Secure State Estimation for Interval Type-2 Fuzzy Systems With FDI Attacks and Event-Triggered WTOD Protocol

Lijuan Zha, Tao Huang, Jinliang Liu, *Senior Member, IEEE*, Engang Tian, Xiangpeng Xie, *Senior Member, IEEE*, and Chen Peng, *Senior Member, IEEE*

***Abstract*—The article designs a secure co-estimation approach for nonlinear systems with false data injection (FDI) attack and network bandwidth limitations, which is described by interval type-2 (IT2) fuzzy system. For mitigating communication load and avoiding network data collision, an event-triggered weighted try-once-discard protocol is implemented to adjust the data transmission frequency. Given the unknown system state and FDI attacks, both of the state observer and the attack observer are put forward. Besides, a new attack compensation controller is proposed under co-design of the observer of the state and FDI attack. The asymptotical stability of the augmented system can be realized by the proposed sufficient conditions for the existence of the fuzzy observer and controller gains, while the prescribed H_∞ performance requirement can be met. Then the secure controller design method is given accordingly. Finally, the validity of the attained results are provided by simulation examples.**

***Index Terms*—Event-triggered control, false data injection attacks (FDI), interval type-2 fuzzy system, weighted try-once discard protocol.**

I. Introduction

DUE TO the higher and higher requirements of industrial automation and control precision, the control objects are constantly changing and expanding to complex nonlinear systems. The existence of the nonlinearity makes the controlled system analysis and design become harder. Nowadays, the Takagi–Sugeno (T–S) fuzzy modeling method is Widely recognized as an effective approach in charactering the nonlinear systems [1], [2], [3]. With membership functions (MFs) and if-then rules, nonlinear networked control systems (NCSs) can be approximated by several linear subsystems [4]. Nowadays, interval type-1 (IT1) fuzzy model and interval type-2 (IT2) fuzzy model are two types of models representing the nonlinear systems [5], [6], [7]. Compared with the former, the advantage of the latter type lies in its flexibility, which can handle the uncertainty in nonlinear systems by the lower and upper MFs [8]. Some control or filtering approach for IT2 fuzzy systems have been proposed, such as the model-predictive control in [9], finite frequency fault detection filter design in [10] and fault-tolerant control in [11] for interval IT2 fuzzy system. Therefore, control or filtering approaches for T-S fuzzy systems continue to receive attention.

As is known, event-triggering control (ETC) is an prominent method to reduce network communication, the key of which is to reasonably utilize limited network resources (LNR) by managing information transmission frequency and controller execution frequency [12], [13], [14]. Compared with the conventional periodic sampling strategy, the execution of control tasks under the event-triggering mechanism (ETM) depends on the designed event-triggering conditions instead of the fixed time [15], [16], [17]. Therefore, benefiting from ETM, the consumption of computing and LNR can be relieved effectively while maintaining the control performance. So far, a variety of ETMs have been proposed for nonlinear NCSs [18], [19], [20]. For example, to deal with output feedback issues, a novel estimate-based control strategy is designed under the dynamic event-triggering (DET) strategy in [21]. In [22], the DET-based integral sliding-mode controller is presented for nonlinear NCSs by robust adaptive dynamic programming. However, the issue of security-ensured DET combined with try-once-discard protocol are rarely investigated for nonlinear network systems.

In addition to the ETMs, various network scheduling protocols are also efficient methods to make reasonable and effective use of LNR [23], [24], [25]. Network communication protocols are usually used to control the transmission order of data, so as to achieve the purpose of reasonable allocation of LNR [26], [27]. Up to now, many different communication

Received 9 June 2024; revised 13 February 2025; accepted 10 May 2025. Date of publication 22 May 2025; date of current version 21 July 2025. This work was supported in part by the National Natural Science Foundation of China under Grant 62273174 and Grant 62373252; in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20230063; and in part by the Startup Foundation for Introducing Talent of NUIST under Grant 2024r063. This article was recommended by Associate Editor F. Xiao. *(Corresponding author: Jinliang Liu.)*

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

Tao Huang is with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China (e-mail: huangtao0117@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).

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).

Xiangpeng Xie is with the School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China, (e-mail: xiexiangpeng1953@163.com).

Chen Peng is with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, China (e-mail: c.peng@shu.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSMC.2025.3569725.

Digital Object Identifier 10.1109/TSMC.2025.3569725

protocols have been applied in nonlinear NCSs [28], [29]. Compared with other protocols, the data transmission sequence regulated by weighted try-once-discard (WTOD) protocol depends on the maximum weight error of sensor points, which has the advantage of initiative and flexibility. At present, WTOD protocol are highly applied in security controller design [30] and sliding-mode control problem [31]. However, WTOD protocol and DET strategy are rarely simultaneously considered which motivates the current brief.

In the nonlinear NCSs, besides the bandwidth constraint, network security is another problem that has received extensive attention [32], [33], [34]. Due to the open and fragile characteristics of the network, the nonlinear NCSs may compromise with malicious attacks by hackers, resulting in destruction of the transmitted signal authenticity and integrity [35], [36], [37], [38], [39]. In NCSs, there exist different security threats in communication networks, such as false data injection (FDI) attacks [40], [41] and denial-of-service (DoS) attacks [42], [43]. FDI attacks destroy the authenticity of data by injecting malicious data into nonlinear NCSs [44]. In [45], the FDI and DoS attacks are considered in designing the resilient control method for multiarea load frequency control systems. The distributed estimation problem is studied in [46] for multiarea power systems against FDI attacks. Given that the DET strategy, the WTOD protocol and the FDI attacks are not constructed in a framework in the mentioned results. The secure co-estimation problem for nonlinear NCSs is still open and needs to be discussed.

In this article, the secure co-estimation and control approach is proposed for nonlinear NCSs subject to LNR and FDI attacks based on IT2 fuzzy model. In contrast to the existing works, the method proposed in this article exhibits good robustness and has the following significant advantages.

1) For easing the network transmission burden, a novel DETTOD protocol is proposed for the nonlinear networked systems under the effect of FDI attacks, under which only one group is accessible to transmit signals over the communication network at the triggering instant. Compared with some existing results [21], [45], the data collisions can be avoided.
2) For the IT2 fuzzy model, considering the DETTOD protocol and the FDI attacks, the observers of state and FDI attacks are co-designed and a new observer-based attack compensation controller is presented to ensure the expected system performance while the negative effects of the FDI attacks is suppressed. Different from [30], the developed observer-based controller can automatically estimate and compensate for FDI attacks without extra restrictions on FDI attacks, which has great advantages to avoid the adverse effect of FDI attacks.

Notation: $\mathbb{R}^m$ stands for the m-dimensional Euclidean space, I is the identity matrix of appropriate dimensions and 0 represents the zero matrix of compatible dimensions. The superscript T stands for matrix transposition. The symbol diag$\{\dots\}$ represents a block-diagonal matrix and $*$ stands for the symmetric term in a symmetric block matrix. $||\cdot||$ is the Euclidean norm of a vector and its induced norm of a matrix. The arguments of functions are sometimes simplified, for example, $h_i(x(k))g_j(\hat{x}(k))$ is donated by $h_{ij}(k)$.

II. Problem Description

A. Interval Type-2 T-S Fuzzy Model

In this article, the ith rule of the IT-2 fuzzy model is

Plant Rule i:

IF ϑ_{1x} is W_1^i, ϑ_{2x} is W_2^i, $\dots$, ϑ_{lx} is W_l^i,

THEN

$$\begin{cases} x(k+1) = A_i x(k) + B_i(u(k) + a(k)) + D_i\omega(k) \\ y(k) = C_i x(k) \\ z(k) = M_i x(k), i = 1, \dots, s \end{cases} \tag{1}$$

where $\vartheta_{vx} = \vartheta_v(x(k))$, W_d^i represents the fuzzy set corresponding to $\vartheta_d(k)$, in which $i = 1, 2, \dots, s$, $d = 1, 2, \dots, l$, $x(k) \in \mathbb{R}^{n_x}$, $u(k) \in \mathbb{R}^{n_u}$, $y(k) \in \mathbb{R}^{n_y}$, $z(k) \in \mathbb{R}^{n_z}$ and $\omega(k) \in \mathbb{L}_2[0, \infty)$ are the system state, the control input, the measurement output, the control output and the disturbance input, respectively. $a(k) \in \mathbb{R}^{n_u}$ represents the unknown FDI attack signal. A_i, B_i, C_i, D_i, and M_i are known constant matrices and B_i is assumed to be full column.

For the ith rule, the firing strength h_{ix} belongs to the interval set S_i with $S_i = [\underline{h}_{ix}, \overline{h}_{ix}]$, where $\underline{h}_{ix} = \prod_{d=1}^{l} \underline{W}_d^i(\vartheta_{dx})$ and $\overline{h}_{ix} = \prod_{d=1}^{l} \overline{W}_d^i(\vartheta_{dx})$ stand for the lower and upper membership value, respectively. In addition, $\overline{W}_d^i(\vartheta_{dx}) \in [0, 1]$ and $\underline{W}_d^i(\vartheta_{dx}) \in [0, 1]$ are the lower and upper MFs, respectively.

The model of the overall system (1) is inferred as

$$\begin{cases} x(k+1) = \sum_{i=1}^{s} h_{ix}[A_i x(k) + B_i(u(k) + a(k)) \\ \qquad\qquad +D_i\omega(k)] \\ y(k) = \sum_{i=1}^{s} h_{ix} C_i x(k) \\ z(k) = \sum_{i=1}^{s} h_{ix} M_i x(k) \end{cases} \tag{2}$$

where

$$h_{ix} = \frac{\varrho_{ix}}{\sum_{i=1}^{s} \varrho_{ix}}$$

which is the normalized membership and satisfies $h_{ix} \geq 0$ and $\sum_{i=1}^{s} h_{ix} = 1$. $\varrho_{ix} = \underline{\alpha}_{ix}\underline{h}_{ix} + \overline{\alpha}_{ix}\overline{h}_{ix}$, in which $0 \leq \underline{\alpha}_{ix} \leq 1$ and $0 \leq \overline{\alpha}_{ix} \leq 1$ are the nonlinear weighting functions (NWFs) with $\underline{\alpha}_{ix} + \overline{\alpha}_{ix} = 1$.

Remark 1: In this article, the interaction channel between the actuator and controller are assumed to be attacked by hackers injecting FDI attacks, resulting in abnormal noise added to the normal control signal or loss of the normal control signal. Therefore, the attack signal $a(k)$ is used in this article to describe the corresponding negative impacts.

B. DETTOD Protocol

In NCSs, the issue of LNR may cause data collisions and network congestion, significantly degrade system performance, and even destabilize the system. Given this, a novel scheduling protocol is presented to determine whether the signals of sensor nodes will be transmitted through a communication network with bandwidth constraints. Specifically, partition sensor measurement $y(k) = [y_1(k), y_2(k), \dots, y_{n_y}(k)]$, the transmitted sensor measurements should satisfy the DET condition first, whether or not the component $y_i(k), i = 1, \dots, n_y$ will be sent into network is governed by WTOD protocol.

To reduce unnecessary channel occupancy and save LNR, a new DET strategy is implemented between sensors and observers. Then, we define the following ETM:

$$t_{n+1} = \min_{k\in\mathbb{N}^+}\{k|k > t_n, \psi(k) \geq 0\} \tag{3}$$

where $\psi(k) = \chi^T(k)\Omega\chi(k) - \sigma(t_n)y^T(k)\Omega y(k)$ and $\chi(k) = y(k) - y(t_n)$, $k \in [t_n, t_{n+1})$. Among them, $y(k)$ is the current sampled signal and $y(t_n)$ is the latest triggering measurement signal. $\sigma(t_n) \in (0, 1)$ and $\Omega > 0$ are the event-triggered threshold and the weighting matrix, respectively.

The threshold variable $\sigma(t_n)$ in (3) is designed as

$$\begin{cases} \sigma(t_n) = \lambda \cdot g(t_n) \\ g(t_n) = 1 - \frac{1}{1+\beta\cdot e^{-\left(||x(t_n)||-||x(t_{n-1})||\right)}} \end{cases} \tag{4}$$

with $\lambda \in (0, 1]$ and $\beta > 0$ being given constants.

It is observed from (3) that the measuring signal will be granted transfer permission if and only if the condition $\psi(k) \geq 0$ holds.

Remark 2: The event-triggered threshold $\sigma(t_n)$ shown in (4) can vary with the change of state evolution. When $||x(t_n)|| < ||x(t_{n-1})||$, it means the system state tends to be stable, then $\sigma(t_n)$ will increase and the trigger frequency will decrease. $||x(t_n)|| \geq ||x(t_{n-1})||$ indicates the system state is unstable, under this case, $\sigma(t_n)$ will reduce and the sampled state will easily be triggered. Therefore, the dynamic ETM threshold $\sigma(t_n)$ designed in this work can help enhance the adaptivity of the ETM. In addition, λ and $\beta > 0$ are pregiven in practice.

For the purpose of further relieve the data collisions, WTOD protocol is introduced to identify the sensor nodes that are granted access to the network. Under WTOD protocol, only one triggered components $y_i(t_n)$ can pass through the communication network. By utilizing a zero-order holder (ZOH), the updated rule of the observer input is

$$\bar{y}_i(k) = \begin{cases} y_i(t_n), & i = \delta(t_n) \\ \bar{y}_i(k-1), & \text{otherwise.} \end{cases} \tag{5}$$

where $\delta(t_n)$ denotes the corresponding sensor point obtains the permission of data transmission at the moment t_n, and $\delta(t_n)$ can be expressed as

$$\delta(t_n) = \arg\max_{1\leq i\leq n_y} (y_i(t_n) - \bar{y}_i(k-1))^T Q_i (y_i(t_n) - \bar{y}_i(k-1)) \tag{6}$$

where Q_i is a known matrix and $\bar{y}_i(t_{n-1})$ stands for the last transmitted signal.

Define

$$\iota(i) = \begin{cases} 0, & i \neq 0 \\ 1, & i = 0. \end{cases} \tag{7}$$

Under the proposed DETTOD protocol's update principle (3), (5), and (6), $\bar{y}(k)$ is expressed as

$$\bar{y}(k) = \Phi_{\delta(t_n)}y(t_n) + \left(I - \Phi_{\delta(t_n)}\right)\bar{y}(k-1) \tag{8}$$

where $\Phi_i \triangleq \text{diag}\{\iota(i-1)I, \iota(i-2)I, \ldots, \iota(\delta(t_n) - n_y)I\}$ $(1 \leq \delta(t_n) \leq n_y)$.

Remark 3: Different from the existing event triggered mechanisms, the DETTOD protocol in this article can further reduce the transmission amount and avoid data collisions. The DETTOD protocol is proposed by organically combining the merits of DET strategy and WTOD protocol. If the current data $y(t_n)$ is triggered by the DET strategy (3), the triggered signal $y(t_n)$ will be scheduled by the WTOD protocol. Only one component $y_i(t_n)$ with the largest weighted error from the last reported value can be permitted to be sent for transmission. Thus, the occurrences of network congestions can be effectively avoided.

Remark 4: Here, the DETTOD protocol is employed to deal with the issue of limited communication capacity in the controlled system. It should be mentioned that this protocol can also be extended to regulate the signal transmission in the fault-tolerant control problem in [11] and the fault estimation for fuzzy systems in [7], which will be our future work.

C. FDI Attacks Model

Similar to [47], the FDI attack signal $a(k)$ in (1) is represented as

$$\begin{cases} \eta(k+1) = E\eta(k) \\ a(k) = F\eta(k) \end{cases} \tag{9}$$

where $\eta(k) \in \mathbb{R}^{n_\eta}$, $E \in \mathbb{R}^{n_\eta\times n_\eta}$ and $F \in \mathbb{R}^{n_u\times n_\eta}$.

Remark 5: In this article, the FDI attack model (9) under consideration is more universal by comparison with some existing models [40], [45], [46]. Specifically, the attacker destroys the transmitted signal by arbitrarily controlling the matrices E and F. As a Hurwitz matrix, the matrix E is usually chosen to limit the bounds of the injected signal $a(k)$. Furthermore, in an effort to make the research more convincing, it is assumed here that all the underlying system information is possible to be maliciously accessed by FDI attackers.

D. Observer-Based Fuzzy Controller

For handling the influences of DETTOD protocol and FDI attacks, the form of the fuzzy controller are designed as

Controller Rule j:

IF $\epsilon_{1\hat{x}}$ is N_1^j, $\epsilon_{2\hat{x}}$ is N_2^j, ..., $\epsilon_{p\hat{x}}$ is N_p^j,

THEN

$$\begin{cases} \hat{x}(k+1) = A_j\hat{x}(k) + B_j(u(k) + a(k)) + L_{j,\delta(t_n)}\left(C_j\hat{x}(k) - \bar{y}(k)\right) \\ \hat{y}(k) = C_j\hat{x}(k) \\ u(k) = K_{j,\delta(t_n)}C_j\hat{x}(k) - \hat{a}(k), j = 1, \ldots, s \end{cases} \tag{10}$$

where $\epsilon_{w\hat{x}} = \epsilon_w(\hat{x}(k))$ $\hat{x}(k)$ is the state estimate, $u(k)$ is the compensation controller under the effect of FDI attacks and $\delta(t_n) = 1, 2, \ldots, n_y$. $L_{j,\delta(t_n)}$ and $K_{j,\delta(t_n)}$ stand for the fuzzy observer gains and the fuzzy controller gains to be devised, respectively.

Denoted the following interval sets as the firing strength of the jth rule:

$$T_j = [\underline{g}_{j\hat{x}}, \overline{g}_{j\hat{x}}]$$

where $\underline{g}_{j\hat{x}} = \prod_{b=1}^{p} \underline{N}_b^j(\epsilon_{b\hat{x}})$ and $\overline{g}_{j\hat{x}} = \prod_{b=1}^{p} \overline{N}_b^j(\epsilon_{b\hat{x}})$ stand for the lower and upper membership value, respectively. In addition, $\overline{N}_b^j(\epsilon_{b\hat{x}}) \in [0,1]$ and $\underline{N}_b^j(\epsilon_{b\hat{x}}) \in [0,1]$ are the lower and upper MFs, respectively.

Thus, the overall observer-based fuzzy controller is formulated as

$$\begin{cases} \hat{x}(k+1) = \sum_{j=1}^{s} g_{j\hat{x}}[A_j\hat{x}(k) + B_j(u(k)+a(k)) \\ \qquad +L_{j,\delta(t_n)}\big(C_j\hat{x}(k) - \bar{y}(k)\big)] \\ \hat{y}(k) = \sum_{j=1}^{s} g_{j\hat{x}}C_j\hat{x}(k) \\ u(k) = \sum_{j=1}^{s} g_{j\hat{x}}[K_{j,\delta(t_n)}C_j\hat{x}(k) - \hat{a}(k)] \end{cases} \tag{11}$$

where

$$g_{j\hat{x}} = \frac{\kappa_{j\hat{x}}}{\sum_{j=1}^{s}\kappa_{j\hat{x}}}$$

which is the normalized membership and satisfies $g_{j\hat{x}} \geq 0$ and $\sum_{j=1}^{s} g_{j\hat{x}} = 1$. Besides, $\kappa_{j\hat{x}} = \underline{c}_{j\hat{x}}\underline{g}_{j\hat{x}} + \overline{c}_{j\hat{x}}\overline{g}_{j\hat{x}}$, in which $\underline{c}_{j\hat{x}}$ and $\overline{c}_{j\hat{x}}$ taking values in $[0,1]$ are NWFs with $\underline{c}_{j\hat{x}} + \overline{c}_{j\hat{x}} = 1$ and the attack estimation $\hat{a}(k) = F\hat{\eta}(k)$.

E. FDI Attacks Observer

In an effort to estimate the magnitude of unknown FDI attack signal $a(k)$, the intermediate variable $\eta(k)$ in (9) should be estimated. Obviously, the solution of system (9) is unique under given initial conditions. Thus, for a given matrix $G_{\delta(t_n)}$, there is a unique solution $m = m(k)$ denoted by

$$m(k) = \eta(k) - G_{\delta(t_n)}\hat{x}(k) \tag{12}$$

for the following system,

$$\begin{aligned} m(k+1) = \sum_{j=1}^{s} g_{j\hat{x}}[&\big(E - G_{\delta(t_{n+1})}B_jF\big)m(k) \\ &+\big(EG_{\delta(t_n)} - G_{\delta(t_{n+1})}A_j \\ &-G_{\delta(t_{n+1})}B_jFG_{\delta(t_n)}\big)\hat{x}(k) - G_{\delta(t_{n+1})}B_ju(k) \\ &-G_{\delta(t_{n+1})}L_{j,\delta(t_n)}\big(C_j\hat{x}(k) - \bar{y}(k)\big)] \end{aligned} \tag{13}$$

which can be derived from (2), (9), (11), and (12).

Assume that there exists a unique solution to (13), the solution $\eta = \eta(k)$ of (9) can be determined uniquely with

$$\eta(k) = m(k) + G_{\delta(t_n)}\hat{x}(k). \tag{14}$$

Based on the previous analysis, the designed indirect-attack observer can described as

$$\begin{cases} \hat{m}(k+1) = \sum_{j=1}^{s} g_{j\hat{x}}[\big(E - G_{\delta(t_{n+1})}B_jF\big)\hat{m}(k) \\ \qquad +\big(EG_{\delta(t_n)} - G_{\delta(t_{n+1})}A_j \\ \qquad -G_{\delta(t_{n+1})}B_jFG_{\delta(t_n)}\big)\hat{x}(k) - G_{\delta(t_{n+1})}B_ju(k) \\ \qquad -G_{\delta(t_{n+1})}L_{j,\delta(t_n)}\big(C_j\hat{x}(k) - \bar{y}(k)\big)] \\ \hat{\eta}(k+1) = \hat{m}(k+1) + G_{\delta(t_{n+1})}\hat{x}(k+1), \\ \qquad j = 1,\ldots,s,\ \delta(t_n) = 1,2,\ldots,n_y. \end{cases} \tag{15}$$

Define $e_x(k) = x(k) - \hat{x}(k)$ and $e_\eta(k) = \eta(k) - \hat{\eta}(k)$. According to (2), (9), (11), (13), and (15), it can be inferred that

$$\begin{aligned} x(k+1) = \sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)[&\big(A_i + B_iK_{j,\delta(t_n)}C_j\big)x(k) \\ &- B_iK_{j,\delta(t_n)}C_je_x(k) + B_iFe_\eta(k) + D_i\omega(k)] \end{aligned} \tag{16}$$

$$\begin{aligned} \hat{x}(k+1) = \sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)[&\big(A_j + B_jK_{j,\delta(t_n)}C_j \\ &+L_{j,\delta(t_n)}C_j - L_{j,\delta(t_n)}\Phi_{\delta(t_n)}C_i\big)x(k) \\ &+ \big(-A_j - B_iK_{j,\delta(t_n)}C_j - L_{j,\delta(t_n)}C_j\big)e_x(k) \\ &+ B_jFe_\eta(k) + L_{j,\delta(t_n)}\Phi_{\delta(t_n)}\chi(k) \\ &- L_{j,\delta(t_n)}\big(I - \Phi_{\delta(t_n)}\big)\bar{y}(k-1)] \end{aligned} \tag{17}$$

$$\begin{aligned} e_\eta(k+1) &= m(k+1) - \hat{m}(k+1) \\ &= \sum_{j=1}^{s} g_{j\hat{x}}[\big(E - G_{\delta(t_{n+1})}B_jF\big)e_\eta(k)] \end{aligned} \tag{18}$$

$$\begin{aligned} e_x(k+1) = \sum_{i=1}^{s}\sum_{j=1}^{s} &h_{ij}(k)\{[\big(A_i - A_j\big) + (B_i \\ &- B_j)K_{j,\delta(t_n)}C_j + L_{j,\delta(t_n)}\big(\Phi_{\delta(t_n)}C_i - C_j\big)]x(k) \\ &+ [\big(A_j - (B_i - B_j)K_{j,\delta(t_n)}C_j + L_{j,\delta(t_n)}C_j\big)] \\ &e_x(k) + \big(B_i - B_j\big)Fe_\eta(k) - L_{j,\delta(t_n)}\Phi_{\delta(t_n)}\chi(k) \\ &+ L_{j,\delta(t_n)}\big(I - \Phi_{\delta(t_n)}\big)\bar{y}(k-1) + D_i\omega(k)\}. \end{aligned} \tag{19}$$

Based on (16)–(18), we can derive:

$$\begin{cases} \xi(k+1) = \sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)[\vec{A}_{ij,\delta(t_n)}\xi(k) \\ \qquad +\vec{B}_{j,\delta(t_n)}\chi(k) + \vec{D}_i\omega(k)] \\ z(k) = \sum_{i=1}^{s} h_{ix}M_ix(k) \end{cases} \tag{20}$$

where

$$\xi(k) = [x^T(k) \quad \bar{y}^T(k-1) \quad e_x^T(k) \quad e_\eta^T(k)]^T$$

$$\vec{A}_{ij,\delta(t_n)} = \begin{bmatrix} \Pi_{11} & 0 & -B_iK_{j,\delta(t_n)}C_j & B_iF \\ \Phi_{\delta(t_n)}C_i & \Gamma(t_n) & 0 & 0 \\ \Pi_{31} & \Pi_{32} & \Pi_{33} & \Pi_{34} \\ 0 & 0 & 0 & \Pi_{44} \end{bmatrix}$$

$$\vec{B}_{j,\delta(t_n)} = \begin{bmatrix} 0 \\ -\Phi_{\delta(t_n)} \\ -L_{j,\delta(t_n)}\Phi_{\delta(t_n)} \\ 0 \end{bmatrix}, \vec{D}_i = \begin{bmatrix} D_i \\ 0 \\ D_i \\ 0 \end{bmatrix}$$

$$\begin{aligned} \Pi_{11} &= A_i + B_iK_{j,\delta(t_n)}C_j,\ \Gamma(t_n) = I - \Phi_{\delta(t_n)} \\ \Pi_{31} &= \big(A_i - A_j\big) + \big(B_i - B_j\big)K_{j,\delta(t_n)}C_j + L_{j,\delta(t_n)} \\ &\quad \big(\Phi_{\delta(t_n)}C_i - C_j\big) \\ \Pi_{32} &= L_{j,\delta(t_n)}\Gamma(t_n) \\ \Pi_{33} &= A_j - \big(B_i - B_j\big)K_{j,\delta(t_n)}C_j + L_{j,\delta(t_n)}C_j \\ \Pi_{34} &= \big(B_i - B_j\big)F,\ \Pi_{44} = E - G_{\delta(t_{n+1})}B_jF. \end{aligned}$$

Definition 1: For any $\zeta > 0$, the mean-square stability of (20) is said to be achieved if there exists $M(\zeta) > 0$ such that $||\xi(k)||^2 < \zeta$, $k > 0$ when $||\xi(0)||^2 < M(\zeta)$. In addition, the global mean-square asymptotical stability is ensured if $\lim ||\xi(k)||^2 = 0$ for any initial condition.

In the following, we are devoted to investigate the control method of nonlinear NCSs (2) with DETTOD protocol under FDI attacks. With the designed observer-based controller, the following requirements are satisfied.

1) The asymptotical stability of (20) is achieved when $\omega(k) \equiv 0$.
2) Under the zero-initial condition, the below condition holds

$$\sum_{k=0}^{\infty} ||z(k)||^2 < \gamma^2 \sum_{k=0}^{\infty} ||\omega(k)||^2. \tag{21}$$

III. Main Results

Note that the imperfectly matched MFs of controlled plant (2) and the observed-based controller (11) lead to the existence of $\sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)$ in (19) and (20). For handling this, similar to [15], we define the lower and the global upper bound of $h_{ij}(k)$ as $\underline{u}_{ij}$ and $\overline{u}_{ij}$. The slack matrices $\underline{R}_{ij} \geq 0$ and $\overline{R}_{ij} \geq 0$ satisfy the conditions as follow:

$$\sum_{i=1}^{s}\sum_{j=1}^{s}\Big(h_{ij}(k) - \underline{u}_{ij}\Big)\underline{R}_{ij} \geq 0 \tag{22}$$

$$\sum_{i=1}^{s}\sum_{j=1}^{s}\big(\overline{u}_{ij} - h_{ij}(k)\big)\overline{R}_{ij} \geq 0. \tag{23}$$

Next, to achieve the stability of the addressed system, a sufficient condition will be developed in Theorem 1. Afterward, the co-design method of the state observer gains $L_{j,\delta(t_n)}$, the attack observer gains $G_{\delta(t_n)}$ and controller gains $K_{j,\delta(t_n)}$ will be acquired in Theorem 2.

Theorem 1: For given $\Omega > 0$, $\lambda \in (0, 1]$, the state observer gains $L_{j,\delta(t_n)}$, the attack observer gains $G_{\delta(t_n)}$, controller gains $K_{j,\delta(t_n)}$ and predefined H_∞ performance index γ, the system (20) is globally mean-square asymptotically stable and performance constraint (21) is achieved if there exist scalars $\mu_q(k) > 0$, matrices $\underline{R}_{ij} > 0$, $\overline{R}_{ij} > 0$ and $P_r > 0$ with $i, j = 1, 2, \ldots, s$ and $r = 1, 2, \ldots, n_y$, such that

$$\Xi_{ij,r} - \overline{R}_{ij} + \underline{R}_{ij} + \sum_{i=1}^{s}\sum_{j=1}^{s}\Big(\overline{u}_{ij}\overline{R}_{ij} - \underline{u}_{ij}\underline{R}_{ij}\Big) < 0 \tag{24}$$

where

$$\Xi_{ij,r} = \begin{bmatrix} \Xi_{i,r}^{11} & * & * & * \\ \Xi^{21} & \Xi^{22} & * & * \\ 0 & 0 & -\gamma^2 I & * \\ \vec{A}_{ij,r} & \vec{B}_{j,r} & \vec{D}_i & -P_{r+1}^{-1} \end{bmatrix}$$

$$\Xi_{i,r}^{11} = -P_r + \lambda H_1^T C_i^T \Omega C_i H_1 + H_1^T M_i^T M_i H_1 - \sum_{q=1}^{n_y} \mu_q(k)(C_i H_1 - H_2)^T \tilde{Q}_q (C_i H_1 - H_2)$$

$$\Xi^{21} = -\sum_{q=1}^{n_y} \mu_q(k)\tilde{Q}_q(C_i H_1 - H_2)$$

$$\Xi^{22} = -\Omega - \sum_{q=1}^{n_y} \mu_q(k)\tilde{Q}_q$$

$$H_1 = \begin{bmatrix} I & 0 & 0 & 0 \end{bmatrix}$$

$$\tilde{Q}_q = \bar{Q}_q - \bar{Q}_r, \bar{Q}_q \triangleq \operatorname{diag}\{Q_1, \ldots, Q_{n_y}\}\Phi_q$$

$$H_2 = \begin{bmatrix} 0 & I & 0 & 0 \end{bmatrix}, r = \delta(t_n).$$

Proof: Construct a Lyapunov–Krasovskii function as

$$V(k) = \xi^T(k) P_r \xi(k). \tag{25}$$

From (20), one can derive

$$\begin{aligned} \triangle V(k) &= V(k+1) - V(k) \\ &= \sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)\Big[\vec{A}_{ij,r}\xi(k) + \vec{B}_{j,r}\chi(k) + \vec{D}_i\omega(k)\Big]^T P_{r+1}\Big[\vec{A}_{ij,r}\xi(k) \\ &\quad + \vec{B}_{j,r}\chi(k) + \vec{D}_i\omega(k)\Big] - \xi^T(k)P_r\xi(k). \end{aligned} \tag{26}$$

Noting (6), we have

$$\begin{aligned} &(y_r(t_n) - \bar{y}_r(k-1))^T Q_r (y_r(t_n) - \bar{y}_r(k-1)) \\ &\geq \big(y_q(t_n) - \bar{y}_q(k-1)\big)^T Q_q \big(y_q(t_n) - \bar{y}_q(k-1)\big) \end{aligned} \tag{27}$$

and it further indicates

$$\begin{aligned} &(y(t_n) - \bar{y}(k-1))^T \bar{Q}_r (y(t_n) - \bar{y}(k-1)) \\ &\geq (y(t_n) - \bar{y}(k-1))^T \bar{Q}_q (y(t_n) - \bar{y}(k-1)). \end{aligned} \tag{28}$$

Based on (1), (3), and (28), we can concluded that

$$\begin{aligned} &\big[C_i x(k) - \chi(k) - \bar{y}(k-1)\big]^T \times \big(\bar{Q}_q - \bar{Q}_r\big) \\ &\times \big[C_i x(k) - \chi(k) - \bar{y}(k-1)\big] \leq 0. \end{aligned} \tag{29}$$

In light of (3), (26), and (29), we can get

$$\begin{aligned} \triangle V(k) \leq &\sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)\Big[\vec{A}_{ij,r}\xi(k) \\ &+ \vec{B}_{j,r}\chi(k) + \vec{D}_i\omega(k)\Big]^T P_{r+1} \\ &\Big[\vec{A}_{ij,r}\xi(k) + \vec{B}_{j,r}\chi(k) + \vec{D}_i\omega(k)\Big] - \xi^T(k)P_r\xi(k) \\ &- \chi^T(k)\Omega\chi(k) + \lambda\xi^T(k)H_1^T C_i^T \Omega C_i H_1 \xi(k) \\ &- \sum_{q=1}^{n_y} \mu_q(k)[(C_i H_1 - H_2)\xi(k) - \chi(k)]^T \\ &\big(\bar{Q}_q - \bar{Q}_r\big)[(C_i H_1 - H_2)\xi(k) - \chi(k)]. \end{aligned} \tag{30}$$

According to schur complement, it can derive that

$$\Delta V(k) \leq \tau^T(k)\Big(\bar{\Xi}_{i,r} + \tilde{\Upsilon}_{ij,r}^T P_{r+1}^{-1} \tilde{\Upsilon}_{ij,r}\Big)\tau(k) \tag{31}$$

where

$$\tau^T(k) = \begin{bmatrix} \xi^T(k) & \chi^T(k) & \omega^T(k) \end{bmatrix}$$

$$\bar{\Xi}_{i,r} = \begin{bmatrix} \Xi_{i,r}^{11} & * & * \\ \Xi^{21} & \Xi^{22} & * \\ 0 & 0 & -\gamma^2 I \end{bmatrix}$$

$$\tilde{\Upsilon}_{ij,r} = \Big[\vec{A}_{ij,r} \quad \vec{B}_{j,r} \quad \vec{D}_i\Big].$$

For any nonzero $\omega(k)$, H_∞ performance requirement of the augmented system (20) will be taken into account under the zero-initial condition. From (22), (23), and (30), it can follows that:

$$\begin{aligned} &\Delta V(k) + z^T(k)z(k) - \gamma^2\omega^T(k)\omega(k) \\ &= \sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)\tau^T(k)\Xi_{ij,r}\tau(k) \\ &\leq \sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)\tau(k)\Bigg[\Xi_{ij,r} + \underline{R}_{ij} - \overline{R}_{ij} \\ &\quad + \sum_{o=1}^{s}\sum_{t=1}^{s}\big(\overline{u}_{ot}\overline{R}_{ot} - \underline{u}_{ot}\underline{R}_{ot}\big)\Bigg]\tau(k). \end{aligned} \tag{32}$$

Apparently, from (24) and (32), we can derive H_∞ performance (21) is held.

When $\omega(k) \equiv 0$, we can get from (31) that

$$\Delta V(k) \leq \sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)\bar{\tau}^T(k)\Big(\tilde{\Xi}_{ij,r} + \Upsilon_{ij,r}^T P_{r+1}^{-1}\Upsilon_{ij,r}\Big)\bar{\tau}(k) \tag{33}$$

where

$$\bar{\tau}(k) = \begin{bmatrix}\xi^T(k) & \chi^T(k)\end{bmatrix}^T$$
$$\tilde{\Xi}_{ij,r} = \begin{bmatrix}\Xi_{i,r}^{11} & * \\ \Xi^{21} & \Xi^{22}\end{bmatrix}, \Upsilon_{ij,r} = \begin{bmatrix}\tilde{A}_{ij,r} & \tilde{B}_{j,r}\end{bmatrix}.$$

One can easily derive $\Delta V(k) < 0$ with $\omega(k) \equiv 0$ from (24) and (33). Therefore, the augmented system can be inferred to be asymptotically stable by the Lyapunov theory.

This completes the proof.

Based on the sufficient conditions in Theorem 1, next, we will present the co-design method of the state observer gains, the attack observer gains and controller gains.

Theorem 2: For given $\Omega > 0$, $\lambda \in (0, 1]$, system (20) is be globally mean-square asymptotically stable and performance constraint (21) is guaranteed if there exist scalars $\mu_q(k) > 0$, $\underline{R}_{ij} > 0$, $\overline{R}_{ij} > 0$, $P_r = \text{diag}\{P_{1,r}, P_{2,r}, P_{3,r}, P_{4,r}\} > 0$, $K_{j,r}$, $L_{j,r}$ and G_r for any $i, j = 1, 2, \ldots, s$ and $r = 1, 2, \ldots, n_y$, such that

$$\Psi_{ij,r} - \overline{R}_{ij} + \underline{R}_{ij} + \sum_{i=1}^{s}\sum_{j=1}^{s}\Big(\overline{u}_{ij}\overline{R}_{ij} - \underline{u}_{ij}\underline{R}_{ij}\Big) < 0 \tag{34}$$

where

$$\Psi_{ij,r} = \begin{bmatrix}\bar{\Psi}_{i,r} & * \\ \tilde{\Upsilon}_{ij,r} & P_{r+1} - 2I\end{bmatrix}$$
$$\bar{\Psi}_{i,r} = \begin{bmatrix}\Psi_{11} & * & * & * & * & * \\ 0 & \Psi_{22} & * & * & * & * \\ 0 & 0 & -P_{3,r} & * & * & * \\ 0 & 0 & 0 & -P_{4,r} & * & * \\ \Psi_{51} & \Psi_{52} & 0 & 0 & \Psi_{55} & * \\ 0 & 0 & 0 & 0 & 0 & -\gamma^2 I\end{bmatrix}$$
$$\Psi_{11} = -P_{1,r} + \lambda C_i^T \Omega C_i + M_i^T M_i - \sum_{q=1}^{n_y}\mu_q(k) C_i^T \tilde{Q}_q C_i$$
$$\Psi_{22} = -P_{2,r} - \sum_{q=1}^{n_y}\mu_q(k)\tilde{Q}_q$$
$$\Psi_{51} = \sum_{q=1}^{n_y}\mu_q(k)\tilde{Q}_q C_i, \Psi_{52} = -\sum_{q=1}^{n_y}\mu_q(k)\tilde{Q}_q$$
$$\Psi_{55} = -\Omega - \sum_{q=1}^{n_y}\mu_q(k)\tilde{Q}_q.$$

Proof: In light of (20) and (24), we can get

$$\bar{\Psi}_{i,r} + \tilde{\Upsilon}_{ij,r}^T P_{r+1}\tilde{\Upsilon}_{ij,r} \leq \sum_{i=1}^{s}\sum_{j=1}^{s} h_{ij}(k)\Big(\bar{\Psi}_{i,r} + \tilde{\Upsilon}_{ij,r}^T P_{r+1}\tilde{\Upsilon}_{ij,r}\Big) \tag{35}$$

TABLE I
UPPER AND LOWER MFs OF (2)

Lower bounds	Upper bounds
$\underline{W}_{1x_1}^1 = 1 - e^{-\frac{x_1^2(k)}{1.2}}$	$\overline{W}_{1x_1}^1 = 0.25e^{-\frac{x_1^2(k)}{0.4}}$
$\underline{W}_{2x_1}^1 = 1 - 0.25e^{-\frac{x_1^2(k)}{0.2}}$	$\overline{W}_{2x_1}^1 = e^{-\frac{x_1^2(k)}{1.6}}$
$\underline{W}_{1x_1}^2 = 0.4e^{-\frac{x_1^2(k)}{0.3}}$	$\overline{W}_{1x_1}^2 = e^{-\frac{x_1^2(k)}{2.4}}$
$\underline{W}_{2x_1}^2 = 1 - e^{-\frac{x_1^2(k)}{2.4}}$	$\overline{W}_{2x_1}^2 = 1 - 0.4e^{-\frac{x_1^2(k)}{0.3}}$

where

$$\tilde{\Upsilon}_{ij,r} = \begin{bmatrix}\vec{A}_{ij,r} & \vec{B}_{j,r} & \vec{D}_i\end{bmatrix}.$$

According to Schur complement, $\Psi_{ij,r} < 0$ is equivalent to

$$\begin{bmatrix}\bar{\Psi}_{i,r} & * \\ \tilde{\Upsilon}_{ij,r} & -P_{r+1}^{-1}\end{bmatrix} < 0 \tag{36}$$

where

$$-P_{r+1}^{-1} = \text{diag}\{-P_{1,r+1}^{-1}, -P_{2,r+1}^{-1}, -P_{3,r+1}^{-1}, -P_{4,r+1}^{-1}\}.$$

Obviously, the fact of

$$(P_{r+1} - I)^T P_{r+1}^{-1}(P_{r+1} - I) \geq 0$$

implies

$$P_{r+1} - 2I \geq -P_{r+1}^{-1}.$$

Based on the above related reasoning, the condition (34) can be ensured. This completes the proof.

IV. NUMERICAL SIMULATION

In this section, the derived control method will be applied to a numerical example and a practical example with aim to validate the effectiveness the developed method on IT2 systems with FDI attacks and DETTOD protocol.

Example 1: Consider system (1) with parameters as

$$A_1 = \begin{bmatrix}0.8506 & 0.2093 \\ -0.4039 & 0.5167\end{bmatrix}, A_2 = \begin{bmatrix}0.6632 & 0.2583 \\ -0.3909 & 0.6537\end{bmatrix}$$
$$B_1 = \begin{bmatrix}0.3129 & 0.2521 \\ 0.2148 & 0.4133\end{bmatrix}, B_2 = \begin{bmatrix}0.4205 & 0.1576 \\ 0.2147 & 0.4389\end{bmatrix}$$
$$C_1 = \begin{bmatrix}2.5 & -1.2 \\ -1.6 & 2\end{bmatrix}, C_2 = \begin{bmatrix}2.4 & -1.2 \\ -1.5 & 2\end{bmatrix}$$
$$D_1 = \begin{bmatrix}0.3121 & 0.2153 \\ 0.0156 & 0.3224\end{bmatrix}, D_2 = \begin{bmatrix}0.4181 & 0.1114 \\ 0.0265 & 0.2131\end{bmatrix}$$
$$M_1 = \begin{bmatrix}0.5789 & -0.1850\end{bmatrix}, M_2 = \begin{bmatrix}0.6062 & -0.4630\end{bmatrix}$$

and the initial conditions are set to be $x(0) = [0.2 \quad -0.1]^T$ and $\hat{x}(0) = [0 \quad 0]^T$. Besides, the upper and lower MFs of (2) and (11) are given in Tables I and II. Let

$$\underline{\alpha}_{ix} = 1 - \cos^2(x_1(k)), \overline{\alpha}_{ix} = 1 - \underline{\alpha}_{ix}$$
$$\underline{c}_{i\hat{x}} = 1 - \cos^2(\hat{x}_1(k)), \overline{c}_{i\hat{x}} = 1 - \underline{c}_{i\hat{x}}.$$

TABLE II
UPPER AND LOWER MFS OF (11)

Lower bounds	Upper bounds
$\underline{N}^1_{1x_1} = e^{-\frac{x_1^2(k)}{0.6}}$	$\overline{N}^1_{1x_1} = \underline{N}^1_1(x_1(k))$
$\underline{N}^1_{2x_1} = e^{-\frac{x_1^2(k)}{0.6}}$	$\overline{N}^1_{2x_1} = \underline{N}^1_2(x_1(k))$
$\underline{N}^2_{1x_1} = e^{-\frac{x_1^2(k)}{0.4}}$	$\overline{N}^2_{1x_1} = \underline{N}^2_1(x_1(k))$
$\underline{N}^2_{2x_1} = e^{-\frac{x_1^2(k)}{0.4}}$	$\overline{N}^2_{2x_1} = \underline{N}^2_2(x_1(k))$

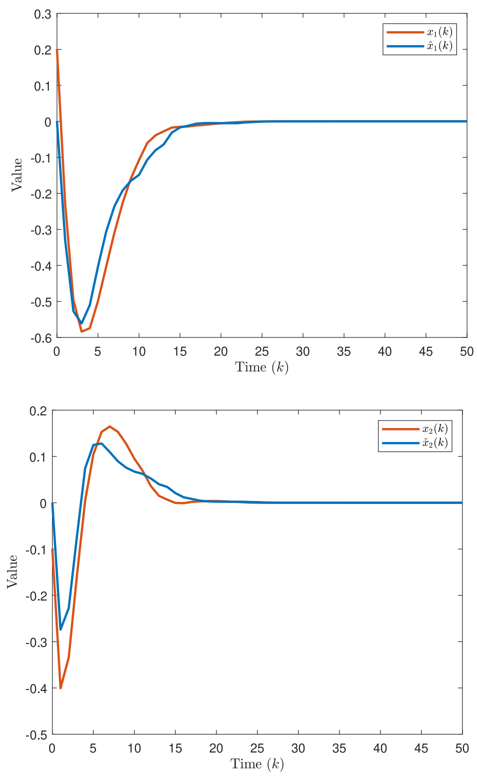


Fig. 1. States evolution $x_1(k)$ and $x_2(k)$ with their observation.

The FDI attacks are set with

$$E = \begin{bmatrix} -0.1 & 0 \\ 0 & -0.1 \end{bmatrix}, F = \begin{bmatrix} 2.7532 & -0.1203 \\ -0.1203 & 2.5189 \end{bmatrix}$$

and the weighted coefficients of the DETTOD are

$$Q_1 = \begin{bmatrix} 0.5 & 0 \\ 0 & 0.5 \end{bmatrix}, Q_2 = \begin{bmatrix} 0.6 & 0 \\ 0 & 0.6 \end{bmatrix}.$$

Under the DETTOD protocol, only one group has permission to transmit signals over the communication network at the triggering instant t_n. Based on the signals being transmitted, $\delta(t_n) \in \{1, 2\}$. The global boundary values in (22) and (23) are set as $\underline{u}_{11} = 0$, $\overline{u}_{11} = 0.048$, $\underline{u}_{12} = 0$, $\overline{u}_{12} = 0.028$, $\underline{u}_{21} = 0.051$, $\overline{u}_{21} = 0.302$, $\underline{u}_{22} = 0.150$, $\overline{u}_{22} = 0.449$. Other parameters are selected as $\gamma = 2$, $\lambda = 0.4$, $\Omega = \text{diag}\{1.5, 2.2\}$, $\omega(k) = [-0.8e^{-0.35k} \quad -0.8e^{0.5-0.35k}]^T$.

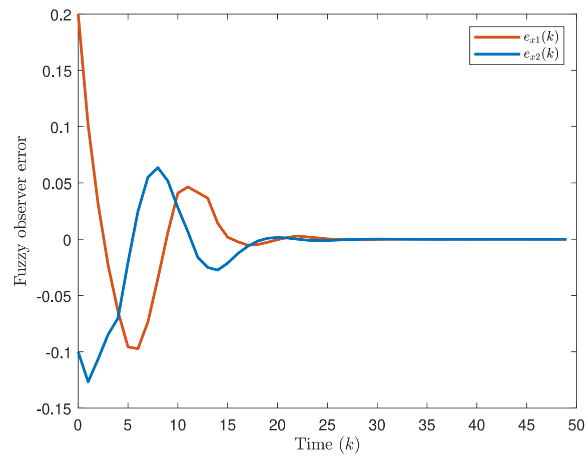


Fig. 2. Trajectories of state estimation error responses $e_x(k)$.

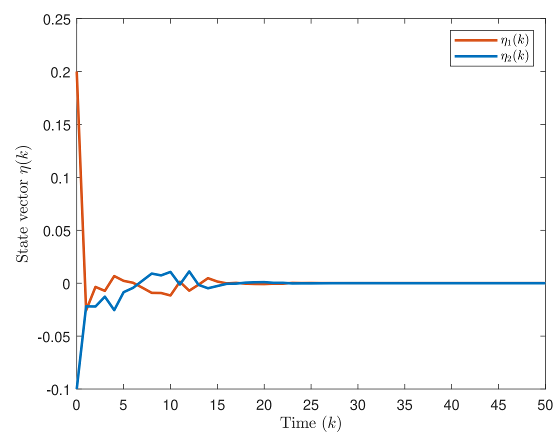


Fig. 3. Intermediate variable responses $\eta(k)$.

Afterwards, by Theorem 2, the state observer gains $L_{j,\delta(t_n)}$, the attack observer gains $G_{\delta(t_n)}$ and the controller gains $K_{j,\delta(t_n)}$ can be calculated as

$$L_{11} = \begin{bmatrix} -0.2495 & 0.0000 \\ 0.1610 & -0.0411 \end{bmatrix}, L_{12} = \begin{bmatrix} -0.1576 & 0.0265 \\ 0.0146 & -0.2148 \end{bmatrix}$$
$$L_{21} = \begin{bmatrix} -0.1782 & -0.0874 \\ 0.1386 & -0.0867 \end{bmatrix}, L_{22} = \begin{bmatrix} -0.0187 & 0.0223 \\ 0.0222 & -0.2339 \end{bmatrix}$$
$$G_1 = \begin{bmatrix} 0.1223 & -0.0510 \\ -0.0620 & 0.1210 \end{bmatrix}, G_2 = \begin{bmatrix} 0.1223 & -0.0510 \\ -0.0620 & 0.1210 \end{bmatrix}$$
$$K_{11} = \begin{bmatrix} -0.5553 & -0.2345 \\ 0.0145 & -0.4043 \end{bmatrix}, K_{12} = \begin{bmatrix} -0.5759 & -0.2083 \\ 0.0304 & -0.4296 \end{bmatrix}$$
$$K_{21} = \begin{bmatrix} -0.9861 & -0.6557 \\ 0.3955 & -0.0354 \end{bmatrix}, K_{22} = \begin{bmatrix} -1.0623 & -0.7627 \\ 0.4642 & 0.0597 \end{bmatrix}.$$

Based on the parameters above, the system states and their observations are presented in Fig. 1. Fig. 2 implies that the errors between system states and observer states converge to zero. Obviously, we can conclude that the designed observer will effectively predict its state to be measured under the FDI attacks.

Besides, the intermediate variable $\eta(k)$ and the unmeasurable FDI attacks estimation error $e_\eta(k)$ are drawn in Figs. 3 and 4, respectively. Fig. 5 depicts the responses of the control input $u(k)$, which indicates the proposed observer-based attack

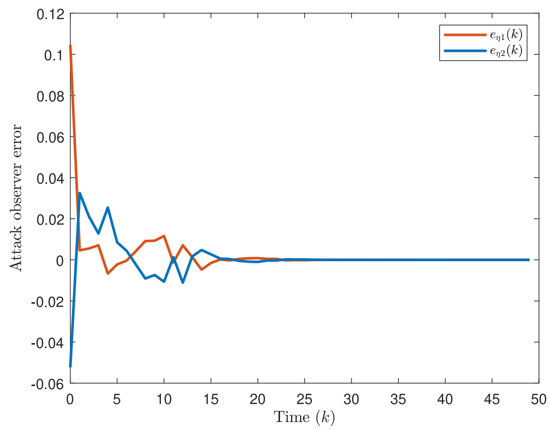


Fig. 4. Trajectories of FDI attacks estimation error $e_\eta(k)$.

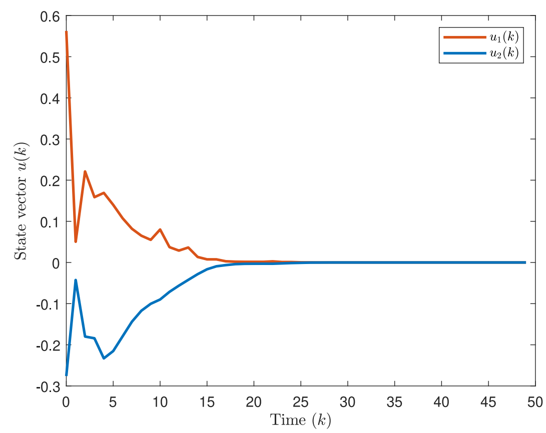


Fig. 5. Control input $u(k)$.

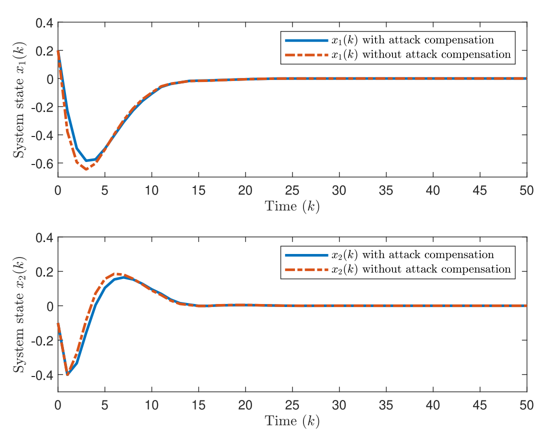


Fig. 6. System state $x(k)$ with and without attack compensation.

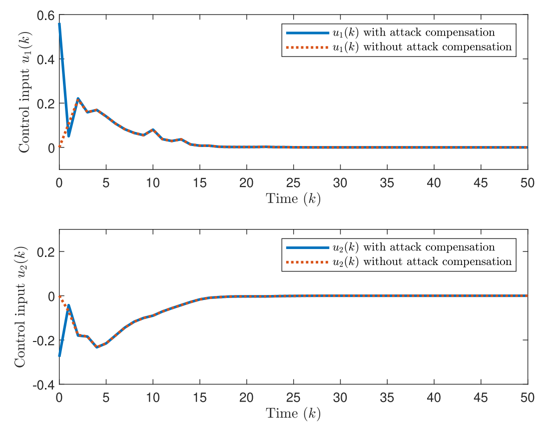


Fig. 7. Control input $u(k)$ with and without attack compensation.

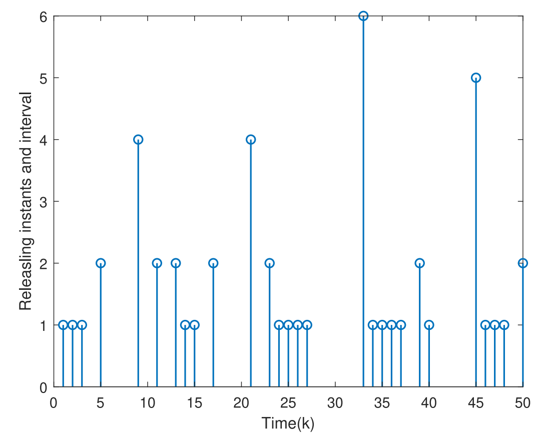


Fig. 8. Triggering instants and intervals under DETTOD protocol.

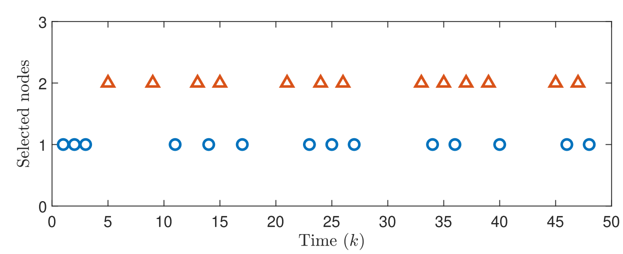


Fig. 9. Selected transmission node governed by WTOD protocol.

TABLE III
AVERAGE SAMPLING PERIOD BY DIFFERENT TRIGGERING SCHEMES

Event-triggering scheme	Average period
The scheme in this paper	0.5686
The scheme (Theorem 1) in [15]	0.5131
The scheme in [17]	0.4816
The scheme (Theorem 5.1) in [48]	0.3917

compensation controller can effectively stabilize the augumented system.

The curves of the system state $x(k)$ and control input $u(k)$ with and without attack compensation have been plotted in Figs. 6 and 7, which clearly demonstrates the better performance can be achieved by using the developed compensation method.

To better illustrate the advance of the adopted DETTOD protocol, the comparison results on the average interval under our scheme and other schemes in [15], [17], and [48] are presented in Table III. The triggering time and departure interval under the DETTOD protocol are plotted in Fig. 8. The selected transmission node governed by WTOD protocol is shown in Fig. 9. From the simulation results, one can see data conflict can be avoided and the pressure on network transmission is also alleviated, which exhibit the advantageous of the proposed DETTOD approach.

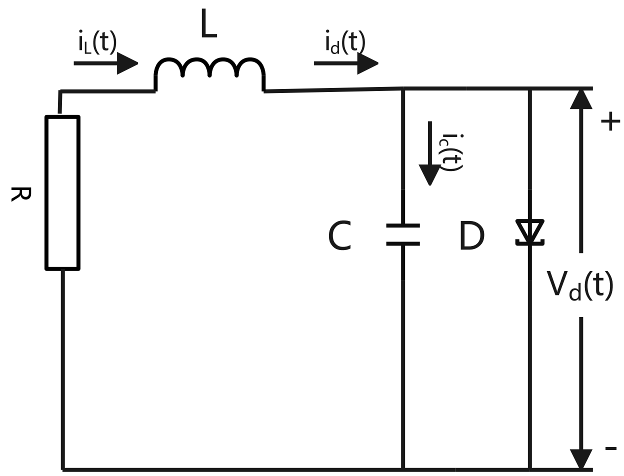


Fig. 10. Tunnel diode circuit system model.

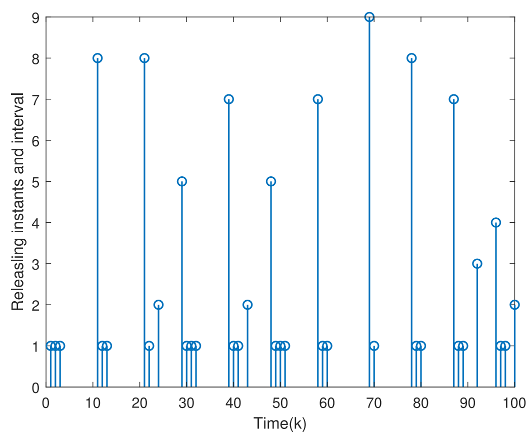


Fig. 11. Triggering instants and interval for tunnel diode circuit system model.

Example 2: Consider the following tunnel diode circuit system plotted in Fig. 10 [49]:

$$i_d(t) = -0.2v_d(t) - 0.01v_d^3(t)$$

where $i_d(t)$ is the current and $v_d(t)$ is the voltage of the tunnel. Define $x_1(t) = v_d(t)$ and $x_2(t) = i_d(t)$, $f(v_d(t)) = 0.2 + 0.01v_d^2(t)$. The adopted circuit system model can be written as

$$\begin{cases} \dot{x}_1(t) = \frac{f(v_d(t))}{C}x_1(t) + \frac{1}{C}x_2(t) \\ \dot{x}_2(t) = -\frac{1}{L}x_1(t) - \frac{R}{L}x_2(t) \ + \frac{1}{L}u(t) \end{cases}. \tag{37}$$

Let the capacitance $C = 0.1F$, the inductance $L = 1H$, the resistances $R = 3\Omega$ and $x_1(t) \in [-3, 3]$, one can get $f_{\max} = 0.29, f_{\min} = 0.2$. Then the following two fuzzy rules can be gotten.

Plant Rule F_1: **IF** $x_1(t)$ is 0, **THEN**

$$\dot{x}(t) = \bar{A}_1x(t) + \bar{B}_1u(t)$$

Plant Rule F_2: **IF** $x_1(t)$ is ± 3, **THEN**

$$\dot{x}(t) = \bar{A}_2x(t) + \bar{B}_2u(t)$$

where

$$\bar{A}_1 = \begin{bmatrix} f_{\min} & 10 \\ -1 & -1 \end{bmatrix}, \bar{A}_2 = \begin{bmatrix} f_{\max} & 10 \\ -1 & -1 \end{bmatrix}, \bar{B}_1 = \bar{B}_2 = \begin{bmatrix} 1.2 & 0 \\ 0 & 1 \end{bmatrix}.$$

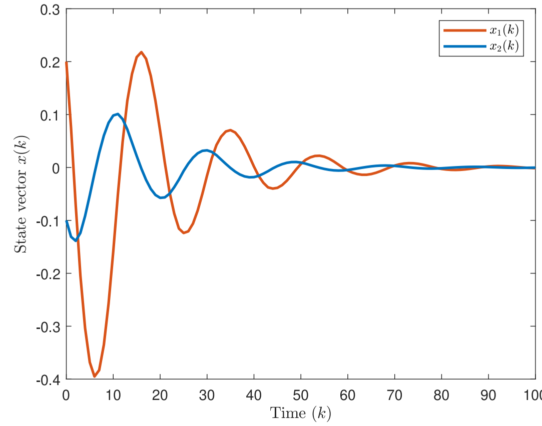


Fig. 12. State responses of tunnel diode circuit system model.

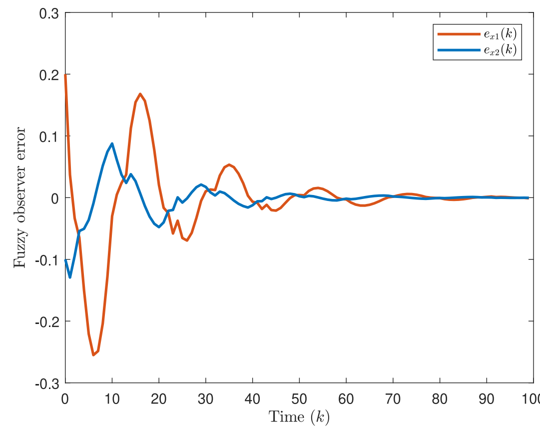


Fig. 13. Trajectories of state estimation error in Example 2 .

Based on the method in [15], the lower and upper MFs can be derived as $\overline{h}_{1x} = \underline{h}_{1x} = (f_{\max} - f(v_d(t))/f_{\max} - f_{\min})$, $\overline{h}_{2x} = 1 - \underline{h}_{1x}$, $\underline{h}_{2x} = 1 - \overline{h}_{1x}$. The lower and upper MFs of the controller are chosen as $\underline{g}_{1\hat{x}_1} = 1 - (1/9)e^{-\hat{x}_1(k)}$, $\overline{g}_{1\hat{x}_1} = 1 - (1/27)e^{-\hat{x}_1(k)}$, $\underline{g}_{2\hat{x}_1} = 1 - \overline{g}_{1\hat{x}_1}$, $\overline{g}_{2\hat{x}_1} = 1 - \underline{g}_{1\hat{x}_1}$, $\underline{c}_{\beta\hat{x}_1} = 0.6$, $\overline{c}_{\beta\hat{x}_1} = 0.4$, where $\beta = 1, 2$.

Discretizing the above system with sampling period $T = 0.1s$, one can derive

$$\begin{cases} x(k+1) = \sum_{i=1}^{2} h_{1x_1}[A_ix(k) + B_i(u(k) + a(k)) \\ \qquad\qquad + D_i\omega(k)] \\ y(k) \quad = \sum_{i=1}^{2} h_{1x_1}C_ix(k) \\ z(k) \quad = \sum_{i=1}^{2} h_{1x_1}M_ix(k) \end{cases}$$

where

$$A_1 = \begin{bmatrix} 0.9716 & 0.9454 \\ -0.09454 & 0.8581 \end{bmatrix}, A_2 = \begin{bmatrix} 0.9805 & 0.9498 \\ -0.09498 & 0.858 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 0.1192 & 0.0483 \\ -0.005796 & 0.09358 \end{bmatrix}, B_2 = \begin{bmatrix} 0.1198 & 0.04845 \\ -0.005813 & 0.09357 \end{bmatrix}$$

$$C_1 = C_2 = \begin{bmatrix} 1 & 0.8 \\ 1.1 & 1 \end{bmatrix}, D_1 = D_2 = \begin{bmatrix} 0.01 & 0.02 \\ 0.03 & 0.01 \end{bmatrix}$$

$$M_1 = M_2 = \begin{bmatrix} 0.1 & 0.1 \end{bmatrix}.$$

According to the control design method in Theorem 2, one has

$$L_{11} = \begin{bmatrix} -0.5191 & -0.1892 \\ -0.1659 & -0.0810 \end{bmatrix}, L_{12} = \begin{bmatrix} -0.1687 & -0.5284 \\ -0.0462 & -0.2076 \end{bmatrix}$$

$$L_{21} = \begin{bmatrix} -0.4512 & -0.2287 \\ -0.1432 & -0.0934 \end{bmatrix}, L_{22} = \begin{bmatrix} -0.2004 & -0.4920 \\ -0.0551 & -0.1943 \end{bmatrix}$$
$$G_1 = \begin{bmatrix} 0.2980 & -0.1355 \\ 0.0343 & 0.4074 \end{bmatrix}, G_2 = \begin{bmatrix} 0.2980 & -0.1355 \\ 0.0343 & 0.4074 \end{bmatrix}$$
$$K_{11} = \begin{bmatrix} -16.0177 & 10.7585 \\ 45.2571 & -40.9185 \end{bmatrix}, K_{12} = \begin{bmatrix} -16.0156 & 10.7568 \\ 45.2568 & -40.9182 \end{bmatrix}$$
$$K_{21} = \begin{bmatrix} -15.9990 & 10.7407 \\ 45.2514 & -40.9132 \end{bmatrix}, K_{22} = \begin{bmatrix} -15.9996 & 10.7411 \\ 45.2515 & -40.9133 \end{bmatrix}.$$

By applying the DETTOD protocol, the transmitted signal will be first determined by the event triggering conditions in (3), then, the triggered signal will be scheduled by the WTOD protocol, which not only saves communication resources solves the data conflicts issue in network. In Fig. 11, the triggering instants and interval under the DETTOD protocol is presented. It can be clearly observed that less triggering instants are generated under the proposed method in our article compared with the periodic time-triggered scheme. Figs. 12 and 13 show the trajectories of state response and state estimation error under the designed control method, respectively. We can see that the overall transient performance of the designed mechanism is excellent. This means that more network communication burden can be reduced under the same conditions, which further evidences the efficiency of using the proposed DETTOD protocol.

V. Conclusion

A fuzzy co-estimation of state and attacks problem for nonlinear NCSs has been addressed under FDI attacks in this article. A novel DETTOD protocol has been presented to reduce the probability of data conflict and relieve the pressure of network transmission, which is organically combined of the DET strategy and the WTOD protocol. Moreover, a sufficient condition ensuring the asymptotic stability as well as the prescribed H_∞ performance requirement has been proposed for the constructed augmented system. Comprehensively taking the FDI attack and the DETTOD protocol into consideration, a fuzzy observer-based attack compensation controller and FDI attacks observer of the augmented nonlinear IT2 fuzzy system is proposed. Finally, the feasibility of the proposed theoretical findings are illustrated by two simulation examples. The future work will include fault tolerant control for cyber-physical system under hybrid attacks and LNR, and filtering design of complex networks with DETTOD protocol.

References

[1] J. Cheng, Y. Wu, Z.-G. Wu, and H. Yan, "Nonstationary filtering for fuzzy Markov switching affine systems with quantization effects and deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 10, pp. 6545–6554, Oct. 2022.

[2] H. Shen, Y.-A. Liu, J. Wang, H. Yan, and M. Chadli, "Sliding-mode control for IT2 fuzzy nonlinear singularly perturbed systems and its application to electric circuits: A dynamic event-triggered mechanism," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 7, pp. 4077–4090, Jul. 2023.

[3] Z. You, H. Yan, H. Zhang, L. Zeng, and M. Wang, "Further stability criteria for sampled-data-based interval type-2 fuzzy systems via a refined two-side looped-functional method," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 1, pp. 265–277, Jan. 2023.

[4] Y. Mu, H. Zhang, Z. Gao, and J. Zhang, "A fuzzy Lyapunov function approach for fault estimation of T–S fuzzy fractional-order systems based on unknown input observer," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 2, pp. 1246–1255, Feb. 2023.

[5] J. Cheng, Y. Shan, J. Cao, and J. H. Park, "Nonstationary control for T–S fuzzy Markovian switching systems with variable quantization density," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 6, pp. 1375–1385, Jun. 2021.

[6] Z. Lian, Y. He, C.-K. Zhang, P. Shi, and M. Wu, "Robust H_∞ control for T–S fuzzy systems with state and input time-varying delays via delay-product-type functional method," *IEEE Trans. Fuzzy Syst.*, vol. 27, no. 10, pp. 1917–1930, Oct. 2019.

[7] R. Sakthivel, R. Kavikumar, A. Mohammadzadeh, O.-M. Kwon, and B. Kaviarasan, "Fault estimation for mode-dependent IT2 fuzzy systems with quantized output signals," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 2, pp. 298–309, Feb. 2021.

[8] Y. Zeng, H.-K. Lam, B. Xiao, and L. Wu, "Tracking control for nonlinear systems with actuator saturation via interval type-2 T–S fuzzy framework," *IEEE Trans. Cybern.*, vol. 53, no. 11, pp. 7085–7094, Nov. 2023.

[9] Y. Dong, Y. Song, and G. Wei, "Efficient model-predictive control for nonlinear systems in interval type-2 T-S fuzzy form under round-robin protocol," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 1, pp. 63–74, Jan. 2022.

[10] M. Wang, G. Feng, J. Qiu, H. Yan, and H. Zhang, "Fault detection filtering design for discrete-time interval type-2 T–S fuzzy systems in finite frequency domain," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 2, pp. 213–225, Feb. 2021.

[11] Q. Zhou, D. Liu, Y. Gao, H.-K. Lam, and R. Sakthivel, "Interval type-2 fuzzy control for nonlinear discrete-time systems with time-varying delays," *Neurocomputing*, vol. 157, pp. 22–32, Jun. 2015.

[12] J. Zhao, Y. Xiao, Z. Liang, P. K. Wong, Z. Xie, and X. Ma, "Adaptive event-triggered interval type-2 T-S fuzzy control for lateral dynamic stabilization of AEVs with intermittent measurements and actuator failure," *IEEE Trans. Transp. Electrif.*, vol. 9, no. 1, pp. 254–265, Mar. 2023.

[13] Y. Zhao, Y. Gao, H. Sang, and S. Yu, "Event-triggered-based antidisturbance switching control for switched T–S fuzzy systems," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 6, pp. 1819–1829, Jun. 2023.

[14] X.-L. Wang, G.-H. Yang, and D. Zhang, "Event-triggered fault detection observer design for T–S fuzzy systems," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 9, pp. 2532–2542, Sep. 2021.

[15] J.-W. Xing, C. Peng, Z. Cao, and W.-B. Xie, "Security-based control for networked interval type-2 fuzzy systems with multiple cyber-attacks: An improved dynamic event-triggered scheme," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 8, pp. 2747–2760, Aug. 2023.

[16] Z. Zhao, Z. Wang, L. Zou, Y. Chen, and W. Sheng, "Event-triggered set-membership state estimation for complex networks: A zonotopes-based method," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1175–1186, May/Jun. 2022.

[17] D. Yue, E. Tian, and Q.-L. Han, "A delay system method for designing event-triggered controllers of networked control systems," *IEEE Trans. Autom. Control*, vol. 58, no. 2, pp. 475–481, Feb. 2013.

[18] X. Zheng, H. Zhang, Z. Wang, C. Zhang, and H. Yan, "Finite-time dynamic event-triggered distributed H_∞ filtering for T-S fuzzy systems," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 7, pp. 2476–2486, Jul. 2022.

[19] Y. Wang, H. Yan, H. Zhang, H. Shen, and H.-K. Lam, "Interval type-2 fuzzy control for hmm-based multiagent systems via dynamic event-triggered scheme," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 8, pp. 3063–3073, Aug. 2022.

[20] W. Song, Z. Wang, J. Wang, F. E. Alsaadi, and J. Shan, "Distributed auxiliary particle filtering with diffusion strategy for target tracking: A dynamic event-triggered approach," *IEEE Trans. Signal Process.*, vol. 69, pp. 328–340, 2021.

[21] J. Sun, J. Yang, S. Li, and W. X. Zheng, "Estimate-based dynamic event-triggered output feedback control of networked nonlinear uncertain systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 5, pp. 3148–3158, May 2021.

[22] D. Yang, T. Li, X. Xie, and H. Zhang, "Event-triggered integral sliding-mode control for nonlinear constrained-input systems with disturbances via adaptive dynamic programming," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 11, pp. 4086–4096, Nov. 2020.

[23] 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.

[24] L. Zou, Z. Wang, Q.-L. Han, and D. Zhou, "Full information estimation for time-varying systems subject to round-robin scheduling: A recursive filter approach," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 3, pp. 1904–1916, Mar. 2021.

[25] 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.

[26] H. Liu, Z. Wang, W. Fei, and H. Dong, "On state estimation for discrete time-delayed memristive neural networks under the WTOD protocol: A resilient set-membership approach," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 4, pp. 2145–2155, Apr. 2022.

[27] 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.

[28] Y. Dong, Y. Song, and G. Wei, "Efficient model-predictive control for networked interval type-2 T–S fuzzy system with stochastic communication protocol," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 2, pp. 286–297, Feb. 2021.

[29] 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.

[30] 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, Nov. 2023.

[31] Z. Zhang, Y. Niu, and H.-K. Lam, "Sliding-mode control of T–S fuzzy systems under weighted try-once-discard protocol," *IEEE Trans. Cybernet.*, vol. 50, no. 12, pp. 4972–4982, Dec. 2020.

[32] D. Yue, Q.-L. Han, and C. Peng, "State feedback controller design of networked control systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 51, no. 11, pp. 640–644, Nov. 2004.

[33] D. Yue, Q.-L. Han, and J. Lam, "Network-based robust H_∞ control of systems with uncertainty," *Automatica*, vol. 41, no. 6, pp. 999–1007, 2005.

[34] 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.

[35] 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.

[36] Y. Li, F. Song, J. Liu, X. Xie, and E. Tian, "Decentralized event-triggered synchronization control for complex networks with nonperiodic DoS attacks," *Int. J. Robust Nonlin. Control*, vol. 32, no. 3, pp. 1633–1653, 2022.

[37] N. Rong and Z. Wang, "Event-based impulsive control of IT2 T–S fuzzy interconnected system under deception attacks," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 6, pp. 1615–1628, Jun. 2021.

[38] H.-Y. Sun, H.-G. Han, J. Sun, H.-Y. Yang, and J.-F. Qiao, "Security control of sampled-data T–S fuzzy systems subject to cyberattacks and successive packet losses," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 4, pp. 1178–1188, Apr. 2023.

[39] J. Liu, T. Yin, D. Yue, H. R. Karimi, and J. Cao, "Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks," *IEEE Trans. Cybern.*, vol. 51, no. 1, pp. 162–173, Jan. 2021.

[40] W. Lei, Z. Pang, H. Wen, W. Hou, and W. Han, "FDI attack detection at the edge of smart grids based on classification of predicted residuals," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 9302–9311, Dec. 2022.

[41] L. Zha, J. Miao, J. Liu, X. Xie, and E. Tian, "State estimation for delayed memristive neural networks with multichannel round-robin protocol and multimodal injection attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 54, no. 6, pp. 3738–3748, Jun. 2024.

[42] M. Fan, E. Tian, X.-p. Xie, D. Yue, and T. Cao, "Stochastic data-based denial-of-service attack strategy design against remote state estimation in interval type-2 T–S fuzzy systems," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 3, pp. 825–834, Mar. 2023.

[43] W. Song, Z. Wang, J. Wang, F. E. Alsaadi, and J. Shan, "Secure particle filtering for cyber-physical systems with binary sensors under multiple attacks," *IEEE Syst. J.*, vol. 16, no. 1, pp. 603–613, Mar. 2022.

[44] H. Zhang, D. Yue, C. Dou, and G. P. Hancke, "Resilient optimal defensive strategy of micro-grids system via distributed deep reinforcement learning approach against FDI attack," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 1, pp. 598–608, Jan. 2024.

[45] X. Chen, S. Hu, Y. Li, D. Yue, C. Dou, and L. Ding, "Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DoS attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2357–2368, May 2022.

[46] S. Weng, P. Weng, B. Chen, S. Liu, and L. Yu, "Distributed secure estimation against unknown FDI attacks and load deviation in multi-area power systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 6, pp. 3007–3011, Jun. 2022.

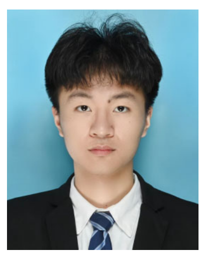
[47] Y. Gu, X. Yu, K. Guo, J. Qiao, and L. Guo, "Detection, estimation, and compensation of false data injection attack for UAVs," *J. Inf. Sci.*, vol. 546, pp. 723–741, Feb. 2021.

[48] X. Wang and M. D. Lemmon, "Self-triggered feedback control systems with finite-gain $\mathcal{L}_2$ stability," *IEEE Trans. Autom. Control*, vol. 54, no. 3, pp. 452–467, Mar. 2009.

[49] H. Shen, M. Xing, Z.-G. Wu, S. Xu, and J. Cao, "Multiobjective fault-tolerant control for fuzzy switched systems with persistent dwell time and its application in electric circuits," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 10, pp. 2335–2347, Oct. 2020.

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

From 2017 to 2024, she was an Associate Professor with the College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, China. From 2018 to 2023, she was a Postdoctoral Research Associate with the School of Mathematics, Southeast University, Nanjing. She is currently an Associate Professor with the College of Science, Nanjing Forestry University, Nanjing. Her current research interests include networked control systems, neural networks, and complex dynamical systems.



Tao Huang received the B.S. degree in mechanical engineering and automation from the Yancheng Institute of Technology, Yancheng, China, in 2021, and the M.S. degree in computer science and technology from the Nanjing University of Finance and Economics, Nanjing, China.

His research interests include nonlinear networked system and networked secure control.

Jinliang Liu (Senior Member, IEEE) received the Ph.D. degree in control theory and control engineering 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 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.

Engang Tian received the B.S. degree in mathematics from the Shandong Normal University, Jinan, China, in 2002, the M.Sc. degree in operations research and cybernetics from the 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 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. 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.

Xiangpeng Xie (Senior Member, IEEE) received the B.S. and Ph.D. degrees in engineering from the 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 School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include fuzzy modeling and control synthesis, state estimation, optimization in process industries, and intelligent optimization algorithms.

Dr. Xie is currently an Associate Editor of IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON FUZZY SYSTEMS, and IEEE TRANSACTIONS ON CYBERNETICS.

Chen Peng (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in coal preparation, and the Ph.D. degree in control theory and control engineering from the Chinese University of Mining Technology, Xuzhou, China, in 1996, 1999, and 2002, respectively.

From 2004 to 2005, he was a Research Associate with the University of Hong Kong, Hong Kong. From 2006 to 2007, he was a Visiting Scholar with the Queensland University of Technology, Brisbane, QLD, Australia. From 2011 to 2012, he was a Postdoctoral Research Fellow with the Central Queensland University, Rockhampton, QLD, Australia. In 2012, he was appointed as an Eastern Scholar with the Municipal Commission of Education, Shanghai, China, and joined Shanghai University, Shanghai, China. He was named a Highly Cited Researcher 2020 and 2021 by Clarivate Analytics. His research interests include networked control systems, distributed control systems, smart grid, and intelligent control systems.

Prof. Peng is an Associate Editor of a number of international journals, including the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Information Sciences*, and *Transactions of the Institute of Measurement and Control*.