FlexRay Protocol-Based Event-Triggered Secure Filtering for IT-2 Fuzzy Systems With Fading Measurements Over High-Rate Communication Networks: The Finite-Horizon Case

Jian Liu, *Member, IEEE*, Shuailong Wang, Jinliang Liu, *Member, IEEE*, Xiangpeng Xie, *Senior Member, IEEE*, and Engang Tian, *Senior Member, IEEE*

***Abstract*—This article investigates the FlexRay (FR) protocol-based dynamic event-triggered (DET) secure filtering problem with the high-rate communication (HRC) network for the interval type-2 (IT-2) fuzzy networked system. For fear of data collisions and preempting limited communication resources, a novel DET-FR (DETFR) protocol is adopted to schedule sensor nodes. Different sensors are employed for distinct protocols and data-holding strategies to reinforce the efficiency of network transmission. Moreover, considering the random occurrence of cyber attacks and fading measurements in the HRC channel, the attack parameters are represented by the Bernoulli process, and measurement attenuation coefficients are expressed by the random variables of equidistribution on a fixed interval. Based on this, to ensure that the error dynamics meet the disturbance attenuation level, several sufficient conditions are given. Subsequently, the DETFR protocol-based secure filtering algorithm is developed to acquire the fuzzy filter parameters. Eventually, the validity of our designed secure filtering algorithm is proved through two examples.**

***Index Terms*—Cyber attacks, dynamic event-triggered (DET) scheme, fading measurements, flexray (FR) protocol, high-rate communication (HRC) network.**

I. Introduction

IN RECENT years, owing to the positive aspects of immediacy, long distance and low cost, networked control systems (NCSs) have received extensive attention and have been studied in many fields, including vehicles [1], power systems [2], mobile robot [3]. Although nonlinear physical systems are in the majority, notably, the Takagi-Sugeno (T–S) fuzzy technology is significant for handling the nonlinear plant [4], [5], [6]. By introducing interval type-1 fuzzy technology, sampled-data synchronization in complex networks has been discussed in [7]. Besides, Zeng et al. [8] employed an interval type-2 (IT-2) fuzzy approach to expand the freedom of controller selection. There is no doubt that the signals are prone to inevitable and unmeasurable noise during network transmission, and therefore a filtering (or state estimation) problem arises for the sake of recovering the true signals. Up to now, filtering technology has been applied for directing against noise with different characteristics, such as Kalman filtering [9], H_∞ filtering [10] as well as set membership filtering [11]. Relevantly, Han et al. [12] discussed the scalable H_∞ filtering problem with censored measurements. Whereafter, in [13], a resilient H_∞ approach to resist gain variations and stochastic disturbances is proposed. Besides, to weaken the adverse effects, Song et al. [14] addressed the state estimation problem of random disturbance in complex networks. Presently, most research focuses on infinite time, while there are no adequate studies on the finite horizon for the IT-2 fuzzy system.

In practice, it is general to configure the communication channel with a higher bandwidth on the sensor with a lower sampling period, which results in multiple data transmissions. The case in point is that the maximum transmission rate of PROFIBUS-DP can reach 12 Mb/s, but the 12-bit DT138 acceleration sensor has a sampling frequency of 1.2 kb/s. Additionally, Zou et al. [15] discussed a shared network with high-rate transmission considering the H_∞ filtering problem. The $L_2 - L_\infty$ filtering issue for the artificial neural networks with high-rate communication (HRC) channels has been discussed in [16]. Nevertheless, in virtue of the complication in dynamic modeling and analysis, the attention paid to significant HRC networks is limited, which has partially stimulated our research interest.

Congestive communication channels and limited resources are known substantive constraints for NCSs. Meanwhile,

Manuscript received 13 December 2023; revised 14 March 2024; accepted 16 June 2024. Date of publication 9 July 2024; date of current version 18 September 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62001210, Grant 62373252, and Grant 61973152; and in part by the Startup Foundation for Introducing Talent of NUIST under Grant 2024r063. This article was recommended by Associate Editor M. Basin. *(Corresponding author: Jinliang Liu.)*

Jian Liu and Shuailong Wang are with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: by.liujian@gmail.com; wangshuailong21@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).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSMC.2024.3416900.

Digital Object Identifier 10.1109/TSMC.2024.3416900

the transmission process may cause data redundancy, which further leads to data anomalies or waste of resources. Accordingly, a series of inevitable network-induced phenomena that grievously wreck system stability occur. As such, to reduce the adverse effects, various triggered strategies [e.g., static event-triggered (SET)] are generally used by reason of their prominent advantages of reducing redundant data transmission and effectively cutting down on the network burden [17], [18], [19]. Subsequently, the so-called dynamic event-triggered (DET) strategy with the dynamically adjustable interval variable is proposed in [20]. Afterwards, the related research on the DET mechanism received considerable attention. For example, Chen et al. [21] investigated the formation-containment control problem under DET, which improves resource utilization by adding auxiliary variables for each agent system. Moreover, Chen et al. [22] designed a novel distributed DET fault-tolerant controller based on the DET mechanism with nonlinear triggering conditions to save bandwidth resources. Nevertheless, the event-triggered mechanism has only received initial attention when it comes to NCSs with the HRC network.

On another scientific frontier, currently, communication protocols that can schedule nodes are also considered to be a positive and effective solution, which can reduce the burden of communication networks. Generally speaking, from the perspective of scheduling sequence, protocols can be roughly divided into static protocols (e.g., round-robin (RR) protocol [23]) and dynamic protocols (e.g., try-once-discard (TOD) protocol [24], [25], [26]). In addition, as a hybrid protocol, FlexRay (FR) protocol with prominent flexibility, strong adaptability, fault tolerance and high reliability has received extensive attention [27], [28]. In the avionics industry, FR protocol has critical applications by virtue of these characteristics. To improve the flexibility of transmission and keep pace with the development of network architectures, a discrete FR protocol was first discussed in [29]. Thus, a novel online optimization algorithm has been introduced with set-membership state estimation under FR protocol in [30]. So far, the most relevant existing works focus on only event-triggered strategies or scheduling protocols. Based on these discussions, exploring the DET-FR (DETFR) protocol under the HRC network in further saving network bandwidth resources partially motivates the current investigation.

Besides, spiteful cyber attacks are also substantive challenges and threats faced by NCSs. Despite the attractive advantages of communication networks, nevertheless, signals may be subjected to random vicious attacks, thereby resulting in varying degrees of deterioration on system performance. From the perspective of different attack modes, several typical attacks include denial-of-service (DoS) attacks [31], [32], deception attacks [33] as well as replay attacks [34]. Thus, the security issues of systems have been the focus of research. To name a few, Liu et al. [35] proposed the matrix extending diagonally to explore the inconsistent matrix dimensions of controllers caused by communication channel attacks, and Gao et al. [36] proposed an asynchronous observer to observe unmeasured state and a novel model of deception attacks, which have different kinds of attack signals on each channel. Therefore, the investigation of secure filtering schemes for NCSs against malignant cyber attacks is considerably imperative.

From the reality of engineering, there are many factors (e.g., machine faults, propagation delay and complicated network circumstances) that cause the fading measurement behavior of signals during transmission. In related literature [37], [38], the fading measurements caused by different factors have been discussed for NCSs. Furthermore, Zhu et al. [39] proposed a novel estimation algorithm with the fusion stage of signal and structural data for fading measurements, where the fading variable satisfies the Rayleigh distribution over the fixed interval. To reflect fading behavior, Zhao et al. [40] introduced a Rice fading model, which is represented by multiple variables. Developing a novel method that integrates the advantages of the DET mechanism into the HRC network with communication protocols and applying them to cope with the secure H_∞ filtering problem of time-varying systems are of great significance, which partially promoted our current research.

Inspired by the aforementioned discussion, this article endeavors to tackle the secure filtering problem of the IT-2 fuzzy system via the HRC channel under the DETFR protocol. The central contributions are listed as follows.

1) To further effectively utilize the network in comparison with [41], a novel DETFR mechanism is put forward as the first attempt, which absorbs the merits of the DET mechanism, RR and TOD protocol. Meanwhile, taking the HRC channel and fading measurements into account, a discrete IT-2 fuzzy system model is established.
2) Considering the data retention strategies used by different nodes and random deception attacks, this article converts the high-rate to single-rate by virtue of the vector augmentation method to obtain the desired filter. Different from [42] and [43], this article focuses on sensor scheduling in the HRC network led by random deception attacks. An effective DETFR protocol-based filtering algorithm over the finite horizon has been proved.
3) To reflect the impact of DETFR protocol on the error dynamics and scheduling, a new Lyapunov functional is constructed. In light of all the factors mentioned above, the parameters of the filtering are readily presented through the filtering algorithm, and several sufficient criteria are derived for fuzzy error dynamics that ensure the disturbance attenuation level.

Notations: The notations used in this article are quite standard. $\mathrm{col}_{1\to n}(y_i(k))$ stands for the column vector $\{y_1^T(k), y_2^T(k), \ldots, y_n^T(k)\}^T$. $\bmod (k, l)$ represents the nonnegative remainder on division of k by l.

II. Problem Formulation

A. FR Protocol

The FR protocol consists of a fixed communication cycle that is repeated from beginning to end. Each cycle has an identical allocatable time interval and embodies four parts: a static segment (SS) composed of fixed and unchangeable

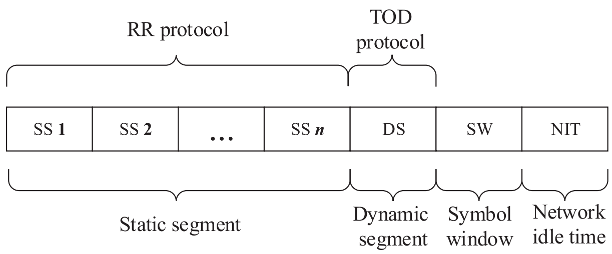


Fig. 1. Framework diagram of FR protocol.

equal-length time slots, a dynamic segment (DS) containing one or more smaller time slots, a symbol window (SW) for transmitting character and the network idle time (NIT) with clock synchronization function. The intervals of SS and DS are much longer than those of the SW and NIT. As a consequence, the time slots of the SW and NIT will be disregarded without loss of generality.

In this article, assuming that there are N nodes and are divided into $\varrho_1 \triangleq \{1, 2, \ldots, \vartheta\}$ and $\varrho_2 \triangleq \{\vartheta + 1, \vartheta + 2, \ldots, N\}$ two parts. Furthermore, it is presumed that the SS employs the RR protocol and the DS adopts the TOD protocol. The framework diagram of a communication cycle of the FR protocol is depicted in Fig. 1.

B. System Model

A IT-2 fuzzy system with h rules is modeled in the following form over the finite-horizon $[0, T-1]$:

RULE g: **IF** $\varpi_1(x(k))$ is u_1^g, $\varpi_2(x(k))$ is u_2^g, $\ldots$, $\varpi_\emptyset$ is $u_\emptyset^g$, **THEN**

$$\begin{cases} x(k+1) = A_g(k)x(k) + B_g(k)\omega(k) \\ y(k) = \Lambda(k)C(k)x(k) + D(k)\omega(k) \\ z(k) = M_g(k)x(k) \end{cases} \quad (1)$$

where u_q^g $(q = 1, 2, \ldots, \emptyset; g = 1, 2, \ldots, h)$ is the gth fuzzy set, $\varpi_q(x(k))$ represents qth premise variable. k $(0 \le k \le T-1)$ represents the kth sampling instant, $x(k) \in \mathbb{R}^{n_x}$ stands the system vector, $\omega(k) \in \mathbb{R}^{n_w}$ is the disturbance input, $y(k) \in \mathbb{R}^{n_y}$ denotes the measured output before transmission. $\Lambda(k) = \mathrm{diag}\{\lambda_1(k), \lambda_2(k), \ldots, \lambda_N(k)\}$ is a diagonal matrix, where $\lambda_i(k)$ $(i = 1, 2, \ldots, N)$ is the attenuation coefficient and uniformly distributed on interval $(\zeta_i, 1)$ $(0 < \zeta_i < 1)$. Then, the mean of the λ_i is set as $\bar{\lambda}_i$ and variance is set as $\tilde{\lambda}_i^2$. $z(k) \in \mathbb{R}^{n_z}$ indicates the signal to be estimated. $A_g(k), B_g(k), C(k), D(k), M_g(k)$ are the coefficient matrices with appropriate dimensions. Set the update period of the fuzzy system (1) to h. Define the gth firing strength as

$$\iota_g(x(k)) = \left[\underline{\varsigma}_g(x(k)), \overline{\varsigma}_g(x(k))\right] \quad (2)$$

where $\underline{\varsigma}_g(x(k)) = \prod_{q=1}^{\emptyset} \underline{u}_q^g(\varpi_q(x(k))) \ge 0, \overline{\varsigma}_g(x(k)) = \prod_{q=1}^{\emptyset} \overline{u}_q^g(\varpi_q(x(k))) \ge 0$ with the lower and upper membership functions (MFs) satisfying $0 \le \underline{u}_q^g(\varpi_q(x(k))) \le \overline{u}_q^g(\varpi_q(x(k))) \le 1$.

Then, a compact fuzzy system is converted as

$$\begin{cases} x(k+1) = \sum_{g=1}^{h} \varsigma_g(x(k))\left[A_g(k)x(k) + B_g(k)\omega(k)\right] \\ y(k) = \Lambda(k)C(k)x(k) + D(k)\omega(k) \\ z(k) = \sum_{g=1}^{h} \varsigma_g(x(k))M_g(k)x(k) \end{cases} \quad (3)$$

where $\varsigma_g(x(k)) = [b_g(x(k))/\sum_{g=1}^{h} b_g(x(k))]$, $b_g(x(k)) = \underline{\varsigma}_g(x(k))\underline{o}_g(x(k)) + \overline{\varsigma}_g(x(k))\overline{o}_g(x(k))$. The weighting functions $\underline{o}_g(x(k))$, $\overline{o}_g(x(k)) \in [0, 1]$ satisfy $\underline{o}_g(x(k)) + \overline{o}_g(x(k)) = 1$. The membership value $\varsigma_g(x(k))$ satisfies $\sum_{g=1}^{h} \varsigma_g(x(k)) = 1$.

Remark 1: Notice that as a disturbance input, $\omega(k)$ can represent the different types of noises. Without losing generality, such processing can not only simplify calculations but also adjust the intensity of different noises (e.g., process noise and measurement noise) through the appropriate dimension matrix mentioned above.

Remark 2: For engineering implementation, the fading phenomena of the signals are unavoidable because of reflection, diffraction and other reasons. It is noticeable that the attenuation coefficient λ_i is uniformly distributed on interval $(\zeta_i, 1)$, and such kind of fading measurements are different from the typical Rayleigh and Rice model [39], [40]. Moreover, according to the mathematical meaning of uniform distribution, therefore, we can know that the mean and variance of λ_i are $(1 + \zeta_i)/2$ and $[(1 - \zeta_i)^2/12]$.

C. DETFR Protocol

Due to the limitations of network resources, packet loss, conflicts, and other network-induced phenomena may occur during transmission. Therefore, a novel scheduling approach that determines which sensor node accesses to HRC network at every instant $k \in [0, T-1]$ is proposed.

The event triggering sequence is described as $\{t_n, n = 0, 1, 2, \ldots\}$, and an internal dynamic variable (IDV) is denoted as $\wp(k)$. The following ET function is presented as:

$$\Delta(k) = \frac{1}{\tau}\wp(k) + \mathfrak{A} \quad (4)$$

where $\mathfrak{A} = \mu y^T(k)y(k) - \sigma^T(k)\sigma(k)$, τ is a given positive scalar, and $\mu \in (0, 1)$ is a DET parameter. $\sigma(k) = y(k) - y(t_n)$ denotes the difference, where $y(t_n)$ is the measurement output that satisfies the DET condition at instant t_n. Consequently, the event triggering sequence is expressed as

$$t_{n+1} = \inf_{0 \le k \le T-1} \{k | k > t_n, \Delta(k) < 0\}. \quad (5)$$

Then, the IDV $\wp(k)$ is dynamically calculated as

$$\wp(k+1) = \psi\wp(k) + \mathfrak{A} \quad (6)$$

where $\psi \in (0, 1)$ is a pregiven scalar and $\wp(0) = \wp_0 \ge 0$.

Furthermore, according to the DETFR protocol, denote $y(k) = [(y^{[1]}(k))^T, (y^{[2]}(k))^T]^T$, where $y^{[1]}(k) = \mathrm{col}_{1\to\vartheta}\{y_i(k)\}$ and $y^{[2]}(k) = \mathrm{col}_{\vartheta+1\to N}\{y_j(k)\}$. Next, let us make the following assumptions to analyze signals transmitted through the HRC network.

Assumption 1: The constant h_r is the update period of high-rate transmission that satisfies $h_r = h/(\vartheta + 1)$.

Assumption 2: The initial transmission time t_0 is equal to 0th sampling time t_0^0.

For the convenience of calculation, define $k^l = k + lh_r$. More concretely, the first ϑth sensor nodes will obey the RR protocol rule at time instant $k + h_r, k + 2h_r, \ldots, k + \vartheta h_r$, and the rest can comply with the TOD protocol rule at time instant k. The RR protocol and TOD protocol will be introduced before considering the impact of the HRC network on signal transmission. In accordance with sequential selection, the criterion of RR protocol is given as

$$\xi_1\left(t_n^l\right) = \mod (l-1, \vartheta) + 1 \tag{7}$$

where $\xi_1(t_n^l)$ represents the node using the network at instant t_n^l. Similarly, the TOD protocol rule is governed by

$$\xi_2(t_n) = \arg\max_{i \in \varrho_2} \left(y_i(t_n) - y_i^\dagger\right)^T \Omega_i \left(y_i(t_n) - y_i^\dagger\right) \tag{8}$$

where $\xi_2(t_n)$ is the node that needs the network resources at the current time, Ω_i is a given weighted matrix, $y_i(t_n)$ is the ith signal before entering the network, as well as $y_i^\dagger$ is the last transmission signal of ith node.

By applying the $\delta(\cdot)$ function, the measurement output scheduled by the RR protocol is as follows:

$$\begin{aligned}\tilde{y}_i\left(k^i\right) &= \delta_i(t_n - k)\left(y_i(t_n) + G_i\left(t_n^i\right)v_i\left(t_n^i\right)\right.\\ &\quad \left.+ \alpha_i\left(t_n^i\right)\hbar_i\left(t_n^i\right)\right)\\ &= \delta_i(t_n - k)\left(\left(1 - \alpha_i\left(t_n^i\right)\right)(y_i(t_n)\right.\\ &\quad \left.+ G_i\left(t_n^i\right)v_i\left(t_n^i\right)) + \alpha_i\left(t_n^i\right)d_i\left(t_n^i\right)\right)\end{aligned} \tag{9}$$

where $G_i(\cdot)(i \in \varrho_1)$ is the coefficient matrix and $v_i(\cdot)$ is the transmission noise. The random variable $\alpha_i(\cdot)$ is characterized by Bernoulli process with the probabilities as

$$\begin{aligned}&\text{Prob}\{\alpha_i(k) = 1\} = E\{\alpha_i(k)\} = \beta_i\\ &\text{Prob}\{\alpha_i(k) = 0\} = 1 - \beta_i\end{aligned} \tag{10}$$

where $\beta_i \in [0, 1]$ denotes a given constant. $\hbar_i(t_n^l) = -(y_i(t_n) + G_i(t_n^l)v_i(t_n^l)) + d_i(t_n^l)$, where $\hbar_i(t_n^l)$ represents the false message sent by the attacker at time instant t_n^l.

Assumption 3 [44]: $d_i(t_n)$ is the energy signal satisfying

$$||d_i(t_n)||_2 \le \bar{d}_i \tag{11}$$

where $\bar{d}_i > 0$ is a given constant.

Remark 3: The system model we have designed has three periods: the plant period, the HRC period, and the FR period. Our main purpose is to establish a single-rate filter structure. In light of the impact of protocol scheduling, only one node can use network transmission at one time instant, which means that only one signal can be transmitted. Therefore, without losing generality, the FR period and HRC period are set to synchronize, namely, the SS is configured on interval $(k, k+1)$, and the DS is configured at instant k.

Denote $\bar{y}(k) = [(\bar{y}^{[1]}(k))^T, (\bar{y}^{[2]}(k))^T]^T$, where $\bar{y}^{[1]}(k) = \text{col}_{1\to\vartheta}\{\bar{y}_i(k)\}$ and $\bar{y}^{[2]}(k) = \text{col}_{\vartheta+1\to N}\{\bar{y}_j(k)\}$, which refers to measurement outputs after network transmission. According to the cycle characteristics of RR protocol and zero-input (ZI) tactics, define $\bar{y}^{[1]}(k) = \text{col}_{1\to\vartheta}\{\tilde{y}_i(k^i)\}$. With (9)-(11), the actual outputs $\bar{y}^{[1]}(k)$ are further derived as

$$\begin{aligned}\bar{y}^{[1]}(k) = \Phi_{\xi_1}&\left(\left(I_{N_1} - \alpha^{[1]}\right)\left(y^{[1]}(t_n) + G^{[1]}(t_n)v^{[1]}(t_n)\right)\right.\\ &\left.+ \alpha^{[1]}d^{[1]}(t_n)\right)\end{aligned} \tag{12}$$

where $G^{[1]}(t_n) = \text{diag}\{G_1(t_n^1), G_2(t_n^2), \ldots, G_n(t_n^\vartheta)\}$, $v^{[1]}(t_n) = \text{col}_{1\to\vartheta}\{v_i(t_n^i)\}$, $d^{[1]}(t_n) = \text{col}_{1\to\vartheta}\{d_i(t_n^i)\}$, $\alpha^{[1]} = \text{diag}\{\alpha_1^T(t_n^1), \alpha_2^T(t_n^2), \ldots, \alpha_\vartheta^T(t_n^\vartheta)\}$, $\Phi_{\xi_1} = \delta_1(t_n - k)\text{diag}\{\delta(1 - \xi_1(t_n^1)), \delta(2 - \xi_1(t_n^2)), \ldots, \delta(\vartheta - \xi_1(t_n^\vartheta))\}$.

Along with the similar line, considering the effects of attacks, zero-order holder (ZOH) technology and TOD protocol, the actual outputs $\bar{y}_i(t_n)$ can be obtained that

$$\bar{y}_i(t_n) = \begin{cases} y_i(t_n) + \alpha(t_n)\hbar_i(t_n), & i = \xi_2(t_n)\\ \bar{y}_i(t_{n-1}), & \text{otherwise}\end{cases} \tag{13}$$

where $\hbar_i(t_n) = -y_i(t_n) + d_i(t_n)$ $(i \in \varrho_2)$. The random variable $\alpha(\cdot)$ satisfies the properties $Prob\{\alpha(k) = 1\} = \beta$ and $\text{Prob}\{\alpha(k) = 0\} = 1 - \beta$. Their connotation is the same as above.

According to (5), (9) and (13), we can obtain that

$$t_n = \begin{cases} k, & \Delta(k) < 0\\ t_{n-1}, & \text{otherwise.}\end{cases} \tag{14}$$

By applying the $\delta(\cdot)$ function, $\bar{y}^{[2]}(k)$ is presented as

$$\begin{aligned}\bar{y}^{[2]}(k) &= \alpha(t_n)\Phi_{\xi_2}d^{[2]}(t_n) + \left(I_{N_2} - \Phi_{\xi_2}\right)\bar{y}^{[2]}(k-1)\\ &\quad + (1 - \alpha(t_n))\Phi_{\xi_2}\left(y^{[2]}(t_n) + G^{[2]}(t_n)v(t_n)\right)\end{aligned} \tag{15}$$

where $\Phi_{\xi_2} = \text{diag}\{\delta(\vartheta + 1 - \xi_2(t_n)), \delta(\vartheta + 2 - \xi_2(t_n)), \ldots, \delta(N - \xi_2(t_n))\}$, $d^{[2]}(t_n) = \text{col}_{\vartheta+1\to N}\{d_i(t_n^i)\}$, $G^{[2]} = \text{col}_{\vartheta+1\to N}\{G_i(t_n)\}$.

Then, recalling the relationship between $\bar{y}(k)$, $\bar{y}^{[1]}(k)$ and $\bar{y}^{[2]}(k)$ yields the following actual output signals:

$$\begin{aligned}\bar{y}(k) &= I_1\bar{y}^{[1]}(k) + I_2\bar{y}^{[2]}(k)\\ &= I_1\Phi_{\xi_1}\left(I_{N_1} - \alpha^{[1]}\right)(\Lambda^{[1]}C^{[1]}x(k) + D^{[1]}w(k)\\ &\quad + G^{[1]}(t_n)v^{[1]}(t_n) - \sigma^{[1]}(k)) + I_1\Phi_{\xi_1}\alpha^{[1]}d^{[1]}(t_n)\\ &\quad + (1 - \alpha(t_n))I_2\Phi_{\xi_2}\left(\Lambda^{[2]}C^{[2]}x(k) + D^{[2]}\omega(k)\right.\\ &\quad \left.+ G^{[2]}v(t_n) - \sigma^{[2]}(k)\right) + \alpha(t_n)I_2\Phi_{\xi_2}d^{[2]}(t_n)\\ &\quad + I_2\left(I_{N_2} - \Phi_{\xi_2}\right)\bar{y}^{[2]}(k-1)\end{aligned} \tag{16}$$

where

$$\begin{aligned}\Lambda^{[1]} &\triangleq \text{diag}\{\lambda_1(k), \lambda_2(k), \ldots, \lambda_\vartheta(k)\}\\ \Lambda^{[2]} &\triangleq \text{diag}\{\lambda_{\vartheta+1}(k), \lambda_{\vartheta+2}(k), \ldots, \lambda_N(k)\}\\ C^{[1]} &\triangleq \text{col}_{1\to\vartheta}\{C_i(k)\}, C^{[2]} \triangleq \text{col}_{\vartheta+1\to N}\{C_i(k)\}\\ D^{[1]} &\triangleq \text{col}_{1\to\vartheta}\{D_i(k)\}, D^{[2]} \triangleq \text{col}_{\vartheta+1\to N}\{D_i(k)\}\\ \sigma^{[1]} &\triangleq \text{col}_{1\to\vartheta}\{\sigma_i(k)\}, \sigma^{[2]}(k) \triangleq \text{col}_{\vartheta+1\to N}\{\sigma_i(k)\}\\ d(t_n) &\triangleq [(d^{[1]}(t_n))^T \quad (d^{[2]}(t_n))^T]^T\\ I_1 &\triangleq \begin{bmatrix} I_{N_1\times N_1}\\ 0_{(N-N_1)\times N_1}\end{bmatrix}, I_2 \triangleq \begin{bmatrix} 0_{(N-N_2)\times N_2}\\ I_{N_2\times N_2}\end{bmatrix}.\end{aligned}$$

Remark 4: In the unified actual measurement outputs, the first ϑth components of $\bar{y}(k)$ adopt the ZI strategy. Therefore, the purpose of setting $\delta_i(t_n - k)$ in (9) is to obtain $\bar{y}^{[1]} = \mathbf{0}$ when $\Delta(k) \ge 0$. Otherwise, when the triggering condition is established (i.e., $t_n = k$), the signal received by the filter will through an insecure HRC channel. Moreover, the reason for using t_n instead of k in (9) is to unify the symbols with (13) and (15), which does not affect the results.

D. System Augmentation

According to (3) and (16), denoting $\bar{x}(k) \triangleq [x^T(k) \quad \bar{y}^T(k-1)]^T$, then, the following augmented system can be reformulated:

$$\begin{cases} \bar{x}(k+1) = \sum_{g=1}^{h} \varsigma_g(x(k))[\mathscr{A}^g \bar{x}(k) + \mathscr{B}^g \bar{w}(k) + \tilde{\Gamma} d(t_n) \\ \quad +\tilde{E}\sigma(k)] \\ \bar{y}(k) = \tilde{C}\bar{x}(k) + \tilde{D}\bar{w}(k) + \Gamma d(t_n) + E\sigma(k) \\ \bar{z}(k) = \sum_{g=1}^{h} \varsigma_g(x(k))\bar{M}_g(k)\bar{x}(k) \end{cases} \tag{17}$$

where

$$\begin{aligned} \bar{M}_g(k) &\triangleq [M_g(k) \ 0], \bar{\omega}(k) \triangleq [w^T(k) \ (v^{[1]}(t_n))^T \ v^T(t_n)]^T \\ \mathscr{A}^g &\triangleq \begin{bmatrix} A_g(k) & 0 \\ \rho_1\Lambda^{[1]}C^{[1]} + \rho_2\Lambda^{[2]}C^{[2]} & I_2(I_{N_2} - \Phi_{\xi_2})I_2^T \end{bmatrix} \\ \mathscr{B}^g &\triangleq \begin{bmatrix} B_g(k) & 0 & 0 \\ \rho_1 D^{[1]} + \rho_2 D^{[2]} & \rho_1 G^{[1]} & \rho_2 G^{[2]} \end{bmatrix} \\ \tilde{\Gamma} &\triangleq \begin{bmatrix} 0 & 0 \\ I_1\Phi_{\xi_1}\alpha^{[1]} & \alpha(t_n)I_2\Phi_{\xi_2} \end{bmatrix}, \tilde{E} \triangleq \begin{bmatrix} 0 & 0 \\ -\rho_1 & -\rho_2 \end{bmatrix} \\ \tilde{C} &\triangleq \left[\rho_1\Lambda^{[1]}C^{[1]} + \rho_2\Lambda^{[2]}C^{[2]} \quad I_2(I_{N_2} - \Phi_{\xi_2})I_2^T\right] \\ \tilde{D} &\triangleq \left[\rho_1 D^{[1]} + \rho_2 D^{[2]} \quad \rho_1 G^{[1]} \quad \rho_2 G^{[2]}\right] \\ \Gamma &\triangleq \left[I_1\Phi_{\xi_1}\alpha^{[1]} \quad \alpha(t_n)I_2\Phi_{\xi_2}\right], E \triangleq \left[-\rho_1 \quad -\rho_2\right] \\ \rho_1 &\triangleq I_1\Phi_{\xi_1}(I_{N_1} - \alpha^{[1]}), \rho_2 \triangleq (1 - \alpha(t_n))I_2\Phi_{\xi_2}. \end{aligned}$$

E. Filter Structure

Considering the fading measurements and deception attacks, the fuzzy filter structure with h rules can be constructed as follows:

RULE j: **IF** $\varpi_1(x(k))$ is u_1^j, and $\ldots$, $\varpi_\o$ is $u_\o^j$, **THEN**

$$\begin{cases} \hat{x}(k+1) = \mathscr{A}^j\hat{x}(k) + K_j(k)\Big(\bar{y}(k) - \tilde{C}\hat{x}(k)\Big) \\ \hat{z}(k) \quad = \bar{M}_j(k)\hat{x}(k) \end{cases} \tag{18}$$

where $\hat{x}(k)$ is the estimation of $\bar{x}(k)$, $\hat{z}(k)$ is the estimation of $\bar{z}(k)$. $K_j(k)$ is the filter parameter to be determined. Therefore, the fuzzy filter can be converted as

$$\begin{cases} \hat{x}(k+1) = \sum_{j=1}^{h} \varsigma_j\big(\hat{x}(k)\big)\Big[\mathscr{A}^j\hat{x}(k) + K_j(k)\Big(\bar{y}(k) - \tilde{C}\hat{x}(k)\Big)\Big] \\ \hat{z}(k) = \sum_{j=1}^{h} \varsigma_j\big(\hat{x}(k)\big)\bar{M}_j(k)\hat{x}(k). \end{cases} \tag{19}$$

Then, the filter error system can be constructed from $e(k) = \bar{x}(k) - \hat{x}(k)$ and $\tilde{z}(k) = \bar{z}(k) - \hat{z}(k)$. Moreover, considering the influence of measurement attenuation parameters and network attack parameters, the error dynamics can be inferred as

$$\begin{cases} e(k+1) = \sum_{g=1}^{h}\sum_{j=1}^{h} \varsigma_g(x(k))\varsigma_j\big(\hat{x}(k)\big)[\mathscr{A}^{gj}\hat{x}(k) \\ +((\mathscr{A}_1^g + \mathscr{A}_2 + \mathscr{A}_3 + \mathscr{A}_4) - K_j(k)(\tilde{C}_1 + \tilde{C}_2 \\ +\tilde{C}_3 + \tilde{C}_4))e(k) + ((\mathscr{B}_1^g + \mathscr{B}_2) - K_j(k) \\ \times(\tilde{D}_1 + \tilde{D}_2))\bar{\omega}(k) + (\tilde{\Gamma}_1 + \tilde{\Gamma}_2 - K_j(k) \\ \times(\Gamma_1 + \Gamma_2))d(t_n) + (\tilde{E}_1 + \tilde{E}_2 - K_j(k)(E_1 \\ +E_2))\sigma(k)] \\ \tilde{z}(k) = \sum_{g=1}^{h}\sum_{j=1}^{h} \varsigma_g(x(k))\varsigma_j\big(\hat{x}(k)\big)[\big(\bar{M}_g(k) - \bar{M}_j(k)\big)\hat{x}(k) \\ +\bar{M}_g e(k)] \end{cases} \tag{20}$$

where

$$\begin{aligned} &\bar{A} \triangleq \left[A_g(k) \quad 0\right], \mathscr{A}_1^g \triangleq \left[\bar{A}^T \quad \tilde{C}_1^T\right]^T, \mathscr{A}_2 \triangleq \left[0 \quad \tilde{C}_2^T\right]^T \\ &\mathscr{A}_3 \triangleq \left[0 \quad \tilde{C}_3^T\right]^T, \mathscr{A}_4 \triangleq \left[0 \quad \tilde{C}_4^T\right]^T, \bar{B} \triangleq \left[B_g(k) \quad 0\right] \\ &\mathscr{B}_1^g \triangleq \left[\bar{B}^T \quad \tilde{D}_1^T\right]^T, \mathscr{B}_2 \triangleq \left[0 \quad \tilde{D}_2^T\right]^T \\ &\tilde{C}_1 \triangleq \left[\rho_5\bar{\Lambda}^{[1]}C^{[1]} + \rho_6\bar{\Lambda}^{[2]}C^{[2]} \quad I_2(I_{N_2} - \Phi_{\xi_2})I_2^T\right] \\ &\tilde{C}_2 \triangleq \left[\rho_5(\Lambda^{[1]} - \bar{\Lambda}^{[1]})C^{[1]} + \rho_6(\Lambda^{[2]} - \bar{\Lambda}^{[2]})C^{[2]} \quad 0\right] \\ &\tilde{C}_3 \triangleq \left[\rho_3\bar{\Lambda}^{[1]}C^{[1]} + \rho_4\bar{\Lambda}^{[2]}C^{[2]} \quad 0\right] \\ &\tilde{C}_4 \triangleq \left[\rho_3(\Lambda^{[1]} - \bar{\Lambda}^{[1]})C^{[1]} + \rho_4(\Lambda^{[2]} - \bar{\Lambda}^{[2]})C^{[2]} \quad 0\right] \\ &\tilde{D}_1 \triangleq \left[\rho_5 D^{[1]} + \rho_6 D^{[2]} \quad \rho_5 G^{[1]} \quad I_2\rho_6 G^{[2]}\right] \\ &\tilde{D}_2 \triangleq \left[\rho_3 D^{[1]} + \rho_4 D^{[2]} \quad \rho_3 G^{[1]} \quad I_2\rho_4 G^{[2]}\right] \\ &\Gamma_1 \triangleq \left[I_1\Phi_{\xi_1}\beta^{[1]} \quad \beta I_2\Phi_{\xi_2}\right], \mathscr{A}^{gj} = \mathscr{A}^g - \mathscr{A}^j \\ &\Gamma_2 \triangleq \left[-\rho_3 \quad -\rho_4\right], \tilde{\Gamma}_1 \triangleq \left[0 \quad \Gamma_1^T\right]^T, \tilde{\Gamma}_2 \triangleq \left[0 \quad \Gamma_2^T\right]^T \\ &E_1 \triangleq \left[-\rho_5 \quad -\rho_6\right], E_2 \triangleq \left[-\rho_3 \quad -\rho_4\right] \\ &\tilde{E}_1 \triangleq \left[0 \quad E_1^T\right]^T, \tilde{E}_2 \triangleq \left[0 \quad E_2^T\right]^T \\ &\beta^{[1]} \triangleq \mathrm{diag}\{\beta_1, \beta_2, \ldots, \beta_\vartheta\}, \bar{\Lambda}^{[1]} \triangleq \mathrm{diag}\{\bar{\lambda}_1, \bar{\lambda}_2, \ldots, \bar{\lambda}_\vartheta\} \\ &\rho_3 \triangleq I_1\Phi_{\xi_1}(\beta^{[1]} - \alpha^{[1]}), \rho_4 \triangleq (\beta - \alpha(t_n))I_2\Phi_{\xi_2} \\ &\rho_5 \triangleq I_1\Phi_{\xi_1}(I_{N_1} - \beta^{[1]}), \rho_6 \triangleq (1 - \beta)I_2\Phi_{\xi_2} \\ &\bar{\Lambda}^{[2]} \triangleq \mathrm{diag}\{\bar{\lambda}_{\vartheta+1}, \bar{\lambda}_{\vartheta+2}, \ldots, \bar{\lambda}_N\}. \end{aligned}$$

The objective of this article is to construct a security filter (19) in an effort meet the finite-horizon H_∞ performance for predefined disturbance attenuation index $\gamma > 0$

$$\begin{aligned} J(k) = E\left\{\sum_{k=0}^{T-1}(||\tilde{z}(k))||^2 - \gamma^2||\bar{\omega}(k)||^2\right\} \\ - \gamma^2 e(0)^T Q(0)e(0) \le 0 \end{aligned} \tag{21}$$

where the positive-definite matrix $Q(0)$ is predefined and $\bar{\omega}(k) \neq 0$.

III. Main Results

In this position, certain sufficient conditions can be proposed that ensure the H_∞ performance index of filtering error dynamics (21) by virtue of the Schur complement and Lyapunov function. An effective DETFR protocol-based secure filtering algorithm is developed to acquire filter gain by the linear matrix inequalities (LMIs) method.

Theorem 1: Take into account the fuzzy filter error dynamics (20) under deception attacks, DETFR protocol and fading measurements. Given the positive definite matrix $Q(0)$, the disturbance attenuation index γ, the filter gain $K_j(k)$ and the positive scalar $\theta(0), \mu, \tau, \psi$, the H_∞ performance index can be guaranteed if there exist scalar $\varphi > 0$ and positive definite matrix $P(k)$ such that

$$\Upsilon_{gj} = \begin{bmatrix} \Upsilon_{11}^{gj} & \Upsilon_{12}^{gj} \\ * & \Upsilon_{22}^{gj} \end{bmatrix} < 0 \tag{22}$$

$$e_0^T\Big(P_0 - \gamma^2 Q_0\Big)e_0 + \theta_0 + \frac{1}{\tau}\wp_0 + T||\bar{d}||_2^2 \le 0 \tag{23}$$

$$\psi - \frac{1}{\tau} \ge 0 \tag{24}$$

where parameters can be seen in the Appendix.

Proof: According to the DETFR protocol (4), it is clear that

$$\Delta(k) = \mu y^T(k)y(k) + \mathfrak{A} \ge 0. \tag{25}$$

In light of (6), (25) and initial value $\wp_0 \geq 0$, the lower bound of the codomain of $\wp(k+1)$ satisfies

$$\begin{aligned}\wp(k+1) &= \psi\wp(k) + \mathfrak{A}\\ &= \psi\wp(k) - \sigma^T(k)\sigma(k) + \mu y^T(k)y(k)\\ &\geq \psi\wp(k) - \frac{1}{\tau}\wp(k) \geq \cdots \geq \left(\psi - \frac{1}{\tau}\right)^{k+1}\wp(0)\\ &\geq 0.\end{aligned} \tag{26}$$

In line with the DETFR protocol, select the Lyapunov function as

$$V(k) = e^T(k)P(k)e(k) + \theta(k) + \frac{1}{\tau}\wp(k). \tag{27}$$

Let $\eta(k) \triangleq \left[1 \quad e^T(k) \quad \bar{\omega}^T(k) \quad d^T(t_n) \quad \sigma^T(k) \quad \sqrt{\wp(k)}^T\right]^T$ and the difference of (27) as $\Delta V(k) = V(k+1) - V(k)$. Then, take expectation and add the zero term $(||\tilde{z}(k)||^2 - \gamma^2||\bar{\omega}(k)||^2) - (||\tilde{z}(k)||^2 - \gamma^2||\bar{\omega}(k)||^2)$ as follows:

$$\begin{aligned}E\Delta V(k) = E\Bigg\{&\sum_{g=1}^{h}\sum_{j=1}^{h}\varsigma_g(x(k))\varsigma_j\big(\hat{x}(k)\big)\Big[\theta(k+1) - \theta(k)\\ &- e^T(k)P(k)e(k) + \eta^T(k)\Xi_{gj}^T(k)P(k+1)\\ &\times \Xi_{gj}(k)\eta(k) + \frac{1}{\tau}(\wp(k+1) - \wp(k))\Big]\\ &+ \Big(||\tilde{z}(k)||^2 - \gamma^2||\bar{\omega}(k)||^2\Big)\\ &- \Big(||\tilde{z}(k)||^2 - \gamma^2||\bar{\omega}(k)||^2\Big)\Bigg\}\\ \leq &\sum_{g=1}^{h}\sum_{j=1}^{h}\varsigma_g(x(k))\varsigma_j\big(\hat{x}(k)\big)\eta^T(k)\Pi_{gj}\eta(k)\\ &- \Big(||\tilde{z}(k)||^2 - \gamma^2||\bar{\omega}(k)||^2\Big)\end{aligned} \tag{28}$$

where

$$\begin{aligned}\Xi_{gj}(k) &\triangleq \begin{bmatrix}\Xi_1(k) & \tilde{\Gamma} - K_j(k)\Gamma & \tilde{E} - K_j(k)E & 0\end{bmatrix}\\ \Xi_1(k) &\triangleq \begin{bmatrix}\mathscr{A}^{gj} & \mathscr{A}^g - K_j(k)\tilde{C} & \mathscr{B}^g - K_j(k)\tilde{D}\end{bmatrix}\\ \Pi_{gj} &= \begin{bmatrix}\Pi_{11} & \Pi_{12} & \Pi_{13} & \Pi_{14} & \Pi_{15} & 0\\ * & \Pi_{22} & \Pi_{23} & \Pi_{24} & \Pi_{25} & 0\\ * & * & \Pi_{33} & \Pi_{34} & \Pi_{35} & 0\\ * & * & * & \Pi_{44} & \Pi_{45} & 0\\ * & * & * & * & \Pi_{55} & 0\\ * & * & * & * & * & \Pi_{66}\end{bmatrix}\\ \Pi_{11} &\triangleq \theta(k+1) - \theta(k) + \frac{\mu}{\tau}\hat{x}^T(k)(\check{C}_1^T\check{C}_1 + \check{C}_2^T\check{C}_2)\hat{x}(k)\\ &\quad + \hat{x}^T(k)(\bar{M}_g(k) - \bar{M}_j(k))^T(\bar{M}_g(k) - \bar{M}_j(k))\hat{x}(k)\\ &\quad + \hat{x}^T(k)\mathscr{A}^{gj^T}P(k+1)\mathscr{A}^{gj}\hat{x}(k)\\ \Pi_{12} &\triangleq \frac{\mu}{\tau}\hat{x}^T(k)(\check{C}_1^T\check{C}_1 + \check{C}_2^T\check{C}_2) + \hat{x}^T(k)(\bar{M}_g(k) - \bar{M}_j(k))^T\\ &\quad \times \bar{M}_g(k) + \hat{x}^T(k)\mathscr{A}^{gj^T}P(k+1)(\mathscr{A}_1^g - K_j(k)\tilde{C}_1)\\ \Pi_{13} &\triangleq \frac{\mu}{\tau}\hat{x}^T(k)\check{C}_1^T\check{D} + \hat{x}^T(k)\mathscr{A}^{gj^T}P(k+1)\\ &\quad (\mathscr{B}_1^g - K_j(k)\tilde{D}_1)\\ \Pi_{14} &\triangleq \hat{x}^T(k)\mathscr{A}^{gj^T}P(k+1)(\tilde{\Gamma}_1 - K_j(k)\Gamma_1)\\ \Pi_{15} &\triangleq \hat{x}^T(k)\mathscr{A}^{gj^T}P(k+1)(\tilde{E}_1 - K_j(k)E_1)\\ \Pi_{22} &\triangleq -P(k) + \bar{M}_g^T\bar{M}_g + \frac{\mu}{\tau}(\check{C}_1^T\check{C}_1 + \check{C}_2^T\check{C}_2)\\ &\quad + (\mathscr{A}_1^g - K_j(k)\tilde{C}_1)^TP(k+1)(\mathscr{A}_1^g - K_j(k)\tilde{C}_1)\\ &\quad + (\bar{\mathscr{A}}_2 - K_j(k)\bar{\tilde{C}}_2)^TP(k+1)(\bar{\mathscr{A}}_2 - K_j(k)\bar{\tilde{C}}_2)\\ &\quad + (\bar{\mathscr{A}}_3 - K_j(k)\bar{\tilde{C}}_3)^TP(k+1)(\bar{\mathscr{A}}_3 - K_j(k)\bar{\tilde{C}}_3)\\ &\quad + (\bar{\mathscr{A}}_4 - K_j(k)\bar{\tilde{C}}_4)^TP(k+1)(\bar{\mathscr{A}}_4 - K_j(k)\bar{\tilde{C}}_4)\\ \Pi_{23} &\triangleq \frac{\mu}{\tau}\check{C}_1^T\check{D} + (\mathscr{A}_1^g - K_j(k)\tilde{C}_1)^TP(k+1)\\ &\quad (\mathscr{B}_1^g - K_j(k)\tilde{D}_1) + (\bar{\mathscr{A}}_3 - K_j(k)\bar{\tilde{C}}_3)^TP(k+1)\\ &\quad (\bar{\mathscr{B}}_2 - K_j(k)\bar{\tilde{D}}_2)\\ \Pi_{33} &\triangleq -\gamma^2 I_{\bar{\omega}} + \frac{\mu}{\tau}\check{D}^T\check{D} + (\mathscr{B}_1^g - K_j(k)\tilde{D}_1)^TP(k+1)\\ &\quad (\mathscr{B}_1^g - K_j(k)\tilde{D}_1) + (\bar{\mathscr{B}}_2 - K_j(k)\bar{\tilde{D}}_2)^TP(k+1)\\ &\quad (\bar{\mathscr{B}}_2 - K_j(k)\bar{\tilde{D}}_2)\\ \Pi_{24} &\triangleq (\mathscr{A}_1^g - K_j(k)\tilde{C}_1)^TP(k+1)(\tilde{\Gamma}_1 - K_j(k)\Gamma_1)\\ &\quad + (\bar{\mathscr{A}}_3 - K_j(k)\bar{\tilde{C}}_3)^TP(k+1)(\bar{\tilde{\Gamma}}_2 - K_j(k)\bar{\Gamma}_2)\\ \Pi_{34} &\triangleq (\mathscr{B}_1^g - K_j(k)\tilde{D}_1)^TP(k+1)(\tilde{\Gamma}_1 - K_j(k)\Gamma_1)\\ &\quad + (\bar{\mathscr{B}}_2 - K_j(k)\bar{\tilde{D}}_2)^TP(k+1)(\bar{\tilde{\Gamma}}_2 - K_j(k)\bar{\Gamma}_2)\\ \Pi_{44} &\triangleq (\tilde{\Gamma}_1 - K_j(k)\Gamma_1)^TP(k+1)(\tilde{\Gamma}_1 - K_j(k)\Gamma_1)\\ &\quad + (\bar{\tilde{\Gamma}}_2 - K_j(k)\bar{\Gamma}_2)^TP(k+1)(\bar{\tilde{\Gamma}}_2 - K_j(k)\bar{\Gamma}_2)\\ \Pi_{25} &\triangleq (\mathscr{A}_1^g - K_j(k)\tilde{C}_1)^TP(k+1)(\tilde{E}_1 - K_j(k)E_1)\\ &\quad + (\bar{\mathscr{A}}_3 - K_j(k)\bar{\tilde{C}}_3)^TP(k+1)(\bar{\tilde{\Gamma}}_2 - K_j(k)\bar{\Gamma}_2)\\ \Pi_{35} &\triangleq (\mathscr{B}_1^g - K_j(k)\tilde{D}_1)^TP(k+1)(\tilde{E}_1 - K_j(k)E_1)\\ &\quad + (\bar{\mathscr{B}}_2 - K_j(k)\bar{\tilde{D}}_2)^TP(k+1)(\bar{\tilde{E}}_2 - K_j(k)\bar{E}_2)\\ \Pi_{45} &\triangleq (\tilde{\Gamma}_1 - K_j(k)\Gamma_1)^TP(k+1)(\tilde{E}_1 - K_j(k)E_1)\\ &\quad + (\bar{\tilde{\Gamma}}_2 - K_j(k)\bar{\Gamma}_2)(\bar{\tilde{E}}_2 - K_j(k)\bar{E}_2)\\ \Pi_{55} &\triangleq -\frac{1}{\tau}I_\sigma + (\tilde{E}_1 - K_j(k)E_1)^TP(k+1)(\tilde{E}_1 - K_j(k)E_1)\\ &\quad + (\bar{\tilde{E}}_2 - K_j(k)\bar{E}_2)^TP(k+1)(\bar{\tilde{E}}_2 - K_j(k)\bar{E}_2)\\ \Pi_{66} &\triangleq \frac{1}{\tau}(\psi - 1).\end{aligned}$$

It follows from the energy signal condition (11) and (28) that one can have:

$$\begin{aligned}E\Delta V(k) \leq E\Bigg\{&\sum_{g=1}^{h}\sum_{j=1}^{h}\varsigma_g(x(k))\varsigma_j\big(\hat{x}(k)\big)\\ &\Big[\eta(k)\Pi_{gj}\eta(k) + d^T(t_n)d(t_n) - d^T(t_n)d(t_n) + \varphi\\ &\Big(\mu \times y^T(k)y(k) - \sigma^T(k)\sigma(k) + \frac{1}{\tau}\wp(k)\Big)\Big]\\ &- \Big(||\tilde{z}(k)||^2 - \gamma^2||\bar{\omega}(k)||^2\Big)\Bigg\}\\ \leq &\sum_{g=1}^{h}\sum_{j=1}^{h}\varsigma_g(x(k))\varsigma_j\big(\hat{x}(k)\big)\eta^T(k)\bar{\Pi}_{gj}\eta(k)\\ &- \Big(||\tilde{z}(k)||^2 - \gamma^2||\bar{\omega}(k)||^2\Big) + ||\bar{d}||_2^2\end{aligned} \tag{29}$$

where $\bar{\Pi}_{gj} = \Pi_{gj} - \Im_1^T \Im_1 - \varphi \Im_2^T \Im_2 + \sum_{i=3}^{5} \Im_i^T \Im_i$,
$\Im_1 = \begin{bmatrix} 0 & 0 & 0 & I_d & 0 & 0 \end{bmatrix}$, $\Im_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & I_\sigma & 0 \end{bmatrix}$,
$\Im_3 = \begin{bmatrix} \mu \check{C}_1 \hat{x}(k) & \mu \check{C}_1 & \mu \check{D} & 0 & 0 & 0 \end{bmatrix}$,
$\Im_4 = \begin{bmatrix} \mu \check{C}_2 \hat{x}(k) & \mu \check{C}_2 & 0 & 0 & 0 & 0 \end{bmatrix}$,
$\Im_5 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & \sqrt{\frac{\varphi}{\tau}} \end{bmatrix}$.

Then, both sides (29) are added from 0 to $T-1$

$$\begin{aligned} \sum_{k=0}^{T-1} \Delta V(k) \leq & \sum_{k=0}^{T-1} \sum_{g=1}^{h} \sum_{j=1}^{h} \varsigma_g(x(k)) \varsigma_j(\hat{x}(k)) \eta^T(k) \bar{\Pi}_{gj} \eta(k) \\ & - \sum_{k=0}^{T-1} E\Big(||\tilde{z}(k)||^2 - \gamma^2 ||\bar{\omega}(k)||^2 \Big) \\ & + \sum_{k=0}^{T-1} ||\bar{d}||_2^2 \end{aligned} \tag{30}$$

that is

$$V(T) - V(0) \leq T||\bar{d}||_2^2 - \sum_{k=0}^{T-1} E\Big(||\tilde{z}(k)||^2 - \gamma^2 ||\bar{\omega}(k)||^2 \Big). \tag{31}$$

Next, we know that

$$J(k) \leq e_0^T \Big(P_0 - \gamma^2 Q_0 \Big) e_0 + \theta_0 + \frac{1}{\tau} \wp_0 + T||\bar{d}||_2^2. \tag{32}$$

Therefore, according to (22)–(24), $J(k) \leq 0$ is satisfied and then, the proof is completed. ■

Having established the analysis results, the filter gain parameters $K_j(k)$ will be obtained using LMIs technology through a filtering algorithm.

Theorem 2: Take into account the fuzzy filter error dynamics (20) under deception attacks, DETFR protocol and fading measurements. For predetermined scalars $\gamma > 0$, $\theta(0) > 0$, μ, τ, ψ, and positive definite matrix $Q(0)$, H_∞ performance can be guaranteed if there exist real-valued matrices $Z_j(k)$ and positive scalar φ such that

$$\bar{\Upsilon}_{gj} = \begin{bmatrix} \Upsilon_{11}^{gj} & \bar{\Upsilon}_{12}^{gj} \\ * & \Upsilon_{22}^{gj} \end{bmatrix} < 0 \tag{33}$$

$$e_0^T \Big(P_0 - \gamma^2 Q_0 \Big) e_0 + \theta_0 + \frac{1}{\tau} \wp_0 + T||\bar{d}||_2^2 \leq 0 \tag{34}$$

$$\psi - \frac{1}{\tau} \geq 0 \tag{35}$$

where $\bar{\Upsilon}_{12}^{gj} = \begin{bmatrix} \hat{x}^T(k) \mathscr{A}^{gj^T} P(k+1) & 0 & 0 & 0 \\ \bar{\Theta}_{21} & \bar{\Theta}_{22} & \bar{\Theta}_{23} & \bar{\Theta}_{24} \\ \bar{\Theta}_{31} & \bar{\Theta}_{32} & 0 & 0 \\ \bar{\Theta}_{41} & \bar{\Theta}_{42} & 0 & 0 \\ \bar{\Theta}_{51} & \bar{\Theta}_{52} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

$\bar{\Theta}_{21} \triangleq \mathscr{A}_1^{g^T} P(k+1) - \tilde{C}_1^T Z_j^T(k)$, $\bar{\Theta}_{22} \triangleq \bar{\mathscr{A}}_3^T P(k+1) - \bar{\tilde{C}}_3^T Z_j^T(k)$, $\bar{\Theta}_{23} \triangleq \bar{\mathscr{A}}_2^T P(k+1) - \bar{\tilde{C}}_2^T Z_j^T(k)$, $\bar{\Theta}_{24} \triangleq \bar{\mathscr{A}}_4^T P(k+1) - \bar{\tilde{C}}_4^T Z_j^T(k)$, $\bar{\Theta}_{31} \triangleq \mathscr{B}_1^{g^T} P(k+1) - \tilde{D}_1^T Z_j^T(k)$, $\bar{\Theta}_{32} \triangleq \bar{\mathscr{B}}_2^T P(k+1) - \bar{\tilde{D}}_2^T Z_j^T(k)$, $\bar{\Theta}_{41} \triangleq \tilde{\Gamma}_1^T P(k+1) - \Gamma_1^T Z_j^T(k)$, $\bar{\Theta}_{42} \triangleq \bar{\tilde{\Gamma}}_2^T P(k+1) - \bar{\Gamma}_2^T Z_j^T(k)$, $\bar{\Theta}_{51} \triangleq \tilde{E}_1^T P(k+1) - E_1^T Z_j^T(k)$, $\bar{\Theta}_{52} \triangleq \bar{\tilde{E}}_2^T P(k+1) - \bar{E}_2^T Z_j^T(k)$.

Algorithm 1: DETFR Protocol-Based Secure Filtering Algorithm

Give initial parameters $\mu, \tau, \psi, P_0, Q_0, \theta_0$ and γ;
for $k \leftarrow 1$ **to** *T-1* **do**
  if $\Delta(k) < 0$ **then**
    $\bar{y}_j(k)$ and $\bar{y}^{[2]}(k) \leftarrow$ Eq. (13)-(15) for $j \in \varrho_2$;
    for $l \leftarrow 1$ **to** ϑ **do**
      $\tilde{y}_l(k^l)$ and $\bar{y}^{[1]}(k) \leftarrow$ Eq. (9) and (12);
    end
    $\bar{y}(k) \leftarrow I_1 \bar{y}^{[1]}(k) + I_2 \bar{y}^{[2]}(k)$;
  else
    $\bar{y}(k) \leftarrow$ Eq. (9)-(16);
  end
  $P(k+1)$ and $Z_j(k) \leftarrow$ Eq. (33);
  $K_j(k) \leftarrow$ Eq. (36);
end

Moreover, if the linear matrix inequality (33) has solutions, the expected filter parameters $K_j(k)$ can be governed by

$$K_j(k) = P(k+1)^{-1} Z_j(k). \tag{36}$$

Proof: Apparently, it can be demonstrated that (22) is guaranteed by (33). Then, the proof is completed. ■

The DETFR protocol-based secure filtering algorithm is given in Algorithm 1 in light of Theorem 2.

IV. Illustrative Examples

To validate the applicability of the proposed DETFR protocol and security fuzzy filter, two numerical examples are subsequently conducted.

Example 1: Consider a system (1) with five sensors. The initial values of state vector are $x(0) = [0.3 \quad 0.3 \quad 0.4 \quad -0.5 \quad 0.5]^T$, and initial values of state estimations are $\hat{x}(0) = [0 \quad 0.5 \quad 0.5 \quad 0.5 \quad 0]^T$. The coefficient matrices are given by

$$A_1(k) = \begin{bmatrix} a_1 & 0 & 0 & 0.2 & 0 \\ -0.1 & 0.6 & 0 & -0.2 & 0 \\ 0.1 & 0.3 & a_3 & 0.5 & 0.25 \\ 0.2 & 0.3 & 0.1 & a_4 & 0.2 \\ 0.4 & 0 & -0.1 & 0.2 & a_5 \end{bmatrix}$$

$$A_2(k) = \begin{bmatrix} a_6 & 0 & 0 & 0.1 & 0 \\ -0.1 & 0.6 & 0 & -0.1 & 0 \\ 0.1 & 0.35 & 0.6 & 0.45 & 0.25 \\ 0.2 & 0.25 & 0.1 & a_7 & 0.15 \\ 0.3 & 0.01 & -0.1 & 0.22 & a_8 \end{bmatrix}$$

$$B_1(k) = [0.1 \quad b_1 \quad 0.1 \quad 0.2 \quad b_2]^T$$
$$B_2(k) = [0.1 \quad 0.15 \quad b_3 \quad 0.2 \quad b_4]^T$$
$$C(k) = \mathrm{diag}\{c_1, c_2, c_3, c_4, c_5\}$$
$$D(k) = [0.2 \quad 0.2 \quad d_3 \quad d_4 \quad d_5]^T$$
$$M_1(k) = \mathrm{diag}\{m_1, 0.015, 0.01, 0.05, m_2\}$$
$$M_2(k) = \mathrm{diag}\{0.01, 0.015, 0.001, m_3, 0.05\}$$
$$G(k) = 0.1 + 0.01\sin(10(k-3))$$

where $a_1 = 0.4 + 0.2\sin(10(k-1))$, $a_3 = 0.6 - 0.05\cos(3(k-1))$, $a_4 = -0.4 - 0.01\sin(4(k-1))$, $a_5 = 0.5 - 0.02\sin(2(k-$

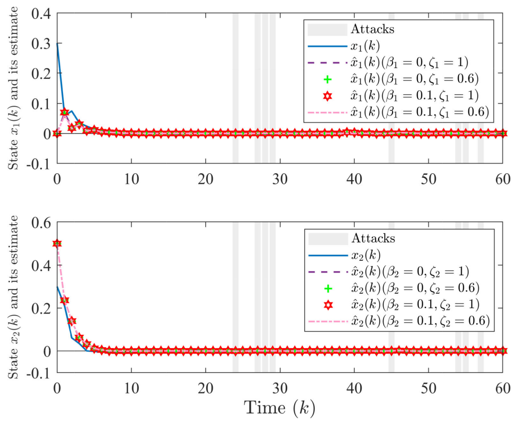


Fig. 2. Curves of states $x_1(k)$ and $x_2(k)$ and their estimations $\hat{x}_1(k)$ and $\hat{x}_2(k)$ under fading measurements and deception attacks.

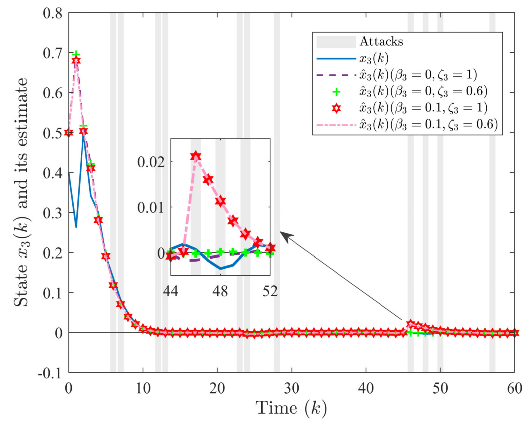


Fig. 3. Curves of state $x_3(k)$ and its estimation $\hat{x}_3(k)$ under fading measurements and deception attacks.

$1)), a_6 = 0.4 + 0.2\sin(10(k-1)), a_7 = -0.4 - 0.01\sin(4(k-1)), a_8 = 0.5 - 0.02\sin(2(k-1)), b_1 = 0.15 - 0.05\cos(2(k-1)), b_2 = 0.1 + 0.2\sin(k-2), b_3 = 0.1 - 0.05\cos(2(k-1)), b_4 = 0.1 + 0.2\sin(k-2), c_1 = 0.5 + 0.3\cos(-2(k-1)), c_2 = 0.5 - 0.1\cos(3(k-1)), c_3 = 0.5 - 0.1\cos(3(k-1)), c_4 = 0.5 + 0.1\sin(2k), c_5 = 0.5 + 0.1\sin(2k), d_3 = 0.17 + 0.27\cos(k), d_4 = 0.2 + 0.1\sin(2k), d_5 = 0.2 + 0.1\sin(2k), m_1 = 0.015 + 0.01\sin(2k), m_2 = 0.011 + 0.01\sin(2k), m_3 = 0.02 + 0.01\sin(2k)$.

The MFs and nonlinear weighting functions are given as: $\underline{u}_1^1 = 1 - e^{[-x_1^2(k)/1.4]}$, $\underline{u}_1^2 = 0.3e^{[-x_1^2(k)/0.2]}$, $\underline{u}_2^1 = 1 - 0.25e^{[-x_1^2(k)/0.4]}$, $\underline{u}_2^2 = 1 - e^{[-x_1^2(k)/3]}$, $\overline{u}_1^1 = 0.25e^{[-x_1^2(k)/0.4]}$, $\overline{u}_1^2 = e^{[-x_1^2(k)/3]}$, $\overline{u}_2^1 = e^{[-x_1^2(k)/1.4]}$, $\overline{u}_2^2 = 1 - 0.3e^{[-x_1^2(k)/0.2]}$, $\overline{o}_g(x(k)) = 1 - \sin^2(x_1(k))$, $\underline{o}_g(x(k)) = 1 - \overline{o}_g(x(k))$.

Take the sampling period $h = 1$ and the time-horizon $T = 60$. Provide the relevant parameters $\gamma = 0.85$, $P_0 = I_{10}$, $Q_0 = 200I_{10}$, $\theta(0) = 50\sqrt{2}$, $w(k) = 0.01\sin(-k+1)$, $\bar{d}_i = 0.5$, $\beta_i = 0.1$ and $v_k = 0.1\sin(-k)$. The attenuation coefficients are given as follows: $\zeta_i = 0.6$ $(i = 1, 2, 3)$, $\zeta_4 = 0.9, \zeta_5 = 0.5$. With the above parameter settings, $e^T(0)(P(0) - \gamma^2 Q(0))e(0) + \theta(0) + (1/\tau)\wp(0) + T||\bar{d}||_2^2 = -104.1210$, then, the sufficient conditions (24) are qualified. Furthermore, choose $N = 5, \vartheta = 3$ and the weighted matrix $\bar{\Omega}(k) = \mathrm{diag}\{0.2, 0.3\}$. We can solve the matrix (33) to obtain the filter parameters by using the algorithm.

To testify to the applicability of the DETFR protocol-based secure filtering algorithm, the four scenarios are discussed: no network-induced phenomenon, only fading measurements, only deception attacks and both fading measurements and deception attacks simultaneously. As can be seen in Figs. 2–5, when attackers launch deception attacks, it will bring an uncertain impact on the system. To be specific, from time 44 to 52 in Fig. 3, the intentional damage caused by deception attacks can be eliminated in a relatively short period. In the meantime, due to multiple factors leading to the signal attenuation phenomenon, a portion of the data will always be lost during transmission. We can clearly see from Figs. 2–5 that the curves of estimations under fading measurements and network attacks can brilliantly follow the curve of the state

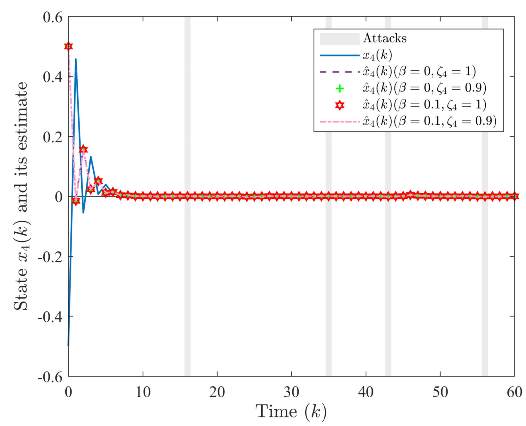


Fig. 4. Curves of state $x_4(k)$ and its estimation $\hat{x}_4(k)$ under fading measurements and deception attacks.

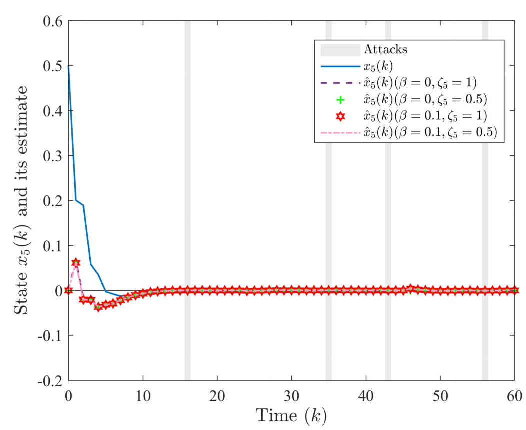


Fig. 5. Curves of state $x_5(k)$ and its estimation $\hat{x}_5(k)$ under fading measurements and deception attacks.

vector. As depicted in Fig. 6, it can arrive that the index predefined in (21) is satisfied for filtering error dynamics, which indicates the excellent performance of the proposed security filter.

Choose the parameters related to DET condition $\mu = 0.4$, $\tau = 30, \psi = 0.7$ and $\wp(0) = 1$. Moreover, the SET mechanism in [45] will be established by $\tau \to \infty$ in (4). According to the DETFR protocol proposed in this article,

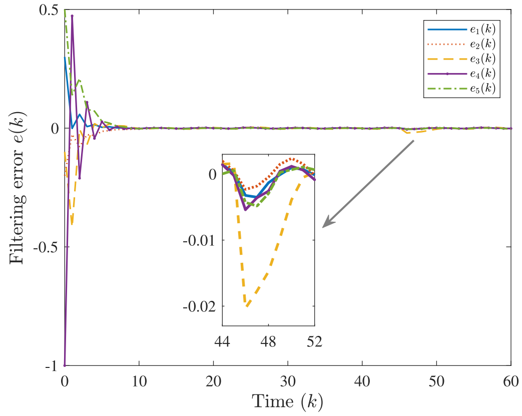


Fig. 6. Filtering error $e(k)$ in Example 1.

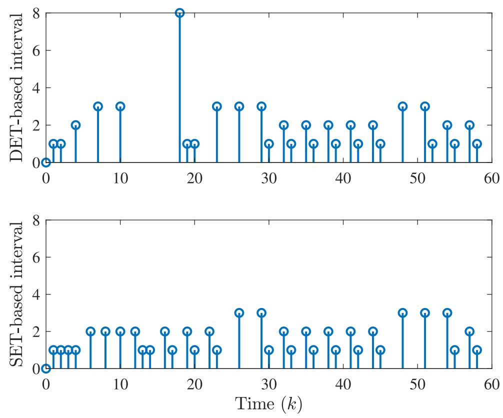


Fig. 7. Release instants of DET and SET strategies.

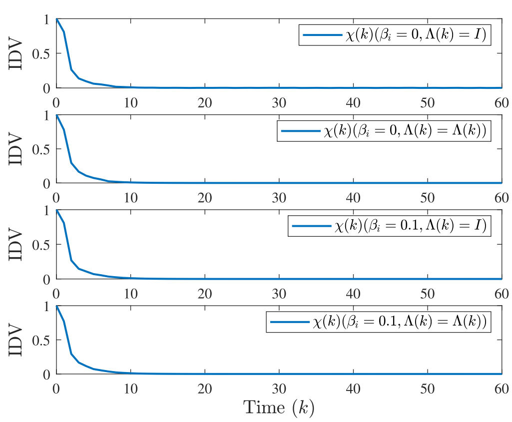


Fig. 8. IDVs $\wp(k)$.

TABLE I
COMPARISON OF THE SET AND DET MECHANISMS

	SET ($\tau \to \infty$)	DET ($\tau = 30$)
Release package	35	29
Transmission rate	58.33%	48.33%

Figs. 7 and 8 plot the triggering instants of nodes applied the DET and SET strategies, and IDVs, respectively. The number of releases under two mechanisms is presented in Table I. In light of Fig. 7, we can see that, compared with the SET protocol, the DET mechanism can significantly reduce network redundancy. In Fig. 8, observing precisely the IDVs for four cases, we can conclude that the decay rate is related to the fading measurements. The triggered threshold can be dynamically adjusted under the influence of IDVs.

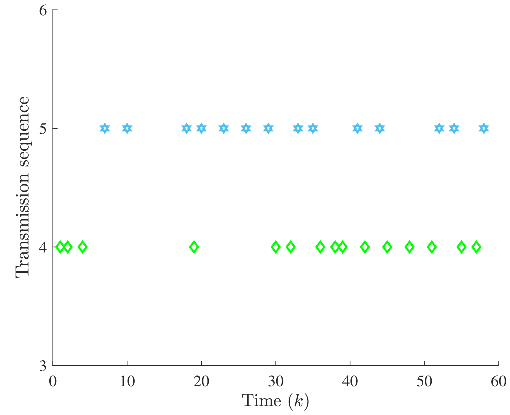


Fig. 9. Selected signal with DETFR protocol.

Fig. 9 plots the distribution diagram of nodes 4 and 5 accessing the network. According to the obtained results, it is commendably discovered that the efficiency of using the network for the four nodes is 51.72%, while the fifth node is 48.28%. These results highlight that the TOD scheduling rule relies on the weight coefficients given by us and the difference between the measurement outputs of the triggering instant and the value of the transmission moment. Meaningfully, the fading phenomenon and DET mechanism may have a certain influence on the scheduling process. In a realistic industry, depending on the importance, nodes may or may not need to set priorities, which means that nodes with higher priorities also need to network more times. Nevertheless, sometimes it is necessary to combine the two strategies in complex and large networks. Additionally, it is worth pointing out that only lists the sequence of nodes scheduled according to the TOD protocol, without the sequence of nodes adopting the RR protocol. According to Assumption 1, in the SS of FR protocol, signals are transmitted by predefined schedules, which are not subjected to external influences. In light of the HRC network, the SS is configured on interval $(k, k+1)$, and the DS is configured at instant k $(k = 0, 1, \ldots, T-1)$. The scheduling sequence of the RR protocol is invariant during each period. However, the TOD protocol needs to determine the nodes that use the network each time instant on the basis of the weighted matrix and measurement outputs. Therefore, according to the simulation results, the effectiveness has been proven.

Example 2: Consider an electric circuit model as the researcher object (motivated by [46]), and take the sampling period $T_s = 0.2s$. Assuming that $x_1(t) \in [-5, 5]$, the corresponding MFs and system parameters are chosen according to the Euler discretization method

$$\underline{\varsigma}_1(x_1(k)) = \frac{0.5x_1^2(k)}{25}, \overline{\varsigma}_1(x_1(k)) = \frac{x_1^2(k)}{25}$$
$$\underline{\varsigma}_2(x_1(k)) = 1 - \overline{\varsigma}_1(x_1(k)), \overline{\varsigma}_2(x_1(k)) = 1 - \underline{\varsigma}_1(x_1(k))$$

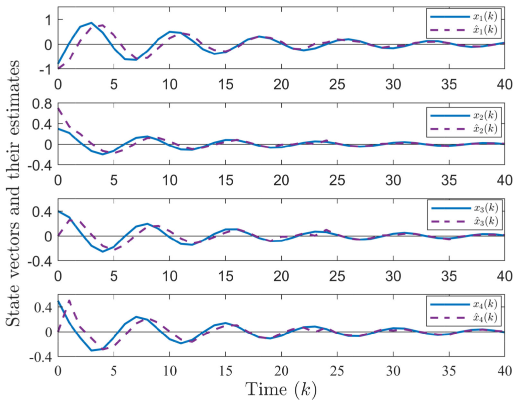


Fig. 10. Actual state $x(k)$ and corresponding estimated vector $\hat{x}(k)$.

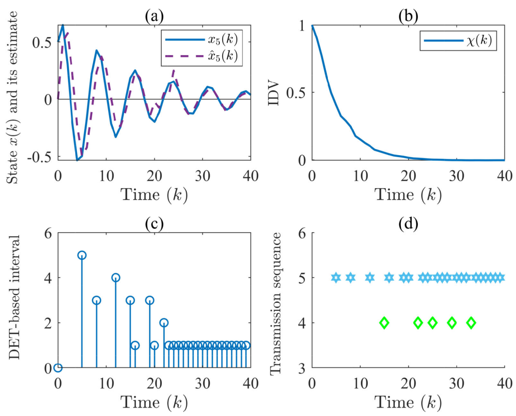


Fig. 11. (a) Actual state $x_5(k)$ and corresponding estimated vector $\hat{x}_5(k)$. (b) IDV $\wp(k)$. (c) Data triggering instants in Example 2. (d) Selected signal with DETFR protocol.

$$A_i = \begin{bmatrix} a_i & 0.5 & 0.5 & 0.5 & 0.5 \\ -0.2 & 0.2 & 0 & 0 & 0 \\ -0.25 & 0 & 0.25 & 0 & 0 \\ -0.5 & 0 & 0 & -0.5 & 0 \\ -0.5 & 0 & 0 & 0 & 0.5 \end{bmatrix}, (i = 1, 2)$$

$$C = \begin{bmatrix} 0.1 & 0 & 0 & 0 & 0 \\ 0 & 0.2 & 0 & 0 & 0 \\ 0 & 0 & 0.1 & 0 & 0 \\ 0.1 & 0 & 0.1 & 0.2 & 0 \\ 0.2 & 0 & 0.1 & 0 & 0.2 \end{bmatrix}$$

$$a_1 = 0.54, a_2 = 1.02$$

$$B_1 = B_2 = [0 \quad 0.2 \quad 0.15 \quad 0.2 \quad 0.3]^T$$

$$D = [0.2 \quad 0.3 \quad 0.4 \quad 0.3 \quad 0.2]^T$$

$$M_1 = M_2 = \text{diag}\{0.015, 0.015, 0.01, 0.05, 0.011\}.$$

The curves of system state and filter error are depicted in Figs. 10–12, where the state trajectories can be tracked well by their estimations, and the release instants and scheduled order of DETFR protocol are shown in the third and fourth figures of Fig. 11, which further illustrates the effectiveness of the proposed algorithm.

V. Conclusion

In this article, the DETFR protocol-based secure filtering issue for IT-2 fuzzy systems over a finite-horizon has been addressed. A novel DETFR scheme that can further alleviate resource constraints has been proposed while being subjected to network attacks and fading measurements. To reflect the real practice, it is presumed that deception attacks in the HRC network are stochastic and the fading measurements also occur randomly in a known interval because of the complicated and confused environments. Taking into consideration the limited network resources, the different segments are configured to different protocols and data-holding strategies (ZI and ZOH). By adopting the matrix augmentation approach, the high-rate is transmitted to single-rate. After that, the filter parameters and errors are obtained through the algorithm, and several sufficient conditions for the filtering error dynamics to reach the specified disturbance attenuation level are given. Besides, two simulation examples are presented to prove the availability of the DETFR protocol-based secure filtering algorithm. In future research, the proposed algorithm will be attempted for multiagent systems and cyber-physical systems.

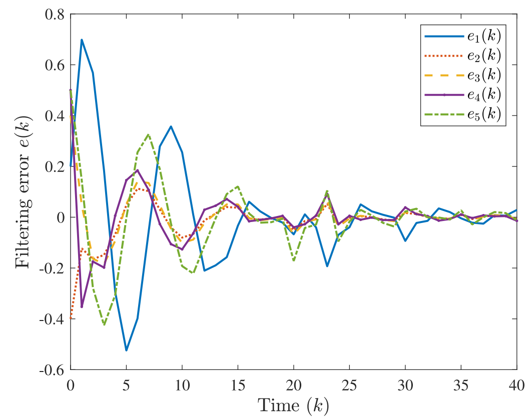


Fig. 12. Filtering error $e(k)$ in Example 2.

Appendix

The parameters in Theorem 1 are as follows:

$$\Upsilon_{11}^{gj} = \begin{bmatrix} \Psi_{11} & \Psi_{12} & \Psi_{13} & 0 & 0 & 0 \\ * & \Psi_{22} & \Psi_{23} & 0 & 0 & 0 \\ * & * & \Psi_{33} & 0 & 0 & 0 \\ * & * & * & -I_d & 0 & 0 \\ * & * & * & * & -(\frac{1}{\tau}+\varphi)I_q & 0 \\ * & * & * & * & * & \Psi_{66} \end{bmatrix}$$

$$\begin{aligned} \Psi_{11} \triangleq\ & \theta(k+1) - \theta(k) + \frac{\mu}{\tau}\hat{x}^T(k)(\check{C}_1^T C_1 + \check{C}_2^T\check{C}_2)\hat{x}(k) \\ & + \varphi\mu\hat{x}^T(k)(\check{C}_1^T C_1 + \check{C}_2^T\check{C}_2)\hat{x}(k) + \hat{x}^T(k)(\bar{M}_g(k) \\ & - \bar{M}_j(k))^T(\bar{M}_g(k) - \bar{M}_j(k))\hat{x}(k) \\ \Psi_{12} \triangleq\ & +\frac{\mu}{\tau}\hat{x}^T(k)(\check{C}_1^T\check{C}_1 + \check{C}_2^T\check{C}_2) + \varphi\mu\hat{x}^T(k)(\check{C}_1^T\check{C}_1 \\ & + \check{C}_2^T\check{C}_2) + \hat{x}^T(k)(\bar{M}_g(k) - \bar{M}_j(k))^T\bar{M}_g(k) \\ \Psi_{13} \triangleq\ & +\frac{\mu}{\tau}\hat{x}^T(k)\check{C}_1^T\check{D} + \varphi\mu\hat{x}^T(k)\check{C}_1^T\check{D} \\ \Psi_{22} \triangleq\ & -P(k) + \bar{M}_g^T(k)\bar{M}_g(k) + \frac{\mu}{\tau}(\check{C}_1^T\check{C}_1 + \check{C}_2^T\check{C}_2) \\ & + \varphi\mu(\check{C}_1^T\check{C}_1 + \check{C}_2^T\check{C}_2) \end{aligned}$$

$$\Psi_{23} \triangleq \frac{\mu}{\tau}\check{C}_1^T\check{D} + \varphi\mu\check{C}_1^T\check{D}, \Psi_{66} \triangleq -\frac{1}{\tau}(1-\psi-\varphi)$$
$$\Psi_{33} \triangleq -\gamma^2 I_{\bar{\omega}} + \mu(\frac{1}{\tau}+\varphi)\check{D}^T\check{D}$$
$$\Upsilon_{12}^{gj} = \begin{bmatrix} \hat{x}(k)\mathscr{A}^{gj} & 0 & 0 & 0 \\ \Theta_{21} & \Theta_{22} & \Theta_{23} & \Theta_{24} \\ \Theta_{31} & \Theta_{32} & 0 & 0 \\ \Theta_{41} & \Theta_{42} & 0 & 0 \\ \Theta_{51} & \Theta_{52} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$
$$\Theta_{21} \triangleq (\mathscr{A}_1^{gT} - \tilde{C}_1^T K_j^T(k))P(k+1), \bar{\mathscr{A}}_2 \triangleq \begin{bmatrix} 0 & \bar{\tilde{C}}_2^T \end{bmatrix}^T$$
$$\Theta_{22} \triangleq (\bar{\mathscr{A}}_3^T - \bar{\tilde{C}}_3^T K_j^T(k))P(k+1), \bar{\mathscr{A}}_3 \triangleq \begin{bmatrix} 0 & \bar{\tilde{C}}_3^T \end{bmatrix}^T$$
$$\Theta_{23} \triangleq (\bar{\mathscr{A}}_2^T - \bar{\tilde{C}}_2^T K_j^T(k))P(k+1), \bar{\mathscr{A}}_4 \triangleq \begin{bmatrix} 0 \; \bar{\tilde{C}}_4^T \end{bmatrix}^T$$
$$\Theta_{24} \triangleq (\bar{\mathscr{A}}_4^T - \bar{\tilde{C}}_4^T K_j^T(k))P(k+1), \bar{\mathscr{B}}_2 \triangleq \begin{bmatrix} 0 & \bar{\tilde{D}}_2^T \end{bmatrix}^T$$
$$\Theta_{31} \triangleq (\mathscr{B}_1^{gT} - \tilde{D}_1^T K_j^T(k))P(k+1), \theta_k \triangleq \frac{\theta_0}{\sqrt{k+1}}$$
$$\Theta_{32} \triangleq (\bar{\mathscr{B}}_2^T - \bar{\tilde{D}}_2^T K_j^T(k))P(k+1), \bar{\tilde{E}}_2 \triangleq [0 \quad \bar{E}_2^T]^T$$
$$\Theta_{41} \triangleq (\tilde{\Gamma}_1^T - \Gamma_1^T K_j^T(k))P(k+1), \bar{\Gamma}_2 \triangleq [-\rho_7 \quad -\rho_8]$$
$$\Theta_{42} \triangleq (\bar{\tilde{\Gamma}}_2^T - \bar{\Gamma}_2^T K_j^T(k))P(k+1), \bar{\tilde{\Gamma}}_2 \triangleq [0 \; \bar{\Gamma}_2^T]^T$$
$$\Theta_{51} \triangleq (\tilde{E}_1^T - E_1^T K_j^T(k))P(k+1), \bar{E}_2 \triangleq [-\rho_7 \; -\rho_8]$$
$$\Theta_{52} \triangleq (\bar{\tilde{E}}_2^T - \bar{E}_2^T K_j^T(k))P(k+1), \check{C}_1 \triangleq [\bar{\Lambda}C(k) \quad 0]$$
$$\bar{\tilde{C}}_2 \triangleq [\rho_5\tilde{\Lambda}^{[1]}C^{[1]} + \rho_6\tilde{\Lambda}^{[2]}C^{[2]} \quad 0], \check{C}_2 \triangleq [\tilde{\Lambda}C(k) \quad 0]$$
$$\bar{\tilde{C}}_3 \triangleq [\rho_7\bar{\Lambda}^{[1]}C^{[1]} + \rho_8\bar{\Lambda}^{[2]}C^{[2]} \quad 0], \check{D} \triangleq [D(k) \quad 0 \quad 0]$$
$$\bar{\tilde{C}}_4 \triangleq [\rho_7\tilde{\Lambda}^{[1]}C^{[1]} + \rho_8\tilde{\Lambda}^{[2]}C^{[2]} \quad 0], \bar{\beta} \triangleq \sqrt{\beta-\beta^2}$$
$$\tilde{D}_2 \triangleq [\rho_7 D^{[1]} + \rho_8 D^{[2]} \; \rho_7 G^{[1]} \; I_2\rho_8 G^{[2]}]$$
$$\Upsilon_{22}^{gj} = \mathrm{diag}\{-P(k+1), -P(k+1), -P(k+1), -P(k+1)\}$$
$$\tilde{\Lambda}^{[1]} \triangleq \mathrm{diag}\left\{\tilde{\lambda}_1, \tilde{\lambda}_2, \ldots, \tilde{\lambda}_\vartheta\right\}, \rho_7 \triangleq I_1\Phi_{\xi_1}\bar{\beta}^{[1]}$$
$$\tilde{\Lambda}^{[2]} \triangleq \mathrm{diag}\left\{\tilde{\lambda}_{\vartheta+1}, \tilde{\lambda}_{\vartheta+2}, \ldots, \tilde{\lambda}_N\right\}, \rho_8 \triangleq \bar{\beta}I_2\Phi_{\xi_2}$$
$$\bar{\beta}^{[1]} \triangleq \mathrm{diag}\left\{\sqrt{\beta_1-\beta_1^2}, \sqrt{\beta_2-\beta_2^2}, \ldots, \sqrt{\beta_\vartheta-\beta_\vartheta^2}\right\}.$$

REFERENCES

[1] I. Ahmad, X. Ge, and Q.-L. Han, "Communication-constrained active suspension control for networked in-wheel motor-driven electric vehicles with dynamic dampers," *IEEE Trans. Intell. Veh.*, vol. 7, no. 3, pp. 590–602, Sep. 2022.

[2] Y. Zhang, C. Peng, C. Cheng, and Y.-L. Wang, "Attack intensity dependent adaptive load frequency control of interconnected power systems under malicious traffic attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 2, pp. 1223–1235, Mar. 2023.

[3] Z. Miao, H. Zhong, J. Lin, Y. Wang, Y. Chen, and R. Fierro, "Vision-based formation control of mobile robots with FOV constraints and unknown feature depth," *IEEE Trans. Control Syst. Technol.*, vol. 29, no. 5, pp. 2231–2238, Sep. 2021.

[4] Z. Wang, D. Xue, and F. Pan, "Admissible H_∞ control of fuzzy singular fractional order multi-agent systems with external disturbances," *IEEE Trans. Autom. Sci. Eng.*, early access, Mar. 30, 2023, doi: 10.1109/TASE.2023.3261891.

[5] J. Cheng, J. H. Park, and Z.-G. Wu, "Observer-based asynchronous control of nonlinear systems with dynamic event-based try-once-discard protocol," *IEEE Trans. Cybern.*, vol. 52, no. 12, pp. 12638–12648, Dec. 2022.

[6] J. Liu, J. Ke, J. Liu, X. Xie, and E. Tian, "Secure event-triggered control for IT-2 fuzzy networked systems with stochastic communication protocol and FDI attacks," *IEEE Trans. Fuzzy Syst.*, vol. 32, no. 3, pp. 1167–1180, Mar. 2024.

[7] X. Wang, J. H. Park, H. Yang, X. Zhang, and S. Zhong, "Delay-dependent fuzzy sampled-data synchronization of T-S fuzzy complex networks with multiple couplings," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 1, pp. 178–189, Jan. 2020.

[8] Y. Zeng, H.-K. Lam, B. Xiao, and L. Wu, "L_2-L_∞ control of discrete-time state-delay interval type-2 fuzzy systems via dynamic output feedback," *IEEE Trans. Cybern.*, vol. 52, no. 6, pp. 4198–4208, Jun. 2022.

[9] H. Geng, Z. Wang, A. Mousavi, F. E. Alsaadi, and Y. Cheng, "Outlier-resistant filtering with dead-zone-like censoring under try-once-discard protocol," *IEEE Trans. Signal Process.*, vol. 70, pp. 714–728, Jan. 2022.

[10] J. Jiao, H. L. Trentelman, and M. K. Camlibel, "$\mathcal{H}_2$ and $\mathcal{H}_\infty$ suboptimal distributed filters design for linear systems," *IEEE Trans. Autom. Control*, vol. 68, no. 4, pp. 2560–2567, Apr. 2023.

[11] D. Bhattacharjee and K. Subbarao, "Set-membership filter for discrete-time nonlinear systems using state-dependent coefficient parameterization," *IEEE Trans. Autom. Control*, vol. 67, no. 2, pp. 894–901, Feb. 2022.

[12] F. Han, Z. Wang, H. Dong, and H. Liu, "Partial-nodes-based scalable H_∞-consensus filtering with censored measurements over sensor networks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 51, no. 3, pp. 1892–1903, Mar. 2021.

[13] H. Liu, Z. Wang, W. Fei, and J. Li, "Resilient H_∞ state estimation for discrete-time stochastic delayed memristive neural networks: A dynamic event-triggered mechanism," *IEEE Trans. Cybern.*, vol. 52, no. 5, pp. 3333–3341, May 2022.

[14] W. Song, Z. Wang, Z. Li, H. Dong, and Q.-L. Han, "Protocol-based particle filtering for nonlinear complex networks: Handling non-gaussian noises and measurement censoring," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 1, pp. 128–139, Jan./Feb. 2023.

[15] L. Zou, Z. Wang, J. Hu, and H. Gao, "On H_∞ finite-horizon filtering under stochastic protocol: Dealing with high-rate communication networks," *IEEE Trans. Autom. Control*, vol. 62, no. 9, pp. 4884–4890, Sep. 2017.

[16] Y. Shen, Z. Wang, B. Shen, F. E. Alsaadi, and A. M. Dobaie, "L_2-L_∞ state estimation for delayed artificial neural networks under high-rate communication channels with round-robin protocol," *Neural Netw.*, vol. 124, pp. 170–179, Apr. 2020.

[17] D. Liu, G.-H. Yang, and M. J. Er, "Event-triggered control for T–S fuzzy systems under asynchronous network communications," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 2, pp. 390–399, Feb. 2020.

[18] K. Zhang, R. Su, H. Zhang, and Y. Tian, "Adaptive resilient event-triggered control design of autonomous vehicles with an iterative single critic learning framework," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 32, no. 12, pp. 5502–5511, Dec. 2021.

[19] X. Li, X. Yang, and J. Cao, "Event-triggered impulsive control for nonlinear delay systems," *Automatica*, vol. 117, Jul. 2020, Art. no. 108981.

[20] A. Girard, "Dynamic triggering mechanisms for event-triggered control," *IEEE Trans. Autom. Control*, vol. 60, no. 7, pp. 1992–1997, Jul. 2015.

[21] W. Chen, Z. Wang, D. Ding, G. Ghinea, and H. Liu, "Distributed formation-containment control for discrete-time multiagent systems under dynamic event-triggered transmission scheme," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 53, no. 2, pp. 1308–1319, Feb. 2023.

[22] J. Chen, B. Chen, and Z. Zeng, "Adaptive dynamic event-triggered fault-tolerant consensus for nonlinear multiagent systems with directed/undirected networks," *IEEE Trans. Cybern.*, vol. 53, no. 6, pp. 3901–3912, Jun. 2023.

[23] 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.

[24] H. Yang, C. Peng, and Z. Cao, "Attack-model-independent stabilization of networked control systems under a jump-like TOD scheduling protocol," *Automatica*, vol. 152, Jun. 2023, Art. no. 110982.

[25] J. Wang and Y. Song, "Resilient RMPC for Cyber-physical systems with polytopic uncertainties and state saturation under TOD scheduling: An ADT approach," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4900–4908, Jul. 2020.

[26] J. Wang, C. Yang, J. Xia, Z.-G. Wu, and H. Shen, "Observer-based sliding mode control for networked fuzzy singularly perturbed systems under weighted try-once-discard protocol," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 6, pp. 1889–1899, Jun. 2022.

[27] Y. Tang, D. Zhang, D. W. C. Ho, and F. Qian, "Tracking control of a class of cyber-physical systems via a FlexRay communication network," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1186–1199, Apr. 2019.

[28] W. Xiong, D. W. C. Ho, and S. Wen, "A periodic iterative learning scheme for finite-iteration tracking of discrete networks based on FlexRay communication protocol," *Inf. Sci.*, vol. 548, pp. 344–356, Feb. 2021.

[29] 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.

[30] S. Liu, Z. Wang, L. Wang, and G. Wei, "Recursive set-membership state estimation over a FlexRay network," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 52, no. 6, pp. 3591–3601, Jun. 2022.

[31] S. Hu, D. Yue, C. Dou, X. Xie, Y. Ma, and L. Ding, "Attack-resilient event-triggered fuzzy interval type-2 filter design for networked nonlinear systems under sporadic denial-of-service jamming attacks," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 1, pp. 190–204, Jan. 2022.

[32] A. Basit, M. Tufail, M. Rehan, M. Riaz, and I. Ahmed, "Distributed state and unknown input estimation under denial-of-service attacks: A dynamic event-triggered approach," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 70, no. 6, pp. 2266–2270, Jun. 2023.

[33] J. Cheng, J. Xu, J. H. Park, and M. V. Basin, "Protocol-based load frequency control for power systems with nonhomogeneous sojourn probabilities," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 53, no. 9, pp. 5742–5750, Sep. 2023.

[34] Y. Yu, W. Yang, W. Ding, and J. Zhou, "Reinforcement learning solution for cyber-physical systems security against replay attacks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2583–2595, 2023.

[35] Z.-W. Liu, Y.-L. Shi, H. Yan, B.-X. Han, and Z.-H. Guan, "Secure consensus of multiagent systems via impulsive control subject to deception attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 70, no. 1, pp. 166–170, Jan. 2023.

[36] X. Gao, F. Deng, C.-Y. Su, and P. Zeng, "Protocol-based fuzzy control of networked systems under joint deception attacks," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 3, pp. 1052–1063, Mar. 2023.

[37] W. Yu, D. Huang, and N. Qin, "Resilient coordinated data-driven control of multiple high-speed trains under fading measurements and denial-of-service attacks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 5690–5701, May 2023.

[38] Y. Wang, Z. Wang, L. Zou, and H. Dong, "Nonfragile dissipative fuzzy PID control with mixed fading measurements," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 11, pp. 5019–5033, Nov. 2022.

[39] M. Zhu, T. Sui, and R. Wang, "Distributed Kalman filtering over sensor networks with fading measurements and random link failures," *J. Frankl. Inst.*, vol. 360, no. 4, pp. 2457–2475, 2023.

[40] D. Zhao, Z. Wang, D. Ding, and G. Wei, "$\mathcal{H}_\infty$ PID control with fading measurements: The output-feedback case," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 6, pp. 2170–2180, Jun. 2020.

[41] X. Bu, J. Song, F. Huo, and F. Yang, "Dynamic event-triggered resilient state estimation for time-varying complex networks with Markovian switching topologies," *ISA Trans.*, vol. 127, pp. 50–59, Aug. 2022.

[42] J. Wang, Y. Gao, Z. Feng, G. Sun, J. Liu, and L. Wu, "Asynchronous sliding mode control under round-robin protocol-based event-triggered communication," *IEEE Trans. Control Netw. Syst.*, vol. 10, no. 3, pp. 1424–1435, Sep. 2023.

[43] Y. Yang, Y. Niu, and H.-K. Lam, "Sliding-mode control for interval type-2 fuzzy systems: Event-triggering WTOD scheme," *IEEE Trans. Cybern.*, vol. 53, no. 6, pp. 3771–3781, Jun. 2023.

[44] J. Wang, Y. Song, and G. Wei, "Security-based resilient robust model predictive control for polytopic uncertain systems subject to deception attacks and RR protocol," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 52, no. 8, pp. 4772–4783, Aug. 2022.

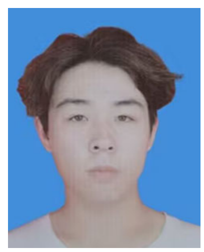
[45] N. Rong, Z. Wang, X. Xie, and S. Ding, "Event-triggered Synchronization for discrete-time neural networks with unknown delays," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 10, pp. 3296–3300, Oct. 2021.

[46] X.-H. Chang, Z.-M. Li, and J. H. Park, "Fuzzy generalized $\mathcal{H}_2$ filtering for nonlinear discrete-time systems with measurement quantization," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 12, pp. 2419–2430, Dec. 2018.

Jian Liu (Member, IEEE) received the Ph.D. degree in signal and information processing from the College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China, in 2018.

He is currently an Associate Professor with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing. He has published more than 40 articles in refereed international journals. His research interests include cyber–physical systems, networked control systems, complex dynamical networks, intelligent optimization algorithms, and network security.

Dr. Liu received the Reward of Outstanding Reviewer for many international journals, such as *Computer Networks* and *Journal of Computational Science*. He has been serving as the Guest Editor for the Special Issue: "*Fuzzy Modeling and Fuzzy Control Systems in Mathematics*" since August 2022.



Shuailong Wang received the B.S. degree in information security from Zhongyuan University of Technology, Zhengzhou, China, in 2022. He is currently pursuing the M.S. degree in computer science and technology with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, China.

His research interests include communication networks, networked control systems, and secure control and filtering.

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

He was a Postdoctoral Research Associate with the School of Automation, Southeast University, Nanjing, China, from December 2013 to June 2016. He was a Visiting Researcher/Scholar with the Department of Mechanical Engineering, University of Hong Kong, Hong Kong, from October 2016 to October 2017. He was a Visiting Scholar with the Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea, from November 2017 to January 2018. From June 2011 to May 2023, he was an Associate Professor and then a Professor with Nanjing University of Finance and Economics, Nanjing. In June 2023, he joined 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 the 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 IEEE TRANSACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON FUZZY SYSTEMS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *International Journal of Fuzzy Systems*, and *International Journal of Control, Automation, and Systems*.

Engang Tian (Senior Member, IEEE) received the B.S. degree in mathematics from Shandong Normal University, Jinan, China, in 2002, the M.Sc. degree in operations research and cybernetics from Nanjing Normal University, Nanjing, China, in 2005, and the Ph.D. degree in control theory and control engineering from Donghua University, Shanghai, China, in 2008.

From 2011 to 2012, he was a Postdoctoral Research Fellow with 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. He has published more than 100 papers in refereed international journals. His research interests include networked control systems, cyber attack, as well as nonlinear stochastic control and filtering.