SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

June 2022, Vol. 65 162205:1–162205:17
https://doi.org/10.1007/s11432-021-3397-2

Active event-driven reliable defense control for interconnected nonlinear systems under actuator faults and denial-of-service attacks

Bin GUO, Songyi DIAN* & Tao ZHAO

College of Electrical Engineering, Sichuan University, Chengdu 610065*, China*

Received 14 July 2021/Revised 5 October 2021/Accepted 30 November 2021/Published online 24 May 2022

Abstract This study investigates the reliable control design for a class of interconnected nonlinear systems subjected to actuator faults, disturbances, and denial-of-service (DoS) attacks. DoS attacks are carried out in both sensor and controller channels. An integrated event-observer-based security sliding mode fault-tolerant control approach is presented to defend against DoS attacks and compensate for faults and disturbances. To be more specific, the fuzzy logic system (FLS) theory is used to approximate the unknown nonlinear component first. Using the output measurement and sensor channel triggered output information, an FLS aided nonlinear estimator is put forward, in which the faults and disturbances are reconstructed. Then, to achieve the trajectory tracking purpose in the presence of DoS attacks, actuator faults, and disturbances, an adaptive sliding mode manifold is established, based on which an event-driven mechanism is established and a reliable controller is designed. In the controller scheme, the fault compensation and disturbance rejection mechanisms are also included synchronously. The tracking ability is analyzed using the Lyapunov method and the FLS theory, followed by applications to an interconnected power network system and an interconnected inverted pendulum system to demonstrate the applicability of the proposed method.

Keywords interconnected nonlinear system, actuator fault, DoS attack, disturbance, fault-tolerant control, event-driven control

Citation Guo B, Dian S Y, Zhao T. Active event-driven reliable defense control for interconnected nonlinear systems under actuator faults and denial-of-service attacks. Sci China Inf Sci, 2022, 65(6): 162205, https://doi.org/10.1007/s11432-021-3397-2

1 Introduction

With the rapid development of the mechanical system design technique, networks communication theory, and advances in electrical hardware, the automation system can be made more complex and multifunctional. To achieve the predetermined control purpose, two layers are included, namely the cyber and physical layers, in which various sensors, controllers, actuators, and networks are embedded [1]. Several challenges arise as the number of components in the automated system increases. On the one hand, the actuator may be experiencing physical layer failures because of long-term operation [2, 3]. On the other hand, unexpected disturbances may also enter into the control system through various channels [4]. Furthermore, the security problem in the cyber layer has become a great challenge because of a malicious attack, such as data injection [5], reply [6], and denial-of-service (DoS) attacks [7].

From the standpoint of system performance maintenance, fault-tolerant control (FTC) emerges as an effective method for compensating for faults and ensuring system reliability [8]. A significant amount of progress has been made in the field of FTC methods for linear and nonlinear systems [9–11]. Ref. [9], for example, investigated the FTC method for a nonaffine nonlinear system subjected to actuator fault and constructed an output feedback control scheme. In [10], the nonlinear mechanical system with actuator fault and disturbance was considered; the fault estimation and backstepping controller were reconfigured. These encouraging findings include fault estimation, reconfiguration, and compensation and their applications. Recently, the integrated fault tolerance and disturbance rejection control framework

* Corresponding author (email: songyi_dian@126.com)

has aroused the interest of scholars. In this control architecture, the controller is determined by the estimator, which can improve the flexibility of the controller design [12–14]. For instance, in [12], the fault compensation problem for a class of nonlinear feedback systems was addressed, a neural network was used to identify the nonlinear characteristic, and an FTC method was designed. However, these achievements have focused on the physical failures while ignoring the security problems, which have now become one of the most important factors affecting the system's performance. Furthermore, the majority of the fault compensation mechanisms considered in these results are based on the measurable system states, which may limit their applications because the states are not always completely measured in many practical systems.

As previously stated, one of the most competitive challenges is the security control problem known as the DoS attack in the automation network [15]. The primary goal of a DoS attack is to disrupt communication transmissions, thereby compromising data availability [16]. In [17], the malicious DoS defense control problem was investigated for a linear system, and a resilient control approach was designed. In [18], the state stability problem was addressed using the DoS attack, which was depicted using the DoS frequency and duration assumptions. With a similar point, the work of the DoS attack defense control methods extended to the fuzzy systems [19, 20] and distributed multiagent systems [21]. However, these results focused primarily on the linear system; few architectures take the interconnected nonlinear system into account. For the interconnected nonlinear system, the network communication channels are more sophisticated, which means that the DoS jammers have more channel options to launch and destroy the communications. Then, it is critical to investigate the active defense control strategy against the attackers for the interconnected nonlinear systems.

It should be noted that communication networks may be limited in terms of sensing and computational capabilities. To conserve communication resources, an event-driven transmission mechanism has been proposed, the feature of which is that data is determined by the event condition rather than at each sampling period. The main challenge of this control framework is determining how to construct the event condition to reduce unnecessary waste while maintaining system control performance. In [22], the global finite-time control method for uncertain nonlinear systems was developed, and an event-driven method was presented based on the backstepping technique, in which the event condition was constructed by the controller triggered error between the virtually applied control and actual signals. In [23], the stability problem of a class of output feedback nonlinear systems was investigated using the state information, and an event mechanism was designed. In [24], the nonlinear networked system in the occurrence of actuator fault and jamming attacks was considered, and a state-based trigger condition was constructed. In [25], the event-based control framework was applied to a nonlinear multiagent system, and a distributed event strategy was established. The adaptive tracking control for a class of feedback uncertain nonlinear systems was considered in [26]; assuming that the system states can be measured, an event-based control approach was developed to save the communication resources, in which the event condition was designed by the triggered controller error with a constant threshold, and the application to the single-link robotic manipulator system demonstrated the effectiveness of the presented approach.

Nevertheless, the aforementioned results are limited to fault compensation or DoS security control with or without the event-driven framework while leaving the synthesis of event-based FTC for actuator fault and active defense control for attacks unexplored, which has remained one of the most difficult challenges in the controller design framework, especially for the interconnected industrial systems. Furthermore, the above results are based on the assumption that the system states can fully be accessible, on which the state-based event condition and controller are designed. This may limit the applications because the measurability cannot always be guaranteed due to the limited computation resources, especially for the interconnected nonlinear systems. Then, the question arises: Is it possible to develop a unified observer-based control architecture that preserves and recovers control performance while achieving the resource-saving requirement for interconnected nonlinear systems with DoS attack, actuator fault, disturbance, and limited state measurable information? And how to investigate this unified control scheme to improve the balance between the controller and resource-saving performance motivates the event-driven observer-based controller design part of this study.

In this study, we consider the synthesis control problem for a class of interconnected nonlinear systems in the presence of DoS attack, actuator fault, disturbance, and limited communication resources; an event-observer-based reliable defense control framework is presented. In comparison to previous achievements, the main contributions of this study are the following.

(1) A novel adaptive event condition mechanism is established. Compared with the results in [23, 24],

where the system states were assumed to be measurable, the trigger conditions only in the control channels are considered, and the event conditions are established based on the triggered state directly, which may cause chattering of the controller if a fault or an attack occurs. This study addresses the event conditions both in the sensor and control channels. The presented trigger mechanism is an adaptive one that can balance the limited transmission resource and information utilization. Furthermore, a minimum time interval can be maintained in this trigger mechanism, avoiding the Zeno phenomenon.

(2) An event-based state, lumped disturbance, and fault index factor integration observation framework for the nonlinear interconnected system is designed. In this estimation scheme, the sensor channel triggered outputs are used, which means that the unknown variables can be estimated with less information. Furthermore, using the neighbor information, the estimation can be realized and convergence ability is explicit characterized.

(3) An event-observer-based reliable defense control framework is investigated, in which the FTC compensation, disturbance attenuation, and active DoS defense section are included to maintain the system control performance in terms of safety while the resource-efficient requirement can be achieved. The tracking performance analysis is formulated and expressed with the help of the fuzzy logic system (FLS) technique. Different from the work in [20], where the nonlinear function is assumed to satisfy the Lipshitz condition and control input is blocked during the attacker active interval, in this study, the data at attacker sleeping\active instant is triggered and used as a compensation part.

The remainder of this study is structured as follows. The problem formulation and the observer-based reliable defense control framework with the event-driven mechanism, as well as the tracking capability are presented in Section 2. Section 3 contains two simulation cases, and Section 4 concludes this work.

2 Problem formulation

Consider the following nonlinear system consists N subsystems, and the ith subsystem can be represented in the form of

$$\begin{cases} \dot{x}_i\left(t\right) = F_i\left(x_i, t\right) + \lambda_i u_i^f\left(t\right) + \sum\limits_{\substack{i=1\\ i\neq j}}^{N} \mathcal{H}_{ij} x_j(t) + \mathcal{W}_i\left(t\right), \\ y_i\left(t\right) = C_i x_i\left(t\right),\ i = 1, 2, \ldots, n, \end{cases} \tag{1}$$

where $x_i\left(t\right) \in \mathbb{R}^n$ is the state vector of the ith subsystem, $F_i(x_i, t)$ represents a smooth unknown nonlinear function, $u_i^f(t)$ denotes the control input, $\mathcal{W}_i(t)$ is the external disturbance, λ_i is the control gain, $y_i(t)$ is the output signal, $\mathcal{H}_{ij}$ and C_i are two known matrices with proper dimensions.

In this study, the actuator fault is considered as

$$u_i^f\left(t\right) = \theta_i u_{mi}\left(t\right) + \eta_i u_{qi}\left(t\right), \tag{2}$$

where $u_{mi}(t) \in \mathbb{R}^d$ represents the real control signal that will be designed, $u_{qi}(t)$ is the bias fault. $\theta_i = \mathrm{diag}(\theta_{i1}, \ldots, \theta_{id})$ is an index factor which expresses the loss efficiency degree of the actuator, and $\theta_{ia} \in (0, 1], a = (1, \ldots, d)$, $\theta_{im} \leqslant \|\theta_i\| \leqslant \theta_{in}$, where θ_{im} and θ_{in} are two constants. Assume $\|\dot{\theta}_i\| \leqslant \theta_{is}$ and θ_{is} is a scalar. $\eta_i \in \{0, 1\}$, which implies the bias fault occurs in the presence of $\eta_i = 1$.

Remark 1. From the actuator fault model in (2), three types of fault model can be covered, i.e., bias fault, partial loss actuator fault, and fault free cases. In the bias fault case, it is characterized by the actuator floating to nominal control response, which means $\eta_i = 1$. In the partial loss actuator fault, the response to the control signal is abnormal, for example, $\theta_i = 0.8$ means that 20% of the control signal cannot be acted. In the fault free case, $\eta_i = 0$ and $\theta_i = 1$. To guarantee the control performance, in this study, we assume that not all the actuators suffer from faults simultaneously.

By substituting the actuator fault model into (1), one has

$$\begin{cases} \dot{x}_i\left(t\right) = F_i\left(x_i, t\right) + \lambda_i \theta_i u_{mi}\left(t\right) + \sum\limits_{\substack{i=1\\ i\neq j}}^{N} \mathcal{H}_{ij} x_j(t) + \mathcal{W}_i\left(t\right) + \lambda_i \eta_i u_{qi}\left(t\right), \\ y_i\left(t\right) = C_i x_i\left(t\right),\ i = 1, 2, \ldots, n. \end{cases} \tag{3}$$

2.1 DoS attack formulation

A DoS attack attempts to impede data sending and reception with disruption resources. In this study, the aperiodic DoS attack problem is taken into account, which exists in the sensor and actuator channels. The attack aims to compromise the transmitted data before arriving at the destinations, which can be represented as

$$\mathcal{J}_{DoS} = \begin{cases} 0, \ t \in [p_n, p_n + l_n), \\ 1, \ t \in [p_n + l_n, p_{n+1}), \end{cases} \tag{4}$$

where $n \in \mathcal{N}$, p_n and l_n denote the instant and the duration time of the nth attack. From (4), it can be checked that during the interval $[p_n, p_n + l_n)$, the attack is sleeping and the communication is permitted, while the period time interval $[p_n + l_n, p_{n+1})$ represents the attack is in action and the communication is blocked.

As the attacker is energy limited, here, the following two assumptions are made.

Assumption 1. For any $t \geqslant t^* \geqslant 0$, there exist two positive scalars m_1 and T_{m1} such that

$$n(t, t^*) \leqslant m_1 + \frac{t - t^*}{T_{m1}}, \tag{5}$$

where $n(t, t^*)$ is the total number of the attack occurrence over the time interval $[t^*, t)$.

Assumption 2. For any $t \geqslant t^* \geqslant 0$, there exist two positive scalars m_2 and T_{m2} such that

$$\Lambda_n(t, t^*) \leqslant m_2 + \frac{t - t^*}{T_{m2}}, \tag{6}$$

where $\Lambda_n(t, t^*)$ denotes the attack action time over the time interval $[t^*, t)$.

Remark 2. The above two assumptions are regarded with the DoS frequency and DoS duration, which are not restrictive and can be seen commonly in [16, 21], here, $T_{m2} > 1$ guarantees that the DoS attacks are not always active.

Inspired by the work in [23], the unknown nonlinear function can be approximated by a suitable fuzzy logic system theory, which means the term $F_i(x_i, t)$ can be approximated as

$$F_i(\hat{x}_i, t) = {\xi_i^*}^{\mathrm{T}} \psi_i(\hat{x}_i, t) + \varsigma_i, \tag{7}$$

where $\psi_i(\hat{x}_i, t)$ is the so called fuzzy basic function, $\hat{x}_i$ is the estimated states. ς_i is the approximation error, ${\xi_i}^*$ is the optimal weight vector, which is given as

$${\xi_i}^* = \arg\min_{\xi_i} \left[\sup_{x \in \Pi(x)} \left| \hat{F}_i(\hat{x}_i, t) - F_i(\hat{x}_i, t) \right| \right], \tag{8}$$

where $\Pi(x)$ represents the compact set of x.

Then the system (3) can be rewritten as

$$\begin{cases} \dot{x}_i(t) = \begin{cases} \lambda_i \theta_i u_{mi}(t) + \sum\limits_{\substack{i=1 \\ i \neq j}}^{N} \mathcal{H}_{ij} x_j(t) + {\xi_i^*}^{\mathrm{T}} \psi_i(\hat{x}_i, t) + \mathcal{V}_i(t), \ t \in \mathcal{G}_{n,1}, \\ \sum\limits_{\substack{i=1 \\ i \neq j}}^{N} \mathcal{H}_{ij} x_j(t) + {\xi^*}^{\mathrm{T}} \psi(x_i, t) + \mathcal{V}_i(t), \ t \in \mathcal{G}_{n,2}, \end{cases} \\ y_i(t) = C_i x_i(t), \ i = 1, 2, \ldots, n, \end{cases} \tag{9}$$

where $\mathcal{G}_{n,1} := [p_n, p_n + l_n)$ and $\mathcal{G}_{n,2} := [p_n + l_n, p_{n+1})$, $\mathcal{V}_i(t) = \mathcal{W}_i(t) + \lambda_i \eta_i u_{qi}(t) + \varsigma_i + \Delta F(x_i, t)$ is the lumped disturbance, $\Delta F(x_i, t) = F(x_i, t) - F(\hat{x}_i, t)$. Similar to the result in [23], where the lumped disturbance is assumed to be bounded with an unknown constant. Here we assume $\|\mathcal{V}_i(t)\| \leqslant \gamma_i \Re(t)$, where γ_i is an unknown scalar, $\Re(t)$ denotes a new vector that will be designed later.

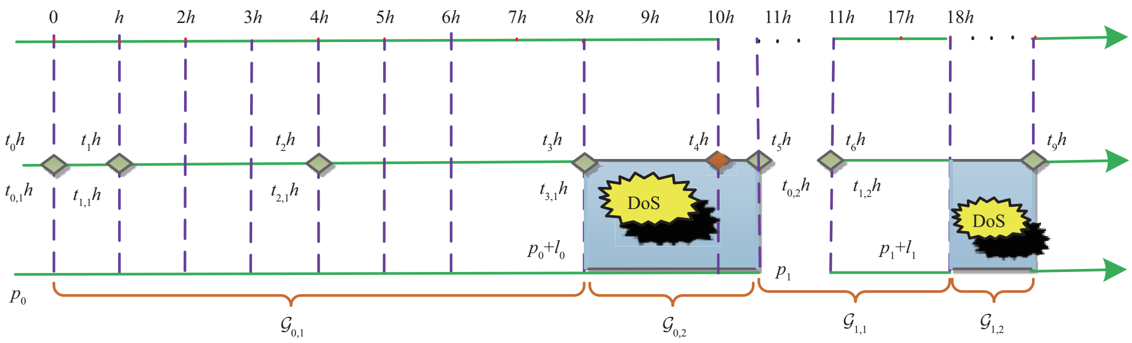

Figure 1 (Color online) The triggered instants with DoS attacks.

2.2 Event condition mechanism design

To reduce the communication resources, the event trigger conditions in the controller and the sensor channels are established. For the sensor channel, the following event condition is designed:

$$e_y(t_kh+qh)^{\mathrm{T}}\psi_k e_y\left(t_kh+qh\right)\leqslant \pi_m\left(t_kh+qh\right)y_i(t_kh)^{\mathrm{T}}\psi_k y_i\left(t_kh\right), \tag{10}$$

where ψ_k is a weighting matrix, $e_y\left(t_kh+qh\right) = y_i\left(t_kh\right) - y_i\left(t_kh+qh\right)$, $q\in N$, $\pi_m\left(t_kh+qh\right)\in[\pi_{m1},\pi_{m2}]$ is a positive parameter which obeys the following updating law $\pi_m\left(t_kh+qh\right) = \pi_{m1} + m_a\left(\pi_{m2}-\pi_{m1}\right)\mathrm{e}^{-m_b\left|\|y_i(t_kh+qh)\|-\|y_i(t_kh+qh)\|\right|}$, where $0\leqslant\pi_{m1}\leqslant\pi_{m2}<1$. m_a and m_b are two threshold adjustment sensitivity parameters with $m_a>1$ and $m_b>1$.

Then the next release time can be obtained as

$$t_{k+1}h = t_kh+\min_{q\geqslant 1}\left\{\begin{array}{l} e_y(t_kh+qh)^{\mathrm{T}}\psi_k e_y\left(t_kh+qh\right)\\ >\pi_m\left(t_kh+qh\right)y_i(t_kh)^{\mathrm{T}}\psi_k y_i\left(t_kh\right)\end{array}\right\}.$$

It is worthy to be noted that the considered aperiodic DoS attack may block the communication in an unexpected way, which implies that the kth triggered output of data may not be transferred to the destination if the DoS occurs. Then the trigger condition may not be applicable to the control performance analysis. To handle this problem, the following resilient trigger condition is presented based on the condition (10):

$$t_{k,n+1}h\in\left\{t_sh|\,t_sh\in\mathcal{G}_{n,1},t_s\in N\right\}\cup\left\{p_n\right\}, \tag{11}$$

where t_sh satisfies the condition (10), $t_{k,n+1}h$ denotes the time instant that the output data transmitted successfully to the sensor. Here $k\in\{0,1,\ldots,k\left(n\right)\}$ and $k\left(n\right)=\max\left\{k\in N|\,p_n+l_n>t_{k,n+1}h\right\}$.

An example of the event scheme with DoS attacks is shown in Figure 1.

Remark 3. From the equation in (10), if the condition is broken, the next transmitted data is triggered. As the attacker will block the communication, which means that the triggered data should not be located in the attack active time interval. Considering the DoS attack, in this study, an attack-resilient trigger condition in (11) is presented. In (11), the triggered time sequences lie in the attack sleeping interval. It can also be derived that if no trigger data meets the condition in (11), then the data at instant p_n will be forced to transfer successfully, which implies the presented trigger mechanism can help to maintain the control performance even the attack is small and aperiodic.

Remark 4. The trigger condition in (10) can be implemented in the presence of the attack-free scenarios. From (10), it is easy to check that the minimum time interval will be no less than h, which means that the time interval between the next data released time and the latest released time will be no smaller than a sampling period, which in return indicates that the Zeno phenomenon can be avoided. Similar analysis can be made for the control channel; i.e., the Zeno avoidance performance can also be maintained in the control channel. From the applicative perspective, an improved trigger countermeasure is established in (11) to tackle the DoS attack. From (11), it can be seen that the data could be triggered when the attack is sleeping and will be released at the sleeping/active switch instant.

Remark 5. Compared with the results in [22, 26], in this study, the presented trigger mechanism threshold is a dynamic one rather a fixed scalar; with this trigger scheme, the trigger condition has a better response to the influences of the actuator fault, lumped disturbance, and DoS attack. More specific,

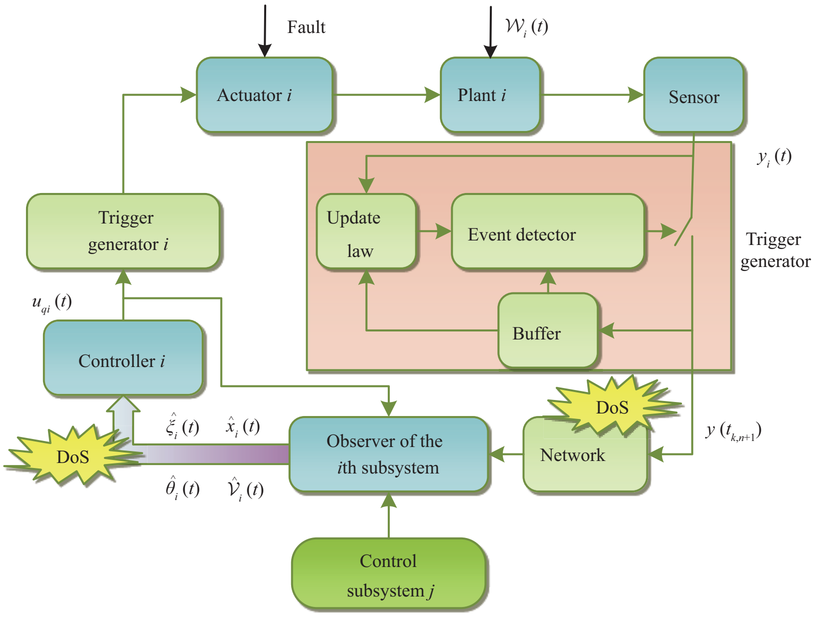

Figure 2 (Color online) Block diagram of the proposed approach.

the threshold $\pi_m(t_kh+qh)$ depends on the output error; i.e., when $|\|y_i(t_kh)\||-|\|y_i(t_kh+qh)\||$ becomes larger, the threshold becomes smaller, which means the trigger condition can be more easily satisfied and the data will be updated frequently enough. On the contrary, when the output error gets smaller, the data will be released in a lower frequency way, which indicates that the communication resources are saved.

The presented control framework is shown in Figure 2, the main purpose of this study is to design an event-observer-based fault-tolerant controller for the system in (9) in the presence of actuator fault, lumped disturbance, DoS attack, and limited communication resources. First, as the states may not be fully measured, while the fault and disturbance can also be unknown, we present a fuzzy-aided observer by utilizing the triggered data in the sensor channel. Then we organize our event-observer-based FTC framework based on the observer outputs, in which the compensation parts are included. Finally, the application to an interconnected power system shows the fault tolerance, disturbance rejection, and DoS compensation abilities of the presented approach.

2.3 Proposed observer design

In this study, the states of the system are regarded as imperfectly measurable, the unexpected actuator fault and lumped disturbance are also unknown. For system (9), the following observer is designed for $t\in[t_kh,t_{k+1}h)$:

$$\begin{cases}\dot{\hat{x}}_i(t)=\lambda_i\hat{\theta}_iu_{mi}(t)+\sum\limits_{\substack{i=1\\i\neq j}}^{N}\mathcal{H}_{ij}\hat{x}_j(t)+\hat{\xi}_i^{\mathrm{T}}\psi_i(\hat{x}_i,t)+L_i(y_i(t_{k,n+1}h)-\hat{y}_i(t))+\Lambda_i(t),\\ \hat{y}_i(t)=C_i\hat{x}_i(t),\ i=1,2,\ldots,n,\ k\in\{0,1,\ldots,,k(n)\},\end{cases}\tag{12}$$

where $\hat{x}_i(t)$, $\hat{\theta}_i$, $\hat{\xi}_i$ and $\hat{y}_i$ are the estimates of $x_i(t)$, θ_i, ξ_i^* and y_i. L_i is the observer gain for the ith subsystem, $\Lambda_i(t)$ is an auxiliary compensator, which is given as

$$\Lambda_i(t)=\frac{P_ie_i(t)}{\|e_i(t)^{\mathrm{T}}P_i\|^2}\left(\sigma_s+\hat{\gamma}_i\left\|e_i(t)^{\mathrm{T}}P_i\right\|\Re(t)-\kappa_s\|\Re(t)\|^2+\left\|e_i(t)^{\mathrm{T}}P_iL_{si}e_i(t)\right\|+\left\|e_i(t)^{\mathrm{T}}P_iL_i\bar{e}_y\right\|\right),\tag{13}$$

where $\kappa_s>0$ is a scalar, $\sigma_s=(\theta_{in}-\theta_{im})(\theta_{in}-\theta_{im}+\theta_{is})$, L_{si} is a chosen matrix, P_i is a symmetric definite positive matrix. e_i is the state estimation error, $\hat{\gamma}_i$ is the estimation of γ_i, $\bar{e}_y=y_i(t_{k,n+1}h)-y_i(t)$.

In the presented observer (12), the estimation $\hat{\theta}_i$ is updated by

$$\dot{\hat{\theta}}_i = \begin{cases} l_m, \\ 0, \quad \text{if} \;\; l_m > 0, \;\; \hat{\theta}_i = \theta_{in} \;\; \text{or} \;\; l_m < 0, \;\; \hat{\theta}_i = \theta_{im}, \end{cases} \tag{14}$$

where $l_m = -\lambda_i u_{mi}(t)^{\mathrm{T}} P_i e_i$.

Let $e_i = x_i\left(t\right) - \hat{x}_i\left(t\right)$. Then the estimation error system can be obtained as

$$\dot{e}_i\left(t\right) = \lambda_i \tilde{\theta}_i u_{mi}\left(t\right) + \sum_{\substack{i=1 \\ i \neq j}}^{N} \mathcal{H}_{ij} e_j(t) + \tilde{\xi}_i^{\mathrm{T}} \psi_i\left(\hat{x}_i, t\right) + \mathcal{V}_i\left(t\right) - L_i \bar{e}_y - L_i C_i e_i\left(t\right) - \Lambda_i\left(t\right), \tag{15}$$

where $\tilde{\theta}_i = \theta_i - \hat{\theta}_i = \operatorname{diag}(\tilde{\theta}_{i1}, \ldots, \tilde{\theta}_{id})$, $e_j\left(t\right) = x_j\left(t\right) - \hat{x}_j\left(t\right)$, $\tilde{\xi}_i = {\xi_i}^* - \hat{\xi}_i$.

In this study, the following auxiliary vector is constructed to provide the lumped disturbance estimation valve:

$$\Re\left(t\right) = \int_0^t \kappa_e e_i\left(t\right) \mathrm{d}t + e_i\left(t\right) - \Im_i\left(t\right), \tag{16}$$

where $\kappa_e > 0$ is a scalar, $\Im_i(t)$ is an intermediate variable which is given as

$$\Im_i\left(t\right) = \lambda_i \tilde{\theta}_i u_{mi}\left(t\right) + \sum_{\substack{i=1 \\ i \neq j}}^{N} \mathcal{H}_{ij} e_j(t) + \tilde{\xi}_i^{\mathrm{T}} \psi_i\left(\hat{x}_i, t\right) - L_i C_i e_i\left(t\right) - \lambda\!\!\!^{-}_i\left(t\right), \tag{17}$$

and $\lambda\!\!\!^{-}_i\left(t\right)$ is constructed as

$$\lambda\!\!\!^{-}_i\left(t\right) = -\left(\kappa_s + \hat{\gamma}_i\right) \Re\left(t\right) - L_i \bar{e}_y - \Lambda_i\left(t\right) + k_e e_i\left(t\right), \tag{18}$$

where κ_s is a positive scalar, $\hat{\gamma}_i$ is updated as

$$\dot{\hat{\gamma}}_i = \kappa_s \left(\left\| \Re\left(t\right) \right\|^2 + \left\| e_i(t)^{\mathrm{T}} P_i \right\| \left\| \Re\left(t\right) \right\| \right). \tag{19}$$

In this study, the lumped disturbance is observed as

$$\hat{\mathcal{V}}_i\left(t\right) = \kappa_e e_i\left(t\right) - \lambda\!\!\!^{-}_i\left(t\right) - L_i \bar{e}_y - \Lambda_i\left(t\right). \tag{20}$$

In this study, an assumption $\|\mathcal{V}_i(t)\| \leqslant \gamma_i \Re(t)$ is made in the observer framework; this is reasonable and not too restrictive. From the definition of the lumped disturbance, as the approximation error of the fuzzy control theory is bounded, the actuator fault and the external disturbance in the actual system are also bounded, and then the lumped disturbance $\mathcal{V}_i(t)$ can be bounded. According to (16), the estimation error is included in the variable $\Re(t)$, which implies that the auxiliary term $\Re(t)$ has the information of the lumped disturbance. As the lumped disturbance is bounded, by utilizing an unknown scalar γ_i, the above assumption can be established.

In the presented observer framework, a compensator is introduced. In the application process, the control signal is transmitted at every sampling period in the attack sleeping interval and each piece of data can be stored. From this perspective, the designed observer is a memory-based one. For example, if the initial valves are given at first time period h, then $e_i(h)$ can be obtained. Then from the iterative view, we have $e_i(2h)$ at the next period time. P_i is solved from (21), $\bar{e}_y = y_i\left(t_{k,n+1}h\right) - y_i\left(t\right)$. Then, with the memory-based mechanism, the compensator can be realized.

Now, we are in the position to verify the effectiveness of the proposed observer, and the following theorem guarantees the convergence performance of the observer.

Theorem 1. With the estimators (12) and (20), the estimation errors for the ith system can be guaranteed if there exist a sequence of symmetric definite positive matrices P_i and the following condition holds

$$\left(\bar{P}\Xi + \bar{P}\bar{L}_s\right)^{\mathrm{T}} + \left(\bar{P}\Xi + \bar{P}\bar{L}_s\right) < 0, \tag{21}$$

where $\bar{P} = \operatorname{diag}\left(P_1, \ldots, P_N\right)$, $\bar{L}_s = \operatorname{diag}\left(L_{s1}, \ldots, L_{sN}\right)$, $\Xi = [\mathcal{H}_{i1}, \mathcal{H}_{i2}, \ldots, \mathcal{H}_{ii-1}, -L_i C_i, \mathcal{H}_{ii+1}, \mathcal{H}_{iN}]$. Here, the sequence of matrices L_{si} $(i = 1, \ldots, N)$ is chosen by the author, and then the solvable ability of the condition (21) can be maintained.

Proof. The Lyapunov function is chosen as

$$V_1(t) = \sum_{i=1}^{N} \left(e_i(t)^{\mathrm{T}} P_i e_i(t) + \Re(t)^{\mathrm{T}} \Re(t) + {\kappa_s}^{-1} \tilde{\gamma}_i^{\mathrm{T}} \tilde{\gamma}_i + \tilde{\theta}_i^{\mathrm{T}} \tilde{\theta}_i + \tilde{\xi}_i^{\mathrm{T}} \tilde{\xi}_i \right), \tag{22}$$

where $\tilde{\gamma}_i = \gamma_i - \hat{\gamma}_i$.

The time derivative along the trajectory of the system (15) can be obtained as

$$\begin{aligned}
\dot{V}_1(t) &= 2\sum_{i=1}^{N} e_i(t)^{\mathrm{T}} P_i (\lambda_i \tilde{\theta}_i u_{mi}(t) + \sum_{\substack{i=1\\ i\neq j}}^{N} \mathcal{H}_{ij} e_j(t) + \tilde{\xi}_i^{\mathrm{T}} \psi_i(\hat{x}_i, t)) \\
&\quad - 2\sum_{i=1}^{N} e_i(t)^{\mathrm{T}} P_i \left(L_i \bar{e}_y + L_i C_i e_i(t) + \Lambda_i(t) \right) - \mathcal{V}_i(t) \\
&\quad + 2\sum_{i=1}^{N} \left(\Re(t)^{\mathrm{T}} \dot{\Re}(t) + {\kappa_s}^{-1} \tilde{\gamma}_i^{\mathrm{T}} \dot{\tilde{\gamma}}_i + \tilde{\theta}_i^{\mathrm{T}} \dot{\tilde{\theta}}_i + \tilde{\xi}_i^{\mathrm{T}} \dot{\tilde{\xi}}_i \right) \\
&= 2e_i(t)^{\mathrm{T}} P_i \left(\lambda_i \tilde{\theta}_i u_{mi}(t) + \tilde{\xi}_i^{\mathrm{T}} \psi_i(\hat{x}_i, t) + \mathcal{V}_i(t) \right) + 2e_i(t)^{\mathrm{T}} P_i \left(\Xi \bar{E} - L_i \bar{e}_y - \Lambda_i(t) \right) \\
&\quad + 2\sum_{i=1}^{N} \left(\Re(t)^{\mathrm{T}} \dot{\Re}(t) + {\kappa_s}^{-1} \tilde{\gamma}_i^{\mathrm{T}} \dot{\tilde{\gamma}}_i + \tilde{\theta}_i^{\mathrm{T}} \dot{\tilde{\theta}}_i + \tilde{\xi}_i^{\mathrm{T}} \dot{\tilde{\xi}}_i \right),
\end{aligned} \tag{23}$$

where $\bar{E} = [e_1, e_2, \ldots, e_N]^{\mathrm{T}}$.

Combing (14) and (20), the following conditions can be achieved:

$$\begin{aligned}
&2e_i(t)^{\mathrm{T}} P_i \lambda_i \tilde{\theta}_i u_{mi}(t) + 2\tilde{\theta}_i^{\mathrm{T}} \dot{\tilde{\theta}}_i = 2e_i(t)^{\mathrm{T}} P_i \lambda_i u_{mi}(t) \tilde{\theta}_i + 2\tilde{\theta}_i^{\mathrm{T}} \left(\dot{\theta}_i - \dot{\hat{\theta}}_i \right) \\
&\quad \leqslant 2(\theta_{in} - \theta_{im})(\theta_{in} - \theta_{im} + \theta_{is}),
\end{aligned} \tag{24}$$

$$\begin{aligned}
&2e_i(t)^{\mathrm{T}} P_i \mathcal{V}_i(t) + 2\Re(t)^{\mathrm{T}} \dot{\Re}(t) + 2{\kappa_s}^{-1} \tilde{\gamma}_i^{\mathrm{T}} \dot{\tilde{\gamma}}_i \\
&\quad \leqslant 2\gamma_i \left\| e_i(t)^{\mathrm{T}} P_i \right\| \Re(t) + 2\Re(t)^{\mathrm{T}} \left(\mathcal{V}_i(t) - \hat{\mathcal{V}}_i(t) \right) + 2{\kappa_s}^{-1} \tilde{\gamma}_i^{\mathrm{T}} \left(\dot{\gamma}_i - \dot{\hat{\gamma}}_i \right) \\
&\quad = 2\gamma_i \left\| e_i(t)^{\mathrm{T}} P_i \right\| \Re(t) - 2\kappa_s \|\Re(t)\|^2 - 2\tilde{\gamma}_i^{\mathrm{T}} \left\| e_i(t)^{\mathrm{T}} P_i \right\| \|\Re(t)\| \\
&\quad = -2\kappa_s \|\Re(t)\|^2 + 2\hat{\gamma}_i \left\| e_i(t)^{\mathrm{T}} P_i \right\| \Re(t).
\end{aligned} \tag{25}$$

It is worthy to be noted that $\sum_{i=1}^{N} (e_i(t)^{\mathrm{T}} P \tilde{\xi}_i^{\mathrm{T}} \psi_i(x,t)) = \bar{E}(t)^{\mathrm{T}} \bar{P} \bar{\psi}_i(x,t) \tilde{\xi}_p$ with $\tilde{\xi}_p = [\tilde{\xi}_1^{\mathrm{T}}, \ldots, \tilde{\xi}_N^{\mathrm{T}}]^{\mathrm{T}}$, $\bar{\psi}(\hat{x}_i, t) = \mathrm{diag}(\psi_1(\hat{x}_i, t), \ldots, \psi_N(\hat{x}_i, t))$. Define the adaptive law as $\dot{\tilde{\xi}}_p = -\bar{\psi}(x,t)^{\mathrm{T}} \bar{P}^{\mathrm{T}} \bar{E}(t) - \tilde{\xi}_p$. Then the following equation can be obtained as

$$\begin{aligned}
\sum_{i=1}^{N} \left(e_i(t)^{\mathrm{T}} P_i \tilde{\xi}_i^{\mathrm{T}} \psi_i(\hat{x}_i, t) + \tilde{\xi}_i^{\mathrm{T}} \dot{\tilde{\xi}}_i \right) &= \bar{E}_i^{\mathrm{T}} \bar{P} \bar{\psi}(\hat{x}_i, t) \tilde{\xi}_p + \tilde{\xi}_p^{\mathrm{T}} \dot{\tilde{\xi}}_p \\
&= \bar{E}_i^{\mathrm{T}} \bar{P} \bar{\psi}(\hat{x}_i, t) \tilde{\xi}_p - \tilde{\xi}_p^{\mathrm{T}} \bar{\psi}(\hat{x}_i, t)^{\mathrm{T}} \bar{P}^{\mathrm{T}} \bar{E}_i - \tilde{\xi}_p^{\mathrm{T}} \tilde{\xi}_p = -\tilde{\xi}_p^{\mathrm{T}} \tilde{\xi}_p.
\end{aligned} \tag{26}$$

Then, it follows that

$$\begin{aligned}
\dot{V}_1(t) &\leqslant 2e_i(t)^{\mathrm{T}} P_i (-L_i \bar{e}_y - \Lambda_i(t)) + e_i(t)^{\mathrm{T}} P_i \Xi \bar{E} + 2(\theta_{in} - \theta_{im})(\theta_{in} - \theta_{im} + \theta_{is}) \\
&\quad - 2\kappa_s \|\Re(t)\|^2 + \hat{\gamma}_i \left\| e_i(t)^{\mathrm{T}} P_i \right\| \Re(t) - \tilde{\xi}_p^{\mathrm{T}} \tilde{\xi}_p - e_i(t)^{\mathrm{T}} P_i L_{si} e_i(t) + e_i(t)^{\mathrm{T}} P_i L_{si} e_i(t).
\end{aligned} \tag{27}$$

From (13), it is straightforward that

$$\begin{aligned}
&- e_i(t)^{\mathrm{T}} P_i \Lambda_i(t) - e_i(t)^{\mathrm{T}} P_i L_i \bar{e}_y - \kappa_s \|\Re(t)\|^2 + 2\hat{\gamma}_i \left\| e_i(t)^{\mathrm{T}} P_i \right\| \Re(t) - e_i(t)^{\mathrm{T}} P_i L_{si} e_i(t) \\
&\quad + (\theta_{in} - \theta_{im})(\theta_{in} - \theta_{im} + \theta_{is})
\end{aligned}$$

$$
\begin{aligned}
&= -e_i(t)^{\mathrm{T}} P_i \frac{P_i e_i(t)}{\left\|e_i(t)^{\mathrm{T}} P_i\right\|^2}\left(\sigma_s + \hat{\gamma}_i \left\|e_i(t)^{\mathrm{T}} P_i\right\| \Re(t)\right. \\
&\quad \left. -\kappa_s \|\Re(t)\|^2 + \left\|e_i(t)^{\mathrm{T}} P_i L_{si} e_i(t)\right\| + \left\|e_i(t)^{\mathrm{T}} P_i L_i \bar{e}_y\right\|\right) + (\theta_{in} - \theta_{im})(\theta_{in} - \theta_{im} + \theta_{is}) \\
&\quad - \kappa_s \|\Re(t)\|^2 + 2\hat{\gamma}_i \left\|e_i(t)^{\mathrm{T}} P_i\right\| \Re(t) - e_i(t)^{\mathrm{T}} P_i L_s e_i(t) = 0.
\end{aligned} \tag{28}
$$

According to (24)–(28), Eq. (23) can be reformulated as

$$
\begin{aligned}
\dot{V}_1(t) &< 2\sum_{i=1}^{N}\left(e_i(t)^{\mathrm{T}} P_i \Xi \bar{E} + 2e_i(t)^{\mathrm{T}} P_i L_{si} e_i(t)\right) - \bar{\xi}_p^{\mathrm{T}} \bar{\xi}_p \\
&= \bar{E}^{\mathrm{T}}\left(\left(\bar{P}\Xi + \bar{P}\bar{L}_s\right)^{\mathrm{T}} + \left(\bar{P}\Xi + \bar{P}\bar{L}_s\right)\right)\bar{E} - \bar{\xi}_p^{\mathrm{T}} \bar{\xi}_p.
\end{aligned} \tag{29}
$$

From (21), one can check that $\dot{V}_1(t) < 0$. For the DoS attack time interval, the control input $u_{mi}(t) = 0$, and the triggered output becomes $y_i\left(t_{k(n),n+1}h\right)$. Based on the Lyapunov method, the similar results can be obtained. Then the estimation error convergence abilities can be guaranteed.

2.4 Presented controller design

Now we are in the position to design the event-driven fault-tolerant controller to achieve the tracking performance based on the sliding mode technology. Assume the desired trajectory of the ith subsystem is $y_{ir}(t)$, and then the tracking error can be calculated as $e_{ir} = y_i(t_{k,n+1}) - y_{ir}(t)$. To achieve the tracking control performance, the control policy is designed as $u_{mi}(t) = u_{mi}^a(t) + u_{mi}^b(t)$, where $u_{mi}^a(t)$ and $u_{mi}^b(t)$ are two parts of the control framework, $u_{mi}^b(t)$ is used to compensate for the effects of fault, disturbance, and attack, and $u_{mi}^a(t)$ is designed to satisfy the reaching performance of the sliding mode manifold.

The sliding mode manifold is constructed as

$$
\delta_i(t) = \int_0^t \left(\mathcal{R}_a\left(e_{ir}(t)^{\beta_1} + e_{ir}(t)^{\beta_2}\right) - C_i \lambda_i \hat{\theta}_i u_{mi}^a(t)\right)\mathrm{d}t + e_{ir}(t), \tag{30}
$$

where $\beta_1 > 0$, $\beta_2 > 0$. $\mathcal{R}_a$ is an adaptive parameter which is constructed as

$$
\mathcal{R}_a = \frac{\beta_a}{\beta_b + \beta_c \exp(-c_a(\|\hat{\mathcal{V}}_i(t)\| + \|e_{ir}\|)^{c_b})},
$$

with $\beta_g > 0$ $(g = a, b, c)$, $c_a > 0$, $c_b > 0$.

In this study, an adaptive parameter $\mathcal{R}_a$ is introduced to help to enhance the robustness and control performance by combing β_1 and β_2. As expressed in the sliding mode manifold, when a fault or disturbance occurs, the distance between the control trajectory and the desired trajectory becomes large, so that $\mathcal{R}_a$ becomes large, and the domain percentage of the two terms $e_i(r)$ and $\dot{e}_i(r)$ will increase, subsequently. With this mechanism, the trajectory convergence can be adjusted with the help of β_1 and β_2, and then the control performance can be maintained.

Substituting (9) and the controller $u_{mi}(t)$ into the sliding mode manifold, then the time derivative of (30) yields

$$
\begin{aligned}
\dot{\delta}_i(t) &= \mathcal{R}_a\left(e_{ir}(t)^{\beta_1} + \dot{e}_{ir}(t)^{\beta_2}\right) - \dot{y}_{ir}(t) \\
&\quad + C_i\left(\lambda_i \hat{\theta}_i u_{mi}^b(t) + \lambda_i \tilde{\theta}_i u_{mi}(t) + \sum_{\substack{i=1\\ i\neq j}}^{N} \mathcal{H}_{ij} x_j(t) + {\xi_i^*}^{\mathrm{T}} \psi_i(\hat{x}_i, t) + \mathcal{V}_i(t)\right).
\end{aligned} \tag{31}
$$

By solving $\dot{\delta}_i(t) = 0$, the equivalent control can be derived as

$$
u_{mi}^{\mathrm{beq}}(t) = -\left(C_i \lambda_i \hat{\theta}_i\right)^{-1}\left(\mathcal{R}_a\left({e_{ir}}^{\beta_1} + {\dot{e}_{ir}}^{\beta_2}\right) - \dot{y}_{ir} + \Psi_s(t)\right), \tag{32}
$$

where $\Psi_s(t) = C_i(\sum_{\substack{i=1\\ i\neq j}}^{N} \mathcal{H}_{ij} x_j(t) + {\xi_i^*}^{\mathrm{T}} \psi_i(\hat{x}_i, t) + \mathcal{V}_i(t) + \lambda_i \tilde{\theta}_i u_{mi}(t))$.

Considering the effects of faults, disturbances, and attacks, in this study, the observer-based reliable defense control framework is presented as

$$u_{mi}^{a}(t) = \begin{cases} -(C_i\lambda_i\hat{\theta}_i)^{-1}\left((\kappa_a + \varpi_a(t)\,\hat{\rho}_{ai})\,\mathrm{sign}(\delta_i)\right), \ t \in \mathcal{G}_{n,1}, \\ -(C_i\lambda_i\hat{\theta}_i)^{-1}\left((\kappa_b + \varpi_b(t)\,\hat{\rho}_{bi})\,\mathrm{sign}(\delta_i)\right), \ t \in \mathcal{G}_{n,2}, \end{cases} \tag{33}$$

$$u_{mi}^{b}(t) = -\left(C_i\lambda_i\hat{\theta}_i\right)^{-1}\left(\mathcal{R}_a\left(e_{ir}(t)^{\beta_1} + \dot{e}_{ir}(t)^{\beta_2}\right) - \dot{y}_{ir} + \Theta_s(t)\right), \tag{34}$$

where $\Theta_s(t) = C_i(\sum_{\substack{i=1\\ i\neq j}}^{N}\mathcal{H}_{ij}\hat{x}_j(t) + \hat{\xi}_i^{\mathrm{T}}\psi_i(\hat{x}_i,t) + \hat{\mathcal{V}}_i(t))$, $\hat{\rho}_{ai}$ and $\hat{\rho}_{bi}$ denote the estimations of ρ_{ai} and ρ_{bi}. Here, ρ_{ai} and ρ_{bi} are two unknown vectors which will be defined later. $\kappa_a > 0$ and $\kappa_b > 0$ are two scalars. $\varpi_a(t)$ and $\varpi_b(t)$ are two new vectors that need to be given later.

In the above controller (33), an inverse matrix exists. From (1), C_i is a known matrix, λ_i is the control gain. $\hat{\theta}_i$ is updated according to (14). From (2) and (14), as not all the actuators suffer from faults simultaneously, one can see that the value $\hat{\theta}_i$ exists even when a fault occurs. Then the singularity problem of the inverse matrix can be avoided.

Particularly, in this study, the event condition in the controller channel is also taken into account to achieve the resource-efficient purpose. Then, under the controller channel trigger condition, the triggered control $u_{mi}^{b}(t)$ is reformulated as

$$u_{mi}^{bt}(t) = \begin{cases} -\left(C_i\lambda_i\hat{\theta}_i(t_z)\right)^{-1}\left(\mathcal{R}_a\left(e_{ir}(t_z)^{\beta_1} + \dot{e}_{ir}(t_z)^{\beta_2}\right) - \dot{y}_{ir}(t_z) + \Theta_s(t_z)\right), \ t_z \in \mathcal{G}_{n,1}\cap\mathcal{B}_{z,1}, \\ -\left(C_i\lambda_i\hat{\theta}_i(t_{p_n+l_n})\right)^{-1}\left(\mathcal{R}_a\left(e_{irn}{}^{\beta_1} + \dot{e}_{irn}^{\beta_2}\right) - \dot{y}_{ir}(t_{p_n+l_n}) + \Theta_s(t_{p_n+l_n})\right), \ t \in \mathcal{G}_{n,2}\cap\mathcal{B}_{z,2}, \end{cases} \tag{35}$$

where $e_{irn} = e_{ir}(t_{p_n+l_n})$. $\mathcal{B}_{z,1}$ and $\mathcal{B}_{z,2}$ denote the control channel DoS attack silent and active time intervals, respectively. t_z is the triggered instant sequence in the controller channel, which is given as

$$\begin{aligned} t_{z+1} = t_z + \min\Big\{&\left\|e_{ir}(t)^{\beta_1} - e_{ir}(t_z)^{\beta_1}\right\| \geqslant \exp(-k_m) + g_m \\ &\text{or } \left\|\dot{e}_{ir}(t)^{\beta_2} - \dot{e}_{ir}(t_z)^{\beta_2}\right\| \geqslant \exp(-k_n) + g_n\Big\}, \end{aligned} \tag{36}$$

where k_m, k_n, g_m and g_n are positive scalars.

Substituting (33) and (35) into (31), it follows that

$$\begin{aligned} \dot{\delta}_i(t) = {} & \mathcal{R}_a\left(e_{ir}(t)^{\beta_1} + \dot{e}_{ir}(t)^{\beta_2}\right) - \dot{y}_{ir}(t) + C_i\Psi_s(t) - C_i\lambda_i\hat{\theta}_i\left(C_i\lambda_i\hat{\theta}_i(t_z)\right)^{-1}\Big(\mathcal{R}_a\Big(e_{ir}(t_z)^{\beta_1} \\ & + \dot{e}_{ir}(t_z)^{\beta_2}\Big) - \dot{y}_{ir}(t_z) + \Theta_s(t_z) + (\kappa_h + \varpi_h(t)\,\hat{\rho}_{ai})\,\mathrm{sign}(\delta_i(t))\Big), \ h = (a,b). \end{aligned} \tag{37}$$

In the following parts, the tracking ability of the system is analyzed even in the presence of actuator fault, disturbance, and attack. First, the sliding mode manifold reaching ability is analyzed, based on which the tracking stability is presented.

Theorem 2. Consider the controller in (33), (35), and the sliding mode manifold in (30), the trajectory of the tracking error for the system will converge to the sliding mode surface even with the DoS attack and triggered mechanism.

Proof. The Lyapunov function takes the following form:

$$V_\delta(t) = \sum_{i=1}^{N}((1-\Im(t))\,V_{\delta1}(t) + \Im(t)\,V_{\delta2}(t)), \tag{38}$$

where $V_{\delta1}(t) = \frac{1}{2}\delta_i(t)^{\mathrm{T}}\delta_i(t) + \frac{1}{2}(\rho_{ai} - \hat{\rho}_{ai})^2$, $\Im(t) = 0, t \in \mathcal{G}_{n,1}\cap\mathcal{B}_{z,1}$, $V_{\delta2}(t) = \frac{1}{2}\delta_i(t)^{\mathrm{T}}\delta_i(t) + \frac{1}{2}(\rho_{bi} - \hat{\rho}_{bi})^2$, $\Im(t) = 1, t \in \mathcal{G}_{n,2}\cap\mathcal{B}_{z,2}$.

For $t \in (\mathcal{G}_{n,1}\cap\mathcal{B}_{z,1})$, defining $\tilde{\theta}_{iz}(t) = \hat{\theta}_i(t) - \hat{\theta}_i(t_z)$, then

$$C_i\lambda_i\hat{\theta}_i(t)\left(C_i\lambda_i\hat{\theta}_i(t_z)\right)^{-1} = \left(C_i\lambda_i\tilde{\theta}_{iz}(t) + C_i\lambda_i\hat{\theta}_i(t_z)\right)\left(C_i\lambda_i\hat{\theta}_i(t_z)\right)^{-1}$$

$$= C_i\lambda_i\tilde{\theta}_{iz}(t)\left(C_i\lambda_i\hat{\theta}_i(t_z)\right)^{-1} + I. \tag{39}$$

By some tedious calculations, Eq. (37) can be simplified as

$$\dot{\delta}_i(t) = \mathcal{R}_a\left(e_{ir}(t)^{\beta_1} - e_{ir}(t_z)^{\beta_1} + e_{ir}(t)^{\beta_2} - e_{ir}(t_z)^{\beta_2}\right) + \Phi_s(t) - (\kappa_a + \varpi_a(t)\hat{\rho}_{ai})\,\mathrm{sign}(\delta_i(t)), \tag{40}$$

where

$$\begin{aligned}\Phi_s(t) = & -\dot{y}_{ir}(t) + \dot{y}_{ir}(t_z) + C_i\Psi_s(t) - C_i\lambda_i\tilde{\theta}_{iz}(t)\left(C_i\lambda_i\hat{\theta}_i(t_z)\right)^{-1}\Big(\mathcal{R}_a\left(e_{ir}(t_z)^{\beta_1} + \dot{e}_{ir}(t_z)^{\beta_2}\right)\\ & -\dot{y}_{ir}(t_z) + \Theta_s(t_z) + (\kappa_a + \varpi_a(t)\hat{\rho}_{ai})\,\mathrm{sign}(\delta_i(t))\Big).\end{aligned}$$

Defining $\Omega_s = \|\mathcal{R}_a(e_{ir}(t)^{\beta_1} - e_{ir}(t_z)^{\beta_1} + \dot{e}_{ir}(t)^{\beta_2} - \dot{e}_{ir}(t_z)^{\beta_2})\| + \|\Phi_s(t)\|$, from the definition of Ω_s, one can check that Ω_s is bounded and unknown. In this subsection, the FLS technique is also used to identify the unknown part Ω_s.

Recalling the FLS technique scheme, we have $\Omega_s = \mathcal{F}^{\mathrm{T}}\mu(t) + \ell_s$, where $\mathcal{F}$, $\mu(t)$ and ℓ_s have similar meanings of (7). Then one has

$$\delta_i(t)\Omega_s \leqslant \|\delta_i(t)\|\left\|\mathcal{F}^{\mathrm{T}}\right\|\|\mu(t)\| + \|\delta_i(t)\|\ell_s = \|\delta_i(t)\|\rho_{ai}\varpi_a(t), \tag{41}$$

where $\rho_{ai} = [\ \|\mathcal{F}^{\mathrm{T}}\|\ \ \ell_s\ ]$, $\varpi_a(t) = [\ \|\mu(t)\|\ \ 1\ ]^{\mathrm{T}}$. Here the estimation $\hat{\rho}_{ai}$ is updated as $\dot{\hat{\rho}}_{ai} = \|\delta_i(t)\|\varpi_a(t)$.

For $\Im(t) = 0, t \in \mathcal{G}_{n,1} \cap \mathcal{B}_{z,1}$, the time derivative of (38) can be calculated as

$$\dot{V}_\delta(t) = \sum_{i=1}^{N}\dot{V}_{\delta 1}(t) = \sum_{i=1}^{N}\left(\delta_i(t)^{\mathrm{T}}\dot{\delta}_i(t) + (\rho_{ai} - \hat{\rho}_{ai})\left(\dot{\rho}_{ai} - \dot{\hat{\rho}}_{ai}\right)\right),\ \Im(t) = 1. \tag{42}$$

From (40), it is straightforward that

$$\begin{aligned}\delta_i(t)^{\mathrm{T}}\dot{\delta}_i(t) & = \mathcal{R}_a\left(e_{ir}(t)^{\beta_1} - e_{ir}(t_z)^{\beta_1} + \dot{e}_{ir}(t)^{\beta_2} - \dot{e}_{ir}(t_z)^{\beta_2}\right) + \Phi_s(t) - (\kappa_a + \varpi_a(t)\hat{\rho}_{ai})\,\mathrm{sign}(e_{ir})\\ & \leqslant \|\delta_i(t)\|\rho_{ai}\varpi_a(t) - \delta_i(t)^{\mathrm{T}}(\kappa_a + \varpi_a(t)\hat{\rho}_{ai})\,\mathrm{sign}(\delta_i(t))\\ & = \|\delta_i(t)\|(\rho_{ai}\varpi_a(t) - (\kappa_a + \varpi_a(t)\hat{\rho}_{ai})).\end{aligned} \tag{43}$$

Then it follows that

$$\begin{aligned}\dot{V}_\delta(t) & \leqslant \sum_{i=1}^{N}(\|\delta_i(t)\|(\rho_{ai}\varpi_a(t) - (\kappa_a + \varpi_a(t)\hat{\rho}_{ai}))) + \sum_{i=1}^{N}\left((\rho_{ai} - \hat{\rho}_{ai})\left(\dot{\rho}_{ai} - \dot{\hat{\rho}}_{ai}\right)\right)\\ & = \sum_{i=1}^{N}(\|\delta_i(t)\|\varpi_a(t)(\rho_{ai} - \rho_{ai}) - \kappa_a\|\delta_i(t)\|) + \sum_{i=1}^{N}\left((\rho_{ai} - \hat{\rho}_{ai})\left(\dot{\rho}_{ai} - \dot{\hat{\rho}}_{ai}\right)\right)\\ & < -\sum_{i=1}^{N}(\kappa_a\|\delta_i(t)\|).\end{aligned} \tag{44}$$

For $t \in (\mathcal{G}_{n,2} \cap\ \mathcal{B}_{z,2})$, by some tedious calculations, the similar results can be obtained, and we omit it here. Then, it is straightforward that $\dot{V}_\delta(t) < 0$, which means that the sliding motion will happen and the reachability of the manifold can be maintained.

Now we are in the position to analyze the tracking stability of the system. From (44), as $\dot{V}_\delta(t) < 0$, the sliding manifold $\delta_i(t) = 0$ can be achieved. From (30), it can be obtained that $\int_0^t R_a(e_{ir}(t)^{\beta_1} + \dot{e}_{ir}(t)^{\beta_2})\mathrm{d}t - \int_0^t C_i\lambda_i\hat{\theta}_i u_{mi}^a(t)\mathrm{d}t + e_{ir}(t) = 0$. By using $e_{ir}(t) = \int_0^t \dot{e}_{ir}(t)\,\mathrm{d}t$, one has $(\mathcal{R}_a(e_{ir}(t)^{\beta_1} + e_{ir}(t)^{\beta_2}) - C_i\lambda_i\hat{\theta}_i u_{mi}^a(t)) + \dot{e}_{ir}(t) = 0$. From $\dot{e}_{ir}(t) = C_i\dot{x}_i(t) - \dot{y}_{ir}(t)$ and (9), it can be obtained that $\dot{e}_{ir}(t) = C_i\lambda_i\theta_i u_{mi}(t) + C_i(\sum_{\substack{i=1\\ i\neq j}}^{N}\mathcal{H}_{ij}x_j(t) + \mathcal{V}_i(t)) - \dot{y}_{ir}(t))$. As $u_{mi}(t) = u_{mi}^a(t) + u_{mi}^b(t)$, then $C_i\lambda_i\theta_i u_{mi}(t) = C_i\lambda_i\theta_i u_{mi}^a(t) + C_i\lambda_i\theta_i u_{mi}^b(t)$. From the definition of $u_{mi}^b(t)$, we have

$$C_i\lambda_i\theta_i u_{mi}^b(t) = -C_i\lambda_i\theta_i(C_i\lambda_i\hat{\theta}_i)^{-1}\left(\mathcal{R}_a\left(e_{ir}(t)^{\beta_1} + e_{ir}(t)^{\beta_2}\right) - \dot{y}_{ir}(t) + \Theta_s(t)\right).$$

Note that $C_i\lambda_i\theta_i(C_i\lambda_i\hat{\theta}_i)^{-1} = (C_i\lambda_i\hat{\theta}_i + C_i\lambda_i\tilde{\theta}_i)(C_i\lambda_i\hat{\theta}_i)^{-1} = I + C_i\lambda_i\tilde{\theta}_i(C_i\lambda_i\hat{\theta}_i)^{-1}$, it can be checked that

$$\begin{aligned} C_i\lambda_i\theta_i u_{mi}^b(t) = &-\left(\mathcal{R}_a\left(e_{ir}(t)^{\beta_1} + e_{ir}(t)^{\beta_2}\right) - \dot{y}_{ir}(t) + \Theta_s(t)\right) \\ &- C_i\lambda_i\tilde{\theta}_i\left(C_i\lambda_i\hat{\theta}_i\right)^{-1}\left(\mathcal{R}_a\left(e_{ir}(t)^{\beta_1} + e_{ir}(t)^{\beta_2}\right) - \dot{y}_{ir}(t) + \Theta_s(t)\right). \end{aligned}$$

By utilizing the above condition, we have

$$\begin{aligned} &R_a\left(e_{ir}(t)^{\beta_1} + \dot{e}_{ir}(t)^{\beta_2}\right) - \lambda_i\hat{\theta}_i u_{mi}^a(t) + C_i\lambda_i\theta_i u_{mi}(t) \\ &+ C_i\left[\sum_{\substack{i=1\\ i\neq j}}^{N}\mathcal{H}_{ij}x_j(t) + {\xi_i}^{*\mathrm{T}}\psi_i(\hat{x}, t) + \mathcal{V}_i(t)\right] - \dot{y}_{ir}(t) \\ &= R_a\left(e_{ir}(t)^{\beta_1} + \dot{e}_{ir}(t)^{\beta_2}\right) + \Xi_a(t) = 0, \end{aligned}$$

where

$$\begin{aligned} \Xi_a(t) = &C_i\lambda_i\tilde{\theta}_i u_{mi}^a(t) + C_i\left[\sum_{\substack{i=1\\ i\neq j}}^{N}\mathcal{H}_{ij}\tilde{x}_j(t) + \tilde{\xi}_i^{\mathrm{T}}\psi_i(\hat{x}, t) + \tilde{\mathcal{V}}_i(t)\right] \\ &- C_i\lambda_i\tilde{\theta}_i\left(C_i\lambda_i\hat{\theta}_i\right)^{-1}\left(-\dot{y}_{ir}(t) + \Theta_s(t) + \mathcal{R}_a\left(e_{ir}(t)^{\beta_1} + e_{ir}(t)^{\beta_2}\right)\right). \end{aligned}$$

As the convergence of the observation errors can be maintained, $\Xi_a(t)$ is bounded. From the above equation, one can deduce that $e_{ir}(t)$ can be bounded, and then the convergence of $e_{ir}(t)$ can be guaranteed. For $t \in \mathcal{G}_{n,2}$, a similar calculation can be obtained, and then we can conclude that the tracking error is bounded.

3 Example analysis

In this section, to show the control performance of the presented approach, two cases are simulated.

Case 1. In this case, an interconnected power network system benchmark in [20] is addressed. The system can be described as

$$\begin{cases} \Delta\dot{\delta}_i(t) = \Delta\omega_i(t), \ i = 1, 2, \\ \Delta\dot{\omega}_i(t) = \frac{D_i}{2H_i}\Delta\omega_i(t) + \frac{\omega_0}{2H_i}\Delta P_{mi} + \frac{\omega_0}{2H_i}\Delta P_{ei}, \\ \frac{\omega_0}{2H_i}\Delta\dot{P}_{mi} = \frac{\omega_0}{2H_iT_i}\left(-\Delta P_{mi} - k_i\Delta\omega_i(t) + u_i(t) + d_i(t)\right), \end{cases} \tag{45}$$

where $\Delta\delta_i$, $\Delta\omega_i$, ΔP_{mi}, and ΔP_{ei} denote the deviations of rotor angle, relative rotorspeed, mechanical input power, and active power of the power system, respectively. $u_i(t)$ is the deviation of the valve opening, which can be acted as the control input. $d_i(t)$ represent the external disturbance. $D_i = 3$, $H_i = 12$, $T_i = 15$, and $\omega_0 = 100$. Here, k_i is assumed to be unknown, the term ΔP_{ei} is defined as

$$\begin{cases} \Delta P_{e1} = \frac{-E_1E_2}{X}\left[\sin(\delta_1 - \delta_2) - \sin(\delta_{10} - \delta_{20})\right], \\ \Delta P_{e2} = -\Delta P_{e1}, \end{cases} \tag{46}$$

where $E_1 = 2$ and $E_2 = 3$ are two constants, $X = 15$, $\delta_{10} = 1$ rad and $\delta_{20} = 1.2$ rad denote the steady state angles of the first and second generator and $\delta_i = \delta_{i0} + \Delta\delta_i$. The measured output rotor angle of each generator is $y_i = \delta_i$ $(i = 1, 2)$.

The state variables are chosen as $[x_{i,1}, x_{i,2}, x_{i,3}] = [\Delta\delta_i(t), \Delta\omega_i(t), (\omega_0/2H_i)\Delta P_{mi}]$, the initial state values are set as $[x_{1,1}(0), x_{1,2}(0), x_{1,3}(0)] = [0.25, 0.05, -0.1]$ and $[x_{2,1}(0), x_{2,2}(0), x_{2,3}(0)] = [0.15, 0.1, -0.1]$. The fuzzy membership functions are chosen as $\mu_{a_i^k} = \exp((\hat{x}_i + 3 - k)^2/8)$ $(i = 1, 2; k = 1, 2, 3, 4, 5)$. In this study, the attack is aperiodic. Here, we give three attack intervals randomly.

Choose

$$L_{s1}=\begin{bmatrix}-2 & -0.4 & -2\\ -4 & -2 & -2\\ -2 & -2 & -2\end{bmatrix},\quad L_{s2}=\begin{bmatrix}-5 & -2.5 & -10\\ -1 & -5 & -5\\ -2.5 & -5 & -5\end{bmatrix}.$$

By solving the condition (21), one has

$$P_1=\begin{bmatrix}1.6366 & -0.5741 & 0.1412\\ -0.5741 & 1.1160 & -0.6411\\ 0.1412 & -0.6411 & 0.8751\end{bmatrix},\quad P_2=\begin{bmatrix}1.6366 & -0.3622 & -0.2293\\ -0.3622 & 0.8684 & -0.5173\\ -0.2293 & -0.6411 & 1.3703\end{bmatrix},\quad L_1=\begin{bmatrix}-0.4412\\ -1.8228\\ -1.8758\end{bmatrix},$$

$$L_2=\begin{bmatrix}-6.4293 & 1.1023 & -23.3534\end{bmatrix}^{\mathrm{T}}.$$

By choosing $\kappa_s=0.5$, $\kappa_e=1$, we have the observer scheme in (12), (14) and (20). Then, we have the estimation values.

Setting the parameters $\beta_1=0.8$, $\beta_2=1.1$, $\beta_a=1$, $\beta_b=1.2$, $\beta_c=1$, $c_a=1$, $c_b=1.1$, $k_m=0.5$, $k_n=0.5$, $g_m=0.01$, $g_n=0.01$, $\kappa_a=0.3$, $\kappa_b=0.4$, one can obtain the sliding mode manifold in (30) and construct the event condition in (36), and subsequently the controller in (35) can be obtained. The other control parameters are listed as $m_a=1.2$, $m_b=1.5$, $\pi_{m1}=0.1$, $\pi_{m2}=0.8$.

The unexpected actuator fault and disturbance are assumed as

$$u_{q1}(t)=u_{q2}(t)=\begin{cases}0.2,\ 0\leqslant t<10,\\ 1.6\sin(2t-3),\ 10\leqslant t<15,\\ 8\sin(2t),\ 15\leqslant t\leqslant 35,\end{cases}\quad \mathcal{W}_1(t)=\begin{cases}0,\ 0\leqslant t<15,\\ 0.2\sin(0.5t),\ 15\leqslant t\leqslant 35,\end{cases}\quad \mathcal{W}_2(t)=0.$$

The simulation results are shown in Figure 3. The rotor angles of generators 1 and 2 are depicted in Figures 3(a) and (b), the grey shadow parts imply that the DoS attackers are active while the left parts mean that the attackers are sleeping. As seen from Figures 3(a) and (b), when DoS is active, the trajectories of the generator deviate from the desired references and the tracking performance are degraded.

Here, to show the effectiveness of the presented scheme, the method in [20] is also applied, where $\alpha=10$, $\mu=580$, $\beta=5$, $c_{i,1}=9.7235$, $c_{i,2}=6$, $c_{i,3}=12$, $\tau_{i,2}=\tau_{i,3}=0.2$, $\sigma_1=\sigma_2=6$, $\Gamma_i=I_2$, $i=1,2$. Meanwhile, the control approach in [27] is also simulated. In addition, the presented compensation mechanisms are also applied to the other two methods to guarantee the fairness of comparison. Furthermore, to show the effects of the attacks, the comparative results of the trajectories without attackers and only with attackers are also plotted. As depicted in Figure 3(c), when we only consider attackers, the proposed method in this study has better recovering performance. One can also see from Figures 3(a) and (b) that the method in [27] may be unstable when attacker is active. The results in [20] can be stable, but the chattering is harder and the recovering time is long compared with the presented control scheme.

On the other hand, during the DoS sleeping period, the tracking accuracy is recovering constantly, and the control performance can be maintained after a short time period. As verified in Figures 3(a) and (b), the designed approach has a better recovering ability, which means once the DoS attack stops, the tracking performance can be recovered with the presented FTC framework even in the presence of a fault and lumped disturbance. The triggered time intervals are shown in Figures 3(d) and (e), from which, 13.14% and 16.28% communication resources are saved in the two subsystems, respectively. Additionally, the estimation performance of the lumped disturbance is given in Figure 3(f), as observed in this figure, one can see that the presented observer has good estimation ability.

Case 2. In this case, an inverted pendulum system that is connected by a spring is considered [3]. The system can be described as

$$\begin{cases}\dot{x}_{1,1}=G_{1,1}(x_{1,1})+x_{1,2}+\Delta f_{1,1}(x,t),\\ \dot{x}_{1,2}=G_{1,2}(x_1)+{\theta_1}^{\mathrm{T}}u_1(t)+\Delta f_{1,2}(x,t)+\Pi_{12}(t),\\ \dot{x}_{2,1}=G_{2,1}(x_{2,1})+x_{2,2}+\Delta f_{2,1}(x,t),\\ \dot{x}_{2,2}=G_{2,2}(x_2)+{\theta_2}^{\mathrm{T}}u_2(t)+\Delta f_{2,2}(x,t)+\Pi_{21}(t),\\ y_i=x_{i,1},\ i=1,2,\end{cases}\tag{47}$$

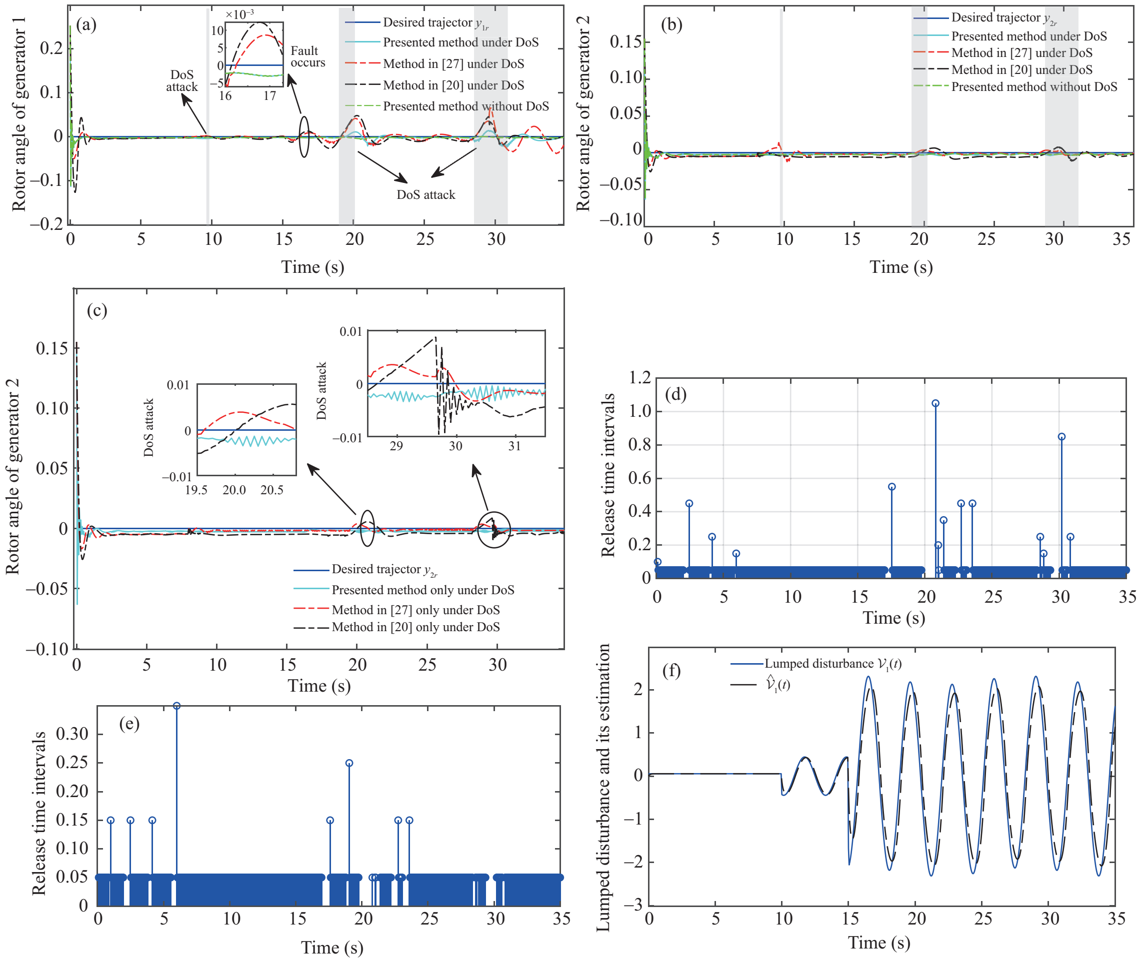

Figure 3 (Color online) Trajectory of the rotor angle for (a) generator 1 under different approaches, (b) generator 2 under different approaches, and (c) generator 2 only under DoS with different approaches; time intervals of the event condition for (d) generator 1 and (e) generator 2; (f) lumped disturbance $\mathcal{V}_1(t)$ and $\hat{\mathcal{V}}_1(t)$.

where $x_{1,1} = \omega_1$, $x_{2,1} = \omega_2$, $G_{1,1}(x_{1,1}) = 0$, $\Delta f_{1,1}(x,t) = 0$, $G_{1,2}(x_1) = (\frac{m_1 gr}{J_1} - \frac{\varpi r^2}{4J_1}) \sin(x_{1,1})$, $\Pi_{12}(t) = \frac{\varpi r^2}{4J_1} \sin(x_{2,1})$, $\Delta f_{1,2}(x,t) = \frac{x_{1,1}}{1+x_{1,1}^2}$, $\theta_1 = [6,6]^{\mathrm{T}}$, $G_{2,1}(x_{2,1}) = 0$, $\Delta f_{2,1}(x,t) = 0$, $G_{2,2}(x_2) = (\frac{m_2 gr}{J_2} - \frac{\varpi r^2}{4J_2}) \sin(x_{2,1})$, $\Delta f_{2,2}(x,t) = \frac{x_{2,1}}{1+x_{2,1}^2}$, $\Pi_{21}(t) = \frac{\varpi r^2}{4J_2} \sin(x_{1,1})$, $\theta_1 = [5,5]^{\mathrm{T}}$. Here ω_1 and ω_2 are the angular displacements of the pendulum system. $m_i\,(i=1,2)$ denote the mass, J_1 and J_2 represent the moments of inertia. ϖ is the spring constant, r denotes the pendulum height. The above parameter values are listed as follows, $m_1 = 2$ kg, $m_2 = 2.5$ kg, $J_1 = 5$ kg$\cdot$m^2, $J_2 = 6.25$ kg$\cdot$m^2, $\varpi = 100$ N/m, $r = 0.5$ m, $g = 9.81$ m/s^2.

Similarly, by choosing the matrix L_{s1} and L_{s2}, we have the observer gains L_1 and L_2; here, L_{s1} and L_{s2} are chosen as in case 1. Setting the controller parameters $\beta_1 = 0.75$, $\beta_2 = 1.2$, $k_m = 0.5$, $k_n = 0.5$, $g_m = 0.01$, $g_n = 0.01$, $\kappa_a = 0.3$, $\kappa_b = 0.4$, one can construct the controller in (35). The fuzzy membership functions are chosen as in case 1, i.e., $\mu_{a_i^k} = \exp((\hat{x}_i + 3 - k)^2/8)\,(i=1,2; k=1,2,3,4,5)$. From the fuzzy logic system theory in (7), the two functions $\hat{G}_{1,2}(x_1) = \hat{\xi}_1^{\mathrm{T}} \psi_1(\hat{x}_1, t)$ and $\hat{G}_{2,2}(x_2) = \hat{\xi}_2^{\mathrm{T}} \psi_2(\hat{x}_2, t)$ can be constructed.

In this case, the attack condition is given randomly. The unexpected faults and disturbances are assumed as

$$u_{q1}(t) = u_{q2}(t) = \begin{cases} 0, \ 0 \leqslant t \leqslant 6, \\ 0.35 \sin(2.5t - 2), \ 6 < t \leqslant 15, \\ 0.6, \ 15 < t \leqslant 35, \end{cases} \qquad \mathcal{W}_1(t) = \mathcal{W}_2(t) = 0.6\cos(t).$$

Given the desired reference as $y_{ir}(t) = 0 \ (i=1,2)$. The initial values are given as $x_{i,1}(0) = x_{i,2}(0) =$

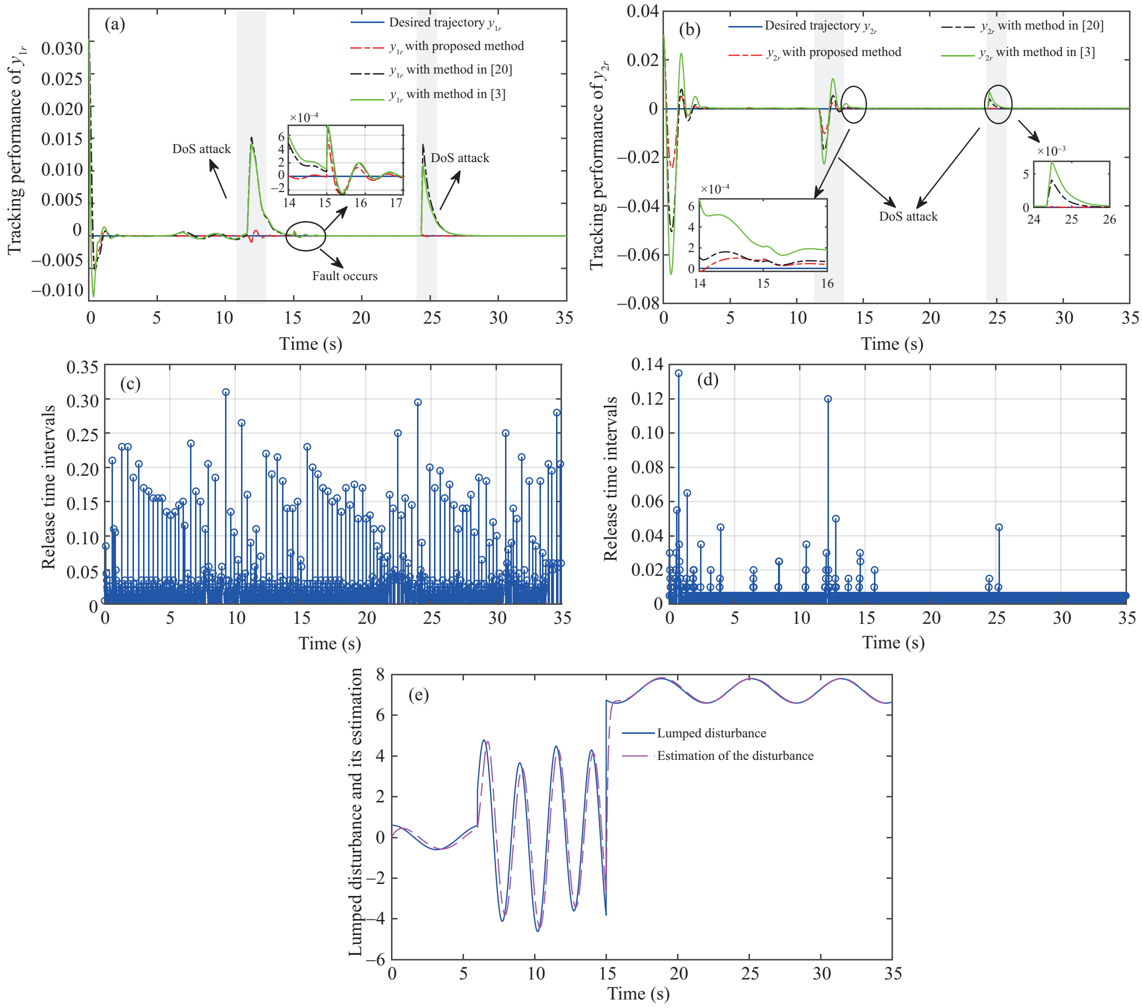

Figure 4 (Color online) Trajectory tracking results of (a) inverted pendulum 1 and (b) inverted pendulum 2 with different methods; time intervals of the event conditions for (c) inverted pendulum 1 and (d) inverted pendulum 2; (e) lumped disturbance and its estimation.

0.03 ($i = 1, 2$). The left design parameters are chosen as in case 1. The simulation results are shown in Figure 4.

Figures 4(a) and (b) show the angular displacements tracking results of the pendulum system. One can see from Figures 4(a) and (b) that the trajectory tracking purpose can be achieved for the two subsystems with the presented reliable defense control method in the occurrence of actuator faults, disturbances, and attacks.

In this case, the DoS attack defense control approach in [20] and the fault tolerance control method in [3] for the interconnected nonlinear system are also applied. Note that the fault tolerance section is not included in the method [20]; additionally, the method in [3, 20] does not involve an event scheme. Here, we add a fault compensation part in [3], and an event scheme is introduced in both [3, 20], so that a fair comparison can be made. As depicted in Figures 4(a) and (b), as both the fault compensation part has been included, the tracking performance can be guaranteed when a fault occurs. However, the methods in [3, 20] do not include the DoS defense control part, the trajectories will deviate from the desired one when the attackers are launched in the communication channels. Moreover, the recovery speeds of the other two methods are slower when the attackers are sleeping compared with the presented method. This implies that when the attackers stop, the trajectory can track the desired one with the control remaining scheme in the proposed method.

Figures 4(c) and (d) express the time intervals of the event conditions for the two subsystems. From the two figures, the transmitted resources in the communication channels are saved. To show the disturbance estimation performance, the disturbance estimated value is shown in Figure 4(e). From Figure 4(e), one

Table 1 Comparison results of RMSE of different methods

Subsystem	Presented method	Method in [3]	Method in [20]
Subsystem 1	0.0015	0.0026	0.0030
Subsystem 2	0.0035	0.0086	0.0065

can see that the presented observer has good estimation performance, which verifies the feasibility of the compensation scheme by utilizing the estimation information to design the controller. Moreover, the root mean square errors (RMSE) of different methods for the two subsystems are listed in Table 1. From the table, one can see that control priorities are better than the other two methods, which in return verifies the fault tolerance ability, disturbance attenuation performance, and attack-defense ability of the proposed method.

4 Conclusion

In this study, an event-driven observer-based FTC architecture is presented for a class of interconnected nonlinear systems in the occurrence of actuator faults, lumped disturbances, and DoS attacks. In this control framework, the fuzzy logic theory is used to approximate the nonlinear function, based on which a fuzzy nonlinear observer is constructed. Using the observer outputs, an adaptive sliding mode manifold is designed, and the equal control law is subsequently derived. To conserve the communication resources, a novel event condition in the control channel is designed, and the event-driven control approach is developed. The tracking performance can be established even in the presence of faults and DoS attacks under the proposed control scheme. Finally, the simulation results demonstrate the fault tolerance, disturbance rejection, and DoS compensation capabilities of the presented approach.

Because of the importance of system performance recovery, our future research will focus on FTC and optimal control for more generalized interconnected stochastic nonlinear systems in the presence of multifaults, disturbances, and attacks.

Acknowledgements This work was supported by Scientific and Technical Programs of Sichuan Province of China (Grant No. 2021YJ0092) and National Key Research and Development of China (Grant No. 2018YFB1307401).

References

1 Keller J Y, Chabir K, Sauter D. Input reconstruction for networked control systems subject to deception attacks and data losses on control signals. Int J Syst Sci, 2016, 47: 814–820
2 Ye D, Diao N N, Zhao X G. Fault-tolerant controller design for general polynomial-fuzzy-model-based systems. IEEE Trans Fuzzy Syst, 2018, 26: 1046–1051
3 Tong S, Huo B, Li Y. Observer-based adaptive decentralized fuzzy fault-tolerant control of nonlinear large-scale systems with actuator failures. IEEE Trans Fuzzy Syst, 2014, 22: 1–15
4 Guo B, Chen Y. Event-triggered robust adaptive sliding mode fault-tolerant control for nonlinear systems. IEEE Trans Ind Inf, 2020, 16: 6982–6992
5 Xiao S, Han Q L, Ge X, et al. Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks. IEEE Trans Cybern, 2020, 50: 1220–1229
6 Chabukswar R, Mo Y, Sinopoli B. Detecting integrity attacks on SCADA systems. IFAC Proc Vol, 2011, 44: 11239–11244
7 Li X, Wen C, Chen C. Resilient cooperative control for networked Lagrangian systems against DoS attacks. IEEE Trans Cybern, 2022, 52: 836–848
8 Chen C C, Xu S S D, Liang Y W. Study of nonlinear integral sliding mode fault-tolerant control. IEEE/ASME Trans Mechatron, 2016, 21: 1160–1168
9 Li Y X, Yang G H. Fuzzy adaptive output feedback fault-tolerant tracking control of a class of uncertain nonlinear systems with nonaffine nonlinear faults. IEEE Trans Fuzzy Syst, 2016, 24: 223–234
10 Shen Q, Yue C, Goh C H, et al. Active fault-tolerant control system design for spacecraft attitude maneuvers with actuator saturation and faults. IEEE Trans Ind Electron, 2019, 66: 3763–3772
11 Jing Y H, Yang G H. Fuzzy adaptive fault-tolerant control for uncertain nonlinear systems with unknown dead-zone and unmodeled dynamics. IEEE Trans Fuzzy Syst, 2019, 27: 2265–2278
12 Wu C, Liu J, Xiong Y, et al. Observer-based adaptive fault-tolerant tracking control of nonlinear nonstrict-feedback systems. IEEE Trans Neural Netw Learn Syst, 2018, 29: 3022–3033
13 Van M, Ge S S. Adaptive fuzzy integral sliding-mode control for robust fault-tolerant control of robot manipulators with disturbance observer. IEEE Trans Fuzzy Syst, 2021, 29: 1284–1296
14 Zhang L, Yang G H. Observer-based adaptive decentralized fault-tolerant control of nonlinear large-scale systems with sensor and actuator faults. IEEE Trans Ind Electron, 2019, 66: 8019–8029
15 Hu S, Yue D, Han Q L, et al. Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. IEEE Trans Cybern, 2020, 50: 1952–1964
16 Ma R, Shi P, Wu L. Dissipativity-based sliding-mode control of cyber-physical systems under denial-of-service attacks. IEEE Trans Cybern, 2021, 51: 2306–2318
17 Wu C, Wu L, Liu J, et al. Active defense-based resilient sliding mode control under denial-of-service attacks. IEEE Trans Inform Forensic Secur, 2020, 15: 237–249
18 de Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service. IEEE Trans Automat Contr, 2015, 60: 2930–2944

19 Jiang X, Mu X, Hu Z. Decentralized adaptive fuzzy tracking control for a class of nonlinear uncertain interconnected systems with multiple faults and denial-of-service attack. IEEE Trans Fuzzy Syst, 2021, 29: 3130–3141
20 An L, Yang G H. Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks. IEEE Trans Cybern, 2019, 49: 827–838
21 Shao X, Ye D. Fuzzy adaptive event-triggered secure control for stochastic nonlinear high-order MASs subject to DoS attacks and actuator faults. IEEE Trans Fuzzy Syst, 2021, 29: 3812–3821
22 Zhang C H, Yang G H. Event-triggered global finite-time control for a class of uncertain nonlinear systems. IEEE Trans Automat Contr, 2020, 65: 1340–1347
23 Wang A, Liu L, Qiu J, et al. Event-triggered robust adaptive fuzzy control for a class of nonlinear systems. IEEE Trans Fuzzy Syst, 2019, 27: 1648–1658
24 Li J, Yang Z, Mu X, et al. Passivity-based event-triggered fault tolerant control for nonlinear networked control system with actuator failures and DoS jamming attacks. J Franklin Institute, 2020, 357: 9288–9307
25 Tang Y, Zhang D, Shi P, et al. Event-based formation control for nonlinear multiagent systems under DoS attacks. IEEE Trans Automat Contr, 2021, 66: 452–459
26 Pan H, Chang X, Zhang D. Event-triggered adaptive control for uncertain constrained nonlinear systems with its application. IEEE Trans Ind Inf, 2020, 16: 3818–3827
27 Li Y M, Tong S C. Prescribed performance adaptive fuzzy output-feedback dynamic surface control for nonlinear large-scale systems with time delays. Inf Sci, 2015, 292: 125–142