_i^{(c)}(t) = \hat{K}_i^{(c)}(t) - K_i^{(c)}(t)$, (A8) can be rewritten as

$$\Delta\hat{P}_i^{(c)}(t|t) = \hat{P}_i^{(c)}(t|t-1) - P_i^{(c)}(t|t-1) - K_i^{(c)}(t)C_i^{(c)}\hat{P}_i^{(c)}(t|t-1)$$

$$-\Delta\hat{K}_i^{(c)}(t)C_i^{(c)}\hat{P}_i^{(c)}(t|t-1)+K_i^{(c)}(t)C_i^{(c)}P_i^{(c)}(t|t-1)$$
$$=[I_n-K_i^{(c)}(t)C_i^{(c)}]\Delta\hat{P}_i^{(c)}(t|t-1)-\Delta\hat{K}_i^{(c)}(t)C_i^{(c)}\hat{P}_i^{(c)}(t|t-1). \quad \text{(A9)}$$

According to (26), (42), (A2), and (A8), $\Delta\hat{K}_i^{(c)}(t)\to 0, t\to\infty$. Furthermore, according to (A9), $\Delta\hat{P}_i^{(c)}(t|t)\to 0$, i.e., (49) is true. This proof is completed.

Appendix B. The Proof of Theorem 4

According to Theorems 1 and 3, the distributed optimal and self-tuning predictors is rewritten as

$$\hat{x}_i^{(c)}(t+1|t)=\Psi_i^{(c)}(t)\hat{x}_i^{(c)}(t|t-1)+AK_i^{(c)}(t)Y_i^{(c)}(t) \quad \text{(A10)}$$

$$\hat{\hat{x}}_i^{(c)}(t+1|t)=\hat{\Psi}_i^{(c)}(t)\hat{\hat{x}}_i^{(c)}(t|t-1)+A\hat{K}_i^{(c)}(t)\hat{Y}_i^{(c)}(t). \quad \text{(A11)}$$

Let $\delta_i(t)=\hat{\hat{x}}_i^{(c)}(t|t-1)-\hat{x}_i^{(c)}(t|t-1)$, we can obtain the dynamic error equation

$$\delta_i(t+1)=\Psi_i^{(c)}(t)\delta_i(t)+u_i(t) \quad \text{(A12)}$$

$$u_i(t)=\Delta\hat{\Psi}_i^{(c)}(t)\hat{\hat{x}}_i^{(c)}(t|t-1)+A\hat{K}_i^{(c)}(t)\hat{Y}_i^{(c)}(t)-AK_i^{(c)}(t)Y_i^{(c)}(t), \quad \text{(A13)}$$

where $\Delta\hat{\Psi}_i^{(c)}(t)=\hat{\Psi}_i^{(c)}(t)-\Psi_i^{(c)}(t)$. We can easily obtain that $\Delta\hat{\Psi}_i^{(c)}(t)\to 0$. According to the proof of Theorem 4, $u_i(t)\to 0$. According to the uniformly asymptotic stability of $\Psi_i^{(c)}(t)$ and Lemma 3, $\delta_i(t)\to 0$ as $t\to\infty$, which leads to (A10). Similarly, (A11) can be proven. Hence, the distributed self-tuning predictor and filter have asymptotic optimality. This proof is completed.

References

1. Sun, S.; Lin, H.; Ma, J. Multi-sensor distributed fusion estimation with applications in networked systems: A review paper. *Inf. Fusion* **2017**, *38*, 122–134. [CrossRef]
2. Zhao, C.; Lam, J.; Lin, H. State estimation of CPSs with deception attacks: Stability analysis and approximate computation. *Neurocomputing* **2021**, *423*, 318–326. [CrossRef]
3. Naghnaeian, M.; Yu, X. Optimal state estimation under the denial-of-service attack: An operator approach. In Proceedings of the American Control Conference (ACC), Denver, CO, USA, 1–3 July 2020; pp. 5334–5339.
4. Mahmoud, M.; Hamdan, H.; Baroudi, U. Modeling and control of cyber-physical systems subject to cyber-attacks: A Survey of recent advances and challenges. *Neurocomputing* **2019**, *338*, 101–115. [CrossRef]
5. Liu, C.; Ning, P.; Reiter, M. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Sec.* **2011**, *14*, 1–133. [CrossRef]
6. Yang, W.; Zhang, Y.; Chen, G. Distributed filtering under false data injection attacks. *Automatica* **2019**, *102*, 34–44. [CrossRef]
7. Weng, P.; Chen, B.; Dong, S.; Yu, L. Fusion estimation for FDI sensor attacks in distributed systems. In Proceedings of the IEEE 16th International Conference on Control & Automation, Singapore, 9–11 October 2020; pp. 260–265.
8. Weng, P.; Chen, B.; Yu, L. Fusion estimate of FDI attack signals. *Acta Autom. Sin.* **2021**, *47*, 2292–2300.
9. Sun, Y.; Yang, G. Event-triggered distributed state estimation for multiagent systems under DoS attacks. *IEEE Trans. Cybern.* **2020**, *99*, 1–10. [CrossRef]
10. Li, L.; Niu, M.; Xia, Y.; Yang, H. Stochastic event-triggered distributed fusion estimation under jamming attacks. *IEEE Trans. Signal Inf. Process. Net.* **2021**, *7*, 309–321. [CrossRef]
11. Liu, Y.; Yang, G. Event-triggered distributed state estimation for cyber-physical systems under DoS attacks. *IEEE Trans. Cybern.* **2020**, *52*, 3620–3631. [CrossRef]
12. Chen, B.; Ho, D.; Zhang, W. Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 455–468. [CrossRef]
13. Xu, M.; Zhang, Y.; Zhang, D.; Chen, B. Distributed robust dimensionality reduction fusion estimation under DoS attacks and uncertain covariances. *IEEE Access* **2021**, *99*, 10328–10337. [CrossRef]
14. Liu, R.; Yu, H.; Hao, F. Optimal DoS attack scheduling for multi-sensor remote state estimation over interference channels. *J. Frankl. Inst.* **2021**, *358*, 5136–5162. [CrossRef]
15. Yang, W.; Zhang, X.; Luo, W.; Zuo, Z. Detection against randomly occurring complex attacks on distributed state estimation. *Inf. Sci.* **2020**, *547*, 539–552. [CrossRef]
16. Chen, B.; Ho, D.W.; Hu, G.; Yu, L. Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. *IEEE Trans. Cybern.* **2018**, *48*, 1862–1876. [CrossRef]

17. Liu, L.; Ma, L.; Wang, Y.; Zhang, J.; Bo, Y. Distributed set-membership filtering for time-varying systems under constrained measurements and replay attacks. *J. Frankl. Inst.* **2020**, *357*, 4983–5003. [CrossRef]
18. Zhang, K.; Keliris, C.; Polycarou, M.; Parisini, T. Discrimination between replay attacks and sensor faults for cyber-physical systems via event-triggered communication. *Eur. J. Control* **2021**, *62*, 47–56. [CrossRef]
19. Su, L.; Ye, D.; Zhao, X. Distributed secure state estimation for cyber-physical systems against replay attacks via multisensor method. *IEEE Syst. J.* **2021**, *16*, 5720–5728. JSYST.2021.3123617. [CrossRef]
20. Tahoun, A.; Arafa, M. Cooperative control for cyber–physical multi-agent networked control systems with unknown false data-injection and replay cyber-attacks. *ISA Trans.* **2021**, *110*, 1–14. [CrossRef]
21. Tahoun, A.; Arafa, M. Secure control design for nonlinear cyber–physical systems under DoS, replay, and deception cyber-attacks with multiple transmission channels. *ISA Trans.* **2022**, *128*, 294–308. [CrossRef]
22. Lin, H.; Lam, J.; Wang, Z. Secure state estimation for systems under mixed cyber-attacks: Security and performance analysis. *Inf. Sci.* **2021**, *546*, 943–960. [CrossRef]
23. Caballero-Águila, R.; Hermoso-Carazo, A.; Linares-Pérez, J. Fusion estimation using measured outputs with random parameter matrices subject to random delays and packet dropouts. *Signal Process.* **2016**, *127*, 12–23. [CrossRef]
24. Tan, H.; Shen, B.; Liu, Y. Event-triggered multi-rate fusion estimation for uncertain system with stochastic nonlinearities and colored measurement noises. *Inf. Fusion* **2017**, *36*, 313–320. [CrossRef]
25. Sun, S. Optimal and self-tuning information fusion Kalman multi-step predictor. *IEEE Trans. Aerosp. Electron. Syst.* **2007**, *43*, 418–427. [CrossRef]
26. Dou, Y.; Sun, S.; Ran, C. Self-tuning full-order WMF Kalman filter for multisensor descriptor systems. *IET Control Theory Appl.* **2017**, *11*, 359–368. [CrossRef]
27. Duan, G.; Sun, S. Self-tuning distributed fusion filter for multi-sensor systems subject to unknown model parameters and missing measurement rates. *IEEE Access* **2018**, *6*, 61519–61528. [CrossRef]
28. Wan, T.; Sun, S. Fusion identification and estimation of multisensor multichannel AR signals with missing measurements and sensor biases. *Digit. Signal Process.* **2020**, *98*, 102636. [CrossRef]
29. Wang, M.; Sun, S. Self-tuning distributed fusion filter for multi-sensor networked systems with unknown packet receiving rates, noise variances, and model parameters. *Sensors* **2019**, *19*, 4436. [CrossRef]
30. Chang, X.; Qiao, M; Zhao, X. Fuzzy energy-to-peak filtering for continuous-time nonlinear singular system. *IEEE Trans. Fuzzy Syst.* **2021**, *30*, 2325–2336. [CrossRef]
31. Hao, G.; Sun, S. Distributed fusion cubature Kalman filters for nonlinear systems. *Int. J. Robust Nonlinear Control* **2019**, *29*, 5979–5991. [CrossRef]
32. Caballero-Águila, R; Hermoso-Carazo, A; Linares-Pérez, J. A two-phase distributed filtering algorithm for networked uncertain systems with fading measurements under deception attacks. *Sensors* **2020**, *20*, 6445. [CrossRef]
33. Ma, J.; Sun, S. Distributed fusion filter for networked stochastic uncertain systems with transmission delays and packet dropouts. *Signal Process.* **2017**, *130*, 268–278. [CrossRef]
34. Boyd, S.; Ghaoui, L.; Feron, E.; Balakrishnan, V. *Linear Matrix Inequalities in System and Control Theory*; The Society for Industrial and Applied Mathematics: Philadelphia, PA, USA, 1994 ; Volume 110, pp. 131–139.
35. Deng, Z. *Information Fusion Estimation Theory and Its Applications*; Science Press: Beijing, China, 2012.
36. Wang, X.; Zhu, Q.; Sun, S. Weighted measurement fusion estimation algorithm with correlated noises and its global optimality. *Syst. Eng. Electron.* **2010**, *32*, 2057–2061.