Outlier-Resistant Distributed Filtering Over Sensor Networks Under Dynamic Event-Triggered Schemes and DoS Attacks

Lijuan Zha, Rongfei Liao, Jinliang Liu, *Member, IEEE*, Xiangpeng Xie, *Senior Member, IEEE*, Engang Tian, and Jinde Cao, *Fellow, IEEE*

***Abstract*— This paper focuses on the problem of outlier-resistant distributed filtering under dynamic event-triggered scheme (DETS) and cyber-attacks over sensor networks. A novel distributed DETS is proposed, which allows us to minimize the data-releasing rate while simultaneously preventing abrupt data from being sent over the network. Consider the situation of measurement outliers in presence, a saturation function is used in distributed filter design to confine the contaminated signals so as to improve filtering performance. The occurrence of stochastic DoS attacks which may corrupt the measurement in the sensor networks are also considered. Sufficient conditions for the expected filter are derived while guaranteeing the asymptotically stability of the filtering error system with a guaranteed H_∞ performance index γ. A numerical simulation is given to illustrate the effectiveness of the theoretical analysis and design method.**

***Note to Practitioners*—The issue of filtering over sensor networks is subject to network impections induced by the limited communication resources and cyber-attacks. Since these imperfections may lead to performance degration or instability of the system, it is critical to take some measures to reduce unnecessary signal communication among sensor nodes and eliminate the adverse effects of cyber-attacks. Besides, the measurement outliers are frequently encountered due to sensor aging or abnormal disturbances, which may impair the accuracy of the estimation resuts. In this paper, the outlier-resistant distributed filtering problem is investigated in sensor networks subject to dynamic event-triggered schemes and DoS attacks. A co-design method of the DETS and the distributed filter is propsed which can gurantee the desired system performance.**

***Index Terms*— Cyber-attacks, distributed filtering, dynamic event-triggered schemes, outlier-resistant.**

Manuscript received 24 February 2023; revised 6 July 2023 and 1 December 2023; accepted 27 January 2024. Date of publication 5 February 2024; date of current version 24 January 2025. This article was recommended for publication by Associate Editor V. Augusto and Editor G. Fortino upon evaluation of the reviewers' comments. This work was supported in part by the National Natural Science Foundation of China under Grant 62273174, Grant 62373252, and Grant 61903182; in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20211290 and Grant BK20230063; and in part by the Qing Lan Project. *(Corresponding author: Jinliang Liu.)*

Lijuan Zha is with the School of Science, Nanjing Forestry University, Nanjing 210037, China (e-mail: zhalijuan@vip.163.com).

Rongfei Liao is with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: liaorongfei110@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).

Jinde Cao is with the School of Mathematics, Southeast University, Nanjing 210096, China, and also with the School of Automation and Electrical Engineering, Linyi University, Linyi 276005, China (e-mail: jdcao@seu.edu.cn).

Digital Object Identifier 10.1109/TASE.2024.3360718

I. Introduction

In THE past few years, networked control systems (NCSs) have attracted widespread attention owing to their potential application in engineered genetic circuits [1], underwater vehicle [2], remote surgery and so on. Different from traditional wire transmission, the components in NCSs communicate and share information via wireless network which reduces the complexity and the maintenance cost of the control systems. The insertion of the wireless network may inevitable bring about some undesired issues such as time delays, package dropouts, missing measurements, etc., [3], [4], [5], [6], [7], and [8]. In recent few years, increasing effort has been devoted to deal with these phenomena in filter and control problems. For example, considering the impact of uncertain time delays introduced by a communication network between plants and controllers in each subsystem, Li et al. [3] provided a discrete-time control approach for complex NCSs. To solve the chance-constrained problems in the control systems, Tian et al. proposed a prominent lemma to transform the chance constraints into deterministic ones, which shortened the gap significantly between the probabilistic purpose and the deterministic ones. Bahreini et al. [6] focused on the robust and reliable output feedback control problem for uncertain NCSs subject to both packet dropouts and time delays. In [7], under the influence of time delays and missing measurements, authors designed a new prediction-based distributed filter, in which the measurement missing probability of each sensor node are unique.

In the wake of developments in wireless sensor, computing and wireless communication technology, sensor networks have been extensively employed in many domain ranging from target tracking [9], battlefield monitoring [10], to industrial automation [11]. The fundamental idea of sensor networks is to utilize several sensor nodes spread out across certain area to supervise and detect realistic ambient conditions or aggregate data from moving data packages through communication network. The wireless sensor network's essential characteristic is that these smart sensor nodes work with one another according to an interaction topology to achieve a shared detecting, tracking, or monitoring goal [18]. In other words, the main aspect of distributed filtering in sensor networks, as opposed to typical single sensor filtering methods, is that the accessible information on each sensor node is from its own measurement and nearby sensors via information sharing. The distributed filtering method is considered to have good filtering performance because it has cooperative information processing and strong robustness to sensor unreliability. Nowadays, the filtering over sensor networks has become a critical research topic [12], [13], [16], [17]. For instance, [12] focused on the distributed set-membership filters design method for discrete-time nonlinear systems under event-triggered (ET) schemes over sensor networks. In [13], Tian et al. proposed the distributed filter design method over sensor networks confined by state constraints and subject to denial-of-service (DoS) attacks. In [14], the problem of distributed filters design was discussed over sensor networks, in which the locally optimal filter gain was derived. Recently, the authors in [15] addressed the detection mechanism for detecting attacks and a secure ET distributed kalman filter over sensor networks was proposed. Up to now, the secure H_∞ distributed filtering over sensor networks with dynamic ET scheme and abnormal data has not been adequately addressed in the literature, which motivates the current research.

As we know, in wireless network, the communication capacity is often constrained resulted by the limited network bandwidth, which has drawn growing attention in recent decades [19], [20], [21], [22]. Some effective methods have been put forward to improve the utilization of network bandwidth [23], [24], [25], [26]. For example, by selecting a sample internal, the self-triggered mechanism of [23] was customized to design a predictive control algorithm while ensuring the quick decrease of prediction costs associated with appropriate predictive control inputs. As opposed to certain current self-triggered mechanisms, a sampled-data-based ET mechanism can provide a positive minimum inter-event time and make it possible to jointly design adequate feedback controllers and ET threshold parameters [27], [28], [29]. In [27], the authors presented an overview of the sampled-data-based ET control problem and conducted a thorough research. The authors developed an adaptive ET mechanism in [28], in which the adaptive threshold is decided by the system's dynamic error rather than a predefined constant. Besides, a dynamic ET technique was used in [29] to improve resource efficiency and the consensus of the mutiagent systems was achieved. However, among most of the above mentioned results, researchers focus on the variations of the error between the newly data packet and the last released one while designing the triggering conditions, neglecting the impacts of the abrupt signals which are triggered mistakenly. How to devise ET conditions and prevent erroneous event is an interesting issue, which gives rise to another motivation of our research.

Aside from the issue of restricted network capacity, cyber-attack is another issue that must be actively addressed in NCSs. As we all know, the flexibility of installation and superiority in maintenance can be improved when data packets transmitted via wireless communication channels. In view of this advantage, wireless network communication has been widely applied in NCSs [30], [31]. However, the openness characteristic of wireless network may also lead to loss of security protection. The high-stakes of being targeted by malevolent adversaries that comes with wireless data transfer is unavoidable. Therefore, data transmission security issue is worth researching [32], [33], [34]. In industry, there are three kinds of attacks commonly encountered, namely, deception attack [35], [36], [37], replay attack [39] and DoS attack [13], [17], [40], [41], which have been paid increasing attention. Deception attacks are a common type of data integrity attacks, through which the hacker attempts to make the system accept certain incorrect data as true. In [35], the author considered the spectacle that hacker disturb the normal running of the system by injecting data into the transmitted data between each pair of sensors. Another common cyber attack is the replay attack, which maliciously reproduces transmitted data to influence system operation. Liu et al. focused on the filter design problem under replay attacks which may have a serious impact on system performance in [39]. The objective of DoS attack is to disrupt data transmission and destroy system performance, which should be considered in system design and analysis. In [13], the DoS attacks has been taken into consideration when the authors designed the distributed filters for stochastic systems. So far, how to protect the NCSs against potential cyber attacks is still one of the challenging issues. Thus, it makes great sense to investigate the distributed filtering problem over sensor networks that are vulnerable to be attacked and abnormal dada.

For different reasons, including operation faults, sensor noises/failures, and external disturbances, the measurement output may face sudden but substantial disturbances, which is called measurement outliers. Measurement outliers can cause anomalous variation, which, if used in the filter implementation, can cause aberrant innovation and, as a result, decrease the filters performance [14], [42], [43]. Obviously, it makes sense to investigate the outlier-resistant filtering problem by eliminating/inhibiting the side-effects generated by measurement outliers [44], [45], [46]. Fortunately, some outlier resistant filtering or control method have been available. In [44], to limit the influence of measurement outliers on the estimation error dynamics, Li et al. proposed a confidence-dependent saturation function. For the sake of maintaining satisfactory filtering performance, the author in [45] designed an outlier-resistant recursive filter which can restrict the signals tainted by measurement outliers. Zhao et al. proposed an outlier-resistant proportional-integral observer design approach handling the negative impacts of deception attacks on the estimation performance in [46]. So far, the methods of the distributed filtering over sensor networks against measurement outliers have not been fulfilled, which also motivates the current research.

Motivated by the above-mentioned analysis, in this paper, we are interested in investigating the outlier-resistant distributed filtering for sensor networks under dynamic event-triggered schemes (DETS) against DoS attacks. The main contributions of this article are summarized as follows.

1) A novel distributed DETS will be designed to determine when each sensor transmits events with its adjacent sensor nodes. The proposed distributed DETS can not only avoid the constant occupancy of communication resources, but also prohibit some abrupt data that is unnecessary to the system from being released into the network;
2) An outlier-resistant distributed filtering method will be presented to tackle the problem that the sensor signals may experience abrupt disturbances induced by unforeseeable sensor failures, unexpected environmental variations, or malicious cyber-attacks, bringing about measurement outliers. Applying the outlier-resistant method, the measurement outliers will be tackled and desired filtering performance will be maintained;
3) To account for the occurrence of DoS attacks in information interchange and transmission, a unified sensor measurement transmission model will be proposed. The model shows how DoS attacks disrupt the exchange of information among adjacent sensors and how the measurement outputs from each sensor to a remote filter is destroyed.

II. System Description

A. Plant

Consider the plant presented as a NCS as follows:

$$\begin{cases} x(k+1) = Ax(k) + B\omega(k) \\ z(k) = Dx(k) \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^{n_x}$ and $z(k) \in \mathbb{R}^{n_z}$ stand for the system state and objective output signal to be estimated, respectively; $\omega(k) \in \mathbb{R}^{n_w}$ represents the exogenous disturbance which belongs to $L_2[0, \infty)$; and $A \in \mathbb{R}^{n_x \times n_x}$, $B \in \mathbb{R}^{n_x \times n_w}$, $D \in \mathbb{R}^{n_z \times n_x}$ are known constant matrices.

B. Sensor Measurement Model

In this paper, there are N sensor nodes distributed in the sensor networks in line with a given topology which can be represented by an directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. $\mathcal{V} = \{1, 2, \cdots, N\}$ and $\mathcal{E} \in \mathcal{V} \times \mathcal{V}$ are the index set of N sensor nodes and the edge set of coupled sensor nodes, respectively. An edge of $\mathcal{G}$ is given by the ordered couple (i, j), which shows that a single direction information exchange from the sensor of node i to the filter of node j. The adjacent matrix of graph $\mathcal{G}$ is express as $\mathcal{A} = [a_{ij}]_{N\times N}$, the element a_{ij} of which associated with edge (i, j) is positive, that is, $a_{ij} = 1$ if $(i, j) \in \mathcal{E}$, otherwise, $a_{ij} = 0$. Moreover, the self-loops of sensor nodes are permitted $a_{ij} = 1$. A group of neighbors of the node i is represented by $\mathcal{N}_i = \{j : (j, i) \in \mathcal{E}\}$.

For each node $i \in \mathcal{V}$, the output measurement model of sensor node i for above system (1) is given as follows:

$$y_i(k) = C_i x(k) \tag{2}$$

where $y_i(k) \in \mathbb{R}^{n_y}$ denotes the measurement output received by the sensor i from the plant. $C_i \in \mathbb{R}^{n_y \times n_x}$ is a known constant matrix.

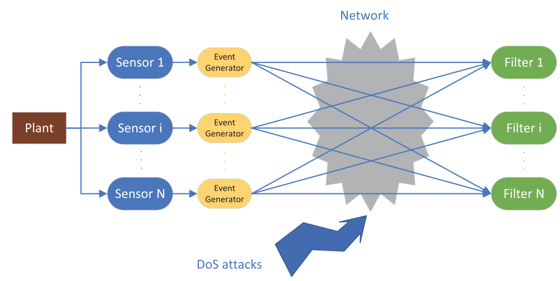

Fig. 1. The structure of outlier-resistant distributed filtering over sensor networks under DETS and DoS attacks.

For the convenience of later analysis, define $\bar{x}(k) \triangleq \mathbf{col}_N\{x(k)\}$, $\bar{y}(k) \triangleq \mathbf{col}_N\{y_i(k)\}$, $\bar{z}(k) \triangleq \mathbf{col}_N\{z(k)\}$, the model of plant and sensors can be describe by

$$\begin{cases} \bar{x}(k+1) = \bar{A}\bar{x}(k) + \bar{B}\omega(k) \\ \bar{y}(k) = \hat{C}\bar{x}(k) \\ \bar{z}(k) = \bar{D}\bar{x}(k) \end{cases} \tag{3}$$

with $\bar{A} \triangleq I_N \otimes A$, $\bar{B} \triangleq \mathbf{col}_N\{B\}$, $\hat{C} \triangleq \mathrm{diag}_N\{C_i\}$, $\bar{D} \triangleq I_N \otimes D$.

C. Distributed Dynamic Event-Triggered Scheme

The purpose of this part is to establish a novel distributed DETS to decide the frequency of each sensor's signals transmitted to the network. In the sensor network shown in Fig. 1, whether the current data package from each sampler should be released to the subfilter is depend on its corresponding DETS. The proposed dynamic ET condition is given by

$$\begin{cases} \lambda_i \phi_i(k) > \theta_i(k) \\ \phi_i(k) = e_i^T(k) G_i e_i(k) - \delta_i y_i^T(T_i^t) G_i y_i(T_i^t) \end{cases} \tag{4}$$

where $\{T_i^t\}$ is the sequence of releasing instants, λ_i and δ_i are given constants, G_i is the dynamic ET matrix to be designed, $\theta_i(k)$ is an auxiliary offset variable updating by the following rules:

$$\begin{cases} \theta_i(k+1) = \varepsilon_i \theta_i(k) - \phi_i(k) \\ \theta_i(0) \geqslant 0 \end{cases} \tag{5}$$

with $\theta_i(k) \geqslant 0$, $\varepsilon_i \in (0, 1)$ in which $\lambda_i \varepsilon_i \geqslant 1$, and the error $e_i(k)$ is defined as $e_i(k) = y_i(T_i^t) - y_i(T_i^t + \Delta)$ with

$$y_i(T_i^t + \Delta) = \mu_i[y_i(k) - y_i(T_i^t)] + y_i(T_i^t) \tag{6}$$

If the dynamic ET condition (4) is violated, the current signal will be released to the wireless network. However, one can see abrupt signals are more likely to violate the condition (4) than those signals with normal variation, that will lead to the consequence that these incorrect package are released to the internet. Therefore, in order to avoid this situation, one can set an adjustment factors $\mu_i \in (0, 1]$ when defining the error $e_i(k)$ for each node i.

Remark 1: In this paper, different from error in traditional DETS with $e_i(k) = y_i(T_i^t) - y_i(k)$, the proposed distributed DETS redefines the error as $e_i(k) = y_i(T_i^t) - y_i(T_i^t + \Delta)$ with an artificial output $y_i(T_i^t + \Delta) = \mu_i[y_i(k) - y_i(T_i^t)] + y_i(T_i^t)$ to prevent the abrupt signals from being released into the wireless network. In (6), if the value of μ_i is 1, the error of proposed distributed DETS reduces to the traditional DETS. However, if μ_i equals to a value between 0 and 1, the result of $y_i(T_i^t+\Delta)$ will be a combination of $y_i(T_i^t)$ and $y_i(k)$.

Remark 2: For the purpose of saving limited network resource, many literatures have already investigated about DETSs. Whereas, the impact of abrupt signals (that may be the incorrect data) have not been taken into consideration in most of the existing literature. As such, we develop DETS in (4) to account for this phenomena in this article. The DETS (4) has not been considered in distributed filter design over sensor networks, which is still a challenging issue.

Remark 3: For all $k \in \mathbb{N}$, the auxiliary offset variable $\theta_i(k) \geq 0, i \in \mathcal{V}$ if the given scalar ε_i and λ_i satisfy $\varepsilon_i \in (0, 1)$ and $\lambda_i \varepsilon_i \geqslant 1$. The details of proof can be found in Lemma 1 of [47].

From the definition of $e_i(k)$ and equation (6), the signal released into the networked transmission channel can be described as follows

$$y_i(T_i^t) = \frac{1}{\mu_i} e_i(k) + y_i(k), \tag{7}$$

then let $\hat{y}(T^t) \triangleq \mathbf{col}_N\{y_i(T_i^t)\}$, $\hat{e}(k) \triangleq \mathbf{col}_N\{e_i(k)\}$, the triggered signals are denoted as follows:

$$\hat{y}(T^t) = \mu_I \hat{e}(k) + \bar{y}(k) \tag{8}$$

where $\mu_I = (\mathrm{diag}_N\{\frac{1}{\mu_i}\}) \otimes I_{n_y}$.

D. Distributed Filter Under DoS Attacks

In this section, the DoS attack is considered when the signal is transmitted through the wireless network. Besides, due to the existence of measurement outliers, which would deteriorate the observer performance or even destabilize the error dynamics, we purposely introduce a saturation function when modeling the distributed filter. Based on above-mentioned, filter i with the following form is developed to estimate system state $x(k)$ of plant:

$$\begin{cases} \hat{x}_i(k+1) = \hat{A}_i \hat{x}_i(k) + \hat{B}_i \chi(\sum\limits_{j \in \mathcal{N}_i} a_{ij}(\alpha_i(k) y_j(T_i^t) \\ \quad -C_j \hat{x}_j(k))) \\ \hat{z}_i(k) = \hat{D}_i \hat{x}_i(k) \end{cases} \tag{9}$$

where $\hat{x}_i(k) \in R^m$ and $\hat{z}_i(k) \in R^q$ stand for the filter state and the estimation output vector of ith filter, respectively; and $\hat{A}_i \in \mathbb{R}^{n_x \times n_x}$, $\hat{B}_i \in \mathbb{R}^{n_x \times n_y}$, $\hat{D}_i \in \mathbb{R}^{n_y \times n_x}$ are filter gain matrices to be designed later. $\alpha_i(k)$ taking values on $\{0, 1\}$ is used to denote the effect of the randomly occurring DoS attacks and satisfies the following condition shown in (10)

$$\mathrm{Prob}\{\alpha_i(k) = 1\} = \bar{\alpha}_i, \mathrm{Prob}\{\alpha_i(k) = 0\} = 1 - \bar{\alpha}_i \tag{10}$$

with $0 < \bar{\alpha}_i < 1$. The saturation function $\chi(\cdot) : R^{n_y N} \longrightarrow R^{n_y N}$ is defined as follows:

$$\chi(o) = \left[\chi_1^T(o_1) \ \chi_2^T(o_2) \ \cdots \ \chi_{n_y N}^T(o_{n_y n})\right]^T \tag{11}$$

with $\chi_p^T(o_p) \triangleq \mathrm{sign}(o_p)\{o_{p,max}, |o_p|\}$, $p = 1, 2, \cdots, n_y N$, where $o_{p,max}$ is the pth element of o_{max}.

Remark 4: It should be explained that the model (9) reflects the influences of the DETS and the DoS attacks. The received signal of the local filter is triggered by the DETS first and then transmitted via the vulnerable network channel. In current works, two methods including hold input mechanism and zero input signal can be found to overcome the impacts of DoS attacks. In this article, we assume the local filter will receive zero input signal instead of the previous triggered measurement signal being applied, similar method can be found in the related works [48], [49].

Denote $S_i = \sum_{j \in \mathcal{N}_i} a_{ij}(\alpha_i(k) y_j(T_i^t) - C_j \hat{x}_j(k))$, and let $S \triangleq \mathbf{col}_N\{S_i\}$, $\chi(S) \triangleq \mathbf{col}_N\{\chi(S_i)\}$, hence,

$$S = \alpha_I(k) \mathcal{A}_I(\mu_I \hat{e}(k) + \hat{C}\bar{x}(k)) - \mathcal{A}_I \hat{C} \hat{x}(k) \tag{12}$$

where $\mathcal{A}_I = \mathcal{A} \otimes I_{n_y}$, $\alpha_I(k) = (\mathrm{diag}_N\{\alpha_i(k)\}) \otimes I_{n_y}$.

Setting $\hat{x}(k) \triangleq \mathbf{col}_N\{\hat{x}_i(k)\}$, $\hat{z}(k) \triangleq \mathbf{col}_N\{\hat{z}_i(k)\}$, the filter model can be regarded as

$$\begin{cases} \hat{x}(k+1) = \hat{A}\hat{x}(k) + \hat{B}\chi(S) \\ \hat{z}(k) = \hat{D}\hat{x}(k) \end{cases} \tag{13}$$

with $\hat{A} = \mathrm{diag}_N\{\hat{A}_i\}$, $\hat{B} = \mathrm{diag}_N\{\hat{B}_i\}$, $\hat{D} = \mathrm{diag}_N\{\hat{D}_i\}$.

Remark 5: Measurement outliers, which are a type of polluted measurement that deviates greatly from the usual, have recently sparked a lot of scientific interest. Sensor aging/failures, operational errors, and environmental conditions are all possible causes of measurement outliers which may result in the computation of anomalous innovation, degrading the filter's performance. As a result, we are working on a filter design strategy that will avoid outliers from degrading estimation accuracy. In the filter structure, a particular saturation function $\chi(\cdot)$ is provided to confine the innovation to a preset range which can be predetermined according to actual conditions.

Remark 6: The signals send to node i from its neighbors node j may be subject to DoS attacks. (9) takes this circumstance into account. A set of Bernoulli distribution variables $\alpha_i(k)$, $i \in \mathcal{V}$ is used to describe the effect of the DoS attacks appearance or not. Specially, if $\alpha_i(k) = 0$, it means the signals $y_j(T_i^t)$, $j \in \mathcal{N}_i$ are hacked by malicious attacks and the real signals received by node i are zero; if $\alpha_i(k) = 1$, the signals will be transmitted as normal.

Remark 7: Nowadays, some technologies have been proposed to detect the occurrence of the DoS attacks (see [50] for example), where the hölder filter is implemented to identify the beginning or ending of DoS attacks. Besides, it is also explained in reference [49] that the detection of DoS attacks is available under the well-known transmission control protocol. The information of the DoS attacks is also assumed to be known in [17], [36], [41], and [49].

Before proceeding further, the following definition and lemma are provided.

Definition 1 ([44]): There exists a nonlinear function $g(\cdot)$ satisfying a sector condition, if

$$(g(S_i) - R_1 S_i)^T (g(S_i) - R_2 S_i) \leq 0 \tag{14}$$

where R_1, R_2 are real matrices, $R = R_2 - R_1 > 0$, and $g(S_i)$ belongs to the sector $[R_1, R_2]$.

Lemma 1: If there are diagonal matrices M and N that satisfy $0 \leq M < I \leq N$, allowing the saturation function $\chi(\cdot)$

in (9) to be separated into a linear and nonlinear component as follows:

$$\chi(S_i) = MS_i + g(S_i) \tag{15}$$

where the nonlinear function $g(\cdot)$ meets the sector condition (14) when $R_1 = 0$ and $R_2 = N - M$, and the following inequality should be met:

$$g^T(S_i)[g(S_i) - R_2 S_i] \leq 0 \tag{16}$$

From Lemma 1 and (13), $\hat{x}(k+1)$ can be obtained as

$$\begin{aligned}\hat{x}(k+1) &= \hat{A}\hat{x}(k) + \hat{B}\hat{M}S + \hat{B}\hat{g}(S)\\ &= \hat{B}\hat{M}\alpha_I(k)\mathcal{A}_I\hat{C}\bar{x}(k) + (\hat{A} - \hat{B}\hat{M}\mathcal{A}_I\hat{C})\hat{x}(k)\\ &\quad + \hat{B}\hat{M}\alpha_I(k)\mathcal{A}_I\mu_I\hat{e}(k) + \hat{B}\hat{g}(S).\end{aligned} \tag{17}$$

where $\hat{g}(S) = \mathbf{col}_N\{g(S_i)\}$, $\hat{M} = \text{diag}_N\{M\}$.

E. Filtering Error Dynamics

Define $\varphi(k) \triangleq \bar{x}(k) - \hat{x}(k)$, from (17) and (3), one can get $\hat{x}(k+1)$ and $\varphi(k+1)$ as follows:

$$\begin{aligned}\hat{x}(k+1) &= \hat{B}\hat{M}\bar{\alpha}_I\mathcal{A}_I\hat{C}\varphi(k)\\ &\quad + [\hat{A} - \hat{B}\hat{M}(I - \bar{\alpha}_I)\mathcal{A}_I\hat{C}]\hat{x}(k)\\ &\quad + \hat{B}\hat{M}\bar{\alpha}_I\mathcal{A}_I\mu_I\hat{e}(k) + \hat{B}\hat{g}(S)\\ &\quad + \sum_{i=1}^{N}(\alpha_i(k) - \bar{\alpha}_i)\hat{B}\hat{M}\hat{E}_i\mathcal{A}_I[\hat{C}\varphi(k)\\ &\quad + \hat{C}\hat{x}(k) + \mu_I\hat{e}(k)]\end{aligned} \tag{18}$$

$$\begin{aligned}\varphi(k+1) &= [\bar{A} - \hat{B}\hat{M}\bar{\alpha}_I\mathcal{A}_I\hat{C}]\varphi(k) + \bar{B}\omega(k)\\ &\quad + [\bar{A} - \hat{A} + \hat{B}\hat{M}(I - \bar{\alpha}_I)\mathcal{A}_I\hat{C}]\hat{x}(k)\\ &\quad - \hat{B}\hat{M}\bar{\alpha}_I\mathcal{A}_I\mu_I\hat{e}(k) - \hat{B}\hat{g}(S)\\ &\quad - \sum_{i=1}^{N}(\alpha_i(k) - \bar{\alpha}_i)\hat{B}\hat{M}\hat{E}_i\mathcal{A}_I[\hat{C}\varphi(k)\\ &\quad + \hat{C}\hat{x}(k) + \mu_I\hat{e}(k)]\end{aligned} \tag{19}$$

where $\bar{\alpha}_I = (\text{diag}_N\{\bar{\alpha}_i\}) \otimes I_{n_y}$, $\hat{E}_i = E_N^i \otimes I_{n_y}$, $E_N^i = \text{diag}\{\overbrace{0, \cdots, 0}^{i-1}, 1, \overbrace{0, \cdots, 0}^{N-i}\}$, $i \in \{1, 2, \cdots, N\}$.

Define $\rho(k) \triangleq \begin{bmatrix}\varphi(k)\\ \hat{x}(k)\end{bmatrix}$, $\tilde{z}(k) \triangleq \bar{z}(k) - \hat{z}(k)$, the augment system can be expressed as

$$\begin{cases}\rho(k+1) = F_A\rho(k) + \hat{F}_B\hat{M}\bar{\alpha}_I\mathcal{A}_I\mu_I\hat{e}(k)\\ \qquad + \bar{F}_B\omega(k) + \hat{F}_B\hat{g}(S)\\ \qquad + \sum_{i=1}^{N}(\alpha_i(k) - \bar{\alpha}_i)[F_C\rho(k) + \hat{F}_B\hat{M}\hat{E}_i\mathcal{A}_I\mu_I\hat{e}(k)]\\ \tilde{z}(k) = F_D\rho(k)\end{cases} \tag{20}$$

where

$$\begin{aligned}F_A &= \begin{bmatrix}\bar{A} - \hat{B}\pi_1 & \bar{A} - \hat{A} - \hat{B}\pi_1 + \hat{B}\pi_2\\ \hat{B}\pi_1 & \hat{A} + \hat{B}\pi_1 - \hat{B}\pi_2\end{bmatrix},\\ \hat{F}_B &= \begin{bmatrix}-\hat{B}\\ \hat{B}\end{bmatrix},\\ \bar{F}_B &= \begin{bmatrix}\bar{B}\\ 0\end{bmatrix},\\ F_C &= \begin{bmatrix}-\hat{B}\hat{M}\hat{E}_i\mathcal{A}_I\hat{C} & -\hat{B}\hat{M}\hat{E}_i\mathcal{A}_I\hat{C}\\ \hat{B}\hat{M}\hat{E}_i\mathcal{A}_I\hat{C} & \hat{B}\hat{M}\hat{E}_i\mathcal{A}_I\hat{C}\end{bmatrix},\\ F_D &= \begin{bmatrix}\bar{D} & \bar{D} - \hat{D}\end{bmatrix},\\ \pi_1 &= \hat{M}\bar{\alpha}_I\mathcal{A}_I\hat{C}, \pi_2 = \hat{M}\mathcal{A}_I\hat{C}.\end{aligned}$$

III. Main Results

In this section, sufficient conditions are firstly established in Theorem 1 to guarantee the discussed augmented system (20) asymptotically stable (AS) with a given performance index γ. Besides, on the basis of Theorem 1, Theorem 2 is given to provides the design method of the gain matrices of distributed filter and ET matrices.

A. H_∞ Stability Analysis

Theorem 1: For given constants $\bar{\alpha}_i \in (0, 1)$, λ_i, $\varepsilon_i \in [0, 1)$ $\mu_i \in (0, 1]$ and γ, dynamic ET matrix sequence G_i, and filter gain matrices $\hat{A}_i$, $\hat{B}_i$ and $\hat{D}_i$, system (20) is AS under the DETSs (4), if there exists a symmetric matrix $P > 0$ and a positive scalar l_0 such that

$$\Pi_1 = \begin{bmatrix}\Xi_2 & * & * & * & * & *\\ PJ_1 & -P & * & * & * & *\\ \tau_1 PJ_{21} & 0 & -P & * & * & *\\ \vdots & \vdots & \vdots & \ddots & * & *\\ \tau_N PJ_{2N} & 0 & 0 & 0 & -P & *\\ J_3 & 0 & 0 & 0 & 0 & -I\end{bmatrix} < 0 \tag{21}$$

where

$$\Xi_2 = \begin{bmatrix}\nu_{11}^1 & * & * & *\\ \nu_{21}^1 & \nu_{22}^1 & * & *\\ \frac{l_0}{2}\hat{R}_2F_\alpha & \frac{l_0}{2}\hat{R}_2\bar{\alpha}_I\mathcal{A}_I\mu_I & -l_0I & *\\ 0 & 0 & 0 & -N\gamma^2I\end{bmatrix}, \tag{22}$$

$$\begin{aligned}J_1 &= \begin{bmatrix}F_A & \hat{F}_B\hat{M}\bar{\alpha}_I\mathcal{A}_I\mu_I & \hat{F}_B & \bar{F}_B\end{bmatrix},\\ J_{2i} &= \begin{bmatrix}F_C & \hat{F}_B\hat{M}\hat{E}_i\mathcal{A}_I\mu_I & 0 & 0\end{bmatrix},\\ & i \in \{1, 2, \cdots, N\},\\ J_3 &= \begin{bmatrix}F_D & 0 & 0 & 0\end{bmatrix},\\ F_\alpha &= \begin{bmatrix}\bar{\alpha}_I\mathcal{A}_I\hat{C} & (\bar{\alpha}_I - I)\mathcal{A}_I\hat{C}\end{bmatrix},\\ \bar{I} &= \begin{bmatrix}I & I\end{bmatrix},\\ \nu_{11}^1 &= -P - \bar{I}^T\hat{C}^T\kappa_I\delta_I\hat{G}\hat{C}\bar{I},\\ \nu_{21}^1 &= -\mu_I^T\kappa_I\delta_I\hat{G}\hat{C}\bar{I},\\ \nu_{22}^1 &= \kappa_I\hat{G} - \mu_I^T\kappa_I\delta_I\hat{G}\mu_I,\\ \tau_i &= \sqrt{\bar{\alpha}_i(1 - \bar{\alpha}_i)}, \delta_I = diag_N\{\delta_i\} \otimes I_{n_y},\\ \kappa_I &= diag_N\{\kappa_i\} \otimes I_{n_y}, \kappa_i = \varepsilon_i - 1 - \frac{1}{\lambda_i}.\end{aligned}$$

Proof: Construct a Lyapunov-Krasovskii functional candidate for the augmented system (20) as

$$V(k) = \rho^T(k)P\rho(k) + \sum_{i=1}^{N}\frac{1}{\lambda_i}\theta_i(k). \tag{23}$$

Define $\Delta V(k)$ as $\Delta V(k) \triangleq V(k+1) - V(k)$, then, one can obtained that

$$\mathbb{E}\{\Delta V(k)\} = \iota_1^T P \iota_1 + \sum_{i=1}^{N} \bar{\alpha}_i(1-\bar{\alpha}_i)\iota_{2i}^T P \iota_{2i} - \rho^T(k) P \rho(k) + \sum_{i=1}^{N} \frac{1}{\lambda_i}((\varepsilon_i - 1)\theta_i(k) - \phi_i(k)) \tag{24}$$

where $\iota_1 = F_A \rho(k) + \hat{F}_B \hat{M} \bar{\alpha}_I \mathcal{A}_I \mu_I \hat{e}(k) + \bar{F}_B \omega(k)$, $\iota_{2i} = F_C \rho(k) + \hat{F}_B \hat{M} \hat{E}_i \mathcal{A}_I \mu_I \hat{e}(k)$.

For $k \in (T_i^t, T_i^{t+1})$, the dynamic ET condition (4) is satisfied, that is to say $\lambda_i \phi_i(k) \leqslant \theta_i(k)$. Then, by combining (5), (8) and $\varepsilon_i - 1 < 0$, one have

$$\begin{aligned}
&\sum_{i=1}^{N} [\frac{1}{\lambda_i}(\varepsilon_i - 1)\theta_i(k) - \phi_i(k)] \\
&\quad \leqslant \sum_{i=1}^{N} (\varepsilon_i - 1 - \frac{1}{\lambda_i})\phi_i(k) \\
&\quad = -[\hat{C}\bar{I}\rho(k) + \mu_I \hat{e}(k)]^T \kappa_I \delta_I \hat{G} [\hat{C}\bar{I}\rho(k) + \mu_I \hat{e}(k)] \\
&\qquad + \hat{e}^T(k) \kappa_I \hat{G} \hat{e}(k)
\end{aligned} \tag{25}$$

Hence, according to (24), (25) and (16), one can obtain the following inequality:

$$\begin{aligned}
\mathbb{E}\{\Delta V(k)\} \leqslant{}& \iota_1^T P \iota_1 + \sum_{i=1}^{N} \bar{\alpha}_i(1-\bar{\alpha}_i)\iota_{2i}^T P \iota_{2i} - \rho^T(k) P \rho(k) \\
& - [\hat{C}\bar{I}\rho(k) + \mu_I \hat{e}(k)]^T \kappa_I \delta_I \hat{G} [\hat{C}\bar{I}\rho(k) + \mu_I \hat{e}(k)] \\
& + \hat{e}^T(k) \kappa_I \hat{G} \hat{e}(k) - l_0 \hat{g}^T(S) \hat{g}(S) \\
& + l_0 \hat{g}^T(S) \hat{R}_2 [F_\alpha \rho(k) + \bar{\alpha}_I \mathcal{A}_I \mu_I \hat{e}(k)] \\
={}& \eta^T(k) [\Xi_1 + J_1^T P J_1 \\
& + \sum_{i=1}^{N} \bar{\alpha}_i(1-\bar{\alpha}_i) J_{2i}^T P J_{2i}] \eta(k),
\end{aligned} \tag{26}$$

where $\eta(k) = \begin{bmatrix} \rho^T(k) & e^T(k) & \hat{g}^T(S) & \omega^T(k) \end{bmatrix}^T$,

$$\Xi_1 = \begin{bmatrix} \nu_{11}^1 & * & * & * \\ \nu_{21}^1 & \nu_{22}^1 & * & * \\ \frac{l_0}{2}\hat{R}_2 F_\alpha & \frac{l_0}{2}\hat{R}_2 \bar{\alpha}_I \mathcal{A}_I \mu_I & -l_0 I & * \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{27}$$

Under the zero-initial condition, it follows from (26) that

$$\begin{aligned}
&\mathbb{E}\sum_{k=0}^{Q} \{\| \tilde{z}(k) \|^2 - N\gamma^2 \| \omega(k) \|^2 + \Delta V(k)\} - \sum_{k=0}^{Q} \Delta V(k) \\
&\leqslant \sum_{k=0}^{Q} \{\eta^T(k) [\Xi_2 + J_1^T P J_1 + \sum_{i=1}^{N} \bar{\alpha}_i(1-\bar{\alpha}_i) J_{2i}^T P J_{2i} \\
&\quad + J_3^T J_3] \eta(k)\} - \mathbb{E}\{V(Q+1)\}
\end{aligned} \tag{28}$$

By utilizing Schur complement method, we can conclude that $\mathbb{E}\{\sum_{k=0}^{Q} \| \tilde{z}(k) \|^2 - N\gamma^2 \sum_{k=0}^{Q} \| \omega(k) \|^2\} < 0$ holds if the condition (21) holds. Let $Q \to \infty$, we prove that the H_∞ performance constraint is ensured. This completes this proof.

B. Design of Event-Triggered Matrices and Filter Gains

In this part, the design method is given in the following Theorem, which is based on Theorem 1.

Theorem 2: When the distributed filter gains are designed by

$$\hat{A} = \bar{P}^{-1} X, \quad \hat{B} = \bar{P}^{-1} Y \quad \text{and} \quad \hat{D} \tag{29}$$

system (20) is AS under the DETSs (4) for given constants $\bar{\alpha}_i \in (0, 1)$, λ_i, $\varepsilon_i \in [0, 1)$, $\mu_i \in (0, 1]$ and γ, if there exists a symmetric matrix $\bar{P} > 0$, dynamic ET matrix sequence G_i and a positive scalar l_0 such that

$$\Pi_2 = \begin{bmatrix} \Xi_3 & * & * & * & * & * \\ Q_1 & \mathcal{P} & * & * & * & * \\ Q_{21} & 0 & \mathcal{P} & * & * & * \\ \vdots & \vdots & \vdots & \ddots & * & * \\ Q_{2N} & 0 & 0 & 0 & \mathcal{P} & * \\ J_3 & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{30}$$

where

$$\begin{aligned}
\Xi_3 &= \begin{bmatrix} \nu_{11}^2 & * & * & * & * \\ \nu_{21}^2 & \nu_{22}^2 & * & * & * \\ \nu_{31}^2 & \nu_{32}^2 & \nu_{33}^2 & * & * \\ \nu_{41}^2 & \nu_{42}^2 & \nu_{43}^2 & -l_0 I & * \\ 0 & 0 & 0 & 0 & -N\gamma^2 I \end{bmatrix}, \\
Q_1 &= \begin{bmatrix} F_A^P & \hat{F}_B^P \hat{M} \bar{\alpha}_I \mathcal{A}_I \mu_I & \hat{F}_B^P & \bar{F}_B^P \end{bmatrix}, \\
Q_{2i} &= \begin{bmatrix} \tau_i F_C^P & \tau_i \hat{F}_B^P \hat{M} \hat{E}_i \mathcal{A}_I \mu_I & 0 & 0 \end{bmatrix}, \quad i = 1, 2, \cdots, N, \\
J_3 &= \begin{bmatrix} F_D & 0 & 0 & 0 \end{bmatrix}, \\
F_A^P &= \begin{bmatrix} \bar{P}\bar{A} - Y\pi_1 & \bar{P}\bar{A} - X - Y\pi_1 + Y\pi_2 \\ Y\pi_1 & X + Y\pi_1 - Y\pi_2 \end{bmatrix}, \\
\hat{F}_B^P &= \begin{bmatrix} -Y \\ Y \end{bmatrix}, \\
\bar{F}_B^P &= \begin{bmatrix} \bar{P}\bar{B} \\ 0 \end{bmatrix}, \\
\mathcal{P} &= \begin{bmatrix} -\bar{P} & 0 \\ 0 & -\bar{P} \end{bmatrix}, \\
F_C^P &= \begin{bmatrix} -Y\hat{M}\hat{E}_i \mathcal{A}_I \hat{C} & -Y\hat{M}\hat{E}_i \mathcal{A}_I \hat{C} \\ Y\hat{M}\hat{E}_i \mathcal{A}_I \hat{C} & Y\hat{M}\hat{E}_i \mathcal{A}_I \hat{C} \end{bmatrix}, \quad (i = 1, 2, \cdots, N) \\
\nu_{11}^2 &= \nu_{22}^2 = -\bar{P} - \hat{C}^T \kappa_I \delta_I \hat{G} \hat{C}, \\
\nu_{21}^2 &= -\frac{1}{2}\hat{C}^T \kappa_I \delta_I \hat{G} \hat{C} - \frac{1}{2}\hat{C}^T \hat{G}^T \kappa_I \delta_I \hat{C}, \\
\nu_{31}^2 &= \nu_{32}^2 = -\mu_I^T \kappa_I \delta_I \hat{G} \hat{C}, \\
\nu_{33}^2 &= \kappa_I \hat{G} - \mu_I^T \kappa_I \delta_I \hat{G} \mu_I, \\
\nu_{41}^2 &= \frac{l_0}{2}\hat{R}_2 \bar{\alpha}_I \mathcal{A}_I \hat{C}, \\
\nu_{42}^2 &= \frac{l_0}{2}\hat{R}_2 (\bar{\alpha}_I - I) \mathcal{A}_I \hat{C}, \\
\nu_{43}^2 &= \frac{l_0}{2}\hat{R}_2 \bar{\alpha}_I \mathcal{A}_I \mu_I.
\end{aligned} \tag{31}$$

Other symbols have been defined in Theorem 1.

Proof: In order to linearize the inequality (21), define $P = \begin{bmatrix} \bar{P} & 0 \\ 0 & \bar{P} \end{bmatrix}$. Then, let $X = \bar{P}\hat{A}$ and $Y = \bar{P}\hat{B}$, we can obtain that (30) holds from the condition (21) shown in Theorem 1. By solving the inequality (30), the augmented distributed filter gains $\hat{A}$, $\hat{B}$, $\hat{D}$ and the augmented dynamic ET matric $\hat{G}$ can be derived. This completes the proof.

If the saturation effects is removed, (9) will become the following conventional filter:

$$\begin{cases} \hat{x}_i(k+1) = \tilde{A}_i\hat{x}_i(k) + \tilde{B}_i(\sum_{j\in\mathcal{N}_i} a_{ij}(\alpha_i(k)y_j(T_i^t) \\ \quad -C_j\hat{x}_j(k)) \\ \hat{z}_i(k) = \tilde{D}_i\hat{x}_i(k) \end{cases} \tag{32}$$

From (1) and (32), we can get

$$\begin{cases} \rho(k+1) = \bar{F}_A\rho(k) + \hat{F}_B\bar{\alpha}_I\mathcal{A}_I\mu_I\hat{e}(k) \\ \qquad + \bar{F}_B\omega(k) \\ \qquad + \sum_{i=1}^{N}(\alpha_i(k) - \bar{\alpha}_i)[\bar{F}_C\rho(k) + \hat{F}_B\hat{E}_i\mathcal{A}_I\mu_I\hat{e}(k)] \\ \tilde{z}(k) = F_D\rho(k) \end{cases} \tag{33}$$

where $\bar{F}_A = \begin{bmatrix} \bar{A} - \hat{B}\bar{\alpha}_I\mathcal{A}_I\hat{C} & \bar{A} - \hat{A} - \hat{B}\bar{\pi}_1 + \hat{B}\pi_2 \\ \hat{B}\pi_1 & \hat{A} + \hat{B}\pi_1 - \hat{B}\pi_2 \end{bmatrix}$, $\bar{\pi}_1 = \bar{\alpha}_I\mathcal{A}_I\hat{C}$, $\pi_2 = \mathcal{A}_I\hat{C}$, $F_C = \begin{bmatrix} -\hat{B}\hat{E}_i\mathcal{A}_I\hat{C} & -\hat{B}\hat{E}_i\mathcal{A}_I\hat{C} \\ \hat{B}\hat{E}_i\mathcal{A}_I\hat{C} & \hat{B}\hat{E}_i\mathcal{A}_I\hat{C} \end{bmatrix}$.

Next, the conventional filter design method in the form (32) will be given in the following corollary by using the same derivation method of Theorem 2.

Corollary 1: When the distributed filter gains are designed by

$$\tilde{A} = \bar{R}^{-1}H, \quad \tilde{B} = \bar{R}^{-1}L \quad \text{and} \quad \tilde{D} \tag{34}$$

system (33) is AS under the DETSs (4) for given constants $\bar{\alpha}_i \in (0,1)$, λ_i, $\varepsilon_i \in [0,1)$, $\mu_i \in (0,1]$ and γ, if there exists a symmetric matrix $\bar{R} > 0$ and dynamic ET matrix sequence G_i such that

$$\bar{\Pi}_2 = \begin{bmatrix} \bar{\Xi}_3 & * & * & * & * & * \\ \bar{Q}_1 & \mathcal{R} & * & * & * & * \\ \bar{Q}_{21} & 0 & \mathcal{R} & * & * & * \\ \vdots & \vdots & \vdots & \ddots & * & * \\ \bar{Q}_{2N} & 0 & 0 & 0 & \mathcal{R} & * \\ J_3 & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0, \tag{35}$$

where

$$\begin{aligned} \bar{\Xi}_3 &= \begin{bmatrix} \bar{\nu}_{11}^2 & * & * & * \\ \nu_{21}^2 & \bar{\nu}_{22}^2 & * & * \\ \nu_{31}^2 & \nu_{32}^2 & \nu_{33}^2 & * \\ 0 & 0 & 0 & -N\gamma^2 I \end{bmatrix}, \\ \bar{Q}_1 &= \begin{bmatrix} F_A^R & \hat{F}_B^R\bar{\alpha}_I\mathcal{A}_I\mu_I & \bar{F}_B^P \end{bmatrix}, \\ \bar{Q}_{2i} &= \begin{bmatrix} \tau_i F_C^R & \tau_i\hat{F}_B^P\hat{E}_i\mathcal{A}_I\mu_I & 0 \end{bmatrix}, \\ & i = 1,2,\cdots,N,\ J_3 = \begin{bmatrix} F_D & 0 & 0 \end{bmatrix}, \\ F_A^R &= \begin{bmatrix} \bar{R}\bar{A} - L\bar{\pi}_1 & \bar{R}\bar{A} - H - L\bar{\pi}_1 + L\bar{\pi}_2 \\ L\bar{\pi}_1 & H + L\bar{\pi}_1 - L\bar{\pi}_2 \end{bmatrix}, \\ \hat{F}_B^R &= \begin{bmatrix} -L \\ L \end{bmatrix}, \bar{F}_B^R = \begin{bmatrix} \bar{R}\bar{B} \\ 0 \end{bmatrix}, \mathcal{R} = \begin{bmatrix} -\bar{R} & 0 \\ 0 & -\bar{R} \end{bmatrix}, \\ F_C^R &= \begin{bmatrix} -L\hat{E}_i\mathcal{A}_I\hat{C} & -L\hat{E}_i\mathcal{A}_I\hat{C} \\ L\hat{E}_i\mathcal{A}_I\hat{C} & L\hat{E}_i\mathcal{A}_I\hat{C} \end{bmatrix}, \\ \bar{\nu}_{11}^2 &= \bar{\nu}_{22}^2 = -\bar{R} - \hat{C}^T\kappa_I\delta_I\hat{G}\hat{C}. \end{aligned} \tag{36}$$

Other symbols have been defined in Theorem 2.

Remark 8: In contrast to the available publications, in this paper, the designed DETS, the DoS attacks and the measurement outliers are firstly considered in filtering design for sensor networks simultaneously, which are the distinctive novelties of the problem addressed. Inspired by References [17], [40], and [44], a novel DETS is proposed and the difficulties of how to deal with the DoS attacks and measurement outliers are overcome. A new secure co-design approach of the distributed filter gains and the dynamic event-triggered matrix are presented to guarantee the desired system performance.

IV. Simulation Examples

In this part, the availability of the designed distributed filter will be demonstrated by a simulation example.

Consider a sensor network containing three nodes whose topology is described as a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with a set of nodes $\mathcal{V} = \{n_1, n_2, n_3\}$, a set of edges $\mathcal{E} = \{(n_1,n_1), (n_1,n_2), (n_1,n_3), (n_2,n_1), (n_2,n_2), (n_2,n_3), (n_3,n_1), (n_3,n_2), (n_3,n_3)\}$ and the adjacency matrix $\mathcal{A} = [a_{ij}]_{3\times3}$ where adjacency elements $a_{ij} = 1$ when $(n_i, n_j) \in \mathcal{E}$; otherwise, $a_{ij} = 0$.

The parameters of (1) considered here are given by

$$A = \begin{bmatrix} 0.0320 & 0.4450 & 0.2480 \\ 0.1640 & 0.2578 & 0.1550 \\ 0.1540 & 0.1470 & 0.3745 \end{bmatrix}, B = \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}, \tag{37}$$

$$D = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \tag{38}$$

with the initial value $x(0) = \begin{bmatrix} 0.6 & 0.3 & -0.5 \end{bmatrix}^T$. The exogenous disturbance input $\omega(k)$ is selected as $\omega(k) = 0.5\sin(0.2k)e^{-0.2k}$. For each i, $(i = 1,2,3)$, the parameters of sensor i is as follows:

$$C_1 = \begin{bmatrix} 0.3 & 0 & 0 \\ 0 & 0.3 & 0 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 0.3 & 0 & 0 \\ 0 & 0 & 0.3 \end{bmatrix}, \quad C_3 = \begin{bmatrix} 0 & 0 & 0.3 \\ 0 & 0.3 & 0 \end{bmatrix}.$$

Choose $\lambda_1 = 2$, $\lambda_2 = 3$, $\lambda_3 = 4$, $\delta_1 = 0.014$, $\delta_2 = 0.01$, $\delta_3 = 0.008$, $\varepsilon_1 = 0.5$, $\varepsilon_2 = 0.4$, $\varepsilon_3 = 0.3$. Set the initial value $\theta_1(0) = \theta_2(0) = \theta_3(0) = 50$. The DoS attack probabilites are taken as $\bar{\alpha}_1 = 0.87$, $\bar{\alpha}_2 = 0.65$, $\bar{\alpha}_3 = 0.63$. Furthermore, set the initial conditions of three filters as $\hat{x}_1(0) = \begin{bmatrix} 0.7 & 0.9 & -0.5 \end{bmatrix}^T$, $\hat{x}_2(0) = \begin{bmatrix} 0 & 0.9 & -0.7 \end{bmatrix}^T$, $\hat{x}_3(0) = \begin{bmatrix} -0.7 & 0.1 & 0.9 \end{bmatrix}^T$.

The saturation function $\chi(s)$ is described as follows:

$$\chi(o) = \begin{cases} o, & if -o_{max} \le o \le o_{max} \\ o_{max}, & if\, o \ge o_{max} \\ -o_{max}, & if\, o \le -o_{max} \end{cases}. \tag{39}$$

By solving the LMI (30), one can obtain filter matrices and trigger matrices as

$$\hat{A}_1 = \begin{bmatrix} 0.0212 & 0.2885 & 0.1625 \\ 0.1204 & 0.1759 & 0.1409 \\ 0.1167 & 0.1308 & 0.2580 \end{bmatrix}, \hat{D}_1 = \begin{bmatrix} 1.0163 \\ 0.0622 \\ 0.0455 \end{bmatrix}^T,$$

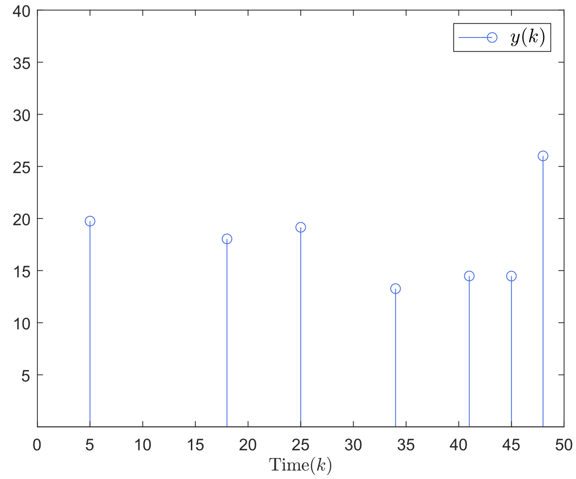

Fig. 2. Abnormal disturbance signal.

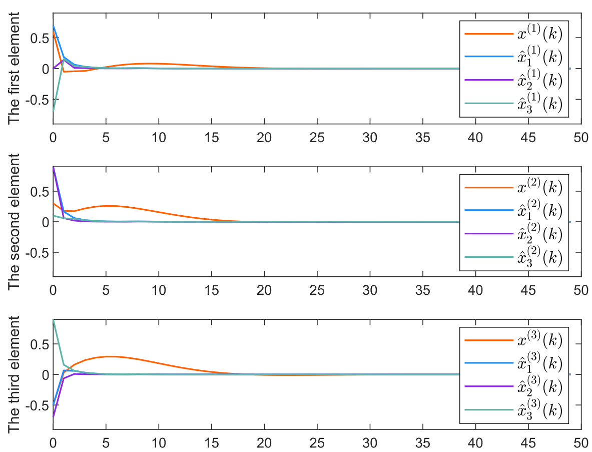

Fig. 3. Trajectory of the system state $x(k)$ and the its estimations $\hat{x}_1(k)$, $\hat{x}_2(k)$ and $\hat{x}_3(k)$.

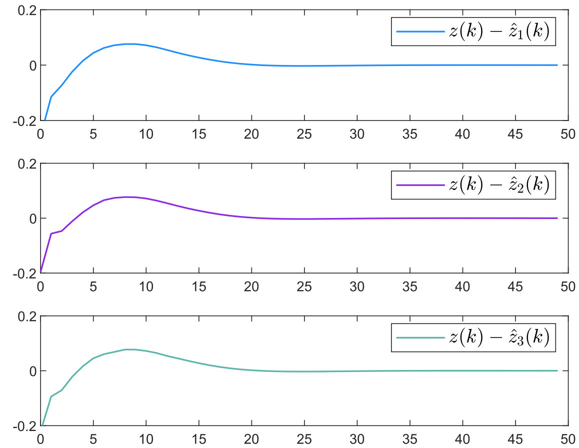

Fig. 4. Errors between $z(k)$ and $\hat{z}_i(k)$ with filter (9) under measurement outliers.

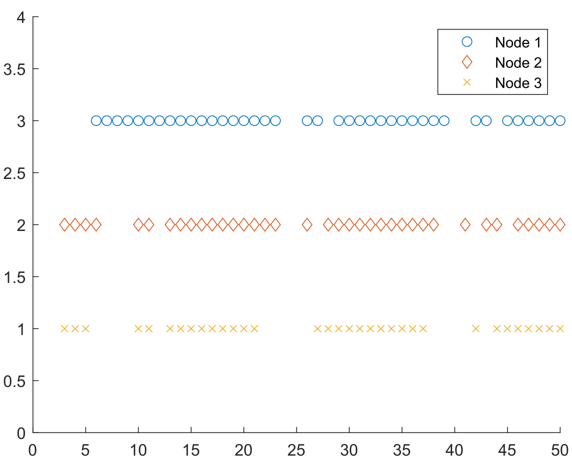

Fig. 5. Releasing instants with the proposed DETS.

$$\hat{A}_2 = \begin{bmatrix} 0.0214 & 0.2882 & 0.1628 \\ 0.1206 & 0.1754 & 0.1414 \\ 0.1170 & 0.1303 & 0.2588 \end{bmatrix}, \hat{D}_2 = \begin{bmatrix} 1.0158 \\ 0.0625 \\ 0.0461 \end{bmatrix}^T,$$

$$\hat{A}_3 = \begin{bmatrix} 0.0211 & 0.2886 & 0.1629 \\ 0.1199 & 0.1759 & 0.1414 \\ 0.1162 & 0.1308 & 0.2586 \end{bmatrix}, \hat{D}_3 = \begin{bmatrix} 1.0147 \\ 0.0620 \\ 0.0453 \end{bmatrix}^T,$$

$$\hat{B}_1 = \begin{bmatrix} -0.0022 & 0.0001 \\ 0.0025 & 0.0028 \\ 0.0022 & 0.0029 \end{bmatrix}, \hat{G}_1 = \begin{bmatrix} 22.8137 & -0.0069 \\ -0.0069 & 22.7634 \end{bmatrix},$$

$$\hat{B}_2 = \begin{bmatrix} 0.0003 & 0.0074 \\ 0.0057 & 0.0068 \\ 0.0059 & 0.0109 \end{bmatrix}, \hat{G}_2 = \begin{bmatrix} 29.3137 & 0.0255 \\ 0.0255 & 29.2740 \end{bmatrix},$$

$$\hat{B}_3 = \begin{bmatrix} 0.0073 & 0.0110 \\ 0.0064 & 0.0075 \\ 0.0106 & 0.0068 \end{bmatrix}, \hat{G}_3 = \begin{bmatrix} 27.7701 & 0.0062 \\ 0.0062 & 27.7564 \end{bmatrix}.$$

Similarly, for the conventional filter, the filter gain parameters can computed by solving LMI (35), which are omitted due to space limitation.

Based on the designed gains of the proposed outlier-resistant filter, under the measurement outliers shown in Fig. 2, the trajectories of system state $x(k)$ and filtering states $\hat{x}_1(k)$, $\hat{x}_2(k)$, $\hat{x}_3(k)$ are illustrated in Fig. 3. Fig. 4 plots the errors between estimated system output $z(k)$ and each estimated filter output $\hat{z}_i(k)(i = 1, 2, 3)$. The triggered times are shown in Fig. 5, which depicts that, by letting the simulation run for 50 times, 39 (37/33) signals are triggered into the network from sensor 1 (sensor 2/sensor 3) under the proposed DETS. It is clearly that proposed DETSs can effectively reduce transmitting frenquency and conserve valuable bandwidth resources. Fig. 6 shows the evolution of filter inputs $\hat{y}_1(k)$, $\hat{y}_2(k)$ and $\hat{y}_3(k)$ and the occurrence of DoS attacks. If DoS attacks occur, the measurement outputs will tend to be zero. For example, when $k = 5$, the measurement output obtained by sensor 3 is zero.

Next, compared with the performance of the conventional filter, the effectiveness of outlier suppression with the proposed outlier-resistant filter will be demonstrated. When measurement outlier depicted in Fig. 2 is in present, the estimation performances of the conventional filter and the proposed outlier-resistant filter are shown in Fig. 7 and Fig. 4, from which we can see the effect of the measurement outliers is well mitigated with the outlier-resistant filter, in contrast, the estimation performance of the conventional filter deviates severely. Thus, it can be drawn from the above comparisons that the proposed outlier-resistant filter outperforms the conventional filter in the case of measurement outlier occurrence.

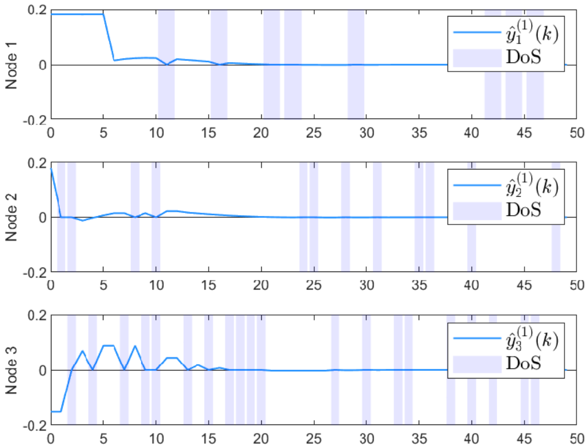

Fig. 6. The first element of filter inputs $\hat{y}_1(k)$, $\hat{y}_2(k)$ and $\hat{y}_3(k)$ under DoS attacks.

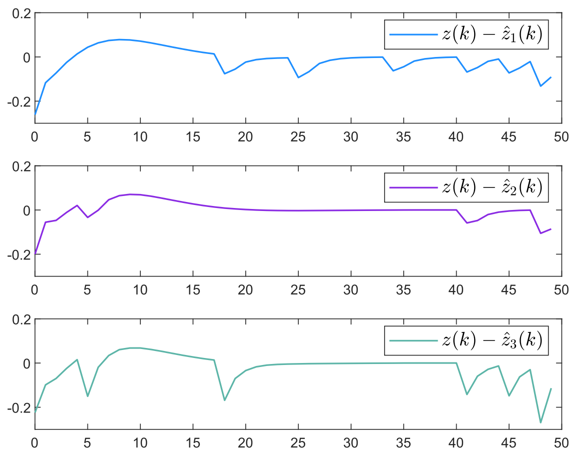

Fig. 7. Errors between $z(k)$ and $\hat{z}_i(k)$ with filter (32) under measurement outliers.

From the simulation results, it is easy to conclude that the proposed distributed dynamic ET filter can perform very well under the influence of measurement outliers and DoS attacks.

V. Conclusion

In this paper, the problem of outlier-resistant H_∞ distributed filter design under dynamic ET over sensor networks against DoS attacks has been addressed. To relieve the pressure of bandwidth, a novel distributed DETS is proposed, which can prevent mutation data from being released into the network. A set of stochastic variables obeying the Bernoulli distribution has been applied to model whether or not the DoS attacks being launched. In the presence of measurement outliers which might cause innovation changes in anomalous magnitude and degenerate or even damage the filter, a saturation function is utilized in the distributed filter model to restrict the signals tainted by the measurement outliers. An augmented filtering error model has been established on account of distributed DETS, DoS attacks and outlier measurements. By using a Lyapunov approach, criteria on the existence of desired distributed filter have been derived ensuring that the augmented filtering error system is AS with a guaranteed H_∞ performance index γ. By calculating a linear inequality matrix given in Theorem 2, the parameters of desired filters and proposed distributed DETS are obtained. Future research directions will include the problem of finite-horizon outlier-resistant distributed filtering over sensor networks under memory-based event-triggered schemes.

References

[1] Y. Qian and D. D. Vecchio, “Robustness of networked systems to unintended interactions with application to engineered genetic circuits,” *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 4, pp. 1705–1716, Dec. 2021.

[2] M. Cai, Y. Wang, S. Wang, R. Wang, L. Cheng, and M. Tan, “Prediction-based seabed terrain following control for an underwater vehicle-manipulator system,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 8, pp. 4751–4760, Aug. 2021.

[3] M. Li, Y. Chen, and C.-C. Lim, “Stability analysis of complex network control system with dynamical topology and delays,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 11, pp. 7228–7237, Nov. 2021.

[4] C. Li, X. Zhao, M. Chen, W. Xing, N. Zhao, and G. Zong, “Dynamic periodic event-triggered control for networked control systems under packet dropouts,” *IEEE Trans. Autom. Sci. Eng.*, vol. 21, no. 1, pp. 906–920, Jan. 2024.

[5] E. Tian, Z. Wang, L. Zou, and D. Yue, “Chance-constrained H_∞ control for a class of time-varying systems with stochastic nonlinearities: The finite-horizon case,” *Automatica*, vol. 107, pp. 296–305, Jul. 2019.

[6] M. Bahreini, J. Zarei, R. Razavi-Far, and M. Saif, “Robust and reliable output feedback control for uncertain networked control systems against actuator faults,” *IEEE Trans. Syst. Man, Cybern., Syst.*, vol. 52, no. 4, pp. 2555–2564, Apr. 2022.

[7] J. Hu, Z. Wang, G.-P. Liu, H. Zhang, and R. Navaratne, “A prediction-based approach to distributed filtering with missing measurements and communication delays through sensor networks,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 11, pp. 7063–7074, Nov. 2021.

[8] 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.

[9] J. Feng and H. Zhao, “Dynamic nodes collaboration for target tracking in wireless sensor networks,” *IEEE Sensors J.*, vol. 21, no. 18, pp. 21069–21079, Sep. 2021.

[10] Y. Yao, Y. Li, D. Xie, S. Hu, C. Wang, and Y. Li, “Coverage enhancement strategy for WSNs based on virtual force-directed ant lion optimization algorithm,” *IEEE Sensors J.*, vol. 21, no. 17, pp. 19611–19622, Sep. 2021.

[11] J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, “Distributed collaborative control for industrial automation with wireless sensor and actuator networks,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 12, pp. 4219–4230, Dec. 2010.

[12] D. Ding, Z. Wang, and Q. Han, “A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks,” *IEEE Trans. Autom. Control*, vol. 65, no. 4, pp. 1792–1799, Apr. 2020.

[13] E. Tian, X. Wang, and C. Peng, “Probabilistic-constrained distributed filtering for a class of nonlinear stochastic systems subject to periodic DoS attacks,” *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 5369–5379, Dec. 2020.

[14] L. Ma, Z. Wang, H. Liu, F. E. Alsaadi, and F. E. Alsaadi, “Neural-network-based filtering for a general class of nonlinear systems under dynamically bounded innovations over sensor networks,” *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1395–1408, May 2022.

[15] A. Mustafa, M. Mazouchi, and H. Modares, “Secure event-triggered distributed Kalman filters for state estimation over wireless sensor networks,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 2, pp. 1268–1283, Feb. 2023.

[16] S. Liu, Z. Wang, L. Wang, and G. Wei, “Finite-horizon H_∞ filtering via a high-rate network with the FlexRay protocol,” *IEEE Trans. Autom. Control*, vol. 68, no. 6, pp. 3596–3603, Jun. 2023, doi: 10.1109/TAC.2022.3190791.

[17] 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.

[18] L. Wang and J. Dong, “Event-based distributed adaptive fuzzy consensus for nonlinear fractional-order multiagent systems,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 9, pp. 5901–5912, Sep. 2022.

[19] Y. Wu, M. Chen, H. Li, and M. Chadli, "Event-triggered-based adaptive NN cooperative control of six-rotor UAVs with finite-time prescribed performance," *IEEE Trans. Autom. Sci. Eng.*, doi: 10.1109/TASE.2023.3241182.

[20] J. Liu, E. Gong, L. Zha, E. Tian, and X. Xie, "Observer-based security fuzzy control for nonlinear networked systems under weighted try-once-discard protocol," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 11, pp. 3853–3865, Jun. 2023.

[21] K. Wang, E. Tian, J. Liu, L. Wei, and D. Yue, "Resilient control of networked control systems under deception attacks: A memory-event-triggered communication scheme," *Int. J. Robust Nonlinear Control*, vol. 30, no. 4, pp. 1534–1548, Mar. 2020.

[22] L. Wang, Z. Wang, D. Zhao, and G. Wei, "Event-based state estimation under constrained bit rate: An encoding–decoding approach," *Automatica*, vol. 143, Sep. 2022, Art. no. 110421.

[23] L. Dai, M. Cannon, F. Yang, and S. Yan, "Fast self-triggered MPC for constrained linear systems with additive disturbances," *IEEE Trans. Autom. Control*, vol. 66, no. 8, pp. 3624–3637, Aug. 2021.

[24] P. Zhang, Y. Yuan, and L. Guo, "Fault-tolerant optimal control for discrete-time nonlinear system subjected to input saturation: A dynamic event-triggered approach," *IEEE Trans. Cybern.*, vol. 51, no. 6, pp. 2956–2968, Jun. 2021.

[25] Z. Cao, Y. Niu, H.-K. Lam, and J. Zhao, "Sliding mode control of Markovian jump fuzzy systems: A dynamic event-triggered method," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 10, pp. 2902–2915, Oct. 2021.

[26] R. Cao and L. Cheng, "Distributed dynamic event-triggered control for Euler–Lagrange multiagent systems with parametric uncertainties," *IEEE Trans. Cybern.*, vol. 53, no. 2, pp. 1272–1284, Feb. 2023.

[27] X.-M. Zhang, Q.-L. Han, and B.-L. Zhang, "An overview and deep investigation on sampled-data-based event-triggered control and filtering for networked systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 4–16, Feb. 2017.

[28] Z. Gu, D. Yue, and E. Tian, "On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems," *Inf. Sci.*, vol. 422, pp. 257–270, Jan. 2018.

[29] W. Hu, C. Yang, T. Huang, and W. Gui, "A distributed dynamic event-triggered control approach to consensus of linear multiagent systems with directed networks," *IEEE Trans. Cybern.*, vol. 50, no. 2, pp. 869–874, Feb. 2020.

[30] L. Wang, E. Tian, C. Wang, and S. Liu, "Secure estimation against malicious attacks for lithium-ion batteries under cloud environments," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 10, pp. 4237–4247, Oct. 2022, doi: 10.1109/TCSI.2022.3187725.

[31] X. Huang and J. Dong, "Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 89–99, Jan. 2020.

[32] S. Gao, H. Zhang, C. Huang, Z. Wang, and H. Yan, "Optimal injection attack strategy for nonlinear cyber-physical systems based on iterative learning," *IEEE Trans. Autom. Sci. Eng.*, vol. 21, no. 1, pp. 56–68, Mar. 2004.

[33] X. Wang, E. Tian, B. Wei, and J. Liu, "Novel attack-defense framework for nonlinear complex networks: An important-data-based method," *Int. J. Robust Nonlinear Control*, vol. 33, no. 4, pp. 2861–2878, Mar. 2023.

[34] E. Tian, H. Chen, C. Wang, and L. Wang, "Security-ensured state of charge estimation of lithium-ion batteries subject to malicious attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2250–2261, May 2023.

[35] H. Song, D. Ding, H. Dong, and Q.-L. Han, "Distributed maximum correntropy filtering for stochastic nonlinear systems under deception attacks," *IEEE Trans. Cybern.*, vol. 52, no. 5, pp. 3733–3744, May 2022.

[36] X. Zheng, H. Zhang, L. Wang, and H. Yan, "Dynamic event-based distributed piecewise filtering over sensor networks under periodic DoS attacks," *IEEE Trans. Control Netw. Syst.*, vol. 10, no. 2, pp. 1–15, Oct. 2023.

[37] 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.

[38] 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, May 2023.

[39] 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.

[40] C. Peng, J. Wu, and E. Tian, "Stochastic event-triggered H_∞ control for networked systems under denial of service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 7, pp. 4200–4210, Jul. 2022.

[41] S. Hu, D. Yue, X. Chen, Z. Cheng, and X. Xie, "Resilient H_∞ filtering for event-triggered networked systems under nonperiodic DoS jamming attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 3, pp. 1392–1403, Mar. 2021.

[42] B. Qu, Z. Wang, B. Shen, and H. Dong, "Outlier-resistant recursive state estimation for renewable-electricity-generation-based microgrids," *IEEE Trans. Ind. Informat.*, vol. 19, no. 5, pp. 7133–7144, May 2023.

[43] H. Chen, E. Tian, L. Wang, and S. Liu, "A joint online strategy of measurement outliers diagnosis and state of charge estimation for lithium-ion batteries," *IEEE Trans. Ind. Informat.*, vol. 19, no. 5, pp. 6387–6397, May 2023.

[44] J. Li, Z. Wang, H. Dong, and G. Ghinea, "Outlier-resistant remote state estimation for recurrent neural networks with mixed time-delays," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 5, pp. 2266–2273, May 2021.

[45] Y. Shen, Z. Wang, B. Shen, and H. Dong, "Outlier-resistant recursive filtering for multisensor multirate networked systems under weighted try-once-discard protocol," *IEEE Trans. Cybern.*, vol. 51, no. 10, pp. 4897–4908, Oct. 2021.

[46] D. Zhao, Z. Wang, Q.-L. Han, and G. Wei, "Proportional–integral observer design for uncertain time-delay systems subject to deception attacks: An outlier-resistant approach," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 8, pp. 5152–5164, Aug. 2022.

[47] X. Ge, Q.-L. Han, and Z. Wang, "A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks," *IEEE Trans. Cybern.*, vol. 49, no. 1, pp. 171–183, Jan. 2019.

[48] D. Ding, H. Liu, H. Dong, and H. Liu, "Resilient filtering of nonlinear complex dynamical networks under randomly occurring faults and hybrid cyber-attacks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2341–2352, Jul. 2022.

[49] W. Chen, D. Ding, H. Dong, and G. Wei, "Distributed resilient filtering for power systems subject to denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1688–1697, Aug. 2019.

[50] Z. Wu, L. Zhang, and M. Yue, "Low-rate DoS attacks detection based on network multifractal," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 5, pp. 559–567, Sep. 2016.

Lijuan Zha received the Ph.D. degree from Donghua University, Shanghai, China, in 2018.

She is currently an Associate Professor with the School of Science, Nanjing Forestry University, Nanjing, China, and also with the Nanjing University of Finance and Economics, Nanjing. From 2018 to 2023, she was a Post-Doctoral Research Associate with the School of Mathematics, Southeast University, Nanjing. Her current research interests include networked control systems, neural networks, and complex dynamical systems.

Rongfei Liao received the B.S. degree in applied mathematics from the Nanjing University of Finance and Economics, Nanjing, China, in 2019, where she is currently pursuing the M.Sc. degree with the College of Information Engineering. Her research interests include T-S fuzzy systems and networked secure control.

Jinliang Liu (Member, IEEE) received the Ph.D. degree in automatic control from the School of Information Science and Technology, Donghua University, Shanghai, China, in 2011.

He was a Post-Doctoral Research Associate with the School of Automation, Southeast University, Nanjing, China, from December 2013 to June 2016. From June 2011 to May 2023, he was an Associate Professor and then a Professor with the Nanjing University of Finance and Economics, Nanjing. In June 2023, he joined the Nanjing University of Information Science and Technology, Nanjing, where he is currently a Professor with the School of Computer Science. His research interests include networked control systems, complex dynamical networks, and time-delay systems.

Xiangpeng Xie (Senior Member, IEEE) received the B.S. and Ph.D. degrees in engineering from Northeastern University, Shenyang, China, in 2004 and 2010, respectively.

From 2010 to 2014, he was a Senior Engineer with Metallurgical Corporation of China Ltd., Beijing, China. He is currently a Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms.

Prof. Xie serves as an Associate Editor for *International Journal of Fuzzy Systems* and *International Journal of Control, Automation, and Systems*.

Engang Tian received the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008.

From 2011 to 2012, he was a Post-Doctoral Research Fellow with The Hong Kong Polytechnic University, Hong Kong. From 2015 to 2016, he was a Visiting Scholar with the Department of Information Systems and Computing, Brunel University London, Uxbridge, U.K. From 2008 to 2018, he was an Associate Professor and then a Professor with the School of Electrical and Automation Engineering, Nanjing Normal University. In 2018, he was appointed as an Eastern Scholar by the Municipal Commission of Education, Shanghai, and joined the University of Shanghai for Science and Technology, Shanghai, where he is currently a Professor with the School of Optical-Electrical and Computer Engineering. His research interests include networked control systems, cyber-attacks, and nonlinear stochastic control and filtering.

Jinde Cao (Fellow, IEEE) received the B.S. degree in mathematics/applied mathematics from Anhui Normal University, Wuhu, China, in 1986, the M.S. degree in mathematics/applied mathematics from Yunnan University, Kunming, China, in 1989, and the Ph.D. degree in mathematics/applied mathematics from Sichuan University, Chengdu, China, in 1998.

He was a Post-Doctoral Research Fellow at the Department of Automation and Computer-Aided Engineering, Chinese University of Hong Kong, Hong Kong, from 2001 to 2002. He is currently an Endowed Chair Professor, the Dean of the Science Department, and the Director of the Research Center for Complex Systems and Network Sciences with Southeast University (SEU), Nanjing, China. He is also the Director of the National Center for Applied Mathematics, SEU-Jiangsu, and the Jiangsu Provincial Key Laboratory of Networked Collective Intelligence of China.

Dr. Cao is a member of Russian Academy of Sciences, the Academy of Europe, the Russian Academy of Engineering, the European Academy of Sciences and Arts, and the Lithuanian Academy of Sciences, a Fellow of the African Academy of Sciences and Pakistan Academy of Sciences. He was the recipient of the National Innovation Award of China, Obada Prize and the Highly Cited Researcher Award in Engineering, Computer Science, and Mathematics by Clarivate Analytics.