Protocol-Based Distributed Security Fusion Estimation for Time-Varying Uncertain Systems Over Sensor Networks: Tackling DoS Attacks

Lijuan Zha, Yaping Guo, Jinliang Liu, *Member, IEEE*, Xiangpeng Xie, *Senior Member, IEEE*, and Engang Tian

***Abstract*—This article studies the distributed fusion estimation (DFE) issue for networked multi-sensor systems (NMSSs) with stochastic uncertainties, bandwidth-constrained network and energy-constrained denial-of-service (DoS) attacks. The stochastic uncertainties reflected in both the state and measurement models are characterized by multiplicative noises. For reducing the communication burden, local estimation signals are subject to dimensionality reduction processing. And the improved Round-Robin (RR) protocol is used on the channels from local estimators to the fusion estimator. To reflect the actual situation, the dimensionality reduction strategy is designed from the defender's point of view in the sense of minimum fusion error covariance (FEC). And the attack strategy is designed from the attacker's point of view in the sense of maximum FEC. Then, based on a compensation model, a recursive distributed Kalman fusion estimation algorithm (DKFEA) is proposed. The stability conditions making the mean square error (MSE) for DFE bounded are derived. In the end, the validity of the presented DKFEA is verified by an illustrative example.**

***Index Terms*—Distributed fusion estimation (DFE), networked multi-sensor systems (NMSSs), dimensionality reduction, Round-Robin (RR) protocol, denial-of-service (DoS) attacks.**

I. Introduction

IN RECENT decades, with the progress of communication technology, networked multi-sensor systems (NMSSs) have attracted much attention. In NMSSs, the components are connected through a shared network, which saves unnecessary wiring, reduces the cost to set up systems, improves the scalability of systems and facilitates remote operations [1], [2], [3], [4]. It is because of these advantages that NMSSs have been applied in vehicle guidance, intelligent weapons, detection of automated processing systems and robotics [5], [6], [7]. In practical applications, stochastic uncertainties are inevitable due to random failures, component impairment or environmental disturbances [8]. Therefore, it is of great practical significance to study the NMSSs with stochastic uncertainties.

A key issue in NMSSs with stochastic uncertainties is fusion estimation, which has shown high application value in target localization, fault detection, pattern recognition and industrial process control [9], [10], [11], [12]. Structurally, fusion estimation can be divided into centralized fusion estimation and distributed fusion estimation (DFE). In contrast to the former, the DFE structure has the advantages of fast computing speed, strong flexibility and strong anti-interference ability [13], [14]. Consequently, the DFE has become a hot research topic. Plenty of DFE algorithms have emerged one after another. In [15], according to the sequential covariance intersection fusion rule, a DFE algorithm for nonlinear NMSSs was proposed. In [16], for a type of multi-rate systems with packet loss, a DFE algorithm based on compensation strategy was developed. In [17], aimed at the nonlinear systems with unknown noise statistics, a robust H_∞ DFE algorithm was presented. In [18], for the unstable systems with limited communication capacity, an H_∞ DFE algorithm based on quantization was provided. Notice that the research achievements above are almost for deterministic NMSSs. When it comes to the DFE algorithms for NMSSs with stochastic uncertainties, few results are available and further exploration is needed.

The insertion of network will inevitably make the NMSSs with stochastic uncertainties subject to resource constraints, which may lead to transmission delay, packet dropouts and packet transmission disorder [19], [20], [21]. These issues will not only degrade the fusion estimation performance, but also have an adverse impact on the system stability. As a consequence, it is necessary to resort to some means to cope with the constrained network bandwidth. Among them, dimensionality reduction and the Round-Robin (RR) protocol have been frequently used in recent years [22], [23], [24]. The dimensionality

Manuscript received 13 August 2023; revised 11 December 2023; accepted 16 January 2024. Date of publication 22 January 2024; date of current version 5 February 2024. This work was supported in part by the National Natural Science Foundation of China under Grants 62273174, 62373252, and 61973152, in part by the Natural Science Foundation of Jiangsu Province of China under Grants BK20211290 and BK20230063, and in part by the Qing Lan Project. The Associate Editor coordinating the review of this manuscript and approving it for publication was Dr. Wee Peng Tay. *(Corresponding author: Jinliang Liu.)*

Lijuan Zha is with the School of Science, Nanjing Forestry University, Nanjing 210037, China, and also with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: zhalijuan@vip.163.com).

Yaping Guo is with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: guoyaping1005@163.com).

Jinliang Liu is with the School of Computer Science, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: liujinliang@vip.163.com).

Xiangpeng Xie is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: xiexiangpeng1953@163.com).

Engang Tian is with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China (e-mail: tianengang@163.com).

Digital Object Identifier 10.1109/TSIPN.2024.3356789

reduction is a technique that converts high-dimensional signals into low-dimensional signals according to a certain algorithm, which helps to diminish the size of packets transmitted in the network. Many research achievements have been made on the dimensionality reduction in [25], [26], [27], [28]. In [25], the dimensionality reduction was used to deal with the inherent bandwidth of networks, and the dimensionality reduction strategies in homogeneous and heterogeneous environments were designed. In [27], the dimensionality reduction was performed on local estimation signals, and a compensation strategy was adopted to minimize the impact on the estimation performance. In [28], from the perspective of the defender, a suboptimal dimensionality reduction solution was provided. Differently, the principle of RR protocol is that data from each sensor is permitted to equally enter the network according to a preset transmission sequence. Although the RR protocol can effectively reduce the amounts of packets transmitted in the network, the performance of DFE may not be guaranteed [29]. In this case, an improved RR protocol is proposed, which allows multiple sensors to access the network at each moment. So far, the DFE issue based on the improved RR protocol has not been fully studied, and few papers have unified dimensionality reduction, the improved RR protocol and DFE under a certain framework model, which motivates our research and is a huge challenge faced by this article.

Moreover, the insertion of network also increases the possibility of malicious attacks on NMSSs with stochastic uncertainties. Common network attacks include denial-of-service (DoS) attacks [30], [31], [32], deception attacks [33], [34], [35], [36] and replay attacks [37], [38]. Among these types of attacks, DoS attacks stand out for their great destructiveness, with the aim of exhausting the network bandwidth and system resources by various means and blocking the communication between system components. For this reason, the secure DFE problem under DoS attacks should be taken seriously and deserves special attention. In [32], periodic DoS attacks were taken into account and sufficient conditions that make the discussed system stable were provided. In [39], a set of stochastic variables following the Bernoulli distribution was employed to model the occurrence of DoS attacks, and a design method for the fusion estimator was presented. In [40], a predictive compensation strategy was adopted to address the packet loss induced by DoS attacks, thereby ensuring the fusion estimation performance. In [41], a secure consensus control approach was developed for leader-following multiagent systems, and the observer estimates were utilized to reduce the impact of DoS attacks. Although new progress has been made in the research of DoS attacks, few scholars design attack strategies in the sense of maximum fusion error covariance (FEC) and few papers focus on the secure DFE for NMSSs with stochastic uncertainties under the energy-constrained DoS attacks, which is another motivation for this article.

Inspired by the analyses mentioned above, this article will focus on the design of the DFE algorithm for NMSSs with stochastic uncertainties subject to bandwidth constraints and energy-constrained DoS attacks. The main contributions of this article include the following three points.

1) A novel DFE model is established, which unifies the dimensionality reduction, the improved RR protocol and the energy-constrained DoS attacks in a specific framework.

2) A dimensionality reduction strategy is designed from the defender's point of view in the sense of minimum FEC while an attack strategy is designed from the attacker's point of view in the sense of maximum FEC.

3) Based on a novel compensation model, a recursive distributed Kalman fusion estimation algorithm (DKFEA) is proposed. The stability conditions reflecting the impacts of dimensionality reduction, the improved RR protocol and energy-constrained DoS attacks are derived such that the mean square error (MSE) for DFE is bounded.

The organization of the remaining parts of this article is as follows. A distributed security fusion estimation model that covers dimensionality reduction, the improved RR protocol and energy-constrained DoS attacks is constructed in Section II. In Section III, the distributed fusion estimator, dimensionality reduction strategy and attack strategy are designed, and a recursive DKFEA is proposed. In Section IV, a smart grid example is utilized to verify the effectiveness of the presented DKFEA. The conclusion is provided in Section V.

Notation: $\mathcal{R}^n$ denotes the Euclidean space with n dimensions. E indicates the mathematical expectation. X^T and X^{-1} stand for the transpose and inverse of the matrix X, respectively. δ_{l,l_1} is the Kronecker function satisfying $\delta_{l,l_1} = 0(l \neq l_1)$ and $\delta_{l,l_1} = 1(l = l_1)$. diag$\{\cdot\}$ represents a block diagonal matrix and $X(i,i)$ means the ith diagonal component of the matrix X. $n!$ symbolizes the factorial of the positive integer n. Tr$\{\cdot\}$ indicates the trace of matrix and $\|\cdot\|_2$ denotes the second norm of matrix. $\sum$ is a summation symbol. $x \perp y$ means that the vectors x and y are orthogonal to each other. $\%$ denotes the remainder operation.

II. Problem Formulation

Consider a class of NMSSs with stochastic uncertainties modeled as follows:

$$x(l+1) = (A_0 + \alpha(l)A_1)x(l) + w(l) \tag{1}$$

$$y_i(l) = (B_{0i} + \beta_i(l)B_{1i})x(l) + v_i(l) \tag{2}$$

where $x(l) \in \mathcal{R}^n$ is the system state and $y_i(l) \in \mathcal{R}^{\acute{n}}(i = 1, 2, \ldots, L)$ is the measurement output of the sensor i. L represents the amount of sensors. $\alpha(l)$ and $\beta_i(l)$ are multiplicative noises with zero mean and variances V_α and V_{β_i}, and are used to characterize the stochastic uncertainties of systems. A_0, A_1, B_{0i}, B_{1i} are system matrices dimensioned appropriately. $w(l)$ and $v_i(l)$ are unrelated Gaussian white noises with zero mean and variances V_w and V_{v_i}. In addition, one has

$$E\{[w(l)^T \quad v_i(l)^T]^T[w(l_1)^T \quad v_j(l_1)^T]\}$$
$$= \delta_{l,l_1}\text{diag}\{V_w, \delta_{i,j}V_{v_i}\}$$

Remark 1: The stochastic uncertainty is often encountered in practical engineering systems (e.g. target tracking systems [26], uninterruptible power systems [42]), which may arise due to the modeling errors, unmodeled dynamics, component impairment and environmental disturbances. A lot of research interest has

been devoted to deal with the significant deterioration or even divergence of these uncertainties on the system performance. It should be noticed that the stochastic uncertainty in this article comes from [42], [43], and thus the system model established in this article is rational.

Assumption 1: $x(0)$ denotes the initial system state and satisfies $E[x(0)] = \lambda_0$ and $E\{[x(0)-\lambda_0][x(0)-\lambda_0]^T\} = V_0$. Besides, $x(0), w(l), v_i(l), \alpha(l)$ and $\beta_i(l)$ are mutually independent.

Assumption 2: [26] $r(A_0 \otimes A_0 + V_\alpha A_1 \otimes A_1) < 1$, where $r(\cdot)$ and $\otimes$ represent the spectrum radius and Kronecker product, respectively. Besides, (A_0, B_{0i}) is detectable and $(A_0, \sqrt{V_{\vec{w}}})$ is stable. $V_{\vec{w}}$ will be given in Lemma 1.

Equation (1) can be converted to

$$x(l+1) = A_0 x(l) + \vec{w}(l) \tag{3}$$

where $\vec{w}(l) = \alpha(l)A_1 x(l) + w(l)$ with the statistical properties as follows.

$$E[\vec{w}(l)] = E[\alpha(l)A_1 x(l) + w(l)] = 0 \tag{4}$$

$$V_{\vec{w}}(l) = E[\vec{w}(l)\vec{w}^T(l)] = V_\alpha A_1 f(l) A_1^T + V_w \tag{5}$$

$$\widetilde{V}_{\vec{w}}(l) = E[\vec{w}(l)\vec{w}^T(l_1)] = 0 \ (l \neq l_1) \tag{6}$$

where $f(l) = E[x(l)x^T(l)]$ is the second-order moment of system state. According to (1), the formula for $f(l)$ is

$$f(l+1) = A_0 f(l) A_0^T + V_\alpha A_1 f(l) A_1^T + V_w \tag{7}$$

with the initial condition $f(0) = V_0 + \lambda_0 \lambda_0^T$.

Similarly, the measurement model (2) is rewritten as

$$y_i(l) = B_{0i} x(l) + \vec{v}_i(l) \tag{8}$$

where $\vec{v}_i(l) = \beta_i(l) B_{1i} x(l) + v_i(l)$ with the statistical properties as follows.

$$E[\vec{v}_i(l)] = E[\beta_i(l) B_{1i} x(l) + v_i(l)] = 0 \tag{9}$$

$$V_{\vec{v}_i}(l) = E[\vec{v}_i(l)\vec{v}_i^T(l)] = V_{\beta_i} B_{1i} f(l) B_{1i}^T + V_{v_i} \tag{10}$$

$$\widetilde{V}_{\vec{v}_i}(l) = E[\vec{v}_i(l)\vec{v}_i^T(l_1)] = 0 \ (l \neq l_1) \tag{11}$$

It is clear that $E[\vec{w}(l)\vec{v}_i(l_1)^T] = 0$. Therefore, $\vec{w}(l)$ and $\vec{v}_i(l)$ are uncorrelated stochastic variables.

In accordance with the design of the Kalman filter, the local state estimator for sensor i is modeled as

$$\hat{x}_i(l) = F_{K_i}(l)\hat{x}_i(l-1) + K_i(l) y_i(l) \tag{12}$$

where $K_i(l)$ is the optimal gain, $F_{K_i}(l) = D_{K_i}(l) A_0$ and $D_{K_i}(l) = I_n - K_i(l) B_{0i}$.

Denote $e_i(l) = x(l) - \hat{x}_i(l)$ as local estimation error and $C_{ii}(l) = E[e_i(l) e_i^T(l)]$ as local estimation error covariance. Then, it has

$$\begin{cases} K_i(l) = C_{ii}^p(l) B_{0i}^T [B_{0i} C_{ii}^p(l) B_{0i}^T + V_{\vec{v}_i}(l)]^{-1} \\ C_{ii}(l) = D_{K_i}(l) C_{ii}^p(l) \\ C_{ii}^p(l) = A_0 C_{ii}(l-1) A_0^T + V_{\vec{w}}(l-1) \end{cases} \tag{13}$$

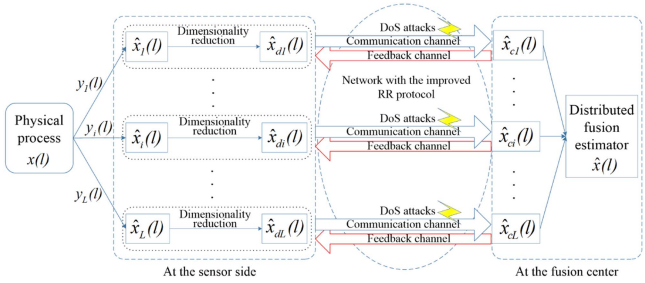

Fig. 1. DFE process for NMSSs.

where $C_{ii}^p(l)$ represents one-step prediction error covariance. Moreover, the formula for the local estimation error cross-covariance $C_{ij}(l)$ $(j = 1, \ldots, L, j \neq i)$ is

$$C_{ij}(l) = D_{K_i}(l)[A_0 C_{ij}(l-1) A_0^T + V_{\vec{w}}(l-1)] D_{K_j}^T(l) \tag{14}$$

Remark 2: Notice that $C_{ii}(l)$ in (13) is dependent on $f(l)$ because $V_{\vec{w}}(l)$ and $V_{\vec{v}_i}(l)$ are closely associated with $f(l)$ according to (5) and (10). Consequently, if $f(l)$ is bounded, $V_{\vec{w}}(l)$ and $V_{\vec{v}_i}(l)$ will be bounded, and then the boundedness of $C_{ii}(l)$ and $C_{ij}(l)$ can be guaranteed.

Lemma 1: For the NMSSs with stochastic uncertainties (1) and (2) under Assumption 2, $f(l)$, the solution to (7) with arbitrary initial value $f(0) \geq 0$ will exponentially converge to a sole value $f(f \geq 0)$, that is, $\lim_{l\to\infty} f(l) = f$. Besides, one has

$$\lim_{l\to\infty} V_{\vec{w}}(l) = V_\alpha A_1 f A_1^T + V_w = V_{\vec{w}}$$

$$\lim_{l\to\infty} V_{\vec{v}_i}(l) = V_{\beta_i} B_{1i} f B_{1i}^T + V_{v_i} = V_{\vec{v}_i}$$

Since almost every sensor network is constrained by the communication bandwidth, it is not realistic to send all $\hat{x}_i(l)$ completely to the fusion center. For addressing this problem as shown in Fig. 1, the dimensionality reduction strategy is first applied and only $t_i (1 \leq t_i < n)$ parts of $\hat{x}_i(l)$ are permitted into the network at each moment [44]. For the selected information of $\hat{x}_i(l)$, there are Λ_i possible cases and

$$\Lambda_i = \frac{n!}{t_i!(n-t_i)!} \tag{15}$$

Denote the signal allowed for transmission as $\hat{x}_{di}(l)$. Obviously, it must be a member of the following set:

$$\mathcal{S}_i = \{\mathcal{H}_i^1 \hat{x}_i(l), \ldots, \mathcal{H}_i^{\acute{m}} \hat{x}_i(l), \ldots, \mathcal{H}_i^{\Lambda_i} \hat{x}_i(l)\} \tag{16}$$

where $\mathcal{H}_i^{\acute{m}}$ is a diagonal matrix including t_i diagonal elements "1" and $n - t_i$ diagonal elements "0". For simplicity, define $G_i(l)$ as the compression matrix and

$$G_i(l) = \text{diag}\{\varepsilon_1^i(l), \ldots, \varepsilon_m^i(l), \ldots, \varepsilon_n^i(l)\} \tag{17}$$

where $\varepsilon_m^i(l) \in \{0, 1\}$ and satisfies

$$\sum_{m=1}^{n} \varepsilon_m^i(l) = t_i \tag{18}$$

In particular, the element $\varepsilon_m^i(l) = 1$ indicates that the mth part of $\hat{x}_i(l)$ is permitted to be transmitted. Then, the signal after the

dimensionality reduction is expressed as

$$\hat{x}_{di}(l) = G_i(l)\hat{x}_i(l) \tag{19}$$

On the other hand, the improved RR protocol is employed to reduce the communication burden. Different from the common RR protocol, the improved RR protocol allows multiple signals to be transmitted in the network at each moment. Denote $N(l) \subseteq \{1, 2, \ldots, L\}$ as the set of labels of sensors that are granted transmission permissions at time l. Let $k(1 < k < L)$ represent the number of sensors allowed to access the network under the current bandwidth conditions. Then, it has

$$N(l) = \{[(l-1)k]\%L + 1, \ldots, [(l-1)k + k - 1]\%L + 1\} \tag{20}$$

The subsequent example is provided to further explain the improved RR protocol. Assume there are three sensors in total, and only two are permitted to access the network with bandwidth constraints, that is, $L = 3$ and $k = 2$. Then, according to (20), it has

$$\begin{aligned} &N(1) = \{1, 2\}, \quad N(2) = \{3, 1\}, \quad N(3) = \{2, 3\}, \\ &N(4) = \{1, 2\}, \quad N(5) = \{3, 1\}, \quad N(6) = \{2, 3\}, \\ &\ldots\ldots \end{aligned}$$

which indicates that $N(l)$ is a periodic sequence and satisfies $N(l) = N(l + 3)$.

To facilitate the following expression, define

$$g(i, N(l)) = \begin{cases} 1, & \text{if } i \in N(l) \\ 0, & \text{otherwise} \end{cases} \tag{21}$$

where $g(i, N(l)) = 1$ implies that sensor i is granted the transmission permission at instant l while $g(i, N(l)) = 0$ implies that sensor i can not access the network. After being scheduled by the improved RR protocol, the signal transmitted in the network is $g(i, N(l))\hat{x}_{di}(l)$.

When signals are sent to the fusion center, attackers are likely to initiate DoS attacks on the channels. However, the attacker's energy budget is limited and cannot successfully launch DoS attacks on all channels simultaneously [45]. It is assumed that only $\tau(1 \leq \tau < L)$ channels will suffer DoS attacks at a time once DoS attacks occur. For modeling the energy-constrained DoS attacks, the stochastic variable $\gamma(l)$ following the Bernoulli distribution is employed to indicate whether the attacker launches DoS attacks or not and $\gamma_i(l) \in \{0, 1\}$ is used to describe whether the data transmitted on the ith channel has suffered DoS attacks. Besides, $E[\gamma(l)] = \gamma$ and $\gamma_i(l)$ is required to satisfy

$$\sum_{i=1}^{L} \gamma_i(l) = \tau \tag{22}$$

Then, the local estimation signal that reaches the fusion center is $(1 - \gamma(l)\gamma_i(l))g(i, N(l))\hat{x}_{di}(l)$.

Remark 3: To be specific, there are three cases regarding the occurrence of the energy-constrained DoS attacks.

1) $\gamma(l) = 0$ suggests that the attacker has not initiated DoS attacks and naturally none of the channels are attacked.

2) $\gamma(l) = 1, \gamma_i(l) = 0$ indicates that the attacker has initiated DoS attacks but the channel i is not influenced by DoS attacks.

3) $\gamma(l) = 1, \gamma_i(l) = 1$ implies that the attacker has launched DoS attacks and the channel i has suffered DoS attacks.

It is undeniable that the dimensionality reduction, the improved RR protocol and the energy-constrained DoS attacks can degrade the performance of fusion estimation. If the fusion is performed directly on the signal $(1 - \gamma(l)\gamma_i(l))g(i, N(l))\hat{x}_{di}(l)$, the estimation performance will be pretty poor. To avoid this situation, the compensating state estimation (CSE) is proposed, the formula for which is

$$\begin{aligned} \hat{x}_{ci}(l) = (1 - \gamma(l)\gamma_i(l))\{&g(i, N(l))[G_i(l)\hat{x}_i(l) \\ &+ (I_n - G_i(l))A_0\hat{x}_{ci}(l-1)] \\ &+ (1 - g(i, N(l))A_0\hat{x}_{ci}(l-1)\} \\ &+ \gamma(l)\gamma_i(l)A_0\hat{x}_{ci}(l-1) \end{aligned} \tag{23}$$

Remark 4: Here are some explanations for the CSE model in (23).

1) $\gamma(l)\gamma_i(l) = 0$: no DoS attacks have occurred on the ith channel and the CSE $\hat{x}_{ci}(l) = g(i, N(l))[G_i(l)\hat{x}_i(l) + (I_n - G_i(l))A_0\hat{x}_{ci}(l-1)] + (1 - g(i, N(l))A_0\hat{x}_{ci}(l-1)$. If $g(i, N(l)) = 1$, the signal after the dimensionality reduction $G_i(l)\hat{x}_i(l)$ will be sent to the fusion center and $(I_n - G_i(l))A_0\hat{x}_{ci}(l-1)$ is the compensation about the untransmitted parts of $\hat{x}_i(l)$. If $g(i, N(l)) = 0$, there will be no signal transmitted on the ith channel at time l. In addition, $A_0\hat{x}_{ci}(l-1)$ equates to $\hat{x}_{ci}(l-1) + (A_0 - I_n)\hat{x}_{ci}(l-1)$, where the first term is to model the situation where sensor i cannot access the network after being scheduled by the improved RR protocol and the second item represents the compensation for this situation.

2) $\gamma(l)\gamma_i(l) = 1$: DoS attacks have occurred on the ith channel and the CSE $\hat{x}_{ci}(l) = A_0\hat{x}_{ci}(l-1)$, where $A_0\hat{x}_{ci}(l-1)$ represents the compensation for DoS attacks.

Based on $\hat{x}_{ci}(l)$, the DFE of the system state $x(l)$, denoted as $\hat{x}(l)$, is calculated by

$$\hat{x}(l) = \sum_{i=1}^{L} \Omega_i(l)\hat{x}_{ci}(l) \tag{24}$$

where $\Omega_i(l)$ is the optimal distributed fusion weighting matrix which meets

$$\sum_{i=1}^{L} \Omega_i(l) = I_n \tag{25}$$

Remark 5: It is indisputable that the design of $\Omega_i(l)$ is closely related to the compression matrix $G_i(l)$ and attack variable $\gamma_i(l)$. Therefore, how to design $G_i(l)$ which satisfies (18) is crucial to defenders and how to design $\gamma_i(l)$ which satisfies (22) is crucial to attackers. From the CSE model in (23), the estimation precision of $\hat{x}_{ci}(l)$ is bound up with that of $\hat{x}_{ci}(l-1)$. On this condition, if there exists a feedback channel from the fusion center to each sensor, the sequence information about $\hat{x}_{di}(l)$ can be decided at the fusion center and then sent to the sensor side correspondingly.

Furthermore, the attacker's choice about which τ channels to attack is based on some specific system information. Due to the difficulty in thoroughly knowing the system, the attacker has to

eavesdrop on the system information. Of course, the information obtained in this way carries certain errors, which may be caused by the defender's interference or from other external disturbances. Consequently, the eavesdropped information is modeled as

$$\begin{cases} z_x(l) = H_x(l)x(l-1) + \omega(l-1) \\ z_{ci}(l) = H_{ci}(l)\hat{x}_{ci}(l-1) + \nu_i(l-1) \end{cases} \tag{26}$$

where $z_x(l)$ represents the eavesdropped system state and $z_{ci}(l)$ represents the eavesdropped CSE. $H_x(l)$ and $H_{ci}(l)$ are observation matrices. $\omega(l)$ and $\nu_i(l)$ are noises, whose means are zero and variances are V_ω and V_{ν_i}, respectively.

So far, there are three issues that need to be addressed in this article when designing a DFE algorithm for NMSSs with stochastic uncertainties considering the dimensionality reduction, the improved RR protocol and the energy-constrained DoS attacks.

$P.I)$: Suppose that $G_i(l)$ and $\gamma_i(l)$ are known in advance. The next objective is to devise the fusion weighting matrices $\Omega_1(l), \cdots, \Omega_L(l)$ to make the MSE for $\hat{x}(l)$ minimized at every moment, which is described as,

$$\begin{cases} [\hat{x}(l), \Omega_1(l), \ldots, \Omega_L(l)] \\ \quad = \arg\min\limits_{\hat{x}_*(l)} E\left\{[x(l) - \hat{x}_*(l)]^T[x(l) - \hat{x}_*(l)]\right\} \\ \text{s.t. (25)} \end{cases} \tag{27}$$

where $\hat{x}_*(l)$ is an arbitrary convex linear combination of the CSE $\hat{x}_{ci}(l)$.

$P.II)$: Utilize the feedback channels, the eavesdropped data (26) and the fusion estimator (27) to devise a scheduling strategy such that $G_i(l)$ and $\gamma_i(l)$ can be acquired by addressing the optimization issue below.

$$\begin{cases} \min\limits_{G_1(l),\ldots,G_L(l)} \max\limits_{\gamma_1(l),\ldots,\gamma_L(l)} E[e^T(l)e(l)] \\ \text{s.t. (18) and (22)} \end{cases} \tag{28}$$

where $e(l) = x(l) - \hat{x}(l)$ denotes the fusion estimation error.

$P.III)$: Seek the conditions related to $G_i(l)$, $g(i, N(l))$ and $\gamma_i(l)$ to make the MSE for $\hat{x}(l)$ bounded, which is described as,

$$\lim_{l\to\infty} E[e^T(l)e(l)] = \lim_{l\to\infty} \mathrm{Tr}\{C(l)\} < a \tag{29}$$

where $C(l) = E[e(l)e^T(l)]$ represents the fusion error covariance and $a(a > 0)$ is a scalar.

Remark 6: Motivated by [1], [11], [16], [17], [18], [21], [26], [27], [28], a novel DKFEA for networked time-varying systems with stochastic uncertainties is proposed in this article, which takes into account the constrained network bandwidth and security issues of the communication environment. Although plenty of DFE problems have been investigated in [1], [11], [16], [17], [18], [21], [26], [27], [28], the discussed issue in this article differs from the existing ones. In [1], [11], [16], [17], [18], [21], [27], the results obtained are all under the assumption that there are no attacks occurring, which is not realistic in practice. [26] and [28] considered the security issues caused by the open network transmission environments, but they only adopted dimensionality reduction method to address the issue of limited communication bandwidth. The essence of dimensionality reduction is to reduce the size of data packets transmitted in the network. For networked systems with numerous sensors, relying solely on dimensionality reduction to handle bandwidth constraints cannot meet the requirements. In addition, the DFE approach proposed in [28] was aimed at time-invariant multi-sensor systems, and not suitable for time-varying networked systems with stochastic uncertainties. Therefore, based on dimensionality reduction and the improved RR protocol, this article proposes a recursive DKFEA for networked time-varying systems with stochastic uncertainties, which can also reduce the amounts of the data packets transmitted in the network and makes up for the shortcomings of the above literatures.

III. Main Results

This section consists of three parts: A, B, and C. The design of the distributed fusion estimator will be presented in part A first, followed by the design of the dimensionality reduction strategy and the attack strategy in part B. Finally, the bounded conditions of the MSE for DFE under the joint influence of the dimensionality reduction, the improved RR protocol and the energy-constrained DoS attacks will be provided in part C.

A. Design of the Distributed Fusion Estimator

Define the CSE error $e_{ci}(l) = x(l) - \hat{x}_{ci}(l)$ and $\vec{I} = [I_n^T, \ldots, I_n^T]^T \in \mathcal{R}^{nL\times n}$. Next, based on [46], the formula for the fusion weighting matrix $\Omega_i(l)$ is

$$[\Omega_1(l), \ldots, \Omega_L(l)] = [\ \vec{I}^T\Xi^{-1}(l)\vec{I}\ ]^{-1}\vec{I}^T\Xi^{-1}(l) \tag{30}$$

where $\Xi(l)$ is defined by

$$\Xi(l) = E\left\{[e_{c1}^T(l), \ldots, e_{cL}^T(l)]^T[e_{c1}^T(l), \ldots, e_{cL}^T(l)]\right\} \tag{31}$$

Moreover, the formula for $C(l)$ is as follows.

$$C(l) = [\ \vec{I}^T\Xi^{-1}(l)\vec{I}\ ]^{-1} \tag{32}$$

Clearly, if $\Xi(l)$ is known, the fusion weighting matrix $\Omega_i(l)$ can be acquired according to (30), thus completing the design of the DFE algorithm. Before the main results are derived, the following lemma should be given for subsequent use.

Lemma 2: [28] For the arbitrary matrices S, U and Φ satisfying $\mathrm{S} = \mathrm{diag}\{s_1, \ldots, s_n\}$, $\mathrm{U} = \mathrm{diag}\{u_1, \ldots, u_n\}$ and

$$\Phi = \begin{bmatrix} \phi_{11} & \cdots & \phi_{1n} \\ \vdots & \ddots & \vdots \\ \phi_{n1} & \cdots & \phi_{nn} \end{bmatrix},$$

if $\phi_{ij}(i, j = 1, \ldots, n)$ in Φ is independent of any $s_h(h = 1, \ldots, n)$ in S and u_h in U, then

$$E[\mathrm{S}\Phi\mathrm{U}] = E[\mathrm{S} \odot \mathrm{U}] \ominus E[\Phi]$$

where the operation "$\ominus$" is defined by $[\Phi^1 \ominus \Phi^2]_{ij} = \Phi_{ij}^1\Phi_{ij}^2$ and the operation "$\odot$" for S and U is designed by

$$\mathrm{S} \odot \mathrm{U} = \begin{bmatrix} s_1u_1 & \cdots & s_1u_n \\ \vdots & \ddots & \vdots \\ s_nu_1 & \cdots & s_nu_n \end{bmatrix}.$$

Theorem 1: Define

$$\begin{cases}\Theta_{ij}(l)=[g(i,N(l))G_i(l)]\odot[g(j,N(l))G_j(l)]\\ \Pi_{ij}(l)=[I_n-g(i,N(l))G_i(l)]\odot[I_n-g(j,N(l))G_j(l)]\\ J_{ij}(l)=[g(i,N(l))G_i(l)]\odot[I_n-g(j,N(l))G_j(l)]\end{cases}\tag{33}$$

Next, the CSE error covariance $\Xi_{ij}(l)=E[e_{ci}(l)e_{cj}^T(l)]$ is given by

$$\begin{cases}\Xi_{ij}(l)=(1-\gamma\gamma_i(l)-\gamma\gamma_j(l)+\gamma\gamma_i(l)\gamma_j(l))\Xi_{ij}^{11}(l)\\ \qquad\quad+\gamma\gamma_j(l)(1-\gamma_i(l))\Xi_{ij}^{12}(l)\\ \qquad\quad+\gamma\gamma_i(l)(1-\gamma_j(l))\Xi_{ij}^{21}(l)\\ \qquad\quad+\gamma\gamma_i(l)\gamma_j(l)\Xi_{ij}^{22}(l)\\ \Xi_{ij}^{11}(l)=\Theta_{ij}(l)\ominus C_{ij}(l)+\Pi_{ij}(l)\ominus\Xi_{ij}^{22}(l)\\ \qquad\quad+J_{ij}(l)\ominus\\ \qquad\quad[F_{K_i}(l)\Gamma_{ij}(l-1)A_0^T+D_{K_i}(l)V_{\vec{w}}(l-1)]\\ \qquad\quad+J_{ji}^T(l)\ominus\\ \qquad\quad[A_0\Gamma_{ji}^T(l-1)F_{K_j}(l)^T+V_{\vec{w}}(l-1)D_{K_j}^T(l)]\\ \Xi_{ij}^{12}(l)=[I_n-g(i,N(l))G_i(l)]\Xi_{ij}^{22}(l)\\ \qquad\quad+g(i,N(l))G_i(l)\times\\ \qquad\quad[F_{K_i}(l)\Gamma_{ij}(l-1)A_0^T+D_{K_i}(l)V_{\vec{w}}(l-1)]\\ \Xi_{ij}^{21}(l)=\Xi_{ij}^{22}(l)[I_n-g(j,N(l))G_j(l)]+\\ \qquad\quad[A_0\Gamma_{ji}^T(l-1)F_{K_j}(l)^T+V_{\vec{w}}(l-1)D_{K_j}^T(l)]\\ \qquad\quad\times g(j,N(l))G_j(l)\\ \Xi_{ij}^{22}(l)=A_0\Xi_{ij}(l-1)A_0^T+V_{\vec{w}}(l-1)\end{cases}\tag{34}$$

where $\Gamma_{ij}(l)=E[e_i(l)e_{cj}^T(l)]$, the formula for which is

$$\begin{aligned}\Gamma_{ij}(l)=&(1-\gamma\gamma_j(l))[C_{ij}(l)-F_{K_i}(l)\Gamma_{ij}(l-1)A_0^T\\&-D_{K_i}(l)V_{\vec{w}}(l-1)]g(j,N(l))G_j(l)\\&+F_{K_i}(l)\Gamma_{ij}(l-1)A_0^T+D_{K_i}(l)V_{\vec{w}}(l-1)\end{aligned}\tag{35}$$

Besides, there is a relationship between DFE and CSE as follows:

$$\mathrm{Tr}\{C(l)\}\le\mathrm{Tr}\{\Xi_{ii}(l)\}\tag{36}$$

where $\Xi_{ii}(l)$ is defined by $\Xi_{ii}(l)=E[e_{ci}(l)e_{ci}^T(l)]$.

Proof: See Appendix A.

In the light of Theorem 1, $\Xi(l)$ can be acquired from (34). Next, $\Omega_i(l)$ can be obtained from (30). At this point, the first problem has been solved.

B. Design of the Dimensionality Reduction Strategy and the Attack Strategy

Since $\hat{x}_{di}(l)$ may be unavailable at the fusion center because of the improved RR protocol and DoS attacks, the dimensionality reduction strategy and the attack strategy are dependent on $\hat{x}_{ci}(l-1)$ instead of $\hat{x}_{di}(l)$. Considering that there are no relationships between the design of the two strategies, the optimization issue in (28) can be converted to the two problems below.

$$\min_{\{G_1(l),\ldots,G_L(l),\forall\gamma_i(l)\}}\mathrm{Tr}\{C(l)\}\quad\text{s.t. (18)}\tag{37}$$

$$\max_{\{\gamma_1(l),\ldots,\gamma_L(l),\forall G_i(l)\}}\mathrm{Tr}\{C(l)\}\quad\text{s.t. (22)}\tag{38}$$

However, finding out the optimal solutions to the two problems above is of great difficulty. On the one hand, $\mathrm{Tr}\{C(l)\}$ is nonlinear and closely related to matrices $G_1(l),\ldots,G_L(l)$ and variables $\gamma_1(l),\ldots,\gamma_L(l)$. On the other hand, the attacker cannot obtain $C(l)$, and $\gamma_i(l)$ can only be devised according to the eavesdropped information in (26). Based on the above analysis, the suboptimal solutions to the two problems will be discussed and presented in the subsequent theorem.

Theorem 2: Define

$$\begin{cases}\hat{x}_a(l-1)=(H_x^T(l)H_x(l))^{-1}H_x^T(l)z_x(l)\\ \hat{x}_a^{ci}(l-1)=(H_{ci}^T(l)H_{ci}(l))^{-1}H_{ci}^T(l)z_{ci}(l)\end{cases}\tag{39}$$

where $\hat{x}_a(l)$ and $\hat{x}_a^{ci}(l)$ represent the estimates of the system state $x(l)$ and CSE $\hat{x}_{ci}(l)$ on the basis of the eavesdropped information, respectively. Then, let

$$\begin{cases}\widehat{\Xi}_{ii}(l-1)=E\{[\hat{x}_a(l-1)-\hat{x}_a^{ci}(l-1)]\\ \qquad\qquad\times[\hat{x}_a(l-1)-\hat{x}_a^{ci}(l-1)]^T\}\\ \mu_m^i(l)=C_{ii}(l)(m,m)-\Xi_{ii}^{22}(l)(m,m)\\ \sigma_i(l)=\mathrm{Tr}\{A_0\widehat{\Xi}_{ii}(l-1)A_0^T\}\\ M_{di}(l)=\{\mu_1^i(l),\ldots,\mu_n^i(l)\}\\ M_a(l)=\{\sigma_1(l),\ldots,\sigma_L(l)\}\end{cases}\tag{40}$$

Next, sort the elements in set $M_{di}(l)$ in ascending order.

$$\mu_{\pi_1}^i(l)\le\cdots\le\mu_{\pi_{t_i}}^i(l)\le\mu_{\pi_{(t_i+1)}}^i(l)\le\cdots\le\mu_{\pi_n}^i(l)\tag{41}$$

And sort the elements in set $M_a(l)$ in descending order.

$$\sigma_{\chi_1}(l)\ge\cdots\ge\sigma_{\chi_\tau}(l)\ge\sigma_{\chi_{(\tau+1)}}(l)\ge\cdots\ge\sigma_{\chi_L}(l)\tag{42}$$

Then, the suboptimal solutions to problems (37) and (38) are given as follows.

$$\begin{cases}\varepsilon_{\pi_1}^i(l)=\cdots=\varepsilon_{\pi_{t_i}}^i(l)=1\\ \varepsilon_{\pi_{(t_i+1)}}^i(l)=\cdots=\varepsilon_{\pi_n}^i(l)=0\end{cases}\tag{43}$$

$$\begin{cases}\gamma_{\chi_1}(l)=\cdots=\gamma_{\chi_\tau}(l)=1\\ \gamma_{\chi_{(\tau+1)}}(l)=\cdots=\gamma_{\chi_L}(l)=0\end{cases}\tag{44}$$

Proof: See Appendix B.

According to Theorem 2, the dimensionality reduction matrices and attack variables can be obtained from (43) and (44), and thus the second problem is addressed.

For making the entire calculation process of the distributed fusion estimate $\hat{x}(l)$ clearer, Algorithm 1 is proposed.

C. Boundedness Analysis

When analyzing the estimation performance of the designed distributed fusion estimator, it is necessary to consider the statistical information of $\gamma(l)$. Let $\Gamma_{ii}^{\gamma}(l)=E\{[e_i(l)e_{ci}^T(l)]|\gamma(l)\}$

Algorithm 1: DFE under the Dimensionality Reduction, the Improved RR Protocol and DoS Attacks.

for $i = 1 : L$ **do**
  Compute $\hat{x}_i(l)$ and $C_{ij}(l)(j \in \{1, \ldots, L\}, j \neq i)$ by (12)-(14);
  Compute $C_{ii}(l)$ and $\Xi_{ii}^{22}(l)$ in the fusion center by (13) and (34);
  Sort the elements in the set $M_{di}(l)$ in ascending order in the fusion center by (41);
  Obtain $\varepsilon_m^i(l)(m \in \{1, \ldots, n\})$ in the fusion center by (43);
  Send the sequence information of the chosen parts to the sensor side through the corresponding feedback channel;
  Obtain $G_i(l)$ at the sensor side;
  Obtain $\hat{x}_{di}(l)$ at the sensor side;
end for
Compute $N(l)$ by (20);
for $i = 1 : L$ **do**
  Obtain $g(i, N(l))$ by (21);
end for
if $\gamma(l) = 0$ **then**
  Go to Step (24);
else
  The attacker computes $\hat{x}_a(l-1)$ by (39);
  for $i = 1 : L$ **do**
    The attacker computes $\hat{x}_a^{ci}(l-1)$ by (39);
  end for
  The attacker sorts the elements in the set $M_a(l)$ in descending order by (42);
  The attacker obtains $\gamma_1(l), \ldots, \gamma_L(l)$ by (44);
end if
for $i = 1 : L$ **do**
  Compute $\hat{x}_{ci}(l)$ by (23);
  Compute $e_{ci}(l)$;
end for
for $i = 1 : L$ **do**
  Compute $\Xi_{ij}(l)$ by (34);
end for
Compute $\Omega_1(l), \ldots, \Omega_L(l)$ by (30);
Compute $\hat{x}(l)$ by (24);

and $\Xi_{ii}^{\gamma}(l) = E\{[e_{ci}(l)e_{ci}^T(l)]|\gamma(l)\}$. Then, from (34), it has

$$\begin{aligned}\Gamma_{ii}^{\gamma}(l) &= (1-\gamma\gamma_i(l))[C_{ii}(l) - D_{K_i}(l)V_{\vec{w}}(l-1)] \\ &\quad \times g(i,N(l))G_i(l) + D_{K_i}(l)V_{\vec{w}}(l-1) \\ &\quad + F_{K_i}(l)\Gamma_{ii}^{\gamma}(l-1)A_0^T \\ &\quad \times [I_n - (1-\gamma\gamma_i(l))g(i,N(l))G_i(l)] \qquad (45) \\ \Xi_{ii}^{\gamma}(l) &= P_{G_i}(l)\mathrm{diag}\{\Xi_{ii}^{\gamma}(l-1), \Xi_{ii}^{\gamma}(l-1)\}P_{G_i}^T(l) \\ &\quad + (1-\gamma\gamma_i(l))J_{ii}(l)\ominus \\ &\quad [F_{K_i}(l)\Gamma_{ii}^{\gamma}(l-1)A_0^T + D_{K_i}(l)V_{\vec{w}}(l-1)] \\ &\quad + (1-\gamma\gamma_i(l))J_{ii}^T(l)\ominus \end{aligned}$$

$$[A_0{\Gamma_{ii}^{\gamma}}^T(l-1)F_{K_i}^T(l) + V_{\vec{w}}(l-1)D_{K_i}^T(l)] \qquad (46)$$

where

$$\begin{cases} P_{G_i}(l) = [b_i(l)[I_n - g(i,N(l))G_i(l)]A_0 \ \sqrt{\gamma\gamma_i(l)}A_0] \\ b_i(l) = \sqrt{1-\gamma\gamma_i(l)} \end{cases} \qquad (47)$$

It is not difficult to find from (45) and (46) that the estimation performance of $\hat{x}_{ci}(l)$ is influenced by $G_i(l)$, $g(i, N(l))$, γ and $\gamma_i(l)$. Next, the bounded conditions of the MSE for DFE will be provided in Theorem 3.

Theorem 3: For the provided parameter $\gamma > 0$, if

$$\begin{aligned}\theta_{G_i} = \max\{\|\sqrt{1-\gamma\gamma_i}(I_n - g_i\mathcal{H}_i^{\acute{m}})A_0 \ \ \sqrt{\gamma\gamma_i}A_0\|_2 \\ |\gamma_i = 0,1; g_i = 0,1; \acute{m} = 1, \ldots, \Lambda_i\} < 1 \qquad (48)\end{aligned}$$

and

$$\begin{aligned}\theta_{\gamma_i} = \max\{\|F_{K_i}\|_2 \ \|A_0^T \ [I_n - (1-\gamma\gamma_i)g_i\mathcal{H}_i^{\acute{m}}] \ \|_2 \\ |\gamma_i = 0,1; g_i = 0,1; \acute{m} = 1, \ldots, \Lambda_i\} < 1 \qquad (49)\end{aligned}$$

where $\mathcal{H}_i^{\acute{m}}$ is given in (16) and $F_{K_i} = \lim_{l\to\infty} F_{K_i}(l)$, then the MSE for DFE $\hat{x}(l)$ is of boundedness. In other words, there exists a parameter $a(a > 0)$ such that

$$\lim_{l\to\infty} \mathrm{Tr}\{C(l)\} < a. \qquad (50)$$

Proof: See Appendix C.

Remark 7: It should be noticed that the performance of the designed distributed fusion estimator can be affected by the factors including stochastic uncertainties, dimensionality reduction, the improved RR protocol and energy-constrained DoS attacks. According to Theorem 3, the stability of the designed fusion estimator can be achieved while the sufficient conditions (48) and (49) are satisfied. Particularly, for the NMSSs with stochastic uncertainties and improved RR protocol, when the compression matrix is given in advance, the maximum allowable rate of DoS attack $\bar{\gamma}$ can be derived from (48) and (49). This means that the security of the designed fusion estimator can be ensured if the attack rate γ is smaller than $\bar{\gamma}$. Otherwise, in case of $\gamma > \bar{\gamma}$, defenders will take effective defensive measures to reduce the attack rate to meet the stability conditions (48) and (49). On the other hand, it is very difficult for attackers to completely disrupt the stability of fusion estimator, unless each CSE becomes unstable while being attacked. Consequently, the distributed fusion estimator designed in the article has good security performance against DoS attacks.

The bounded conditions of the MSE for DFE have been given in Theorem 3. All three problems have been resolved.

IV. Simulation Examples

Consider the issue of the distributed security fusion estimation for a smart grid. To observe the working state of the smart grid, three sensors are utilized. The relevant parameters required for the simulation process are given in Table I.

To avoid contingency, 100 tests have been carried out. On the basis of Algorithm I, using MATLAB software, the distributed fusion weighting matrices are obtained and presented in

TABLE I
PARAMETER NAMES AND CORRESPONDING VALUES

Parameter name	Parameter value
A_0	$\begin{bmatrix} 0.7 & 0.1 & 0 & 0 \\ 0 & 0.6 & 0.1 & 0 \\ 0 & 0 & 0.7 & 0.1 \\ 0.1 & 0 & 0 & 0.6 \end{bmatrix}$
A_1	$\begin{bmatrix} 0.1 & 0.1 & 0 & 0 \\ 0 & 0.1 & 0.1 & 0 \\ 0 & 0 & 0.1 & 0.1 \\ 0.1 & 0 & 0 & 0.1 \end{bmatrix}$
$B_{01}(l)$	$\begin{bmatrix} 1 & 0 & 1 & 0.2 \\ 0 & 1 & 0.2 & 1 \end{bmatrix}$
$B_{02}(l)$	$\begin{bmatrix} 1 & 0 & 0.2 & 1 \\ 0 & 1 & 1 & 0.2 \end{bmatrix}$
$B_{03}(l)$	$\begin{bmatrix} 0 & 1 & 1 & 0.2 \\ 1 & 0 & 0.2 & 1 \end{bmatrix}$
$B_{11}(l)$	$\begin{bmatrix} 0.02 & 0.01 & 0 & 0.02 \\ 0 & 0.01 & 0.02 & 0 \end{bmatrix}$
$B_{12}(l)$	$\begin{bmatrix} 0.02 & 0 & 0.01 & 0 \\ 0 & 0.02 & 0.01 & 0.02 \end{bmatrix}$
$B_{13}(l)$	$\begin{bmatrix} 0.02 & 0.01 & 0.02 & 0 \\ 0 & 0.01 & 0 & 0.02 \end{bmatrix}$
V_α, V_{β_2}	0.04
V_{β_1}, V_{β_3}	0.01
V_w	$\begin{bmatrix} 0.09 & & & \\ & 0.08 & & \\ & & 0.08 & \\ & & & 0.09 \end{bmatrix}$
V_{v_1}	$\begin{bmatrix} 0.08 & \\ & 0.09 \end{bmatrix}$
V_{v_2}, V_{v_3}	$\begin{bmatrix} 0.09 & \\ & 0.08 \end{bmatrix}$
t_1, t_2, t_3	3
k	2
τ	1
γ	0.3
$H_x(l)$	$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
$H_{c1}(l)$	$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
$H_{c2}(l)$	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$
$H_{c3}(l)$	$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
V_ω, V_{ν_1}	$\begin{bmatrix} 0.08 & & \\ & 0.06 & \\ & & 0.09 \end{bmatrix}$
V_{ν_2}	$\begin{bmatrix} 0.08 & & \\ & 0.09 & \\ & & 0.06 \end{bmatrix}$
V_{ν_3}	$\begin{bmatrix} 0.06 & & \\ & 0.08 & \\ & & 0.09 \end{bmatrix}$

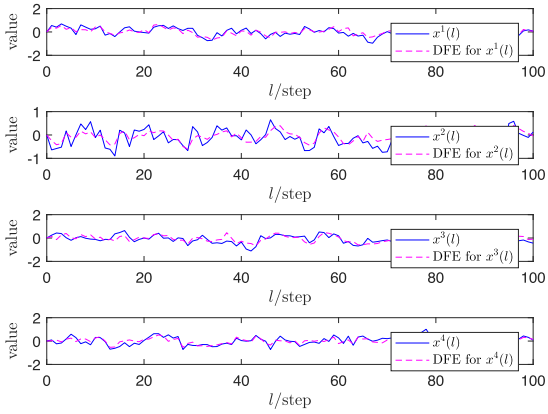

Fig. 2. Trajectories of $x^i(l)$ and DFE for $x^i(l)$.

Table II. The results show that $\| F_{K_1} \|_2 = 0.9805 < 1$, $\| F_{K_2} \|_2 = 0.9189 < 1$ and $\| F_{K_3} \|_2 = 0.9194 < 1$.

For the purpose of demonstrating the results of fusion estimation on each dimension more intuitively, let $x^i(l)$ represent the value on the ith dimension of the system state $x(l)$. The trajectories of $x^i(l)$ and DFE for $x^i(l)$ are given in Fig. 2, which indicates that the proposed DFE algorithm can effectively estimate the system state under the joint influence of the dimensionality reduction, the improved RR protocol and the energy-constrained DoS attacks.

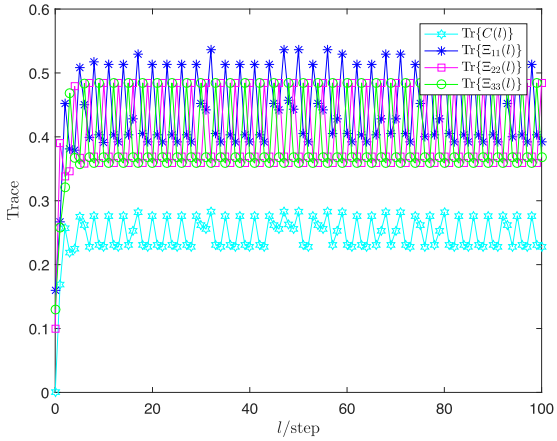

Fig. 3. Performance for DFE and compensating state estimation.

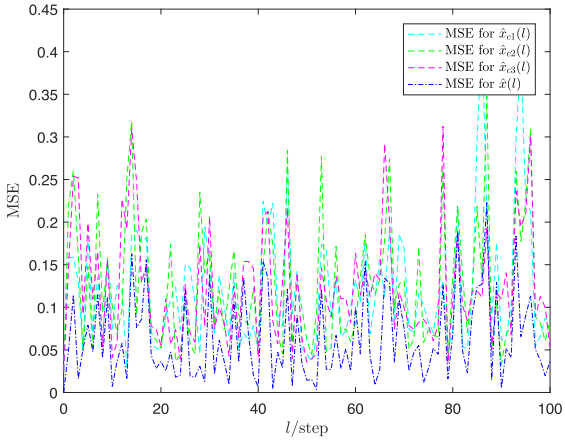

Fig. 4. MSEs for $\hat{x}_{c1}(l)$, $\hat{x}_{c2}(l)$, $\hat{x}_{c3}(l)$ and $\hat{x}(l)$.

As is known to all, the trace of estimation error covariance can be used as an evaluation indicator for estimation performance. In Fig. 3, the traces of $C(l)$, $\Xi_{11}(l)$, $\Xi_{22}(l)$ and $\Xi_{33}(l)$ are depicted. Obviously, the trace of $C(l)$ is smaller than that of any $\Xi_{ii}(l)(i = 1, 2, 3)$, which implies that the performance of the DFE is better than that of any compensating state estimation.

On the other hand, MSE is also an index to reflect the estimation performance. From Fig. 4, the MSE for $\hat{x}(l)$ is always less than that for any $\hat{x}_{ci}(l)(i = 1, 2, 3)$. This also demonstrates that the performance of the DFE is better than that of any compensating state estimation. In addition, what is noteworthy is that the MSE for each CSE $\hat{x}_{ci}(l)$ is no larger than 0.45, which illustrates the rationality of the proposed CSE model.

Under the designed attack strategy, the occurrence of DoS attacks on each channel is shown in Fig. 5. The long gray bars in the figure indicate that the attacker has initiated DoS attacks. The meaning of $\gamma_i(l) = 1$ and $\gamma_i(l) = 0$ has been explained in Section II. From Fig. 5, it can be seen that the first channel always suffers DoS attacks while the other two channels are always not attacked, which is consistent with the results in Fig. 3.

TABLE II
FUSION WEIGHTING MATRICES

l	$\Omega_1(l)$	$\Omega_2(l)$	$\Omega_3(l)$
l=1	$\begin{bmatrix} 0.7139 & 0.2736 & 0.0013 & -0.2091 \\ -0.2773 & 0.2010 & 0.0013 & 0.6286 \\ 0.0157 & -0.7289 & 0.9992 & -0.1389 \\ -0.3351 & 0.2296 & 0.0015 & 0.7358 \end{bmatrix}$	$\begin{bmatrix} -0.1768 & -0.1026 & -0.0339 & -0.0530 \\ -0.1433 & -0.0842 & -0.0267 & -0.0560 \\ 0.3483 & 0.1926 & 0.0735 & -0.0148 \\ -0.1640 & -0.0964 & -0.0306 & -0.0644 \end{bmatrix}$	$\begin{bmatrix} 0.4629 & -0.1710 & 0.0326 & 0.2622 \\ 0.4207 & 0.8832 & 0.0255 & -0.5726 \\ -0.3639 & 0.5363 & -0.0727 & 0.1537 \\ 0.4991 & -0.1332 & 0.0291 & 0.3286 \end{bmatrix}$
l=2	$\begin{bmatrix} 0.3150 & -0.2067 & 0.1463 & -0.4774 \\ 0.0784 & 0.0546 & -0.9099 & 0.0206 \\ 0.4722 & -0.1308 & -0.0310 & -0.4706 \\ -0.5011 & 0.1253 & -0.0942 & 0.4022 \end{bmatrix}$	$\begin{bmatrix} 0.6779 & 0.0266 & 0.0124 & -0.1739 \\ 1.4740 & 0.1571 & 0.8834 & -1.7382 \\ -0.0193 & 0.0290 & 0.5982 & -0.0126 \\ 0.0008 & -0.0004 & -0.0166 & 0.5577 \end{bmatrix}$	$\begin{bmatrix} 0.0071 & 0.1801 & -0.1586 & 0.6514 \\ -1.5524 & 0.7883 & 0.0265 & 1.7176 \\ -0.4529 & 0.1017 & 0.4328 & 0.4832 \\ 0.5003 & -0.1249 & 0.1108 & 0.0400 \end{bmatrix}$
l=99	$\begin{bmatrix} 0.3855 & -0.1980 & 0.4438 & -0.1800 \\ -0.1889 & 0.2553 & -0.0854 & 0.5473 \\ 0.4455 & -0.1614 & 0.3534 & -0.1621 \\ -0.6537 & -0.1805 & 0.4468 & 0.7315 \end{bmatrix}$	$\begin{bmatrix} 0.6437 & -0.7095 & 0.3751 & -0.1367 \\ 0.0149 & 1.5013 & -0.6128 & -0.0607 \\ -0.3084 & -0.4195 & 1.1038 & -0.0361 \\ 0.6055 & -1.0275 & 0.8008 & -0.1386 \end{bmatrix}$	$\begin{bmatrix} -0.0292 & 0.9074 & -0.8189 & 0.3167 \\ 0.1741 & -0.7566 & 0.6982 & -0.4866 \\ -0.1371 & 0.5809 & -0.4572 & 0.1982 \\ 0.0583 & 1.2080 & -1.2475 & 0.4071 \end{bmatrix}$
l=100	$\begin{bmatrix} 0.7482 & 0.2301 & -0.0474 & -0.3739 \\ -0.1637 & 0.3175 & -0.0483 & 0.3525 \\ 0.8012 & 0.2905 & -0.0364 & -0.3421 \\ -0.2407 & 0.4112 & -0.1096 & 0.4044 \end{bmatrix}$	$\begin{bmatrix} 0.0303 & -0.4090 & 0.3555 & -0.2485 \\ -0.0521 & 0.7882 & -0.6249 & 0.1033 \\ -0.0779 & -0.3536 & 0.4192 & -0.1913 \\ 0.1014 & -0.4272 & 0.2817 & -0.0913 \end{bmatrix}$	$\begin{bmatrix} 0.2214 & 0.1789 & -0.3081 & 0.6224 \\ 0.2158 & -0.1057 & 0.6733 & -0.4558 \\ -0.7233 & 0.0631 & 0.6172 & 0.5334 \\ 0.1392 & 0.0160 & -0.1721 & 0.6869 \end{bmatrix}$

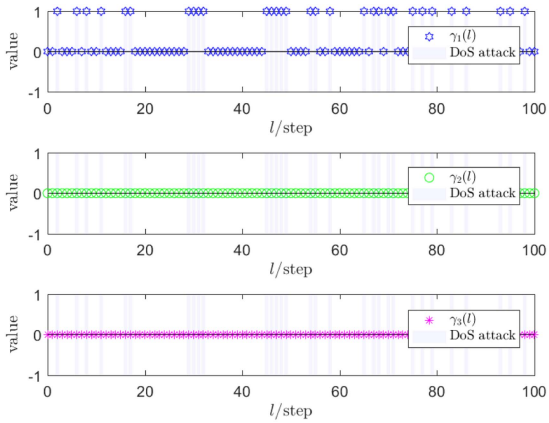

Fig. 5. Occurrence of DoS attacks in three communication channels.

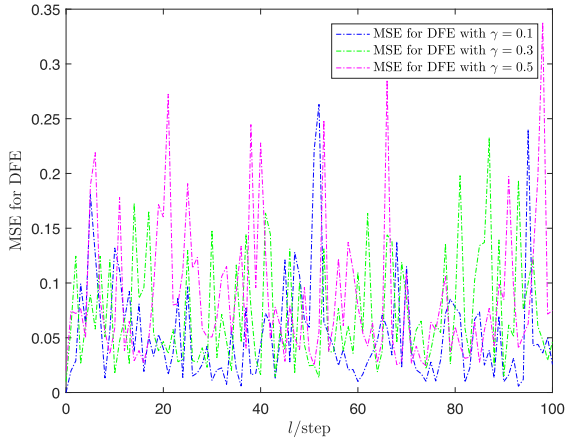

Fig. 6. MSE for DFE under different attack probabilities.

To explore the impact of DoS attack probability on the performance of DFE, Fig. 6 is given. By observing the relative position of MSE for DFE with $\gamma = 0.1$, $\gamma = 0.3$ and $\gamma = 0.5$, it can be drawn that in general, the smaller the attack probability is, the better the performance of DFE will be. Furthermore, even when the attack probability reaches 0.5, the MSE for DFE never exceeds 0.35, which reflects the validity and superiority of the adopted compensation strategy.

V. CONCLUSION

The secure DFE for NMSSs has been investigated in this article, in which the stochastic uncertainties, the inherent bandwidth constraints of the network and the limited energy budget of attackers are taken into account. For reducing the communication pressure on the network, the dimensionality reduction and the improved RR protocol are employed. To be more realistic, the dimensionality reduction strategy and the attack strategy are designed from the perspective of the defender and attacker, respectively. Then, a novel compensation model has been established to resist the influence of the dimensionality reduction, the improved RR protocol and the energy-constrained DoS attacks on the performance of DFE. Based on the CSE model, a recursive DKFEA has been proposed. The stability conditions have been provided such that the MSE for DFE is bounded. In the end, the effectiveness of the proposed DKFEA has been verified by a smart grid example.

Note that attack detection has become a key issue in the DFE for NMSSs with stochastic uncertainties. The joint-design of attack detector and distributed fusion estimator has attracted our attention and is a future research direction for us.

APPENDIX A
PROOF OF THEOREM 1

From (3), (8), (12) and (23), it can be derived that

$$e_i(l) = F_{K_i}(l)e_i(l-1) + D_{K_i}(l)\vec{w}(l-1) - K_i(l)\vec{v}_i(l) \tag{51}$$

$$\begin{aligned} e_{ci}(l) = {} & (1-\gamma(l)\gamma_i(l))\{g(i,N(l))G_i(l)e_i(l) \\ & + [I_n - g(i,N(l))G_i(l)]A_0e_{ci}(l-1) \\ & + [I_n - g(i,N(l))G_i(l)]\vec{w}(l-1)\} \\ & + \gamma(l)\gamma_i(l)[A_0e_{ci}(l-1) + \vec{w}(l-1)] \end{aligned} \tag{52}$$

Since $x(0), w(l), v_i(l), \alpha(l)$ and $\beta_i(l)$ are mutually independent, combining (51) and (52), it can be deduced that

$$\begin{cases} e_i(l) \perp \vec{w}(l_1),\ l \le l_1 \\ e_i(l) \perp \vec{v}_j(l_1),\ i = j, l < l_1 \text{ or } i \ne j, \forall l, l_1 \\ e_{ci}(l) \perp \vec{w}(l_1),\ l \le l_1 \\ e_{ci}(l) \perp \vec{v}_j(l_1),\ i = j, l < l_1 \text{ or } i \ne j, \forall l, l_1 \end{cases} \tag{53}$$

Based on (53), it yields that

$$\begin{cases} E[e_i(l)e_{cj}^T(l-1)] = F_{K_i}(l)\Gamma_{ij}(l-1) \\ E[e_i(l)\vec{w}^T(l-1)] = D_{K_i}(l)V_{\vec{w}}(l-1) \end{cases} \tag{54}$$

Then, according to (52) and (54), (35) can be obtained. Before $\Xi_{ij}(l)$ is computed, some mathematical expectations need to be clarified.

$$\begin{cases} E[(1-\gamma(l)\gamma_i(l))(1-\gamma(l)\gamma_j(l))] = 1-\gamma\gamma_i(l)-\gamma\gamma_j(l) \\ \qquad\qquad +\gamma\gamma_i(l)\gamma_j(l) \\ E[(1-\gamma(l)\gamma_i(l))\gamma(l)\gamma_j(l)] = \gamma\gamma_j(l)(1-\gamma_i(l)) \\ E[\gamma(l)\gamma_i(l)(1-\gamma(l)\gamma_j(l))] = \gamma\gamma_i(l)(1-\gamma_j(l)) \\ E[\gamma(l)\gamma_i(l)\gamma(l)\gamma_j(l)] = \gamma\gamma_i(l)\gamma_j(l) \end{cases} \tag{55}$$

On the basis of (52)–(55), (33) and (35), (34) can be acquired. Besides, $\Xi_{ii}(l)$ is calculated by

$$\Xi_{ii}(l) = (1-\gamma\gamma_i(l))\Xi_{ii}^{11}(l) + \gamma\gamma_i(l)\Xi_{ii}^{22}(l) \tag{56}$$

where $\Xi_{ii}^{11}(l)$ and $\Xi_{ii}^{22}(l)$ can be acquired from (34). Next, applying the Schwartz matrix inequality to the fusion error covariance martix $C(l)$, one has

$$\begin{aligned} C(l) &= [\vec{I}^T\Xi^{-1}(l)\vec{I}]^{-1} \\ &= [(\Xi^{-\frac{1}{2}}(l)\vec{I})^T(\Xi^{-\frac{1}{2}}(l)\vec{I^i})]^T \\ &\times [(\Xi^{-\frac{1}{2}}(l)\vec{I})^T(\Xi^{-\frac{1}{2}}(l)\vec{I})]^{-1} \\ &\times [(\Xi^{-\frac{1}{2}}(l)\vec{I})^T(\Xi^{-\frac{1}{2}}(l)\vec{I^i})] \\ &\leq (\Xi^{-\frac{1}{2}}(l)\vec{I^i})^T(\Xi^{-\frac{1}{2}}(l)\vec{I^i}) = \Xi_{ii}(l) \end{aligned} \tag{57}$$

where $\vec{I^i} = [0,\ldots,I_n,\ldots,0]^T \in \mathcal{R}^{nL\times n}$ and I_n is the ith block matrix of $\vec{I^i}$. Based on the above analysis, (36) is derived. That's the end of the proof.

Appendix B
Proof of Theorem 2

Let $C_\Xi(l) = \min\{\text{Tr}\{\Xi_{11}(l)\},\ldots,\text{Tr}\{\Xi_{LL}(l)\}\}$. Since $\text{Tr}\{C(l)\} \leq \text{Tr}\{\Xi_{ii}(l)\}$, then $\text{Tr}\{C(l)\} \leq C_\Xi(l)$. Under this relaxation condition, (37) can be transformed into

$$\min_{\{G_1(l),\ldots,G_L(l),\forall\gamma_i(l)\}} C_\Xi(l) \quad \text{s.t. (18)} \tag{58}$$

As previously pointed out, when it comes to the dimensionality reduction strategy, there is no need to take into account the attack parameters. Moreover, $\Xi_{ii}^{22}(l)$ is stable, and thus $\text{Tr}\{\Xi_{ii}(l)\}$ is supposed to be replaced by $\text{Tr}\{\Xi_{ii}^{11}(l)\}$. Furthermore, the computation process of $\Xi_{ii}^{11}(l)$ is merely dependent on $g(i,N(l))$, $G_i(l)$ and $\Xi_{ii}(l-1)$. Consequently, (58) can be decomposed into L subproblems as follows.

$$\begin{cases} \min\limits_{G_i(l)} \ \text{Tr}\{\Xi_{ii}^{11}(l)\} \\ \text{s.t. (18) and } \varepsilon_m^i(l) \in \{0,1\} \end{cases} \tag{59}$$

From (33), it is easy to find that for matrix $J_{ii}(l)$, any diagonal element is 0. Combining the definition of "$\ominus$", it can be drawn that

$$\begin{aligned} &\text{Tr}\{J_{ii}(l) \ominus [F_{K_i}(l)\Gamma_{ii}(l-1)A_0^T + D_{K_i}(l)V_{\vec{w}}(l-1)]\} = 0 \\ &\text{Tr}\{J_{ii}^T(l) \ominus [A_0\Gamma_{ii}^T(l-1)F_{K_i}^T(l) + V_{\vec{w}}(l-1)D_{K_i}^T(l)]\} = 0 \end{aligned}$$

Accordingly,

$$\begin{aligned} \text{Tr}\{\Xi_{ii}^{11}(l)\} &= \text{Tr}\{\Theta_{ii}(l) \ominus C_{ii}(l) + \Pi_{ii}(l) \ominus \Xi_{ii}^{22}(l)\} \\ &= \sum_{m=1}^{n} \{[C_{ii}(l)(m,m) - \Xi_{ii}^{22}(l)(m,m)]\varepsilon_m^i(l)\} \\ &\quad + \text{Tr}\{\Xi_{ii}^{22}(l)\} \end{aligned} \tag{60}$$

Next, (59) can be converted to

$$\begin{cases} \min_{G_i(l)} \ \sum\limits_{m=1}^{n} \{[C_{ii}(l)(m,m) - \Xi_{ii}^{22}(l)(m,m)]\varepsilon_m^i(l)\} \\ \qquad + \text{Tr}\{\Xi_{ii}^{22}(l)\} \\ \text{s.t. (18) and } \varepsilon_m^i(l) \in \{0,1\} \end{cases} \tag{61}$$

Since $\text{Tr}\{\Xi_{ii}^{22}(l)\}$ is a constant and $\varepsilon_m^i(l) \in \{0,1\}$, thus (43) is the optimal solution to (61) and the suboptimal solution to (37).

In addition, according to (32), (38) can be transformed into

$$\max_{\{\gamma_1(l),\ldots,\gamma_L(l),\forall G_i(l)\}} \text{Tr}\{\Xi(l)\} \quad \text{s.t. (22)} \tag{62}$$

Notice that $\text{Tr}\{\Xi(l)\} = \sum_{i=1}^{L}\text{Tr}\{\Xi_{ii}(l)\}$, and $\text{Tr}\{\Xi_{ii}(l)\}$ is supposed to be replaced by $\gamma_i(l)\text{Tr}\{\Xi_{ii}^{22}(l)\}$ because the attack strategy is independent of dimensionality reduction strategy. Moreover, $\sum_{i=1}^{L}\gamma_i(l)\text{Tr}\{\Xi_{ii}^{22}(l)\} = \sum_{i=1}^{L}\gamma_i(l)\text{Tr}\{A_0\Xi_{ii}(l-1)A_0^T\} + \tau\text{Tr}\{V_{\vec{w}}(l-1)\}$ and $\tau\text{Tr}\{V_{\vec{w}}(l-1)\}$ is a constant. Therefore, (62) turns into

$$\begin{cases} \max\limits_{\{\gamma_1(l),\ldots,\gamma_L(l)\}} \ \sum_{i=1}^{L}\gamma_i(l)\text{Tr}\{A_0\Xi_{ii}(l-1)A_0^T\} \\ \text{s.t. (22) and } \gamma_i(l) \in \{0,1\} \end{cases} \tag{63}$$

The attackers have difficulty in obtaining $\Xi_{ii}(l-1)$, but they can acquire inexact $x(l-1)$ and $\hat{x}_{ci}(l-1)$ by eavesdropping. Then, utilizing the least square estimation method, $\hat{x}_a(l-1)$ and $\hat{x}_a^{ci}(l-1)$ can be acquired. Moreover, $E[\hat{x}_a(l-1)] = E[x(l-1)]$ and $E[\hat{x}_a^{ci}(l-1)] = E[\hat{x}_{ci}(l-1)]$. For this reason, the attacker can replace $\Xi_{ii}(l-1)$ with $\widehat{\Xi}_{ii}(l-1)$, which is defined by

$$\begin{aligned} \widehat{\Xi}_{ii}(l-1) &= E\{[\hat{x}_a(l-1) - \hat{x}_a^{ci}(l-1)] \\ &\quad \times [\hat{x}_a(l-1) - \hat{x}_a^{ci}(l-1)]^T\} \end{aligned} \tag{64}$$

Then, (63) can be converted to

$$\begin{cases} \max\limits_{\{\gamma_1(l),\ldots,\gamma_L(l)\}} \ \sum_{i=1}^{L}\gamma_i(l)\text{Tr}\{A_0\widehat{\Xi}_{ii}(l-1)A_0^T\} \\ \text{s.t. (22) and } \gamma_i(l) \in \{0,1\} \end{cases} \tag{65}$$

Since $\gamma_i(l) \in \{0,1\}$, thus (44) is the optimal solution to (65) and the suboptimal solution to (38). That's the end of the proof.

APPENDIX C
PROOF OF THEOREM 3

By Lemma 1, it is not hard to deduce that

$$\begin{cases} \lim_{l\to\infty} D_{K_i}(l) = D_{K_i} \\ \lim_{l\to\infty} F_{K_i}(l) = F_{K_i} \\ \lim_{l\to\infty} C_{ii}(l) = C_{ii} \end{cases} \tag{66}$$

where F_{K_i} is stable. Consequently, in terms of (45) and (66), there must exist a positive integer ξ_{γ_i} such that when $l \geq \xi_{\gamma_i}$,

$$\begin{aligned} \Gamma_{ii}^{\gamma}(l) = {} & F_{K_i}\Gamma_{ii}^{\gamma}(l-1)A_0^T \\ & \times [I_n - (1-\gamma\gamma_i(l))g(i,N(l))G_i(l)] \\ & + \Delta\Gamma_{ii}^{\gamma}(l) \end{aligned} \tag{67}$$

where $\Delta\Gamma_{ii}^{\gamma}(l)$ is defined by $\Delta\Gamma_{ii}^{\gamma}(l) = (1-\gamma\gamma_i(l))(C_{ii} - D_{K_i}V_{\vec{w}})g(i,N(l))G_i(l) + D_{K_i}V_{\vec{w}}$. Considering the structure of $G_i(l)$, there must be a scalar $\psi_{\gamma_i} > 0$ ensuring

$$\|\Delta\Gamma_{ii}^{\gamma}(l)\|_2 \leq \psi_{\gamma_i} \quad (l \geq \xi_{\gamma_i}) \tag{68}$$

Based on (67) and (68), it yields that

$$\begin{aligned} \|\Gamma_{ii}^{\gamma}(l)\|_2 & \leq \psi_{\gamma_i} + \theta_{\gamma_i}\|\Gamma_{ii}^{\gamma}(l-1)\|_2 \\ & \leq \theta_{\gamma_i}^{l-\xi_{\gamma_i}}\|\Gamma_{ii}^{\gamma}(\xi_{\gamma_i})\|_2 + \sum_{o=0}^{l-\xi_{\gamma_i}+1} \theta_{\gamma_i}^{o}\psi_{\gamma_i} \end{aligned} \tag{69}$$

where θ_{γ_i} is given in (49). Since $\theta_{\gamma_i} < 1$, it can be concluded that $\lim_{l\to\infty}\theta_{\gamma_i}^{l-\xi_{\gamma_i}} = 0$ and $\lim_{l\to\infty}\sum_{o=0}^{l-\xi_{\gamma_i}+1}\theta_{\gamma_i}^{o}\psi_{\gamma_i} = \frac{\psi_{\gamma_i}}{1-\theta_{\gamma_i}}$. Then, one has

$$\lim_{l\to\infty}\|\Gamma_{ii}^{\gamma}(l)\|_2 \leq \frac{\psi_{\gamma_i}}{1-\theta_{\gamma_i}} \tag{70}$$

In this situation, according to (46), (66) and (70), there must exist a positive integer ξ_{G_i} satisfying $\xi_{G_i} > \xi_{\gamma_i}$ such that when $l \geq \xi_{G_i}$,

$$\begin{aligned} \Xi_{ii}^{\gamma}(l) = {} & P_{G_i}(l)\mathrm{diag}\{\Xi_{ii}^{\gamma}(l-1), \Xi_{ii}^{\gamma}(l-1)\}P_{G_i}^T(l) \\ & + \Delta\Xi_{ii}^{\gamma}(l) \end{aligned} \tag{71}$$

where $\Delta\Xi_{ii}^{\gamma}(l)$ is defined by $\Delta\Xi_{ii}^{\gamma}(l) = (1-\gamma\gamma_i(l))\{J_{ii}(l) \ominus [F_{K_i}\Gamma_{ii}^{\gamma}(l-1)A_0^T + D_{K_i}V_{\vec{w}}] + J_{ii}^T(l) \ominus [A_0{\Gamma_{ii}^{\gamma}}^T(l-1)F_{K_i}^T + V_{\vec{w}}D_{K_i}^T]\}$. Similarly, in light of the structure of $G_i(l)$, there must be a scalar $\psi_{G_i} > 0$ ensuring

$$\|\Delta\Xi_{ii}^{\gamma}(l)\|_2 \leq \psi_{G_i} \quad (l \geq \xi_{G_i}) \tag{72}$$

In addition, one has

$$\begin{cases} \|\mathrm{diag}\{\Xi_{ii}^{\gamma}(l-1), \Xi_{ii}^{\gamma}(l-1)\}\|_2 = \|\Xi_{ii}^{\gamma}(l-1)\|_2 \\ \|P_{G_i}(l)\|_2 \leq \theta_{G_i} \end{cases} \tag{73}$$

where θ_{G_i} is given in (48). Consequently, on the basis of (71)–(73), it can be derived that

$$\begin{aligned} \|\Xi_{ii}^{\gamma}(l)\|_2 & \leq \psi_{G_i} + \theta_{G_i}\|\Xi_{ii}^{\gamma}(l-1)\|_2 \\ & \leq \theta_{G_i}^{l-\xi_{G_i}}\|\Xi_{ii}^{\gamma}(\xi_{G_i})\|_2 + \sum_{o=0}^{l-\xi_{G_i}+1} \theta_{G_i}^{o}\psi_{G_i} \end{aligned} \tag{74}$$

Since $\theta_{G_i} < 1$, it can be deduced that $\lim_{l\to\infty}\theta_{G_i}^{l-\xi_{G_i}} = 0$ and $\lim_{l\to\infty}\sum_{o=0}^{l-\xi_{G_i}+1}\theta_{G_i}^{o}\psi_{G_i} = \frac{\psi_{G_i}}{1-\theta_{G_i}}$, and thus one has

$$\lim_{l\to\infty}\|\Xi_{ii}^{\gamma}(l)\|_2 \leq \frac{\psi_{G_i}}{1-\theta_{G_i}} \tag{75}$$

According to the aforementioned analysis, it can be inferred that $\lim_{l\to\infty}\mathrm{Tr}\{\Xi_{ii}^{\gamma}(l)\}$ is bounded when the conditions (48) and (49) are satisfied. Then, based on (36), it yields that

$$\lim_{l\to\infty}\mathrm{Tr}\{C(l)\} \leq \lim_{l\to\infty}\mathrm{Tr}\{\Xi_{ii}^{\gamma}(l)\} \tag{76}$$

As a consequence, when (48) and (49) hold, there must exist a positive scalar a that makes (29) hold. That's the end of the proof.

REFERENCES

[1] Z. Xing, Y. Xia, L. Yan, K. Lu, and Q. Gong, "Multisensor distributed weighted Kalman filter fusion with network delays, stochastic uncertainties, autocorrelated, and cross-correlated noises," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 5, pp. 716–726, May 2018.

[2] D. Ding, Z. Wang, Q. L. Han, and X. M. Zhang, "Recursive secure filtering over gilbert-elliott channels in sensor networks: The distributed case," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 7, pp. 75–86, 2021.

[3] H. Song, H. Yao, P. Shi, D. Zhang, and L. Yu, "Distributed secure state estimation of multi-sensor systems subject to two-channel hybrid attacks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 1049–1058, 2022.

[4] Y. Shi, C. Liu, and Y. Wang, "Secure state estimation of multiagent systems with homologous attacks using average consensus," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 3, pp. 1293–1303, Sep. 2021.

[5] B. Chen, D. W. C. Ho, G. Hu, and L. Yu, "Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks," *IEEE Trans. Cybern.*, vol. 48, no. 6, pp. 1862–1876, Jun. 2018.

[6] H. Geng, Z. Wang, F. E. Alsaadi, K. H. Alharbi, and Y. Cheng, "Protocol-based fusion estimator design for state-saturated systems with deadzone-like censoring under deception attacks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 37–48, 2022.

[7] L. Ma, Z. Wang, Y. Chen, and X. Yi, "Probability-guaranteed distributed secure estimation for nonlinear systems over sensor networks under deception attacks on innovations," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 7, pp. 465–477, 2021.

[8] Z. Gu, P. Shi, D. Yue, S. Yan, and X. Xie, "Memory-based continuous event-triggered control for networked T-S fuzzy systems against cyberattacks," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 10, pp. 3118–3129, Oct. 2021.

[9] Z. Xing and Y. Xia, "Distributed federated Kalman filter fusion over multisensor unreliable networked systems," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 63, no. 10, pp. 1714–1725, Oct. 2016.

[10] J. Ding, S. Sun, J. Ma, and N. Li, "Fusion estimation for multi-sensor networked systems with packet loss compensation," *Inf. Fusion*, vol. 45, pp. 138–149, 2019.

[11] H. Yan, P. Li, H. Zhang, X. Zhan, and F. Yang, "Event-triggered distributed fusion estimation of networked multisensor systems with limited information," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 12, pp. 5330–5337, Dec. 2020.

[12] L. Lan, G. Wei, and D. Ding, "Distributed fusion with unknown inputs under bandwidth-aware event-triggered mechanisms: Monotonicity and boundedness," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 9, pp. 521–530, 2023.

[13] H. Lin, S. Lu, P. Lu, H. Que, and P. Sun, "Centralized fusion estimation over wireless sensor-actuator networks with unobservable packet dropouts," *J. Franklin Inst.*, vol. 359, no. 2, pp. 1569–1584, 2022.

[14] J. Ma and S. Sun, "Centralized fusion estimators for multisensor systems with random sensor delays, multiple packet dropouts and uncertain observations," *IEEE Sensors J.*, vol. 13, no. 4, pp. 1228–1235, Apr. 2013.

[15] L. Li, M. Niu, Y. Xia, and H. Yang, "Stochastic event-triggered distributed fusion estimation under jamming attacks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 7, pp. 309–321, 2021.

[16] T. Tian and S. Sun, "Distributed fusion estimation for multisensor multirate systems with packet dropout compensations and correlated noises," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 51, no. 9, pp. 5762–5772, Sep. 2021.

[17] R. Wang, B. Chen, and L. Yu, "Distributed nonlinear fusion estimation without knowledge of noise statistical information: A robust design approach," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 5, pp. 3107–3117, Oct. 2021.
[18] B. Xiang, B. Chen, and L. Yu, "Distributed fusion estimation for unstable systems with quantized innovations," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 51, no. 10, pp. 6381–6387, Oct. 2021.
[19] C. Gao, Z. Wang, J. Hu, Y. Liu, and X. He, "Consensus-based distributed state estimation over sensor networks with encoding-decoding scheme: Accommodating bandwidth constraints," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 6, pp. 4051–4064, Nov./Dec., 2022.
[20] S. Wu, K. Ding, P. Cheng, and L. Shi, "Optimal scheduling of multiple sensors over lossy and bandwidth limited channels," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 3, pp. 1188–1200, Sep. 2020.
[21] B. Chen, G. Hu, D. W. C. Ho, and L. Yu, "Distributed covariance intersection fusion estimation for cyber-physical systems with communication constraints," *IEEE Trans. Autom. Control*, vol. 61, no. 12, pp. 4020–4026, Dec. 2016.
[22] X. Zheng, H. Zhang, X. Yang, and H. Yan, "Distributed dimensionality reduction filtering for CPSs under DoS attacks," *IEEE/CAA J. Automatica Sinica*, vol. 10, no. 4, pp. 1080–1082, Apr. 2023.
[23] L. Zou, Z. Wang, Q. Han, and D. Zhou, "Full information estimation for time-varying systems subject to round-robin scheduling: A recursive filter approach," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 51, no. 3, pp. 1904–1916, Mar. 2021.
[24] J. Liu, E. Gong, L. Zha, X. Xie, and E. Tian, "Outlier-resistant recursive security filtering for multirate networked systems under fading measurements and round-robin protocol," *IEEE Trans. Control Netw. Syst.*, vol. 10, no. 4, pp. 1962–1974, Dec. 2023.
[25] J. Fang and H. Li, "Optimal/near-optimal dimensionality reduction for distributed estimation in homogeneous and certain inhomogeneous scenarios," *IEEE Trans. Signal Process.*, vol. 58, no. 8, pp. 4339–4353, Aug. 2010.
[26] S. Fan, H. Yan, H. Zhang, Y. Wang, Y. Peng, and S. Xie, "Distributed dimensionality reduction fusion estimation for stochastic uncertain systems with fading measurements subject to mixed attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 52, no. 11, pp. 7053–7064, Nov. 2022.
[27] B. Chen, D. W. C. Ho, G. Hu, and L. Yu, "Delay-dependent distributed kalman fusion estimation with dimensionality reduction in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 52, no. 12, pp. 13557–13571, Dec. 2022.
[28] B. Chen, D. W. C. Ho, W. A. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 2, pp. 455–468, Feb. 2019.
[29] Y. Chen, Z. Wang, L. Wang, and W. Sheng, "Finite-horizon H_∞ state estimation for stochastic coupled networks with random inner couplings using round-robin protocol," *IEEE Trans. Cybern.*, vol. 51, no. 3, pp. 1204–1215, Jan. 2021.
[30] Y. Zhang, Z. Wang, L. Zou, H. Dong, and X. Yi, "Neural-network-based secure state estimation under energy-constrained denial-of-service attacks: An encoding-decoding scheme," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 4, pp. 2002–2015, Jul./Aug. 2023.
[31] F. Han, Z. Wang, H. Dong, F. E. Alsaadi, and K. H. Alharbi, "A local approach to distributed H_∞-consensus state estimation over sensor networks under hybrid attacks: Dynamic event-triggered scheme," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 8, pp. 556–570, 2022.
[32] Z. Gu, C. K. Ahn, D. Yue, and X. Xie, "Event-triggered H_∞ filtering for T-s fuzzy-model-based nonlinear networked systems with multisensors against DoS attacks," *IEEE Trans. Cybern.*, vol. 52, no. 6, pp. 5311–5321, Jun. 2022.
[33] S. Weng, P. Weng, B. Chen, S. Liu, and L. Yu, "Distributed secure estimation against unknown FDI attacks and load deviation in multi-area power systems," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 69, no. 6, pp. 3007–3011, Jun. 2022.
[34] L. Zha, R. Liao, J. Liu, X. Xie, E. Tian, and J. Cao, "Dynamic event-triggered output feedback control for networked systems subject to multiple cyber attacks," *IEEE Trans. Cybern.*, vol. 52, no. 12, pp. 13800–13808, Dec. 2022.
[35] F. Qu, E. Tian, and X. Zhao, "Chance-constrained H_∞ state estimation for recursive neural networks under deception attacks and energy constraints: The finite-horizon case," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 9, pp. 6492–6503, Sep. 2023.
[36] J. Shen, P. Weng, Y. Shen, B. Chen, and L. Yu, "Distributed fusion estimation for nonlinear cyber-physical systems with attacked control signals," *IEEE Syst. J.*, vol. 17, no. 1, pp. 1216–1223, Mar. 2023.
[37] J. Liu, Y. Wang, J. Cao, D. Yue, and X. Xie, "Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack," *IEEE Trans. Cybern.*, vol. 51, no. 8, pp. 4000–4010, Aug. 2021.
[38] L. Su, D. Ye, and X. Zhao, "Distributed secure state estimation for cyber-physical systems against replay attacks via multisensor method," *IEEE Syst. J.*, vol. 16, no. 4, pp. 5720–5728, Dec. 2022.
[39] H. Geng, Z. Wang, J. Hu, F. E. Alsaadi, and Y. Cheng, "Outlier-resistant sequential filtering fusion for cyber-physical systems with quantized measurements under denial-of-service attacks," *Inf. Sci.*, vol. 628, pp. 488–503, 2023.
[40] L. Zhang and S. Sun, "Distributed H_∞ fusion filtering for multi-sensor networked systems with DoS attacks and sensor saturations," *Digit. Signal Process.*, vol. 134, 2023, Art. no. 103908, doi: 10.1016/j.dsp.2023.103908.
[41] Y. Yang, Y. Li, D. Yue, Y. Tian, and X. Ding, "Distributed secure consensus control with event-triggering for multiagent systems under DoS attacks," *IEEE Trans. Cybern.*, vol. 51, no. 6, pp. 2916–2928, Jun. 2021.
[42] S. Sun, F. Peng, and H. Lin, "Distributed asynchronous fusion estimator for stochastic uncertain systems with multiple sensors of different fading measurement rates," *IEEE Trans. Signal Process.*, vol. 66, no. 3, pp. 641–653, Feb. 2018.
[43] H. Geng, Z. Wang, Y. Chen, F. E. Alsaadi, and Y. Cheng, "Multi-sensor filtering fusion with parametric uncertainties and measurement censoring: Monotonicity and boundedness," *IEEE Trans. Signal Process.*, vol. 69, pp. 5875–5890, 2021.
[44] B. Chen, W. A. Zhang, L. Yu, G. Hu, and H. Song, "Distributed fusion estimation with communication bandwidth constraints," *IEEE Trans. Autom. Control*, vol. 60, no. 5, pp. 1398–1403, May 2015.
[45] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.
[46] S. Sun and Z. Deng, "Multi-sensor optimal information fusion kalman filter," *Automatica*, vol. 40, no. 6, pp. 1017–1023, 2004.