Memory-Based Continuous Event-Triggered Control for Networked T–S Fuzzy Systems Against Cyberattacks

Zhou Gu, Peng Shi, *Fellow, IEEE*, Dong Yue, *Senior Member, IEEE*, Shen Yan, and Xiangpeng Xie

***Abstract*—This article investigates the problem of resilient control for the Takagi–Sugeno (T–S) fuzzy systems against bounded cyberattack. A novel memory-based event triggering mechanism (ETM) is developed, by which the past information of the physical process through the window function is utilized. Using such an ETM cannot only lead to a lower data-releasing rate but also reduce the occurrence of wrong triggering event. Furthermore, the frequency of event generation is relatively smoother than existing ETMs. From the current releasing instant to the next, two periods are designed. The ETM works only when the first period ends, thereby avoiding the Zeno behavior that commonly exists in continuous ETM designs. The control system is then formulated as a switched fuzzy control system with two modes in each releasing period. Based on an assumption of secure control, and the proposed ETM, sufficient conditions are obtained to guarantee the exponential stability of networked T–S fuzzy systems in the presence of deception attacks in secure sense. Finally, a single-link rigid robot is taken as an example to illustrate the advantages of theoretical results.**

***Index Terms*—Deception attacks, memory-based event-triggered mechanism, networked Takagi–Sugeno (T–S) fuzzy systems.**

I. Introduction

As IS WELL known, most of the physical dynamical systems have a nonlinear nature. The Takagi–Sugeno (T–S) fuzzy model is a popular method to approximate nonlinear systems by using a set of local linear systems that are interpolated by membership functions [1]. A large amount of research results on the T–S fuzzy model can be found in many fields, to mention a few, in [2], the T–S fuzzy model was utilized to characterize uncertainties of active suspension control systems. The nonlinear dynamic in [3] was modeled by an interval type-2 fuzzy system with bounded lower and upper membership functions. T–S fuzzy-model-based power management was studied for energy storage systems in [4]. The problem of H_∞ control was studied in [5] for discrete-time T–S fuzzy systems by using a finite-sum inequality to get a less conservative result.

Over the past few years, cyber–physical systems (CPSs) have become an emergent approach, which has aroused intensive interest in the scientific community [6]. The physical elements among CPSs interact information via network. Due to the advantages of low cost, ease of maintenance, and high flexibility, CPS has a wide range of application, and has a high impact on industrial automation. One of a critical issue in designing CPSs is the analysis and synthesis of networked control systems (NCSs), especially for nonlinear NCSs. As a communication media of control information, the network with a limited bandwidth will affect the physical processes and vice versa [6], [7].

The previous research has shown that the ETM can make more effective utilization of network bandwidth in NCSs compared to the conventional time-triggered mechanism (TTM) [8], [9]. However, there are at least two important issues need to be considered in designing ETMs: 1) constructing a reasonable event-triggering condition to generate releasing event at a proper instant; and 2) making a tradeoff between the network performance and the control performance of physical processes. Under the TTM, the releasing period is fixed, while under the ETM, the release period is determined by the event triggering condition. Therefore, the period of TTM usually has conservativeness that may result in data redundancy during information transmission, which increases the burden of NCSs. Hence, there is no doubt that the ETM is a promising alternative to TTM for NCSs, although there are many challenges in theory and implementation, such as stability and stabilization and Zeno behavior. In the last decades, the research on ETM has gained fruitful achievements in the fields of control and filter design [10]. Generally, there are twofold in developing the ETM: continuous type [11]–[13] and discrete type [14]–[16]. In [11], the authors designed an ETM-based NCS using the two-step design method. The interevent time (IET, the time from the current releasing instant to the next) was theoretically proven to be positive under some special cases

Manuscript received December 23, 2019; revised March 22, 2020 and June 6, 2020; accepted July 24, 2020. Date of publication July 29, 2020; date of current version October 6, 2021. This work was supported by the National Natural Science Foundation of China under Grant 61473156 and Grant 61773221. *(Corresponding author: Zhou Gu.)*

Zhou Gu is with the College of Mechanical, and Electronic Engineering, Nanjing Forestry University, Nanjing 210037, China, and also with the School of Electrical, and Electronic Engineering, University of Adelaide, Adelaide, SA 5005, Australia (e-mail: gzh1808@163.com).

Peng Shi is with the School of Electrical, and Electronic Engineering, University of Adelaide, Adelaide, SA 5005, Australia (e-mail: peng.shi@adelaide.edu.au).

Dong Yue and Xiangpeng Xie are with the Institute of Advanced Technology, Nanjing University of Posts, and Telecommunications, Nanjing 210023, China (e-mail: medongy@vip.163.com; xiexiangpeng1953@163.com).

Shen Yan is with the College of Mechanical and Electronic Engineering, Nanjing Forestry University, Nanjing 210037, China (e-mail: yanshenzdh@gmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TFUZZ.2020.3012771.

Digital Object Identifier 10.1109/TFUZZ.2020.3012771

in [12], however, for some cases IET possibly tends to be zero, which is called Zeno behavior. The authors in [13] proposed an integral-based ETM for linear time invariant (LTI) systems. It is noticed that the most difficult issue in designing continuous type ETM for NCSs is to overcome Zeno behavior. For this purpose, the authors in [17] studied an approach by dividing each releasing period into two intervals, the first interval is a waiting period, and the other is triggering period, that is, the IET is always greater than the waiting period. Another difficulty for continuous type ETM is the problem of codesign of both the ETM and the controller. In this context, the discrete type ETM was investigated in [14]. Under this type of ETM, the discrete sampling data are utilized in the event-triggering condition. Consequently, the IET is at least greater than the sampling period, and the controller is convenient to be obtained by converting the hybrid systems into the delay systems. However, the discrete type ETM is more conservative compared to the continuous type ETM. Furthermore, it is hard to use the past information under discrete type ETMs. In [15], two-step sampling data are utilized to improve the efficacy of discrete type ETM. On the contrary, continuous type ETM is more convenient to introduce the past information into the ETM, for example, in [18], the authors constructed an integral ETM for fault detection filter design of unmanned vehicles. However, it is unreasonable for all the past information with a same weight in each integral interval, which is a main motivation of the current study.

For NCSs, the signal transmission depends on the network. Therefore, the control system becomes more vulnerable to attack. The malicious attack may degrade the performance of control systems or cause severe consequences. Over the past few decades, much attention has been paid to the issue of secure control, see [19]–[24] and references therein. For example, the estimation and detection connected vehicle systems with consideration of denial of service type cyberattacks were studied in [19].

The authors in [20] investigated a resilient state feedback control against DoS attack by modeling the closed-looped NCSs as an aperiodic sampled-data control system.

The authors discussed the problem of secure control when the system suffers from replay attacks in [21]. The networked filtering problem was studied for stochastic LTI systems subject to deception attacks in [24] and [22] from the perspective of security assurance. The problem of secure control of LTI systems considering deception attacks and ETM was investigated in [25].

However, few results concern with the cyberattacks and continuous type ETM simultaneously for T–S fuzzy systems with unmatched premise variables, which is another motivation of our study.

This article mainly focuses on constructing a novel memory-based continuous ETM and developing a resilient secure control approach for networked T–S fuzzy systems against unknown but bounded deception attacks. The main contributions of this article are listed as follows.

1) A novel memory-based continuous ETM with a window function that introduces the past information is established. This window function like a *forgetting factor* takes different weight for the past information. Besides the merit of further reducing the data releasing rate, the occurrence of wrong data-releasing event can be decreased with the aid of the proposed ETM.
2) The networked fuzzy control system with the proposed memory-based ETM is formulated as a switched time-delayed fuzzy system for the purpose of avoiding Zeno behavior. Taking the unknown but bounded deception attacks and asynchronous premise variables into account, a codesign method is put forward in the light of Lyapunouv theory and some inequalities that can give rise to less conservative results.

Notation: $\mathbb{R}^n$ is used to denote the n-dimensional Euclidean space and $\mathbb{R}^{n\times m}$ stands for the set of $n \times m$ real matrices. $\|\cdot\|$ represents the Euclidean vector norm. A real symmetric matrix $M > 0 (< 0)$ denotes the matrix is a positive (negative) definite matrix. $\mathbf{He}(S) \triangleq S + S^T$. $\otimes$ means Kronecker product. I_a indicates $a \times a$ dimension identity matrix. $\mathbb{E}\{\cdot\}$ represents mathematical expectation.

II. Problem Formulation

In this article, the following nonlinear physical plant described by the T–S fuzzy-model will be considered as follows.

Plant rule i: IF $\varphi_1(t)$ is $G_{i1}, \ldots,$ and $\varphi_q(t)$ is G_{iq}, THEN

$$\dot{x}(t) = (A_i + \Delta A_i(t))x(t) + B_i u(t) \tag{1}$$

for $i \in \mathscr{I} \triangleq \{1, 2, \ldots, r\}$, where i means the ith fuzzy rule, $\varphi_j(t)$ and G_{ij} for $i \in \mathscr{I}, j \in \{1, 2, \ldots, q\}$ denote the jth premise variable and fuzzy set, respectively. $x(t) \in \mathbb{R}^n$ and $u(t) \in \mathbb{R}^{n_u}$ are the state and the control input vector, respectively. A_i and B_i are known matrices with appropriate dimensions. In addition, $\Delta A_i(t) = \alpha(t)A_{0i}$ denotes the random uncertainty of the system. $\alpha(t)$ is a random variable with $\mathbb{E}(\alpha(t)) = \bar{\alpha}$ and $Var(\alpha(t)) = \hat{\alpha}^2$. A_{0i} is a constant matrix that reflects the nominal uncertainty.

Remark 1: The parameter uncertainty is often induced by some unknown disturbance in practices. The amplitude of this kind of uncertainty is governed by a random distribution like the one in (1).

Define $\varphi(t) = [\varphi_1(t), \ldots, \varphi_q(t)]$ and $g_i(\varphi(t)) = \Pi_{j=1}^{q} G_{ij}$ $(\varphi_j(t))$, we can obtain the membership function $\mu_i(\varphi(t))$ as

$$\mu_i(\varphi(t)) = \frac{g_i(\varphi(t))}{\sum_{i=1}^{r} g_i(\varphi(t))}. \tag{2}$$

It is known that $0 \le \mu_i(\varphi(t)) \le 1$ and $\sum_{i=1}^{r} \mu_i(\varphi(t)) = 1$.

With the aid of center-average defuzzifier, product interference, and singleton fuzzifier, the whole T–S fuzzy systems can be written by

$$\dot{x}(t) = \sum_{i=1}^{r} \mu_i(\varphi(t))[(A_i + \alpha(t)A_{0i})x(t) + B_i u(t)]. \tag{3}$$

Suppose the control signal is transmitted over the communication network at instant t_k, and $\{t_k\}_{t_k=0}^{\infty}$ is a monotone increasing sequence. Then, the T–S fuzzy-based feedback control law of the jth ($j \in \mathscr{I}$) rule can be expressed by

Control rule j: IF $\varphi_1(t_k)$ is $G_{i1}, \ldots,$ and $\varphi_q(t_k)$ is G_{iq}, THEN

$$\bar{u}(t) = K_j x(t_k) \tag{4}$$

for $t \in [t_k, t_{k+1})$, where K_j is the controller gain to be designed. Using a similar method, we can get the overall fuzzy controller as

$$\bar{u}(t) = \sum_{j=1}^{r} \mu_j(\varphi(t_k))K_j x(t_k). \tag{5}$$

Similar to [26], we assume the membership function has the following property:

$$\mu_j(\varphi(t_k)) > \rho_j \mu_j(\varphi(t)) \tag{6}$$

for $t \in [t_k, t_{k+1})$, where $\rho_j > 0$ is a known constant.

The control signal is vulnerable to tampering by malicious adversaries when it transmits over a communication network. In this study, we suppose the adversaries inject false data into the control information with the following form:

$$u(t) = \bar{u}(t) + \bar{u}_a(t) \tag{7}$$

where $\bar{u}_a(t) = \beta(t)u_a(t)$ and $\beta(t) \in \{0, 1\}$ are a random variable with $\mathbb{E}\{\beta(t) = 1\} = \bar{\beta}$, $u_a(t)$ is the attack signal that satisfies

$$\|u_a(t)\| \leq \varrho^2 \tag{8}$$

where $\varrho > 0$ is a predefined constant.

Remark 2: For the purpose of evading detection, the adversaries usually launch the attack intermittently, here $\beta(t)$ taking "1" means a successful attack at instant t. Besides, the magnitude of the attack is constrained as well.

Combining (3) and (7), we can obtain the closed-loop control system for $t \in [t_k, t_{k+1})$ as follows:

$$\begin{aligned} \dot{x}(t) = \sum_{i=1}^{r}\sum_{j=1}^{r} \mu_i(\varphi(t))\mu_j(\varphi(t_k))[(A_i + \alpha(t)A_{0i})x(t) \\ + B_i K_j x(t_k) + \beta(t)B_i u_a(t_k)]. \end{aligned} \tag{9}$$

To alleviate the burden of the network bandwidth, ETM is adopted in most literature, such as in [14], [27], and [28], however, the signal discretized by a sampler will lost some useful information that exists between adjacent sampling instants. Therefore, the conservativeness will be decreased if the designed ETM can utilize continuous signals from the physical process that is assumed to be conveniently available. This transmission mechanism is called the continuous type ETM. Notice that this type ETM often engenders Zeno phenomena. Motivated by [17], we divide the releasing interval $[t_k, t_{k+1})$ into two subintervals: $\mathscr{I}_1 \triangleq [t_k, t_k + h_1)$ and $\mathscr{I}_2 \triangleq [t_k + h_1, t_{k+1})$, where $0 < h_1 < t_{k+1} - t_k$. It is clear that $\mathscr{I}_1 \cup \mathscr{I}_2 = [t_k, t_{k+1})$. To avoid Zeno phenomena, the ETM only works after $t_k + h_1$. It indicates that h_1 is a waiting period.

Based on the abovementioned intention, we define

$$\psi(t) = e^T(t)\Theta e(t) - \varpi x^T(t_k)\Theta x(t_k) \tag{10}$$

where $0 < \varpi < 1$ is a prescribed scalar, $e(t)$ is a state error, and $\Theta > 0$ is a weight matrix to be designed.

The next releasing event is designed by

$$t_{k+1} = \inf\{t > t_k + h_1 | \psi(t) > 0\}. \tag{11}$$

To get a better performance of the ETM, we will reconstruct the state error $e(t)$. Before doing this, we first define a column vector $f(v) = \mathbf{col}\{f_1(v), \ldots, f_p(v)\}$, where $f_1(v)$ satisfies $\int_{-h_2}^{0} f_1(v)dv = 1$. The other items $f_i(v)$ for $i = 2 \cdots p$ are chosen to satisfy $\dot{F}(v) = \mathbb{F}F(v)$, where $\mathbb{F} \in \mathbb{R}^{pn \times pn}$, and $F(v) = f(v) \otimes I_n$. Based on these definitions, we then define a new variable that is different from the existing ETMs as follows:

$$\tilde{x}(t) \triangleq \int_{t-h_2}^{t} F(s-t)x(s)ds. \tag{12}$$

The new state error of the ETM is then defined by

$$e(t) = H\tilde{x}(t) - x(t_k) \tag{13}$$

where $H = [I_n 0_{n\times(p-1)n}]$.

Remark 3: We call $f_1(v)$ in (13) as a window function. The scale of this moving window is from $t - h_2$ to t. Usually, $f_1(v)$ is selected as an increasing function in interval $[-h_2, 0)$, such as in Section IV, we choose $f_1(v) = \frac{\pi}{2h_2}\cos(\frac{\pi}{2h_2}v)$ for $v \in [-h_2, 0]$. That means the earlier the information is, the smaller weight it has. So we also call this term as a *forgetting factor*.

Remark 4: Although (11) has a similar format to traditional ETMs, we can see from (12) that the proposed ETM takes the past information into account, that is, it is a memory-based continuous-time ETM since the state error in (13) introduces the past information from $x(t - h_2)$ to $x(t)$ via the window function. Hence, h_2 here is called the width of window function (WWF).

Remark 5: Owning to the average information used in the proposed memory-based ETM instead of the instantaneous state, the case of wrong triggering induced by some impulse disturbance can be greatly reduced.

Defining $d(t) = t - t_k$ for $t \in \mathscr{I}_1$ follows that

$$x(t_k) = \begin{cases} x(t - d(t)) & t \in \mathscr{I}_1 \\ H\tilde{x}(t) - e(t) & t \in \mathscr{I}_2. \end{cases} \tag{14}$$

Then, it has

$$0 \leq d(t) \leq h_1. \tag{15}$$

Therefore, system (9) can be converted into a switched system with two modes as follows:

$$\dot{x}(t) = \sum_{i=1}^{r}\sum_{j=1}^{r} \mu_i(\varphi(t))\mu_j(\varphi(t_k))[\vartheta_{ij\sigma(t)}(t) + \pi_{ij}(t)] \tag{16}$$

for $t \in [t_k, t_{k+1}) = \mathscr{I}_1 \cup \mathscr{I}_2$, where

$$\sigma(t) = \begin{cases} 1 & t \in \mathscr{I}_1 \\ 2 & t \in \mathscr{I}_2 \end{cases} \tag{17}$$

and

$$\begin{aligned} \vartheta_{ij1}(t) &= (A_i + \bar{\alpha}A_{0i})x(t) + B_i K_{1j} x(t - d(t)) + \bar{\beta}B_i u_a(t_k) \\ \vartheta_{ij2}(t) &= (A_i + \bar{\alpha}A_{0i})x(t) + B_i K_{2j} H\tilde{x}(t) - B_i K_{2j} e(t) \\ &\quad + \bar{\beta}B_i u_a(t_k) \\ \pi_{ij}(t) &= (\alpha(t) - \bar{\alpha})A_{0i}x(t) + (\beta(t) - \bar{\beta})B_i u_a(t_k). \end{aligned}$$

Therefore, K_{kj} in (16) is the switched controller gain for $t \in \mathscr{I}_k$ with $k = 1, 2$.

For convenience of description, in the following, we denote $\mu_i(\varphi(t))$ and $\mu_j(\varphi(t_k))$ with μ_i^t and $\mu_j^{t_k}$, respectively.

Assumption 1: System (3) is assumed to be stable in the mean-square and secure sense if the state satisfies

$$\mathbb{E}\{\|Lx(t)\|\} \leq \gamma^2 \tag{18}$$

when the control signal is attacked by adversaries, where γ and L are a given scalar and matrix, respectively.

The objective of this article is to develop a design method of resilient control using the continuous memory-based ETM in (11) such that the fuzzy-based nonlinear system in (3) is secure when the control signal is subject to cyberattacks.

III. Main Results

In this section, the memory-based resilient control design will be given for networked T–S fuzzy systems (3) in the presence of cyberattacks.

For convenience of description, we make the following definitions:

$$\zeta_0(t) \triangleq \begin{bmatrix} x^T(t) & \tilde{x}^T(t) \end{bmatrix}^T$$

$$\zeta_1^T(t) \triangleq [\dot{x}^T(t)\zeta_0^T(t)x^T(t-d(t))x^T(t-h_1)x^T(t-h_2)$$
$$u_a^T(t_k)]$$

$$\zeta_2^T(t) \triangleq [\dot{x}^T(t)\zeta_0^T(t)e^T(t)x^T(t-h_1)x^T(t-h_2)u_a^T(t_k)]$$

$$\digamma(v, U) \triangleq x^T(v)Ux(v)$$

$$\digamma^*(v, U) \triangleq \dot{x}^T(v)U\dot{x}(v)$$

$$\mathbb{I}_s \triangleq \begin{bmatrix} 0_{a\times sn} & I_{a\times a} & 0_{a\times[(5-s)a+n_u]} \end{bmatrix}$$

where $a = \begin{cases} n & s \in \mathbb{N}, s \leq 5 \\ n_u & s = 6 \end{cases}$.

Before giving the main results, a useful lemma will be presented first.

Lemma 1 (see [29]): For a matrix $R > 0$ and a given interval $\mathcal{U}$, one has

$$\int_{\mathcal{U}} \digamma(v, R)dv \geq \phi^T(\cdot)(\mathscr{F} \otimes R)\phi(\cdot) \tag{19}$$

where $\phi(\cdot) = \int_{\mathcal{U}} F(v)x(v)dv$, $\mathscr{F} = (\int_{\mathcal{U}} f(v)f^T(v)dv)^{-1}$, $f(v)$, and $F(v)$ are defined in (12).

Theorem 1: For given scalars γ, ϱ, δ, $\bar{\alpha}$, $\bar{\beta}$, ρ_k, h_k, λ, ϖ, and matrix K_{kj}, the T–S fuzzy system (3) against unknown but bounded cyberattacks is stable in the mean-square and secure sense under the continuous memory-based ETM in (13), if there exist matrices $W > 0, \Theta > 0, Q_k > 0, R_k > 0$, symmetric matrices P, Λ_k, and matrix S with appropriate dimensions such that

$$\hat{P} = P + \text{diag}\{0_n, e^{-2\delta h_2}\mathcal{M}_1\} > 0 \tag{20}$$

$$\Pi_k^{ij} - \Lambda_i < 0 \tag{21}$$

$$\mathcal{V}_{ii} < 0 \tag{22}$$

$$\mathcal{V}_{ij} + \mathcal{V}_{ji} < 0, \quad (i, j \in \mathscr{I}, i < j) \tag{23}$$

for $k = 1, 2$ and $i, j \in \mathscr{I}$, where

$$\begin{aligned}
\Pi_k^{ij} &= \bar{\Pi}_{k1}^{ij} + \Pi_{k2}, \bar{\Pi}_{k1}^{ij} = \Pi_{k1}^{ij} + \mathbf{He}(\Upsilon_0\Upsilon_k^{ij}) \\
\mathcal{V}_{ij} &= \rho_j(\Pi_k^{ij} - \Lambda_i) + \Lambda_i \\
\Pi_{11}^{ij} &= \Gamma_1^{ij} + h_1^2\mathbb{I}_0^T R_1\mathbb{I}_0 + \mathbb{I}_1^T(Q_1 + Q_2 + h_2R_2)\mathbb{I}_1 \\
&\quad -e^{-2\delta h_1}\mathbb{I}_4^T Q_1\mathbb{I}_4 - e^{-2\delta h_2}\mathbb{I}_5^T Q_2\mathbb{I}_5 \\
&\quad -e^{-2\delta h_1}\begin{bmatrix} \mathbb{I}_1 - \mathbb{I}_3 \\ \mathbb{I}_3 - \mathbb{I}_4 \end{bmatrix}^T \Omega_1 \begin{bmatrix} \mathbb{I}_1 - \mathbb{I}_3 \\ \mathbb{I}_3 - \mathbb{I}_4 \end{bmatrix} \\
&\quad -e^{-2\delta h_2}\mathbb{I}_2\mathcal{M}_2\mathbb{I}_2 - \mathbb{I}_6^T(\gamma/\varrho)^2 I\mathbb{I}_6 \\
\Pi_{21}^{ij} &= \Gamma_2^{ij} + h_1^2\mathbb{I}_0^T R_1\mathbb{I}_0 + \mathbb{I}_1^T(Q_1 + Q_2 + h_2R_2)\mathbb{I}_1 \\
&\quad -e^{-2\delta h_1}\mathbb{I}_4^T Q_1\mathbb{I}_4 - e^{-2\delta h_2}\mathbb{I}_5^T Q_2\mathbb{I}_5 \\
&\quad -e^{-2\delta h_1}\begin{bmatrix} \mathbb{I}_1 \\ \mathbb{I}_4 \end{bmatrix}^T \Omega_2 \begin{bmatrix} \mathbb{I}_1 \\ \mathbb{I}_4 \end{bmatrix} \\
&\quad -e^{-2\delta h_2}\mathbb{I}_2^T\mathcal{M}_2\mathbb{I}_2 - \mathbb{I}_6^T(\gamma/\varrho)^2 I\mathbb{I}_6 - \mathbb{I}_3^T\Theta\mathbb{I}_3 \\
&\quad +\varpi[H\mathbb{I}_2 - \mathbb{I}_3]^T\Theta[H\mathbb{I}_2 - \mathbb{I}_3] \\
\Pi_{k2} &= \mathbb{I}_1 L^T L\mathbb{I}_1, \mathcal{M}_1 = \mathscr{F} \otimes Q_2, \mathcal{M}_2 = \mathscr{F} \otimes R_2 \\
\mathscr{F} &= \left(\int_{-h_2}^0 f(s)f^T(s)ds\right)^{-1} \\
\Omega_1 &= \begin{bmatrix} R_1 & * \\ S & R_1 \end{bmatrix}, \Omega_2 = \begin{bmatrix} R_1 & * \\ -R_1 & R_1 \end{bmatrix} \\
\Gamma_k^{ij} &= \mathbf{He}\left(\begin{bmatrix} \mathbb{I}_1 \\ \mathbb{I}_2 \end{bmatrix}^T P\left(\begin{bmatrix} \mathbb{I}_0 \\ \mathfrak{F} \end{bmatrix} + \delta\begin{bmatrix} \mathbb{I}_1 \\ \mathbb{I}_2 \end{bmatrix}\right)\right) \\
\mathfrak{F} &= F(0)\mathbb{I}_1 - \mathbb{F}\mathbb{I}_2 - F(-h_2)\mathbb{I}_5 \\
\Upsilon_0 &= (W\mathbb{I}_0)^T + (\lambda W\mathbb{I}_1)^T \\
\Upsilon_1^{ij} &= -\mathbb{I}_0 + (A_i + \bar{\alpha}A_{0i})\mathbb{I}_1 + B_iK_{1j}\mathbb{I}_3 + \bar{\beta}B_i\mathbb{I}_6 \\
\Upsilon_2^{ij} &= -\mathbb{I}_0 + (A_i + \bar{\alpha}A_{0i})\mathbb{I}_1 + B_iK_{2j}H\mathbb{I}_2 \\
&\quad -B_iK_{2j}\mathbb{I}_3 + \bar{\beta}B_i\mathbb{I}_6.
\end{aligned}$$

Proof: See the Appendix. ■

Sufficient conditions for the stability of fuzzy systems in the sense of security have been given in Theorem 1. However, they are not feasible LMI conditions. Next, we will seek a design method based on Theorem 1 for the switched controllers and the memory-based ETM of system (3).

Theorem 2: For given scalars $\gamma, \varrho, \delta, \bar{\alpha}, \bar{\beta}, \rho_k, h_k, \lambda, \varpi$, the fuzzy system (3) against cyberattacks in (8) with a known boundary is stable in the mean-square and secure sense under the continuous memory-based ETM in (13), if there exist $X > 0, \tilde{\Theta} > 0, \tilde{Q}_k > 0, \tilde{R}_k > 0$, symmetric matrices $\tilde{P}, \tilde{\Lambda}_i$ and matrix $\tilde{S}, Y_{kj}$ with appropriate dimensions such that

$$\tilde{P} + \text{diag}\{0_n, e^{-2\delta h_2}\tilde{\mathcal{M}}_1\} > 0 \tag{24}$$

$$\begin{bmatrix} \tilde{\Pi}^{ij}_k - \tilde{\Lambda}_i & * \\ LX\mathbb{I}_1 & -I \end{bmatrix} < 0 \tag{25}$$

$$\begin{bmatrix} \tilde{\mathcal{V}}_{ii} & * \\ \rho_i LX\mathbb{I}_1 & -\rho_i I \end{bmatrix} < 0 \tag{26}$$

$$\begin{bmatrix} \tilde{\mathcal{V}}_{ij} + \tilde{\mathcal{V}}_{ji} & * & * \\ \rho_i LX\mathbb{I}_1 & -\rho_i I & * \\ \rho_j LX\mathbb{I}_1 & 0 & -\rho_j I \end{bmatrix} < 0, \quad (i < j) \tag{27}$$

for $k = 1, 2$ and $i, j \in \mathscr{I}$, where

$$\begin{aligned}
\tilde{\Pi}^{ij}_k &= \tilde{\Pi}^{ij}_{k1} + \mathbf{He}(\tilde{\Upsilon}_0 \tilde{\Upsilon}_k) \\
\tilde{\mathcal{V}}_{ij} &= \rho_j(\tilde{\Pi}^{ij}_k - \tilde{\Lambda}_i) + \tilde{\Lambda}_i \\
\tilde{\Pi}^{ij}_{11} &= \tilde{\Gamma}^{ij}_1 + h_1^2 \mathbb{I}_0^T \tilde{R}_1 \mathbb{I}_0 + \mathbb{I}_1^T(\tilde{Q}_1 + \tilde{Q}_2 + h_2 \tilde{R}_2)\mathbb{I}_1 \\
&\quad -e^{-2\delta h_1} \mathbb{I}_4^T \tilde{Q}_1 \mathbb{I}_4 - e^{-2\delta h_2} \mathbb{I}_5^T \tilde{Q}_2 \mathbb{I}_5 \\
&\quad -e^{-2\delta h_1} \begin{bmatrix} \mathbb{I}_1 - \mathbb{I}_3 \\ \mathbb{I}_3 - \mathbb{I}_4 \end{bmatrix}^T \tilde{\Omega}_1 \begin{bmatrix} \mathbb{I}_1 - \mathbb{I}_3 \\ \mathbb{I}_3 - \mathbb{I}_4 \end{bmatrix} \\
&\quad -e^{-2\delta h_2} \mathbb{I}_2 \tilde{\mathcal{M}}_2 \mathbb{I}_2 - \mathbb{I}_6^T (\gamma/\varrho)^2 I \mathbb{I}_6 \\
\tilde{\Pi}^{ij}_{21} &= \tilde{\Gamma}^{ij}_2 + h_1^2 \mathbb{I}_0^T \tilde{R}_1 \mathbb{I}_0 + \mathbb{I}_1^T(\tilde{Q}_1 + \tilde{Q}_2 + h_2 \tilde{R}_2)\mathbb{I}_1 \\
&\quad -e^{-2\delta h_1} \mathbb{I}_4^T \tilde{Q}_1 \mathbb{I}_4 - e^{-2\delta h_2} \mathbb{I}_5^T \tilde{Q}_2 \mathbb{I}_5 \\
&\quad -e^{-2\delta h_1} \begin{bmatrix} \mathbb{I}_1 \\ \mathbb{I}_4 \end{bmatrix}^T \tilde{\Omega}_2 \begin{bmatrix} \mathbb{I}_1 \\ \mathbb{I}_4 \end{bmatrix} \\
&\quad -e^{-2\delta h_2} \mathbb{I}_2 \tilde{\mathcal{M}}_2 \mathbb{I}_2 - \mathbb{I}_6^T (\gamma/\varrho)^2 I \mathbb{I}_6 - \mathbb{I}_3^T \tilde{\Theta} \mathbb{I}_3 \\
&\quad +\varpi[\mathbb{I}_2 - \mathbb{I}_3]^T \tilde{\Theta} [\mathbb{I}_2 - \mathbb{I}_3] \\
\tilde{\Omega}_{1k} &= \begin{bmatrix} \tilde{R}_1 & * \\ \tilde{S} & \tilde{R}_1 \end{bmatrix}, \tilde{\Omega}_2 = \begin{bmatrix} \tilde{R}_1 & * \\ -\tilde{R}_1 & \tilde{R}_1 \end{bmatrix} \\
\tilde{\mathcal{M}}_1 &= \mathscr{F} \otimes \tilde{Q}_2, \tilde{\mathcal{M}}_2 = \mathscr{F} \otimes \tilde{R}_2 \\
\Gamma^{ij}_k &= \mathbf{He}\left(\begin{bmatrix} \mathbb{I}_1 \\ \mathbb{I}_2 \end{bmatrix}^T \tilde{P} \left(\begin{bmatrix} \mathbb{I}_0 \\ \mathfrak{F} \end{bmatrix} + \delta \begin{bmatrix} \mathbb{I}_1 \\ \mathbb{I}_2 \end{bmatrix} \right) \right) \\
\tilde{\Upsilon}_0 &= \mathbb{I}_0^T + \lambda \mathbb{I}_1^T \\
\tilde{\Upsilon}^{ij}_1 &= -X\mathbb{I}_0 + (A_i + \bar{\alpha} A_{0i}) X \mathbb{I}_1 + B_i Y_{1j} \mathbb{I}_3 + \bar{\beta} B_i X \mathbb{I}_6 \\
\tilde{\Upsilon}^{ij}_2 &= -X\mathbb{I}_0 + (A_i + \bar{\alpha} A_{0i}) X \mathbb{I}_1 + B_i Y_{2j} H \mathbb{I}_2 - B_i Y_{2j} \mathbb{I}_3 \\
&\quad +\bar{\beta} B_i X \mathbb{I}_6.
\end{aligned}$$

Moreover, the switched controller gain can be derived by $K_{kj} = Y_{kj} X^{-1}$ for $k = 1, 2,\ j \in \mathscr{I}$ and the parameter of memory-based ETM is given by $\Theta = X^{-1} \tilde{\Theta} X^{-1}$.

Proof: Using Schure complement for (21) yields that

$$\begin{bmatrix} \bar{\Pi}^{ij}_{k1} - \Lambda_i & * \\ L\mathbb{I}_1 & -I \end{bmatrix} < 0. \tag{28}$$

Define $X = W^{-1}, Y_{kj} = K_{kj} W, \mathcal{X}_1 = \mathrm{diag}\{\underbrace{X \cdots X}_{p}\}$, $\mathcal{X}_2 = \mathrm{diag}\{X, \mathcal{X}_1\}, \mathcal{X}_3 = \mathrm{diag}\{X, \mathcal{X}_2, X, X, X, I\}$, $\mathcal{X} = \mathrm{diag}\{\mathcal{X}_3, I\}$, $\tilde{\Lambda}_i = \mathcal{X}_3 \Lambda_i \mathcal{X}_3$, $\tilde{R}_k = X R_k X$, $\tilde{Q}_k = X Q_k X$, $\tilde{\Theta} = X \Theta X$, and $\tilde{P} = \mathcal{X}_2 P \mathcal{X}_2$.

Then, pre- and postmultiple (20) with $\mathcal{X}_2$, it follows that (24). Pre- and postmultiplying (28) with $\mathcal{X}$ yields (25). Using similar method, we can ensure (26) and (27) hold from (22) and (23), respectively. ■

TABLE I
PARAMETERS OF PHYSICAL QUANTITIES

$g\ (N/m^2)$	$M\ (kg)$	$m\ (kg)$	$l\ (m)$
9.8	3	1.5	0.5

IV. Example

A single-link rigid robot borrowed from [30] is utilized to manifest the effectiveness of the proposed method. The kinematic equation is given as follows:

$$\mathcal{J}\ddot{\theta} = \mathcal{W} \sin\theta + u$$

where θ and u denote the joint rotation angle in radians and the control torque applied at the joint in N·m, respectively. M and m are the mass of the rigid link and load, respectively. g is the acceleration of gravity, l is the length of robot link. $\mathcal{J} = Ml^2 + 1/3ml^2$ denotes the moment of inertia in $\mathrm{kg} \cdot \mathrm{m}^2$ and $\mathcal{W} = -(0.5\, m + M)gl$. The other physical quantities are given in Table I.

By defining a new state variable as

$$x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} = \begin{bmatrix} \theta \\ \dot{\theta} \end{bmatrix}$$

one can model it as a T–S fuzzy system with the format of (1), of which the parameters can be derived by

$$A_1 = \begin{bmatrix} 0 & 1 \\ \frac{\mathcal{W}}{\mathcal{J}} & 0 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 1 \\ \frac{2\mathcal{W}}{\pi\mathcal{J}} & 0 \end{bmatrix}$$

$$B_1 = B_2 = \begin{bmatrix} 0 \\ \frac{1}{\mathcal{J}} \end{bmatrix}.$$

The related parameters of uncertain matrices $\Delta A(t)$ are selected by $\bar{\alpha} = 0.2$ and

$$A_{01} = A_{02} = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix}.$$

The expectation of successful cyberattacks is $\bar{\beta} = 0.2$. The membership functions are set by $\mu_1^t = 1 - \frac{\pi}{2}|x_1(t)|$ and $\mu_2^t = \frac{\pi}{2}|x_1(t)|$.

The window function of the memory-based ETM in (11) is selected as

$$\begin{cases} f_1(v) = \dfrac{\pi}{2h_2} \cos\left(\frac{\pi}{2h_2} v\right) \\ f_2(v) = \dfrac{\pi}{2h_2} \sin\left(\frac{\pi}{2h_2} v\right) \end{cases} \tag{29}$$

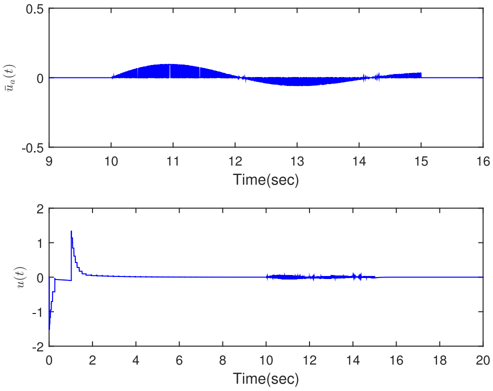


Fig. 1. Cyberattacks and the control input based on the ETM with the window functions in (29) and the parameters in (30).

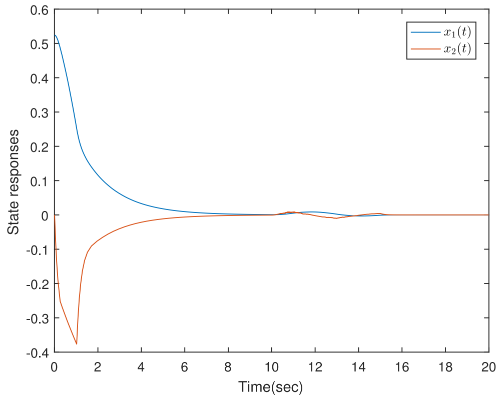


Fig. 2. State responses of the system against cyberattacks based on the ETM with the window functions in (29) and the parameters in (30).

for $v \in [-h_2, 0]$. Here, the window function $f_1(v)$ for $v \in [-h_2, 0]$ is an increasing function, which means the more forward the information, the smaller its weight.

Obviously, $\int_{-h_2}^{0} f_1(v)dv = 1$, and

$$\mathbb{F} = \begin{bmatrix} 0 & -\frac{\pi}{2h_2} \\ \frac{\pi}{2h_2} & 0 \end{bmatrix} \otimes I_2.$$

Choose $h_1 = 0.004$, $h_2 = 0.02$, $\delta = 0.02$, $\varpi = 0.1$, $\lambda = 2$, $\gamma = 0.5$, $\varrho = 0.35$, $\bar{\beta} = 0.5$, $\rho_1 = 0.8$, $\rho_2 = 0.9$, and $L = 0.5I$, the switched controller gains and the weight matrix of memory-based ETM can be obtained from Theorem 2 as

$$K_{11} = \begin{bmatrix} -3.0365 & -5.6185 \end{bmatrix}$$

$$K_{12} = \begin{bmatrix} -2.7211 & -5.3593 \end{bmatrix}$$

$$K_{21} = \begin{bmatrix} -2.7945 & -4.8751 \end{bmatrix}$$

$$K_{22} = \begin{bmatrix} -2.3366 & -4.8508 \end{bmatrix}$$

$$\Theta = \begin{bmatrix} 35.7134 & -95.7770 \\ -95.7770 & 300.3735 \end{bmatrix}. \tag{30}$$

Set the initial state as $x(0) = \begin{bmatrix} \frac{\pi}{6} & 0 \end{bmatrix}^T$. To show the impact of the cyberattack on the system, we suppose the adversary launches the attack with the abovementioned boundary parameters from 10 s to 15 s, which is shown in Fig. 1. Using the controller gains and the parameters of memory-based ETM in (30), we can get the state responses of the system against cyberattacks, as shown in Fig. 2. It can be observed that the system using the proposed resilient controller operates in security when random false data are injected into the control input. Owning to the proposed memory-based ETM, only 169 data packets (in 20 s of runtime) are needed to meet the control requirement in secure sense. The maximum IET is up to 0.75 s. Fig. 3 depicts the sequence of event-generating instants. From Fig. 4 together with Assumption 1, one can conclude that this type of attack can be well suppressed by the proposed resilient control method.

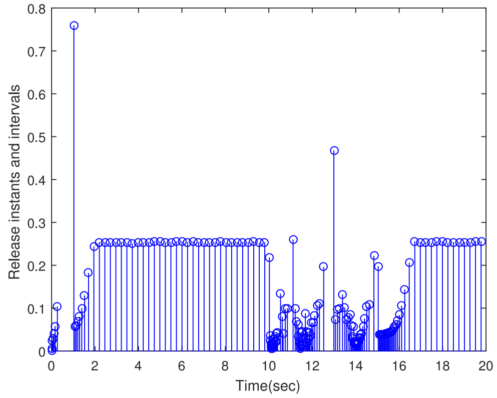


Fig. 3. Releasing sequence based on the ETM with the window functions in (29) and the parameters in (30).

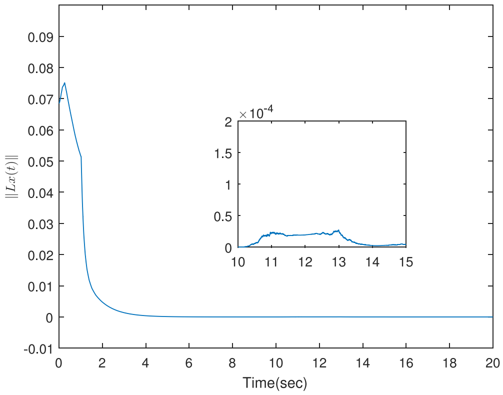


Fig. 4. Level of suppression of the system against cyberattacks.

Next, we take a series of values of WWF (h_2) to study the impact of WWF on the triggering event. By comparing these data shown in Table II with different WWFs, one can see that the larger WWF, the less number of data packet are needed to release into the network. However, it needs the more historical information to make a decision of data releasing and to obtain the control input, which may occupy more computation and memory resource.

TABLE II
TOTAL NUMBER OF EVENT-GENERATION ($\mathscr{N}$) UNDER THE ETM WITH DIFFERENT WINDOW FUNCTIONS DURING 0–20 S

WWF	$\mathscr{N}$ under (29)	$\mathscr{N}$ under (31)
$h_2 = 0.006$	224	292
$h_2 = 0.012$	192	254
$h_2 = 0.02$	169	244

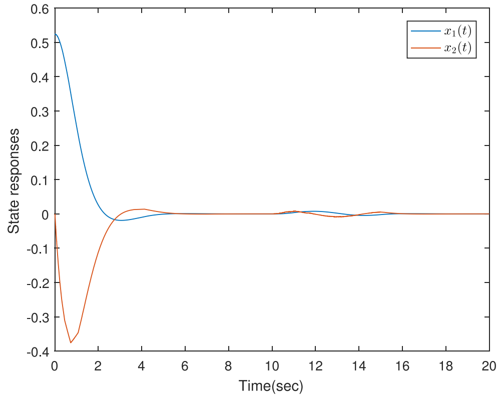


Fig. 5. State responses of the system against cyberattacks based on the ETM with the window functions (31) and the parameters in (32).

In the first case, we investigate the memory-based ETM with a forgetting factor. Next we will study the case that $f_1(v)$ is chosen as a constant function, which follows that

$$\begin{cases} f_1(v) = \dfrac{1}{h_2} \\ f_2(v) = \dfrac{1}{h_2} v \end{cases} \tag{31}$$

Then, it has

$$\mathbb{F} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \otimes I_2.$$

Under this case, we can get the following parameters of the controller and the ETM with the same initial parameters as the first case

$$K_{11} = \begin{bmatrix} -2.1193 & -2.3339 \end{bmatrix}$$

$$K_{12} = \begin{bmatrix} -1.4845 & -2.2115 \end{bmatrix}$$

$$K_{21} = \begin{bmatrix} -1.7088 & -1.8309 \end{bmatrix}$$

$$K_{22} = \begin{bmatrix} -1.1950 & -1.7925 \end{bmatrix}$$

$$\Theta = \begin{bmatrix} 22.4758 & -23.1471 \\ -23.1471 & 146.3428 \end{bmatrix}. \tag{32}$$

Figs. 5 and 6 present the state responses and the sequence of event-generating instants of the system under the attack $\bar{u}_a(t)$ shown in Fig. 1, respectively. From Fig. 6 and Table II, one can see that the number of data releasing under (29) is much lower than the one under (31) within the same runtime, however, the system still be stable in secure sense under the proposed memory-based ETM with forgetting factor. Since the window function is set by an increasing function from $t - h_2$ to t, that is, the closer the information is to the current, the more useful it is to the controller, it is more in line with the idea of control design in practice comparing with the ETM with a constant window function.

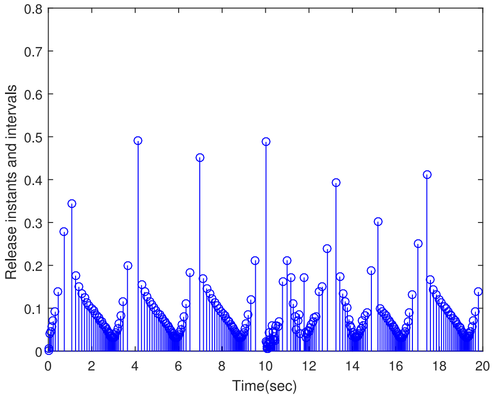


Fig. 6. Releasing sequence based on the ETM with the window functions (31) and the parameters in (32).

To further illustrate the proposed method can improve the control performance against deception attacks, we consider a scenarios that a standard controller is used to control the system with deception attacks. Here, the standard controller refers to the controller obtained without considering cyberattacks in the design process. By using a similar method to Theorem 2, we can obtain the standard controller and the parameter of ETM as follows:

$$K_{11} = \begin{bmatrix} -1.6695 & 0.7373 \end{bmatrix}$$

$$K_{12} = \begin{bmatrix} -1.3737 & 0.1557 \end{bmatrix}$$

$$K_{21} = \begin{bmatrix} -1.4672 & -1.0060 \end{bmatrix}$$

$$K_{22} = \begin{bmatrix} -1.3653 & -0.0479 \end{bmatrix}$$

$$\Theta = \begin{bmatrix} 20.2626 & -26.0320 \\ -21.0320 & 156.5505 \end{bmatrix}. \tag{33}$$

On the other hand, we can get the resilient controller as follows by using Theorem 2 with the same parameters as mentioned above except that $\varrho = 0.8$

$$K_{11} = \begin{bmatrix} -2.1038 & -2.3496 \end{bmatrix}$$

$$K_{12} = \begin{bmatrix} -1.4734 & -2.2272 \end{bmatrix}$$

$$K_{21} = \begin{bmatrix} -1.7000 & -1.8445 \end{bmatrix}$$

$$K_{12} = \begin{bmatrix} -1.1875 & -1.8062 \end{bmatrix}$$

$$\Theta = \begin{bmatrix} 22.2626 & -23.0320 \\ -23.0320 & 146.5505 \end{bmatrix}. \tag{34}$$

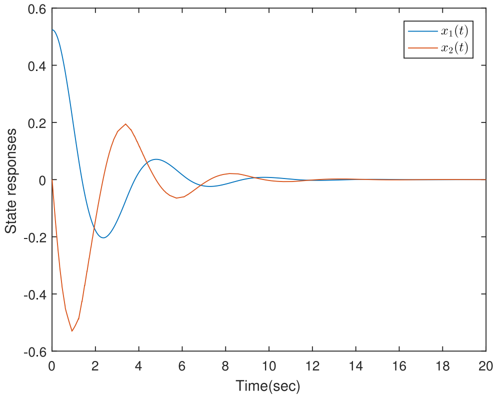


Fig. 7. State responses of the system without deception attacks by using standard controller in (33).

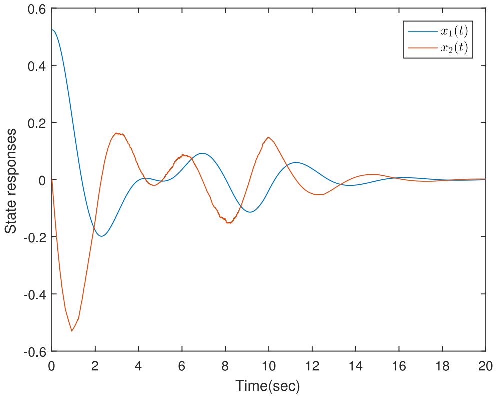


Fig. 8. State responses of the system with deception attacks by using standard controller in (33).

It is noted that the duration of deception attacks is set from 2 to 10 s, and the bounded magnitude is given by $\varrho = 0.8$ to gain a better presentation of comparison results. Fig. 7 shows the state responses of the system without deception attacks by using standard controller in (33), from which one can see that the system has a good control performance by using such a controller when there is no attack signal on the system. Fig. 8 implies that the control performance is deteriorative due to the injection of the deception attack from 2 to 10 s. Under the same scenarios as in Fig. 8, we can obtain the state responses shown in Fig. 9 by using the proposed method with parameters in (34). Comparing with Figs. 8 and 9, one can conclude that our proposed resilient controller can lead to a better control performance against deception attacks while the performance of the system with standard controller becomes worse under the deception attacks. Meanwhile, both the resilient controller and the standard controller can guarantee the stability of the system after 10 s, during which the deception attack is removed.

V. Conclusion

In this article, the problem of memory-based resilient control of networked T–S fuzzy systems in the presence of cyberattacks was investigated. A window function was introduced in designing the novel memory-based ETM, by which the past information is matched with different reasonable weights. Using such an ETM can result in a lower data-releasing rate, moreover, the occurrence of wrong triggering event due to some abrupt state variation can be reduced. To avoid the Zeno behavior, the ETM was designed to take effect after a waiting period. The networked T–S fuzzy system was then formulated as a switched time-delayed system. A codesign method for both ETM and the switched resilient control were put forward to guarantee the exponential stability of the T–S fuzzy system subject to deception attacks in secure sense. Finally, a single-linked robot was taken as an example to manifest the effectiveness of the proposed method.

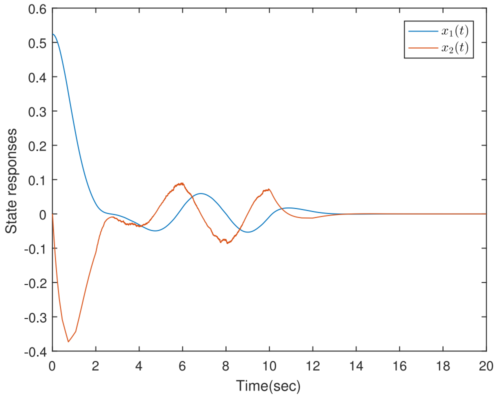


Fig. 9. State responses of the system with deception attacks by using the proposed resilient controller in (34).

Appendix A
Proof of Theorem 1

Construct the following Lyapunov–Krasovskii function as

$$V(t) = \sum_{i=1}^{4} V_i(t) \tag{35}$$

where

$$\begin{aligned}
V_1(t) &= \zeta_0^T(t)P\zeta_0(t)\\
V_2(t) &= \sum_{i=1}^{2}\int_{t-h_i}^{t} e^{2\delta(s-t)}\digamma(s,Q_i)ds\\
V_3(t) &= h_1\int_{-h_1}^{0}\int_{t+s}^{t} e^{2\delta(s-t)}\digamma^*(v,R_1)dvds\\
V_4(t) &= \int_{t-h_2}^{t} e^{2\delta(s-t)}(s-t+h_2)\digamma(s,R_2)ds.
\end{aligned}$$

Utilizing Lemma 1 and Jensen's inequality yields that

$$\begin{aligned}
&\int_{t-h_2}^{t} e^{2\delta(s-t)}\digamma(s,Q_2)ds\\
&\qquad = \int_{-h_2}^{0} e^{2\delta v}x^T(t+v)Q_2x(t+v)dv\\
&\qquad \geq e^{-2\delta h_2}\tilde{x}^T\mathcal{M}_1\tilde{x}(t).
\end{aligned} \tag{36}$$

It follows that

$$\begin{aligned}V(t) &\geq \zeta_0^T(t)\hat{P}\zeta_0(t) + \int_{t-h_1}^{t} e^{2\delta(s-t)}\digamma(s, Q_1)ds \\ &\quad + V_3(t) + V_4(t) \\ &\triangleq \bar{V}(t).\end{aligned}$$

From (20) and the properties of $\digamma(\cdot, Q_i) > 0$ and $\digamma(\cdot, R_i) > 0$ for $i = 1, 2$, one can obtain that

$$V(t) \geq \bar{V}(t) > 0. \tag{37}$$

It is noted that the random variables $\alpha(t)$ and $\beta(t)$ have the following properties:

$$\mathbb{E}\{\alpha - \bar{\alpha}(t)\} = 0, \mathbb{E}\{\beta - \bar{\beta}(t)\} = 0. \tag{38}$$

Taking the expectation of the time derivative of $V(t)$ along the trajectories of (16), we have

$$\begin{aligned}\mathbb{E}\{\dot{V}_1(t)\} &= \mathbb{E}\bigg\{ - 2\delta V_1(t) + 2\zeta_0^T(t)P\dot{\zeta}_0(t) \\ &\quad + 2\delta\zeta_0^T(t)P\zeta_0(t)\bigg\} \\ \mathbb{E}\{\dot{V}_2(t)\} &= \mathbb{E}\left\{-2\delta V_2(t) + \digamma(t, (Q_1 + Q_2))\right\} \\ &\quad - \mathbb{E}\left\{\sum_{i=1}^{2} e^{-2\delta h_i}\digamma((t - h_i), Q_i)\right\} \\ \mathbb{E}\{\dot{V}_3(t)\} &= \mathbb{E}\left\{-2\delta V_3(t) + h_1^2\digamma^*(t, R_1)\right\} \\ &\quad - \mathbb{E}\left\{h_1 e^{-2\delta h_1}\int_{t-h_1}^{t}\digamma^*(s, R_1)ds\right\} \\ \mathbb{E}\{\dot{V}_4(t)\} &\leq \mathbb{E}\left\{-2\delta V_4(t) + h_2\digamma(t, R_2)\right. \\ &\quad - \mathbb{E}\left\{e^{-2\delta h_2}\int_{t-h_2}^{t}\digamma(s, R_2)ds\right\}.\end{aligned} \tag{39}$$

Similar to the derivation of (36), we can get

$$\begin{aligned}&-\int_{t-h_2}^{t}\digamma(s, R_2)ds \\ &\quad = -\int_{-h_2}^{0}\digamma((s + t), R_2)ds \\ &\quad \leq -\int_{-h_2}^{0} x^T(s + t)F^T(s)\mathcal{M}_2F(s)x(s + t)ds \\ &\quad \leq -\tilde{x}^T(t)\mathcal{M}_2\tilde{x}(t).\end{aligned} \tag{40}$$

From (17), one knows that the switched system in (16) has two modes for t casting into different time intervals. First, we consider the case of $t \in \mathscr{I}_1$, that is, $\sigma(t) = 1$.

From the definition of $\tilde{x}(t)$ in (14), one can obtain

$$\begin{aligned}\mathbb{E}\{\dot{\tilde{x}}(t)\} &= \mathbb{E}\left\{\frac{d}{dt}\int_{t-h_2}^{t} F(v - t)x(v)dv\right\} \\ &= \mathbb{E}\left\{\mathfrak{F}\zeta_1(t)\right\}.\end{aligned} \tag{41}$$

Then, the item of $\mathbb{E}\{\dot{V}_1(t)\}$ in (39) can be further derived by

$$\begin{aligned}&\mathbb{E}\left\{\zeta_0^T(t)P\dot{\zeta}_0(t) + \delta\zeta_0^T(t)P\zeta_0(t)\right\} \\ &\quad = \mathbb{E}\left\{\zeta_0^T(t)P\begin{bmatrix}\mathbb{I}_0 \\ \mathfrak{F}\end{bmatrix}\zeta_1(t) + \delta\zeta_0^T(t)P\zeta_0(t)\right\} \\ &\quad = \mathbb{E}\left\{\zeta_1^T(t)\begin{bmatrix}\mathbb{I}_1 \\ \mathbb{I}_2\end{bmatrix}^T P\begin{bmatrix}\mathbb{I}_0 \\ \mathfrak{F}\end{bmatrix}\zeta_1(t)\right. \\ &\qquad \left. + \delta\zeta_1^T(t)\begin{bmatrix}\mathbb{I}_1 \\ \mathbb{I}_2\end{bmatrix}^T P\begin{bmatrix}\mathbb{I}_1 \\ \mathbb{I}_2\end{bmatrix}\zeta_1(t)\right\}.\end{aligned} \tag{42}$$

Notice that

$$h_1^2\mathbb{E}\left\{\dot{x}^T(t)R_1\dot{x}(t)\right\} = h_1^2\mathbb{E}\left\{\zeta_1^T(t)\mathbb{I}_0^T R_1\mathbb{I}_0\zeta_1(t)\right\}.$$

By using Jessen inequality [31], [32], we have

$$\begin{aligned}&-h_1\int_{t-h_1}^{t}\digamma^*(s, R_1)ds \\ &\quad \leq -\zeta_1^T(t)\begin{bmatrix}\mathbb{I}_1 - \mathbb{I}_3 \\ \mathbb{I}_3 - \mathbb{I}_4\end{bmatrix}^T\Omega_1\begin{bmatrix}\mathbb{I}_1 - \mathbb{I}_3 \\ \mathbb{I}_3 - \mathbb{I}_4\end{bmatrix}\zeta_1(t).\end{aligned} \tag{43}$$

Combining with (39)–(43), one can obtain that

$$\begin{aligned}&\mathbb{E}\left\{\dot{V}(t) + 2\delta V(t)\right\} \\ &\leq \mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^{t_k}\Big[\zeta_1^T(t)\Gamma_1^{ij}\zeta_1(t)\right. \\ &\quad + \digamma(t, (Q_1 + Q_2 + h_2R_2)) \\ &\quad - \sum_{i=1}^{2} e^{-2\delta h_i}x^T(t - h_i)Q_ix(t - h_i) \\ &\quad + h_1^2\zeta_1^T(t)\mathbb{I}_0^T R_1\mathbb{I}_0\zeta_1(t) - e^{-2\delta h_2}\tilde{x}^T(t)\mathcal{M}_2\tilde{x}(t) \\ &\quad \left. - e^{-2\delta h_1}\zeta_1^T(t)\begin{bmatrix}\mathbb{I}_1 - \mathbb{I}_3 \\ \mathbb{I}_3 - \mathbb{I}_4\end{bmatrix}^T\Omega_1\begin{bmatrix}\mathbb{I}_1 - \mathbb{I}_3 \\ \mathbb{I}_3 - \mathbb{I}_4\end{bmatrix}\zeta_1(t)\Big]\right\}.\end{aligned}$$

According to Assumption 1, one can come to a conclusion that the system is stable in the sense of security if the state satisfies (18). Otherwise, if the system is out of the secure filed, i.e., $\mathbb{E}\{x^T(t)L^TLx(t)\} > \gamma^2$, it follows from (8) that

$$\mathbb{E}\left\{x^T(t)L^TLx(t) - (\gamma/\varrho)^2u_a^T(t_k)u_a^T(t_k)\right\} > 0. \tag{44}$$

From (16) with $\sigma(t) = 1$, it follows that

$$\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^{t_k}\zeta_1^T(t)\left\{\mathbf{He}(\Upsilon_0\Upsilon_1^{ij})\right\}\zeta_1(t)\right\} = 0. \tag{45}$$

Therefore, for the requirement of security control, it needs that

$$\begin{aligned}&\mathbb{E}\left\{\dot{V}(t)+2\delta V(t)\right\}\\&\quad\le\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^{t_k}\zeta_1^T(t)\Pi_1^{ij}\zeta_1(t)\right\}\end{aligned}\tag{46}$$

where $\Pi_1^{ij}=\Pi_{11}^{ij}+\Pi_{12}+\mathbf{He}(\Upsilon_0\Upsilon_1^{ij})$.

Next, we will discuss another case that $t\in\mathscr{I}_2$, that is, $\sigma(t)=2$.

Similar to (42), one can get

$$\mathbb{E}\left\{\zeta_0^T(t)P\dot{\zeta}_0(t)\right\}=\mathbb{E}\left\{\zeta_0^T(t)P\begin{bmatrix}\mathbb{I}_0\\\mathfrak{F}\end{bmatrix}\zeta_2(t)\right\}.\tag{47}$$

By using Jessen inequality, we can obtain that

$$-h_1\int_{t-h_1}^{t}\digamma^*(s,R_1)ds\le\zeta_2^T(t)\begin{bmatrix}\mathbb{I}_1\\\mathbb{I}_4\end{bmatrix}^T\Omega_2\begin{bmatrix}\mathbb{I}_1\\\mathbb{I}_4\end{bmatrix}\zeta_2(t).\tag{48}$$

It is known that the event-triggering condition $\psi(t)>0$ in (11) is equivalent to

$$\zeta_2^T(t)(\varpi[H\mathbb{I}_2-\mathbb{I}_3]^T\Theta[H\mathbb{I}_2-\mathbb{I}_3]-\mathbb{I}_3^T\Theta\mathbb{I}_3)\zeta_2(t)>0.\tag{49}$$

It follows from (16) with $\sigma(t)=2$ that

$$\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^{t_k}\zeta_2^T(t)\left\{\mathbf{He}(\Upsilon_0\Upsilon_2^{ij})\right\}\zeta_2(t)\right\}=0.\tag{50}$$

Taking the security of the control system into account from Assumption 1, it requires

$$\begin{aligned}&\mathbb{E}\left\{\dot{V}(t)+2\delta V(t)\right\}\\&\quad\le\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^{t_k}\zeta_2^T(t)\Pi_2^{ij}\zeta_2(t)\right\}\end{aligned}\tag{51}$$

where $\Pi_2^{ij}=\Pi_{21}^{ij}+\Pi_{22}+\mathbf{He}(\Upsilon_0\Upsilon_2^{ij})$.

In the light of the property of fuzzy membership that $\sum_{i=1}^r\mu_j^t=\sum_{j=1}^r\mu_j^{t_k}=1$, one has

$$\begin{aligned}&\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t(\mu_j^t-\mu_j^{t_k})\zeta_k^T(t)\Lambda_i\zeta_k(t)\right\}\\&=\mathbb{E}\left\{\sum_{i=1}^{r}\mu_i^t\left(\sum_{j=1}^{r}\mu_j^t-\sum_{j=1}^{r}\mu_j^{t_k}\right)\zeta_k^T(t)\Lambda_i\zeta_k(t)\right\}=0\end{aligned}\tag{52}$$

for matrix $\Lambda_i(i\in\mathscr{I})$ and $k=1,2$.

Then, we have

$$\begin{aligned}&\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^{t_k}\zeta_k^T(t)\Pi_k^{ij}\zeta_k(t)\right\}\\&=\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^{t_k}\zeta_k^T(t)\Pi_k^{ij}\zeta_k(t)\right.\\&\quad\left.+\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t(\mu_j^t-\mu_j^{t_k})\zeta_k^T(t)\Lambda_i\zeta_k(t)\right\}\\&=\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^{t_k}\zeta_k^T(t)(\Pi_k^{ij}-\Lambda_i)\zeta_k(t)\right.\\&\quad\left.+\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^t\zeta_k^T(t)\Lambda_i\zeta_k(t)\right\}.\end{aligned}\tag{53}$$

Combining (6) and (21), we have

$$\begin{aligned}&\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^{t_k}\zeta_k^T(t)\Pi_k^{ij}\zeta_k(t)\right\}\\&\le\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^t\zeta_k^T(t)\rho_j(\Pi_k^{ij}-\Lambda_i)\zeta_k(t)\right.\\&\quad\left.+\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^t\zeta_k^T(t)\Lambda_i\zeta_k(t)\right\}\\&\le\mathbb{E}\left\{\sum_{i=1}^{r}\sum_{j=1}^{r}\mu_i^t\mu_j^t\zeta_k^T(t)\left[\rho_i(\Pi_k^{ii}-\Lambda_i)+\Lambda_i\right]\zeta_k(t)\right.\\&\quad+\sum_{i=1}^{r}\sum_{i<j}\mu_i^t\mu_j^t\zeta_k^T(t)\Big[\rho_j(\Pi_k^{ij}-\Lambda_i)+\Lambda_i\\&\quad\left.+\rho_i(\Pi_k^{ji}-\Lambda_j)+\Lambda_j\Big]\zeta_k(t)\right\}.\end{aligned}\tag{54}$$

By borrowing the method of reducing the conservativeness in [33], it follows that (20)–(23) are sufficient conditions to ensure $\mathbb{E}\{\dot{V}(t)+2\delta V(t)\}<0$ from (37), (46), (51), and (54). On the basis of the definition of the exponential stability in [34] and [35], together with Assumption 1, we can conclude that using the proposed memory-based continuous ETM, the fuzzy system (9) with resilient switched controllers in the presences of bounded cyberattacks is exponentially stable in the mean-square and secure sense.

REFERENCES

[1] C.-S. Tseng, B.-S. Chen, and H.-J. Uang, "Fuzzy tracking control design for nonlinear dynamic systems via TS fuzzy model," *IEEE Trans. Fuzzy Syst.*, vol. 9, no. 3, pp. 381–392, Jun. 2001.

[2] H. Li, H. Liu, H. Gao, and P. Shi, "Reliable fuzzy control for active suspension systems with actuator delay and fault," *IEEE Trans. Fuzzy Syst.*, vol. 20, no. 2, pp. 342–357, Apr. 2012.

[3] H.-K. Lam and L. D. Seneviratne, “Stability analysis of interval type-2 fuzzy-model-based control systems,” *IEEE Trans. Syst., Man, Cybern., Part B*, vol. 38, no. 3, pp. 617–628, Jun. 2008.

[4] J. Talla, L. Streit, Z. Peroutka, and P. Drabek, “Position-based TS fuzzy power management for tram with energy storage system,” *IEEE Trans. Ind. Electron.*, vol. 62, no. 5, pp. 3061–3071, May 2015.

[5] X.-M. Zhang, Q.-L. Han, and X. Ge, “A novel finite-sum inequality-based method for robust H_∞ control of uncertain discrete-time Takagi–Sugeno fuzzy systems with interval-like time-varying delays,” *IEEE Trans. Cybern.*, vol. 48, no. 9, pp. 2569–2582, Sep. 2018.

[6] E. A. Lee, “Cyber physical systems: Design challenges,” in *Proc. 11th IEEE Int. Symp. Object Component-Oriented Real-Time Distrib. Comput.*, 2008, pp. 363–369.

[7] 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.*, to be published, doi: 10.1109/TCYB.2020.2970556.

[8] Z. Gu, J. H. Park, D. Yue, Z.-G. Wu, and X. Xie, “Event-triggered security output feedback control for networked interconnected systems subject to cyber-attacks,” *IEEE Trans. Syst., Man, Cybern.: Syst.*, to be published, doi: 10.1109/TSMC.2019.2960115.

[9] X.-M. Zhang *et al.*, “Networked control systems: a survey of trends and techniques,” *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 1, pp. 1–17, Jan. 2020.

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

[11] W. Heemels, K. H. Johansson, and P. Tabuada, “An introduction to event-triggered and self-triggered control,” in *Proc. 51st IEEE Conf. Decis. Control*, Maul, Hawaii, USA, Dec. 10–13, 2012, pp. 3270–3285.

[12] D. N. Borgers and W. M. Heemels, “Event-separation properties of event-triggered control systems,” *IEEE Trans. Autom. Control*, vol. 59, no. 10, pp. 2644–2656, Oct. 2014.

[13] S. H. Mousavi, M. Ghodrat, and H. J. Marquez, “A novel integral-based event triggering control for linear time-invariant systems,” in *Proc. 53rd IEEE Conf. Decis. Control*, 2014, pp. 1239–1243.

[14] 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.

[15] Z. Gu, X. Zhou, T. Zhang, F. Yang, and M. Shen, “Event-triggered filter design for nonlinear cyber-physical systems subject to deception attacks,” *ISA Trans.*, 2019, to be published, doi: 10.1016/j.isatra.2019.02.036.

[16] X. Su, Y. Wen, P. Shi, and H.-K. Lam, “Event-triggered fuzzy filtering for nonlinear dynamic systems via reduced-order approach,” *IEEE Trans. Fuzzy Syst.*, vol. 27, no. 6, pp. 1215–1225, Jun. 2019.

[17] A. Selivanov and E. Fridman, “Event-triggered H_∞ control: A switching approach,” *IEEE Trans. Autom. Control*, vol. 61, no. 10, pp. 3221–3226, Oct. 2016.

[18] X. Wang, Z. Fei, H. Gao, and J. Yu, “Integral-based event-triggered fault detection filter design for unmanned surface vehicles,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5626–5636, Oct. 2019.

[19] Z. A. Biron, S. Dey, and P. Pisu, “Real-time detection and estimation of denial of service attack in connected vehicle systems,” *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

[20] X.-M. Zhang, Q.-L. Han, X. Ge, and L. Ding, “Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks,” *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020.

[21] Y. Mo and B. Sinopoli, “Secure control against replay attacks,” in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput.*, Oct. 2009, pp. 911–918.

[22] D. Ding, Q.-L. Han, Z. Wang, and X. Ge, “A survey on model-based distributed control and filtering for industrial cyber-physical systems,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2483–2499, May 2019.

[23] Y. He, G. J. Mendis, and J. Wei, “Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism,” *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[24] Z. Wang, D. Wang, B. Shen, and F. E. Alsaadi, “Centralized security-guaranteed filtering in multirate-sensor fusion under deception attacks,” *J. Franklin Inst.*, vol. 355, no. 1, pp. 406–420, 2018.

[25] J. Liu, Z.-G. Wu, D. Yue, and J. H. Park, “Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks,” *IEEE Trans. Syst., Man, Cybern.: Syst.*, to be published, doi: 10.1109/TSMC.2018.2888633.

[26] C. Peng, M. Wu, X. Xie, and Y.-L. Wang, “Event-triggered predictive control for networked nonlinear systems with imperfect premise matching,” *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 5, pp. 2797–2806, Oct. 2018.

[27] J. Liu, Y. Wang, L. Zha, and H. Yan, “Event-based control for networked TS fuzzy cascade control systems with quantization and cyber attacks,” *J. Franklin Inst.*, vol. 356, no. 16, pp. 9451–9473, 2019.

[28] E. Tian, Z. Wang, L. Zou, and D. Yue, “Probabilistic-constrained filtering for a class of nonlinear systems with improved static event-triggered communication,” *Int. J. Robust Nonlinear Control*, vol. 29, no. 5, pp. 1484–1498, 2019.

[29] Q. Feng and S. K. Nguang, “Stabilization of uncertain linear distributed delay systems with dissipativity constraints,” *Syst. Control Lett.*, vol. 96, pp. 60–71, 2016.

[30] H. Zhang, J. Yang, and C.-Y. Su ,“T–S fuzzy-model-based robust H_∞ design for networked control systems with uncertainties,” *IEEE Trans. Ind. Informat.*, vol. 3, no. 4, pp. 289–301, Nov. 2007.

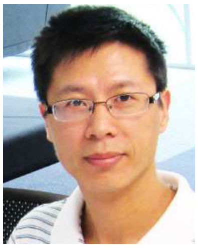
[31] A. Seuret and F. Gouaisbaut, “Wirtinger-based integral inequality: Application to time-delay systems,” *Automatica*, vol. 49, no. 9, pp. 2860–2866, 2013.

[32] Z. Gu, P. Shi, D. Yue, and Z. Ding, “Decentralized adaptive event-triggered H_∞ filtering for a class of networked nonlinear interconnected systems,” *IEEE Trans. Cybern.*, vol. 49, no. 5, pp. 1570–1579, May 2019.

[33] S. Xu, J. Lam, B. Zhang, and Y. Zou, “New insight into delay-dependent stability of time-delay systems,” *Int. J. Robust Nonlinear Control*, vol. 25, no. 7, pp. 961–970, 2015.

[34] Z. Fei, C. Guan, and H. Gao, “Exponential synchronization of networked chaotic delayed neural network by a hybrid event trigger scheme,” *IEEE Trans. Neural Netw.Learn. Syst.*, vol. 29, no. 6, pp. 2558–2567, Jun. 2018.

[35] E. Fridman, “A refined input delay approach to sampled-data control,” *Automatica*, vol. 46, no. 2, pp. 421–427, 2010.



Zhou Gu received the B.S. degree in automation from North China Electric Power University, Beijing, China, in 1997 and the M.S. and Ph.D. degrees in control science and engineering from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2007 and 2010, respectively.

From September 1996 to January 2013, he was with the School of Power Engineering, Nanjing Normal University, Nanjing, China, as an Associate Professor. He is currently a Professor with Nanjing Forestry University, Nanjing, China. His current research interests include networked control systems, time-delay systems, reliable control, and their applications.

Peng Shi (Fellow, IEEE) received the Ph.D. degree in electrical engineering from the University of Newcastle, Callaghan NSW, Australia, in 1994, the Dr.Sci. degree in electrical engineering from the University of Glamorgan, Wales, U.K., in 2006, and the Dr.Eng. degree in electrical engineering from the University of Adelaide, Adelaide, SA, Australia, in 2015.

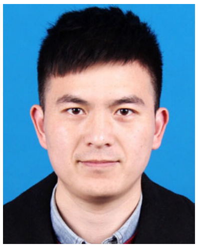
He is currently a Professor with the University of Adelaide. His current research interests include system and control theory, intelligent systems, and operational research.

Prof. Shi was the recipient of the Andrew Sage Best Transactions Paper Award from IEEE SMC Society in 2016. He has served on the editorial board of a number of journals, including *Automatica*; IEEE TRANSACTIONS ON AUTOMATIC CONTROL, IEEE TRANSACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON FUZZY SYSTEMS, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS; IEEE CONTROL SYSTEMS LETTERS, *Information Sciences*, and *Signal Processing*. He is a Member-at-Large of Board of Governors, IEEE Systems, Man, and Cybernetics Society (SMCS), and an IEEE SMCS Distinguished Lecturer. He is a Fellow of the Institution of Engineering and Technology and the Institute of Engineers, Australia.

Dong Yue (Senior Member, IEEE) received the Ph.D. degree in control science and engineering from the South China University of Technology, Guangzhou, China, in 1995.

He is currently a Changjiang Professor and the Dean of the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include analysis and synthesis of networked control systems, multiagent systems, optimal control of power systems, and the Internet of Things.

Prof. Yue is currently an Associate Editor for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON NEURAL NETWORKS and *Learning Systems*, *Journal of The Franklin Institute*, *International Journal of Systems Science*, and the IEEE Control Systems Society Conference Editorial Board.



Shen Yan received the B.S. degree in automation and Ph.D. degree in power engineering automation from the College of Electrical Engineering and Control Science of Nanjing Technology University, Nanjing, China.

He is currently a Lecturer with the College of Mechanical and Electronic Engineering, Nanjing Forestry University, Nanjing, China. His current research interests include networked control systems, nonlinear systems, and event-triggered control.

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

From 2012 to 2014, he was a Postdoctoral Fellow with the Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, China. He is currently a Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms.