Available online at www.sciencedirect.com

ScienceDirect

Journal of the Franklin Institute 357 (2020) 2851–2867

www.elsevier.com/locate/jfranklin

Security control for T-S fuzzy systems with multi-sensor saturations and distributed event-triggered mechanism

Lijuan Zha[a,b,*], Jinliang Liu[a], Jinde Cao[b]

[a] *College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, Jiangsu, China*
[b] *School of Mathematics, Southeast University, Nanjing, Jiangsu, China*

Received 26 August 2019; received in revised form 12 January 2020; accepted 11 February 2020
Available online 26 February 2020

Abstract

This paper addresses security control for a class of Takagi-Sugeno (T-S) fuzzy systems with multi-sensor saturations and distributed event-triggered mechanism (DETM). As sensors can be located in different places, we will introduce a DETM to reduce the transmission rate of the network. The output measurements of each sensor are released into the network or not is dependent on the corresponding event-triggered condition. A new T-S fuzzy model is constructed, which characterizes the influences of multi-sensor saturations and cyber-attacks. Sufficient conditions are derived for ensuring the asymptotical stability of the augmented closed-loop system. The explicit expressions of the controller gains are obtained. Finally, the feasibility of the designed algorithm is shown by a numerical example.

1. Introduction

During the past decades, Takagi-Sugeno (T-S) fuzzy system technique has received much attention in approximating complex nonlinear systems by using a set of IF-THEN rules and a group of local linear systems [1–4]. Fruitful results on controller and filter design problem for

[*] Corresponding author at: College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, Jiangsu, China.

E-mail addresses: zhalijuan@vip.163.com (L. Zha), liujinliang@vip.163.com (J. Liu), jdcao@seu.edu.cn (J. Cao).

https://doi.org/10.1016/j.jfranklin.2020.02.013

nonlinear systems via T-S fuzzy model have been achieved [5–7]. For instances, considering the mismatched premises of the system and the controller, the event triggering parameters and controller gain were co-designed in [5] for networked T-S fuzzy systems. The authors concentrated on the robust $\mathcal{H}_\infty$ control for nonlinear networked systems [6] with multiple missing measurements and multiple probabilistic delays. In [7], the fault detection problem was addressed for continuous-time fuzzy semi-Markov jump systems via an interval type-2 fuzzy approach.

Compared with traditional control systems, networked control systems (NCSs) are superior in lower installation costs, more flexibility and simpler maintainability. In NCSs, controllers communicate information with the sensors and plants via network. However, the network bandwidth in NCSs are limited. It is necessary to design an suitable data communication scheme to reduce the transmitted data packets. In recent years, many efforts are devoted to deal with this problem and various transmission mechanisms are proposed [8–15]. Specifically, compared with time-triggered schemes, event-triggered mechanisms is more effective in lightening the load of networked communication, which has been proved by simulation results in related publications (see [9] for example). Event-triggered control and filtering problems have been investigated by lots of researchers. In [9], the authors proposed an event-triggered scheme which was implemented via monitoring the sampled system state at discrete instants. In [12], the authors addressed the distributed event-triggered control for NCSs under hybrid wired-wireless networks. In [13], the distributed event-triggered filtering problem over sensor networks was discussed. However, to the best of the authors' knowledge, the security control has not been addressed for T-S fuzzy systems subject to multi-sensor saturations and DETM at present, which motivates this study.

Moreover, the insertion of the network also brings the NCSs vulnerable to cyber-attacks [16–19]. The security of NCSs has become one of the main concerns in control field. The attackers can launch denial of service (DoS) attacks or deception attacks [20–22] to destruct the NCSs. The goal of DoS attacks is to interrupt the information communication between system components [23]. While deception attacks aim to tamper data packets [24]. Recently, lots of researchers have taken the cyber-attacks into the analysis and design of networked systems [25–27]. Considering the effects of deception attacks, the authors in [25] investigated the distributed recursive filtering problem for discrete time-delayed systems with quantization. The security-guaranteed centralized filter was designed in [27] for linear time-invariant systems under deception attacks.

To the best of our knowledge, event-triggered control for nonlinear networked systems has not been fully studied, not to mention the situation when the cyber-attacks and sensor saturations are involved. Hence, it makes practical sense to take the sensor saturation and the occurrence of cyber-attacks into account when investigating the security control for distributed event-triggered T-S fuzzy systems. To shorten such a gap, in this paper, the security control problem is investigated for T-S fuzzy systems with multi-sensor saturations and DETM. The main contributions can be summarized as follows. First, a DETM is introduced to alleviate the burden of the network and increase the lifespan of the batteries of the sensors. Each event generator at the corresponding sensor can determine triggered events based on the local information. Second, the influence of stochastic cyber-attacks and the sensor saturation phenomena are taken into consideration simultaneously. Third, a desired security controller is designed which can ensure the stability of the addressed system.

The rest of this paper is organized as follows. A new T-S fuzzy model is constructed in Section 2. The main results are presented in Section 3. A numerical example is given in Section 4.

2. Problem formulation

Consider the following T-S fuzzy model with r rules, the ith fuzzy rule is
Plant Rule i: IF $\eta_1(x(t))$ is H_1^i and … and $\eta_l(x(t))$ is H_l^i, THEN

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

$$y(t) = sat(C_i x(t)) \tag{2}$$

where $\eta_1(x(t)), \eta_2(x(t)), \dots, \eta_l(x(t))$ represent the premise variables, $H_1^i, H_2^i, \dots, H_l^i$ are the fuzzy sets, $i \in \{1, 2, \dots, r\}$, r is the number of IF-THEN rules, $x(t) \in \mathbb{R}^n$ is the state vector, $u(t) \in \mathbb{R}^s$ denotes the control input, $y(t)$ is the measurement output of the sensor with saturation, A_i, B_i and C_i are known matrices with appropriate dimensions, $sat(\cdot)$ is the saturation function.

Assumption 1. [28] The saturation function $sat(C_i x(t))$ can be decomposed into a linear function and a nonlinear function as follows:

$$sat(C_i x(t)) = C_i x(t) - \varphi(C_i x(t)) \tag{3}$$

and the nonlinear function $\varphi(C_i x(t))$ satisfies the following condition

$$x^T(t) C_i^T C_i x(t) \geq \varphi^T(C_i x(t)) \varphi(C_i x(t)) \tag{4}$$

By the use of a singleton fuzzifier and center-average defuzzifier, from Eqs. (1) and (2), we can get

$$\dot{x}(t) = \sum_{i=1}^{r} h_i(\eta(x))[A_i x(t) + B_i u(t)] \tag{5}$$

$$y(t) = \sum_{i=1}^{r} h_i(\eta(x)) sat(C_i x(t)) \tag{6}$$

where $\eta(x) = \begin{bmatrix} \eta_1(x), & \dots, \eta_l(x) \end{bmatrix}$, $\eta_u(x)$ is the abbreviation of $\eta_u(x(t)), u = 1, 2, \dots, l$, $h_i(\eta(x)) = \frac{\mu_i(\eta(x))}{\sum_{i=1}^{r} \mu_i(\eta(x))}$, $\mu_i(\eta(x)) = \prod_{u=1}^{l} H_u^i(\eta_u(x))$, $H_u^i(\eta_u(x))$ is the membership value of $\eta_u(x)$ in H_u^i. The membership functions $h_i(\eta(x))$ satisfy $h_i(\eta(x)) \geq 0$, $\sum_{i=1}^{r} h_i(\eta(x)) = 1$.

As is shown in Fig. 1, the outputs $y(t)$ are grouped into n nodes and $y(t) = \begin{bmatrix} y_1(t), & \dots & y_n(t) \end{bmatrix}^T$. Each sensor node is equipped with an event generator to decrease the waste of network resources and reduce the amount of event-triggering events. The n sensors sample their output measurements $y_p(t)(p = 1, 2, \dots, n)$ from the plant, respectively. The sampled signals are then transmitted to the corresponding event generator. Whether the sampled data at each sensor are sent into the network transmission channel or not is subject to the following judgement:

$$(e_k^p(t))^T \Omega^p e_k^p(t) - \sigma y_p(t_k^p h + l^p h)^T \Omega^p y_p(t_k^p h + l^p h) < 0 \tag{7}$$

where $\sigma \in [0, 1)$, $\Omega^p > 0$, h is the constant sampling period, $y_p(t_k^p h)$ is the latest released sensor measurement, $y_p(t_k^p h + l^p h)$ is the current sampled sensor measurement, $e_k^p(t) = y_p(t_k^p h) -$

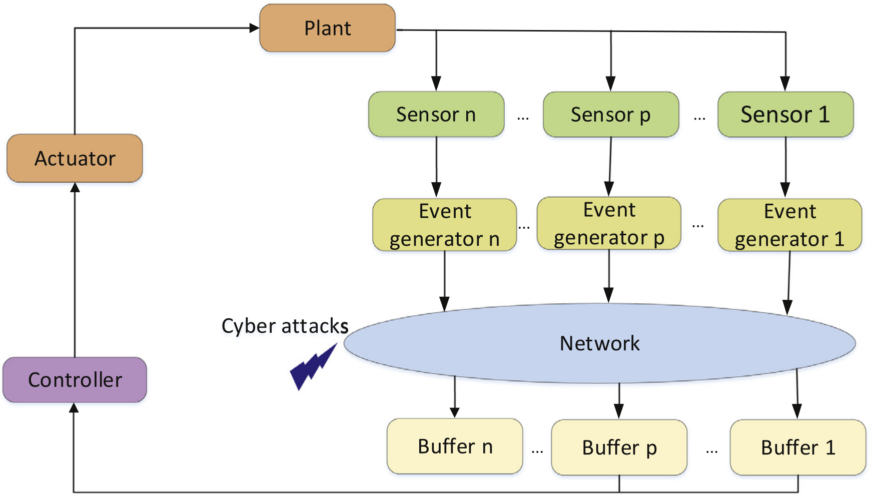

Fig. 1. Control system structure subject to cyber-attacks and DETM.

$y_p(t_k^p h + l^p h)$ is the error between the current sampled sensor measurement and the latest released one. Only when condition (7) is satisfied, the newly sampled signal $y_p(t_k^p h + l^p h)$ will be transmitted trough the network. Obviously, if $t_k^p h$ represents the latest released instant when the sampled signal at the pth sensor is transmitted into the network, the next triggering instants $t_{k+1}^p h$ for the pth sensor can be represented as follows:

$$t_{k+1}^p h = t_k^p h + \min_{l^p \in S} \left\{ l^p h | (e_k^p(t))^T \Omega^p e_k^p(t) - \sigma y_p(t_k^p h + l^p h)^T \Omega^p y_p(t_k^p h + l^p h) < 0 \right\} \tag{8}$$

With the effect of the DETM, the output measurements of each sensor can be transmitted at different instants. The transmission times of the distributed sensors are not required to be the same. That is, the triggering instant of each event generator is irrelevant. Motivated by Ref. [29], to make the introduced DETM practicable, we can set a series of buffers before the controllers to store the triggered time-stamped sensor measurements. Notice that an identical time-stamp will be attached from the sensor to the controller if one local event-triggered condition is triggered. Only the latest available store signal from the buffers with the same time-stamp can be selected as the controller input. Hence, the updated time sequence of the controller is

$$t_{k+1} h = t_k h + lh \tag{9}$$

in which

$$lh = argmin_{p \in \mathbb{S}} \{ l^p h | \Lambda_p(t) < 0, p \in \mathbb{S} \}$$
$$\Lambda_p(t) = (e_k^p(t))^T \Omega^p e_k^p(t) - \sigma y_p(t_k^p h + l^p h)^T \Omega^p y_p(t_k^p h + l^p h)$$
$$\mathbb{S} = \{1, 2, \ldots\}$$

From Eq. (7) and the use of the buffers, we can deduce that the controller input satisfies

$$(e_k(t))^T \Omega e_k(t) - \sigma y(t_k h + lh)^T \Omega y(t_k h + lh) < 0 \tag{10}$$

where $\Omega = diag\{\Omega^1, \dots, \Omega^n\}$, $e_k^p(t)$ and $y_p(t_k^p h + l^p h)$ in (7) represent the pth components of $e_k(t)$ and $y(t_k h + lh)$ in Eq. (10).

Remark 1. It should be noted that owing to the existence of transmission delay, the set of released sensor measurements $y_p(t_0^p h), y_p(t_1^p h), y_p(t_2^p h), \dots$ will reach the controller at instants $t_0^p h + \tau_{t_0^p h}, t_1^p h + \tau_{t_1^p h}, t_2^p h + \tau_{t_2^p h}, \dots,$ respectively.

Remark 2. The judgement algorithm (7) is implemented to decrease the waste of network resources and reduce the amount of event-triggering events. Only when the newly sampled data violate (7) can they be released into the network. The use of judgement algorithm (7) leads to low transmission frequency, reduction in the release times of the sensor and reduction in calculation cost of controller.

Similar to Ref. [9], the control input keeps constant for the holding interval $\left[t_k h + \tau_{t_k}, t_{k+1} h + \tau_{t_{k+1}}\right)$, which can be represented as $\bigcup_{l=0}^{\mu} \mathbb{U}_l$, $\mathbb{U}_l = \left[t_k h + lh + \tau_{t_k+l}, t_k h + lh + h + \tau_{t_k+l+1}\right)$ $(l = 0, 1, \dots, \mu)$, $\mu = t_{k+1} - t_k - 1$. Define $\tau(t) = t - t_k h - lh$, it is easy to see that $0 \le \tau_{t_k+l} \le \tau(t) \le \tau_{t_k+l+1} + h \triangleq \tau_M$. Then, combining the equality (10) and the definition of $\tau(t)$, Eq. (10) can be rewritten as

$$(e_k(t))^T \Omega e_k(t) \le \sigma y^T (t - \tau(t)) \Omega y(t - \tau(t)) \tag{11}$$

Remark 3. It is worth noting that the event-triggering condition designed in this paper is different from the ones in [30,31]. In [30], from the aspect of privacy protection, the triggering condition is devised based on the control input. By applying the proposed event-triggered approach, the authors in [30] investigated the secure consensus problem in multiagent systems with denial-of -service attacks. In [31], the event-driven criterion was related to the error between the current measurements and the latest transmitted ones, and the event-driven fault-detection issue was addressed for discrete-time interval type-2 fuzzy systems. Different from the results in [30,31], the distributed event-triggering condition in this paper is designed with consideration of the occurrence of sensor saturation, based on the DETM, we consider the security control for T-S fuzzy systems with cyber-attacks.

Based on the above definition $e_k(t)$ and $\tau(t)$, combining (3) and (6), for $t \in \left[t_k h + \tau_{t_k}, t_{k+1} h + \tau_{t_{k+1}}\right)$, the controller input under the DETM can be expressed as follows

$$\begin{aligned} \bar{y}(t) &= y(t_k h) \\ &= y(t - \tau(t)) + e_k(t) \\ &= \sum_{i=1}^{r} h_i(\eta(x))[C_i x(t - \tau(t)) - \varphi(C_i x(t - \tau(t))) + e_k(t)] \end{aligned} \tag{12}$$

Considering the fact that the network may suffer malicious attacks, the information $\bar{y}(t)$ transmitted through the network channel may be tampered with by the attackers, which means that the controller may not receive the accurate information $\bar{y}(t)$. In this paper, the normal transmission data $\bar{y}(t)$ is assumed to be replaced by the malicious signal $f(x(t))$ randomly, then, the real inputs of the controller can be expressed as

$$\hat{y}(t) = \alpha(t) f(x(t - d(t))) + (1 - \alpha(t))\bar{y}(t) \tag{13}$$

where $f(x(t - d(t))) = \left[f_1^T(x^1(t - d(t))), \quad \dots, \quad f_n^T(x^n(t - d(t)))\right]^T$, $d(t) \in [0, d_M]$, d_M is a known constant. $\alpha(t) \in \{0, 1\}$ is a Bernoulli distributed variable with $\mathbb{E}\{\alpha(t)\} = \bar{\alpha}$. Then, the mathematical variance of $\alpha(t)$ is easily to obtained as $\mu^2 = \bar{\alpha}(1 - \bar{\alpha})$.

In this paper, considering the DETM and the stochastic occurring cyber-attacks, the jth rule of the fuzzy controller is designed as

Controller Rule j: IF $\eta_1(x(t))$ is H_1^j and … and $\eta_l(x(t))$ is H_l^j, THEN

$$u(t) = K_j\hat{y}(t) \tag{14}$$

where K_j denotes the output feedback controller parameter to be determined, $j \in \{1, 2, \ldots, r\}$. Then, the fuzzy output feedback controller can be described as

$$u(t) = \sum_{j=1}^{r} h_j(\eta(x)K_j\hat{y}(t) \tag{15}$$

Remark 4. As is well known that limited resources and cyber-attacks are unavoidable in network. In this paper, we only assume that only the network channel between sensors and controller is subject to limited resources and cyber-attacks. The network between controller and actuator is assumed to work normally.

Remark 5. For equality (13), when $\alpha(t) = 1$, the malicious signals will replace the normal transmitted data, the real input of the controller is $\hat{y}(t) = f(x(t - d(t)))$. When $\alpha(t) = 0$, the triggered signals are delivered through the network without being attacked and can arrive at the controller successfully, that is $\hat{y}(t) = \bar{y}(t)$.

Substitute (13) into (15), the output feedback controller (15) can be rewrited as

$$u(t) = \sum_{j=1}^{r} h_j(\eta(x)K_j\{\alpha(t)f(x(t - d(t))) + (1 - \alpha(t))[y(t - \tau(t)) + e_k(t)]\} \tag{16}$$

By combining equality (5) and (16), the closed-loop output feedback control system is

$$\begin{aligned}\dot{x}(t) = \sum_{i=1}^{r}\sum_{j=1}^{r} h_i(\eta(x))h_j(\eta(x))\{A_ix(t) + (1 - \alpha(t))B_iK_j\big[C_jx(t - \tau(t)) + e_k(t) \\ -\varphi(C_jx(t - \tau(t)))\big] + \alpha(t)B_iK_jf(x(t - d(t)))\big\}\end{aligned} \tag{17}$$

Assumption 2. [32] $f(x(t))$ in Eq. (13) is a continuous function, there exists a matrix F such that

$$||f(x(t))||_2 \leq ||Fx(t)||_2 \tag{18}$$

Remark 6. The key idea of this paper is to discuss the security control for distributed event-triggered T-S fuzzy systems with muti-sensor saturations and cyber-attacks. The distributed event-triggered scheme in this paper is motivated by the scheme proposed in Ref. [9]. The simulation results in Ref. [9] have shown the event-triggered scheme is superior to some existing ones by comparison. It is worth mentioning that numerous methods were proposed to address sensor saturation and the cyber-attacks. In [33], the saturation and the network resource limitation were considered for event-triggered control for multi-agent systems with sensor faults, while the cyber-attacks are not. In [34], the multiple attacks was considered for state-dependent uncertain systems with limited communication resources, however, the sensor saturation is not. The strategies in [9,33,34] may not effective if the three phenomena occur simultaneously. It is meaningful to think about the three factors together. Therefore, we firstly investigate the security control for T-S fuzzy systems against sensor saturations, cyber-attacks and limited network resources.

3. Main results

In the following, sufficient conditions will be derived to guarantee the stability of the controlled plant (1). The controller and the DETM will be co-designed.

Theorem 1. *Let time delays τ_M, d_M, $\bar{\alpha}$, triggering scalar σ, matrices F and K_j be given, the asymptotically stability of augmented system (17) is achieved if there exist matrices $P>0$, $Q_q>0$, $R_q>0$, $U_q>0$ $(q=1,2)$, and Ω such that*

$$\Psi_{ij}+\Psi_{ji}<0(i,j=1,2,\dots,r,i\leq j) \tag{19}$$

$$\begin{bmatrix} R_q & * \\ U_q & R_q \end{bmatrix} \geq 0 \tag{20}$$

where

$$\Psi_{ij}=\begin{bmatrix} \Xi_{ij}^{11} & * & * & * \\ \Xi_{ij}^{21} & \Xi_{ij}^{22} & * & * \\ \Xi_{ij}^{31} & 0 & \Xi_{ij}^{33} & * \\ \Xi_{ij}^{41} & 0 & 0 & \Xi_{ij}^{44} \end{bmatrix}$$

in which

$$\Xi_{ij}^{11}=\begin{bmatrix} \Xi_{ij}^{111} & * \\ \Xi_{ij}^{112} & \Xi_{ij}^{113} \end{bmatrix}, \quad \Xi_{ij}^{111}=\begin{bmatrix} \Gamma_{ij}^{11} & * & * & * \\ \Gamma_{ij}^{21} & \Gamma_{ij}^{22} & * & * \\ U_1 & R_1-U_1 & -Q_1-R_1 & * \\ R_2-U_2 & 0 & 0 & \Gamma_{ij}^{44} \end{bmatrix}$$

$$\Gamma_{ij}^{11}=PA_i+A_i^TP+Q_1+Q_2-R_1-R_2,$$

$$\Gamma_{ij}^{21}=\bar{\alpha}_1C_j^TK_j^TB_i^TP+R_1-U_1$$

$$\Xi_{ij}^{112}=\begin{bmatrix} U_2 & 0 & 0 & R_2-U_2 \\ \bar{\alpha}_1K_j^TB_i^TP & 0 & 0 & 0 \\ \bar{\alpha}K_j^TB_i^TP & 0 & 0 & 0 \\ -\bar{\alpha}_1K_j^TB_i^TP & -\sigma\Omega C_i & 0 & 0 \end{bmatrix}$$

$$\Xi_{ij}^{113}=\begin{bmatrix} -Q_2-R_2 & * & * & * \\ 0 & -\Omega & * & * \\ 0 & 0 & -I & * \\ 0 & 0 & 0 & -I+\sigma\Omega \end{bmatrix}$$

$$\Gamma_{ij}^{22}=\tilde{\Omega}-2R_1+U_1+U_1^T, \quad \bar{\alpha}_1=1-\bar{\alpha}, \tilde{\Omega}=C_j^T\sigma\Omega C_j$$

$$\Gamma_{ij}^{44}=-2R_2+U_2+U_2^T, \quad \Xi_{ij}^{21}=\begin{bmatrix} 0 & C_j & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & F & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\Xi_{ij}^{22} = diag\{-I, -I\}, \quad \Xi_{ij}^{31} = \begin{bmatrix} \Xi_{ij}^{311} & \Xi_{ij}^{312} \end{bmatrix}$$

$$\Xi_{ij}^{311} = \begin{bmatrix} \tau_M PA_i & \bar{\alpha}_1 \tau_M PB_i K_j C_j & 0 & 0 & 0 \\ d_M PA_i & \bar{\alpha}_1 d_M PB_i K_j C_j & 0 & 0 & 0 \end{bmatrix}$$

$$\Xi_{ij}^{312} = \begin{bmatrix} \bar{\alpha}_1 \tau_M PB_i K_j & \bar{\alpha} \tau_M PB_i K_j & -\bar{\alpha}_1 \tau_M PB_i K_j \\ \bar{\alpha}_1 d_M PB_i K_j & \bar{\alpha} d_M PB_i K_j & -\bar{\alpha}_1 d_M PB_i K_j \end{bmatrix}$$

$$\Xi_{ij}^{41} = \begin{bmatrix} \Xi_{ij}^{411} & \Xi_{ij}^{412} \end{bmatrix}, \quad \Xi_{ij}^{411} = \begin{bmatrix} 0 & -\mu \tau_M PB_i K_j C_j & 0 & 0 & 0 \\ 0 & -\mu d_M PB_i K_j C_j & 0 & 0 & 0 \end{bmatrix}$$

$$\Xi_{ij}^{412} = \begin{bmatrix} -\mu \tau_M PB_i K_j & \mu \tau_M PB_i K_j & \mu \tau_M PB_i K_j \\ -\mu d_M PB_i K_j & \mu d_M PB_i K_j & \mu d_M PB_i K_j \end{bmatrix}$$

$$\Xi_{ij}^{33} = \Xi_{ij}^{44} = diag\{-PR_1^{-1}P, -PR_2^{-1}P\}$$

Proof. See Appendix A. □

Based on Theorem 1, next, a new method to design the security output feedback controller (16) will be given for the discussed plant (1).

Theorem 2. *Given time delays τ_M, d_M, ϵ_1, ϵ_2, $\bar{\alpha}$, triggering scalar σ, ω, matrix F, the asymptotically stability of the augmented system (17) is met with output feedback gain $K_j = X^{-1}Y_j$ if there exist matrices $P > 0$, $Q_q > 0$, $R_q > 0$, $U_q > 0$ $(q = 1, 2)$, Ω, Y_j and D such that*

$$\bar{\Psi}_{ij} + \bar{\Psi}_{ji} < 0 (i, j = 1, 2, \ldots, r, i \leq j) \tag{21}$$

$$\begin{bmatrix} R_q & * \\ U_q & R_q \end{bmatrix} \geq 0 \tag{22}$$

$$\begin{bmatrix} \omega I & * \\ PB_i - B_i X & -I \end{bmatrix}, \omega \to 0 \tag{23}$$

where

$$\bar{\Psi}_{ij} = \begin{bmatrix} \bar{\Xi}_{ij}^{11} & * & * & * \\ \Xi_{ij}^{21} & \Xi_{ij}^{22} & * & * \\ \bar{\Xi}_{ij}^{31} & 0 & \bar{\Xi}_{ij}^{33} & * \\ \bar{\Xi}_{ij}^{41} & 0 & 0 & \bar{\Xi}_{ij}^{44} \end{bmatrix}$$

in which

$$\bar{\Xi}_{ij}^{11} = \begin{bmatrix} \bar{\Xi}_{ij}^{111} & * \\ \bar{\Xi}_{ij}^{112} & \bar{\Xi}_{ij}^{113} \end{bmatrix}, \quad \bar{\Xi}_{ij}^{111} = \begin{bmatrix} \Gamma_{ij}^{11} & * & * & * \\ \bar{\Gamma}_{ij}^{21} & \Gamma_{ij}^{22} & * & * \\ U_1 & R_1 - U_1 & -Q_1 - R_1 & * \\ R_2 - U_2 & 0 & 0 & \Gamma_{ij}^{44} \end{bmatrix}$$

$$\bar{\Xi}_{ij}^{112} = \begin{bmatrix} U_2 & 0 & 0 & R_2 - U_2 \\ \bar{\alpha}_1 Y_j^T B_i^T & 0 & 0 & 0 \\ \bar{\alpha} Y_j^T B_i^T & 0 & 0 & 0 \\ -\bar{\alpha}_1 Y_j^T B_i^T & -\sigma \Omega C_j & 0 & 0 \end{bmatrix}$$

$$\bar{\Xi}_{ij}^{113} = \begin{bmatrix} -Q_2 - R_2 & * & * & * \\ 0 & -\Omega & * & * \\ 0 & 0 & -I & * \\ \text{!‘!‘0} & 0 & 0 & -I + \sigma \Omega \end{bmatrix}$$

$$\bar{\Xi}_{ij}^{31} = \begin{bmatrix} \bar{\Xi}_{ij}^{311} & \bar{\Xi}_{ij}^{312} \end{bmatrix}, \quad \bar{\Xi}_{ij}^{311} = \begin{bmatrix} \tau_M P A_i & \bar{\alpha}_1 \tau_M B_i Y_j C_j & 0 & 0 & 0 \\ d_M P A_i & \bar{\alpha}_1 d_M B_i Y_j C_j & 0 & 0 & 0 \end{bmatrix}$$

$$\bar{\Xi}_{ij}^{312} = \begin{bmatrix} \bar{\alpha}_1 \tau_M B_i Y_j & \bar{\alpha} \tau_M B_i Y_j & -\bar{\alpha}_1 \tau_M B_i Y_j \\ \bar{\alpha}_1 d_M B_i Y_j & \bar{\alpha} d_M B_i Y_j & -\bar{\alpha}_1 d_M B_i Y_j \end{bmatrix}, \quad \bar{\Xi}_{ij}^{41} = \begin{bmatrix} \bar{\Xi}_{ij}^{411} & \bar{\Xi}_{ij}^{412} \end{bmatrix}$$

$$\bar{\Xi}_{ij}^{411} = \begin{bmatrix} 0 & -\mu \tau_M B_i Y_j C_j & 0 & 0 & 0 \\ 0 & -\mu d_M B_i Y_j C_j & 0 & 0 & 0 \end{bmatrix}$$

$$\bar{\Xi}_{ij}^{412} = \begin{bmatrix} -\mu \tau_M B_i Y_j & \mu \tau_M B_i Y_j & \mu \tau_M B_i Y_j \\ -\mu d_M B_i Y_j & \mu d_M B_i Y_j & \mu d_M B_i Y_j \end{bmatrix}$$

$$\bar{\Gamma}_{ij}^{21} = \bar{\alpha}_1 C_j^T Y_j^T B_i^T + R_1 - U_1$$

$$\bar{\Xi}_{ij}^{33} = \bar{\Xi}_{ij}^{44} = diag\{-2\epsilon_1 P + \epsilon_1^2 R_1, -2\epsilon_2 P + \epsilon_2^2 R_2\}$$

Proof. Due to

$$(R_k - \epsilon_k^{-1} P) R_k^{-1} (R_k - \epsilon_k^{-1} P) \geq 0, (k = 1, 2) \tag{24}$$

then, $-P R_k^{-1} P \leq -2\epsilon_k P + \epsilon_k^2 R_k$ can be obtained.

Notice there are many nonlinear terms $P B_i K_j C_i$ and $P B_i K_j$ in Eq. (19), we can not solve the controller gain K_j directly. Motivated by Zha et al. [35], in order to obtain feasible controller gains, we define $B_i Y_j = P B_i K_j$, $P B_i = B_i X$, which implies the controller gains $K_j = X^{-1} Y_j$, where X and Y_j are matrices with appropriate dimensions to be solved.

Replace $P B_i K_j C_i$, $P B_i K_j$ and $-P R_k^{-1} P$ by $B_i Y_j C_i$, $B_i Y_j$ and $-2\epsilon_k P + \epsilon_k^2 R_k$, respectively, then Eq. (21) can be derived from Eq. (19).

Since $P B_i = B_i X$ is not a strict inequality, note that $(P B_i - B_i X)^T (P B_i - B_i X) = 0$ can be derived from $P B_i = B_i X$, then we transform this problem into the following optimization problem

$$\begin{bmatrix} \omega I & * \\ P B_i - B_i X & -I \end{bmatrix}, \omega \to 0 \tag{25}$$

which is Eq. (23).

This completes the proof. □

Remark 7. It is noted that the results in [36,37] are distinct from this paper in the following aspects. (1) The work in [36] dealt with adaptive fuzzy control for stochastic switched nonlinear systems with full state constraints. The work in [37] studied the problem of adaptive neural network control for multi-input and multi-output nonlinear systems. However, this paper addresses security control for T-S fuzzy systems with sensor saturation and cyber-attacks. (2) The methodologies of the system performance analysis and the controller design approach are obviously different. The results in [36,37] were obtained based on the backstepping technique. Whereas the main results in this paper are obtained by using the Lyapunov functional method and linear matrix inequality technique. (3) The cyber-attacks, sensor saturation and the limited network resources are considered in this paper, while [36,37] did not take these phenomena into consideration.

When the plant (1) is without cyber-attacks, the closed-loop control system can be formulated as

$$\dot{x}(t) = \sum_{i=1}^{r}\sum_{j=1}^{r} h_i(\eta(x))h_j(\eta(\hat{x}))\big\{A_i x(t) + B_i K_j\big[C_j x(t-\tau(t)) + e_k(t) - \varphi(C_j x(t-\tau(t)))\big]\big\} \tag{26}$$

Similar to the proof of Theorem 2, the following Corollary can be derived.

Corollary 1. *For given τ_M, ω, ϵ_1, triggering scalar σ, the augmented system (26) with output feedback gain $K_j = X^{-1}Y_j$ is asymptotically stable if there exist matrices $P > 0$, $Q_1 > 0$, $R_1 > 0$, $U_1 > 0$, Ω, Y_j and D such that Eq. (23) and the following equalities hold*

$$\hat{\Psi}_{ij} + \hat{\Psi}_{ij} < 0 (i, j = 1, 2, \ldots, r, i \leq j) \tag{27}$$

$$\begin{bmatrix} R_1 & * \\ U_1 & R_1 \end{bmatrix} \geq 0 \tag{28}$$

where

$$\hat{\Psi}_{ij} = \begin{bmatrix} \hat{\Xi}_{ij}^{11} & * & * \\ \hat{\Xi}_{ij}^{21} & -2\epsilon_1 P + \epsilon_1^2 R_1 & * \\ \hat{\Xi}_{ij}^{31} & 0 & -I \end{bmatrix}$$

$$\bar{\Gamma}_{ij}^{11} = PA_i + A_i^T P + Q_1 - R_1, \quad \bar{\Gamma}_{ij}^{21} = C_j^T Y_j^T B_i^T + R_1 - U_1$$

$$\hat{\Xi}_{ij}^{11} = \begin{bmatrix} \bar{\Gamma}_{ij}^{11} & * & * & * & * \\ \bar{\Gamma}_{ij}^{21} & \bar{\Gamma}_{ij}^{22} & * & * & * \\ U_1 & R_1 - U_1 & -Q_1 - R_1 & * & * \\ Y_j^T B_i^T & 0 & 0 & -\Omega & * \\ Y_j^T B_i^T & -\sigma\Omega C_j & 0 & 0 & -I + \sigma\Omega \end{bmatrix}$$

$$\bar{\Gamma}_{ij}^{22} = -2R_1 + U_1 + U_1^T + \tilde{\Omega}$$

$$\hat{\Xi}_{ij}^{21} = \begin{bmatrix} \tau_M P A_i & \tau_M B_i Y_j C_j & 0 & \tau_M B_i Y_j & -\tau_M B_i Y_j \end{bmatrix}$$

$$\hat{\Xi}_{ij}^{31} = \begin{bmatrix} 0 & C_j & 0 & 0 & 0 \end{bmatrix}$$

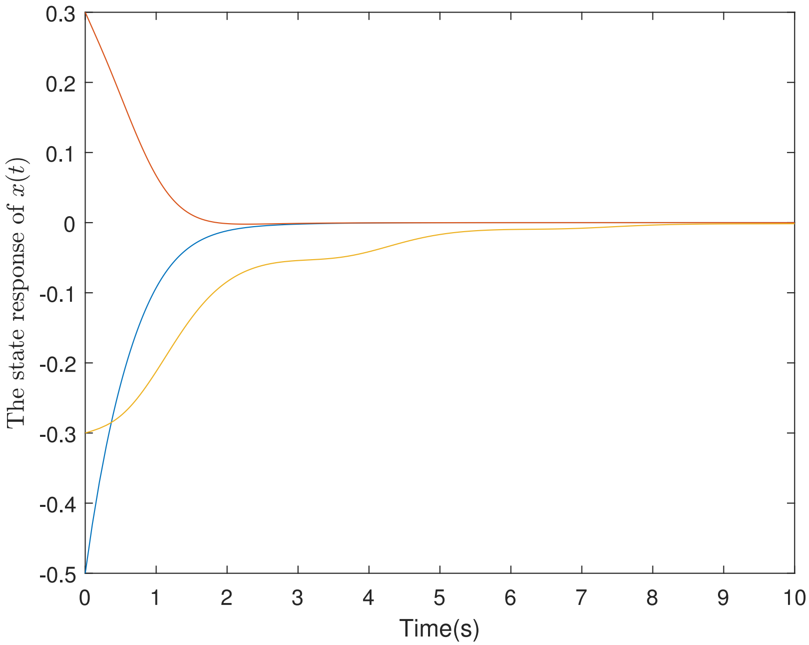

Fig. 2. The state response of $x(t)$.

4. Illustrative example

In this section, the feasibility of the proposed design method will be illustrated by the following numerical example.

Consider system (5) with the following system matrices

$$A_1 = \begin{bmatrix} -2.1 & 0.1 & 0 \\ 1 & -2 & 0 \\ 0 & 0 & -1 \end{bmatrix}, A_2 = \begin{bmatrix} -1.9 & 0 & 0 \\ -0.2 & -1.1 & 0 \\ 0 & 0 & -0.1 \end{bmatrix}, B_1 = \begin{bmatrix} -1.1 \\ 0.1 \\ 1 \end{bmatrix}$$

$$B_2 = \begin{bmatrix} -1.1 \\ -1.2 \\ 0.9 \end{bmatrix}, C_1 = \begin{bmatrix} 1 & 0.2 & 0 \\ 0.3 & 0.1 & 0 \\ 0 & 0 & 0.1 \end{bmatrix}, C_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0.5 & -0.6 & 0 \\ 0 & 0 & 0.3 \end{bmatrix}$$

$$h_1(\eta(x)) = sin^2x, h_2(\eta(x)) = 1 - h_1(\eta(x))$$

The cyber-attack is assumed to be

$$f(x(t)) = \begin{bmatrix} \tanh(0.1x_1(t)) \\ \tanh(0.3x_2(t)) \\ \tanh(0.5x_3(t)) \end{bmatrix}$$

which satisfies Assumption 2 with $F = diag\{0.1, 0.2, 0.1\}$.

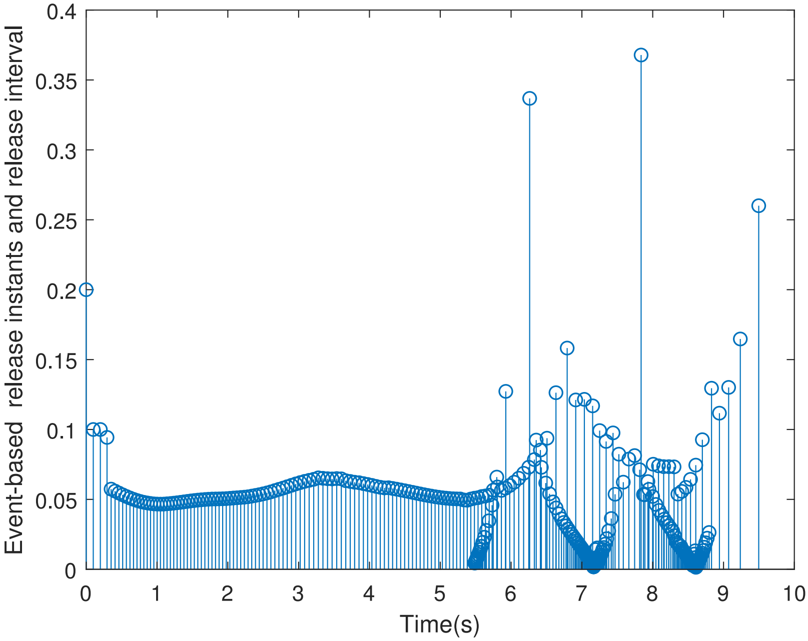

Fig. 3. Event-triggered instants of sensor 1.

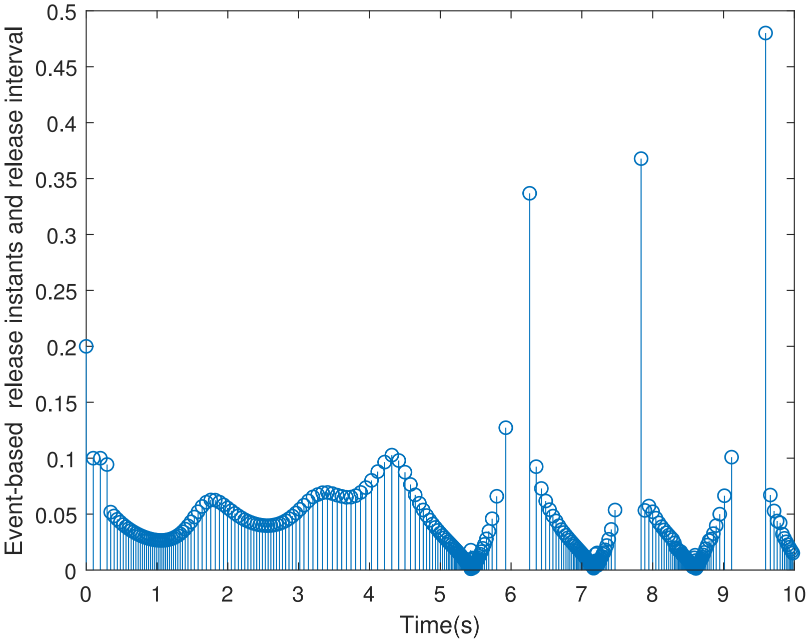

Fig. 4. Event-triggered instants of sensor 2.

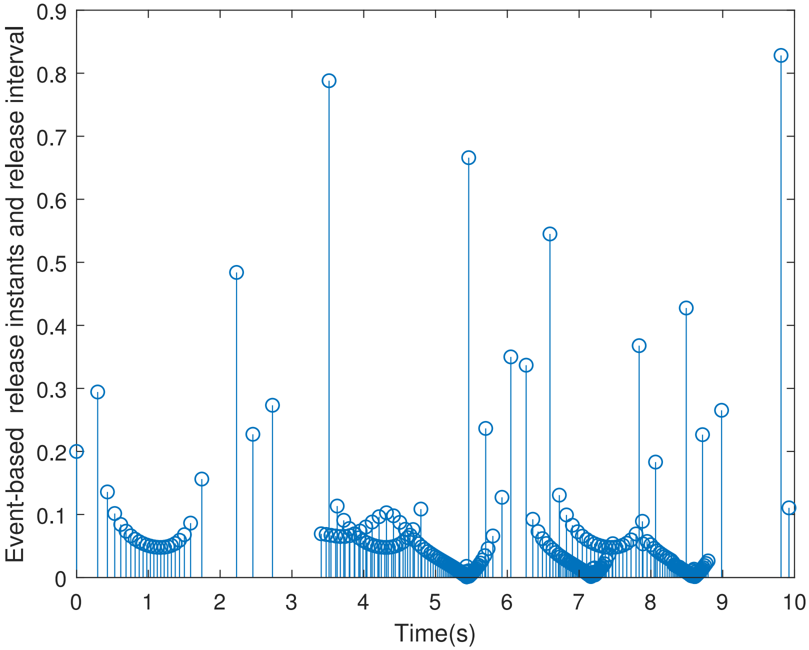

Fig. 5. Event-triggered instants of sensor 3.

For simulation purpose, we can set the initial state as $x_0 = \begin{bmatrix} -0.5 & 0.3 & -0.3 \end{bmatrix}^T$.

For given $\bar{\alpha} = 0.1$ and $\sigma = 0.3$, sampling period $h = 0.01$, time delays $\tau_M = 0.4$, $d_M = 0.3$, $\epsilon_1 = \epsilon_2 = 1$. By using LMI toolbox in MATLAB, the controller gains can be obtained as follows

$$K_1 = \begin{bmatrix} 0.0036 & 0.0011 & -0.0000 \end{bmatrix}$$

$$K_2 = \begin{bmatrix} 0.0006 & -0.0002 & -0.0025 \end{bmatrix}$$

$$\Omega = \begin{bmatrix} 47.3956 & 0 & 0 \\ 0 & 47.6031 & 0 \\ 0 & 0 & 47.7026 \end{bmatrix}$$

The response of the state is presented in Fig. 2. The event-triggered instants and releasing intervals of the three trigger schemes are represented in Figs. 3–5. From the simulated results above, we can see that the stability of the output feedback control system is ensured by the designed output feedback controller and the network communication is alleviated considerably. It can be found that the derived output feedback controller method is effective even if the augmented system is subject to sensor saturation and cyber-attacks.

5. Conclusion

In this paper, the security output feedback control problem has been investigated for T-S fuzzy systems by considering multi-sensor saturations and DETM. To mitigate the burden of networked traffic, a DETM is applied in T-S fuzzy systems. Considering the effects of multi-sensor saturations and cyber-attacks, a mathematical model is built. Sufficient conditions have been obtained to guarantee the stability of the discussed nonlinear system. Furthermore, a new design method of the output feedback controller gains has been derived. Finally, a numerical example shows the effectiveness of the designed algorithm.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China under Grant 61903182 and Grant 61973152, in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20190794 and Grant BK20171481, in part by the major project supported by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant 19KJA510005, in part by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant 18KJB120002, in part by China Postdoctoral Science Foundation under Grant 2019M651651, and in part by the Qing Lan Project.

Appendix A

Proof of Theorem 1. Consider the following Lyapunov functional

$$V(x_t)=V_1(x_t)+V_2(x_t)+V_3(x_t) \tag{29}$$

where

$$\begin{aligned}
V_1(x_t)&=x^T(t)Px(t)\\
V_2(x_t)&=\int_{t-\tau_M}^{t}x^T(s)Q_1x(s)ds+\int_{t-d_M}^{t}x^T(s)Q_2x(s)ds\\
V_3(x_t)&=\tau_M\int_{t-\tau_M}^{t}\int_{s}^{t}\dot{x}^T(v)R_1\dot{x}(v)dvds+d_M\int_{t-d_M}^{t}\int_{s}^{t}\dot{x}^T(v)R_2\dot{x}(v)dvds
\end{aligned}$$

Take the derivative and mathematical expectation of equality (29), the following equalities can be obtained

$$\mathbb{E}\{\dot{V}_1(x_t)\}=\sum_{i=1}^{r}\sum_{j=1}^{r}h_i(\eta(x))h_j(\eta(x))2x^T(t)P\mathcal{A}_{ij} \tag{30}$$

$$\mathbb{E}\{\dot{V}_2(x_t)\}=x^T(t)(Q_1+Q_2)x(t)-x^T(t-\tau_M)Q_1x(t-\tau_M)-x^T(t-d_M)Q_2x(t-d_M) \tag{31}$$

$$\mathbb{E}\{\dot{V}_3(x_t)\}=\mathbb{E}\Big\{\dot{x}^T(t)\tilde{R}\dot{x}(t)\Big\}-\tau_M\int_{t-\tau_M}^{t}\dot{x}^T(s)R_1\dot{x}(s)ds-d_M\int_{t-d_M}^{t}\dot{x}^T(s)R_2\dot{x}(s)ds \tag{32}$$

where

$$\mathcal{A}_{ij}=A_ix(t)+(1-\bar{\alpha})B_iK_j\big[C_jx(t-\tau(t)+e_k(t)-\varphi(C_jx(t-\tau(t)))\big]+\bar{\alpha}B_iK_jf(x(t-d(t)))$$

Note that

$$\mathbb{E}\left\{\dot{x}^T(t)\tilde{R}\dot{x}(t)\right\} = \sum_{i=1}^{r}\sum_{j=1}^{r} h_i(\eta(x))h_j(\eta(x))\left\{\mathcal{A}_{ij}^T\tilde{R}\mathcal{A}_{ij} + \mu^2\mathcal{B}_{ij}^T\tilde{R}\mathcal{B}_{ij}\right\} \tag{33}$$

in which

$$\tilde{R} = \tau_M^2 R_1 + d_M^2 R_2, \quad \mathcal{B}_{ij} = B_i K_j\left[f(x(t-d(t))) + \varphi(C_j x(t-\tau(t)) - C_j x(t-\tau(t)) - e_k(t)\right]$$

By using Lemma 1 in [22], if there exist U_1 and U_2 satisfying Eq. (20), one can get

$$-\tau_M\int_{t-\tau_M}^{t}\dot{x}^T(s)R_1\dot{x}(s)ds \le \varsigma_1^T(t)M_1\varsigma_1(t) \tag{34}$$

$$-d_M\int_{t-d_M}^{t}\dot{x}^T(s)R_2\dot{x}(s)ds \le \varsigma_2(t)^T M_2\varsigma_2(t) \tag{35}$$

where

$$\varsigma_1(t) = \begin{bmatrix} x(t) \\ x(t-\tau(t)) \\ x(t-\tau_M) \end{bmatrix}, \varsigma_2(t) = \begin{bmatrix} x(t) \\ x(t-d(t)) \\ x(t-d_M) \end{bmatrix}$$

$$M_q(t) = \begin{bmatrix} -R_q & * & * \\ R_q - U_q & -2R_q + U_q + U_q^T & * \\ U_q & R_q - U_q & -R_q \end{bmatrix}, \quad q = 1, 2$$

From Eqs. (11) and (2), one has

$$\sigma[C_j x(t-\tau(t)) - \varphi(C_j x(t-\tau(t)))]^T\Omega[C_j x(t-\tau(t)) - \varphi(C_j x(t-\tau(t)))] - e_k^T(t)\Omega e_k(t) \ge 0 \tag{36}$$

Recalling Assumption 1, we have

$$x^T(t-\tau(t))C_j^T C_j x(t-\tau(t)) - \varphi^T(C_j x(t-\tau(t)))\varphi(C_j x(t-\tau(t))) \ge 0 \tag{37}$$

Based on Assumption 2, we get

$$x^T(t-d(t))F^T F x(t-d(t)) - f^T(x(t-d(t)))f(x(t-d(t))) \ge 0 \tag{38}$$

Define

$$\xi^T(t) = \begin{bmatrix}\xi_1^T(t) & \xi_2^T(t)\end{bmatrix}^T$$

$$\xi_1^T(t) = \begin{bmatrix}\varsigma_1^T(t) & x^T(t-d(t)) & x^T(t-d_M) & e_k^T(t)\end{bmatrix}^T$$

$$\xi_2^T(t) = \begin{bmatrix}f^T(x(t-d(t))) & \varphi^T(C_j x(t-\tau(t)))\end{bmatrix}^T$$

Combining Eqs. (30)–(38), it yields that

$$
\begin{aligned}
\mathbb{E}\big(\dot{V}(x_t)\big) \leq{}& \sum_{i=1}^{r}\sum_{j=1}^{r} h_i(\eta(x))h_j(\eta(x))\big\{2x^T(t)P\mathcal{A}_{ij} + x^T(t)(Q_1+Q_2)x(t) \\
& -x^T(t-\tau_M)Q_1x(t-\tau_M) - x^T(t-d_M)Q_2x(t-d_M) + \mathcal{A}_{ij}^T\tilde{R}\mathcal{A}_{ij} + \mu^2\mathcal{B}_{ij}^T\tilde{R}\mathcal{B}_{ij} \\
& +\sigma[C_jx(t-\tau(t)) - \varphi(C_jx(t-\tau(t)))]^T\Omega[C_jx(t-\tau(t)) - \varphi(C_jx(t-\tau(t)))] \\
& -e_k^T(t)\Omega e_k(t) + x^T(t-\tau(t))C_j^TC_jx(t-\tau(t)) - \varphi^T(C_jx(t-\tau(t)))\varphi(C_jx(t-\tau(t))) \\
& +x^T(t-d(t))F^TFx(t-d(t)) - f^T(x(t-d(t)))f(x(t-d(t))) \\
& +\varsigma_1^T(t)M_1\varsigma_1(t) + \varsigma_2^T(t)M_2\varsigma_2(t)\big\} \\
\leq{}& \sum_{i=1}^{r}\sum_{j=1}^{r} h_i(\eta(x))h_j(\eta(x))\big\{\xi^T(t)\Xi_{ij}^{11}\xi(t) + x^T(t-\tau(t))C_j^TC_jx(t-\tau(t)) \\
& +x^T(t-d(t))F^TFx(t-d(t)) + \mathcal{A}_{ij}^T\tilde{R}\mathcal{A}_{ij} + \mu^2\mathcal{B}_{ij}^T\tilde{R}\mathcal{B}_{ij}\big\} \qquad (39)
\end{aligned}
$$

By using Schur complement, we obtain that $\mathbb{E}\big(\dot{V}(x_t)\big) < 0$ can be guaranteed by (19) in Theorem 1.

This completes the proof. □

References

[1] D. Liu, G. Yang, M. J. Er, Event-triggered control for T-S fuzzy systems under asynchronous network communications, IEEE Trans. Fuzzy Syst.10.1109/TFUZZ.2019.2906857

[2] L. Zha, J. Fang, J. Liu, E. Tian, Reliable control for hybrid-driven T-S fuzzy systems with actuator faults and probabilistic nonlinear perturbations, J. Frankl. Inst. 354 (2017) 3267–3288.

[3] J. Cervantes, W. Yu, S. Salazar, I. Chairez, Takagi-Sugeno dynamic neuro-fuzzy controller of uncertain nonlinear systems, IEEE Trans. Fuzzy Syst. 25 (6) (2017) 1601–1615.

[4] J. Liu, T. Yin, J. Cao, D. Yue, H.R. Karimi, Security control for T-S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks, IEEE Trans. Syst. Man Cybern.-Syst.10.1109/TSMC.2019.2963143

[5] S. Yan, M. Shen, S.K. Nguang, G. Zhang, L. Zhang, A distributed delay method for event-triggered control of T-S fuzzy networked systems with transmission delay, IEEE Trans. Fuzzy Syst. 27 (10) (2019) 1963–1973.

[6] H. Dong, Z. Wang, D.W.C. Ho, H. Gao, Robust $\mathcal{H}_\infty$ fuzzy output-feedback control with multiple probabilistic delays and multiple missing measurements, IEEE Trans. Fuzzy Syst. 18 (4) (2010) 712–725.

[7] L. Zhang, H.-K. Lam, Y. Sun, H. Liang, Fault detection for fuzzy semi-Markov jump systems based on interval type-2 fuzzy approach, IEEE Trans. Fuzzy Syst.10.1109/TFUZZ.2019.2936333

[8] E. Tian, Z. Wang, L. Zou, D. Yue, Probabilistic-constrained filtering for a class of nonlinear systems with improved static event-triggered communication, Int. J. Robust Nonlinear Control 29 (5) (2019) 1484–1498.

[9] D. Yue, E. Tian, Q.L. Han, A delay system method for designing event-triggered controllers of networked control systems, IEEE Trans. Autom. Control 58 (2) (2013) 475–481.

[10] Z. Gu, P. Shi, D. Yue, Z. Ding, Decentralized adaptive event-triggered h_∞ filtering for a class of networked nonlinear interconnected systems, IEEE Trans. Cybern. 49 (5) (2019) 1570–1579.

[11] J. Liu, W. Suo, L. Zha, E. Tian, X. Xie, Security distributed state estimation for nonlinear networked systems against denial-of-service attacks, Int. J. Robust Nonlinear Control 30 (3) (2020) 1156–1180.

[12] D. Du, B. Qi, M. Fei, Z. Wang, Quantized control of distributed event-triggered networked control systems with hybrid wiredwireless networks communication constraints, Inf. Sci. 380 (2017) 74–91.

[13] X. Ge, Q.L. Han, Distributed event-triggered $\mathcal{H}_\infty$ filtering over sensor networks with communication delays, Inf. Sci. 291 (2015) 128–142.

[14] G. Wang, M. Chadli, H. Chen, Z. Zhou, Event-triggered control for active vehicle suspension systems with network-induced delays, J. Frankl. Inst. 356 (1) (2019) 147–172.
[15] T. Li, Z. Li, L. Zhang, S. Fei, Improved approaches on adaptive event-triggered output feedback control of networked control systems, J. Frankl. Inst. 355 (5) (2018) 2515–2535.
[16] X. Zhang, Q. Han, Network-based h_∞ filtering using a logic jumping-like trigger, Automatica 49 (5) (2013) 1428–1435.
[17] C. Peng, D. Yue, M.R. Fei, A higher energy-efficient sampling scheme for networked control systems over IEEE 802.15.4 wireless networks, IEEE Trans. Ind. Inf. 12 (5) (2016) 1766–1774.
[18] Y. Yang, H. Xu, D. Yue, Observer-based distributed secure consensus control of a class of linear multi-agent systems subject to random attacks, IEEE Trans. Circuits Syst. I: Regul. Pap. 66 (8) (2019) 3089–3099.
[19] J. Liu, M. Yang, E. Tian, J. Cao, S. Fei, Event-based security controller design for state-dependent uncertain systems under hybrid-attacks and its application to electronic circuits, IEEE Trans. Circuits Syst. I: Regul. Pap. 66 (12) (2019a) 4817–4828.
[20] J. Liu, Y. Gu, X. Xie, D. Yue, J.H. Park, Hybrid-driven-based h_∞ control for networked cascade control systems with actuator saturations and stochastic cyber attacks, IEEE Trans. Syst. Man Cybern.-Syst. 49 (12) (2019b) 2452–2463.
[21] J. Liu, Z.-G. Wu, D. Yue, J.H. Park, Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber-attacks, IEEE Trans. Syst. Man Cybern.-Syst.10.1109/TSMC.2018.2888633
[22] L. Zha, J. Liu, J. Cao, Resilient event-triggered consensus control for nonlinear muti-agent systems with dos attacks, J. Frankl. Inst. 356 (13) (2019) 7071–7090.
[23] H. Sun, C. Peng, W. Zhang, T. Yang, Z. Wang, Security-based resilient event-triggered control of networked control systems under denial of service attacks, J. Frankl. Inst. 356 (17) (2019) 10277–10295.
[24] L. Hu, Z. Wang, Q.L. Han, X. Liu, State estimation under false data injection attacks: Security analysis and system protection, Automatica 87 (2018) 176–183.
[25] D. Ding, Z. Wang, D.W.C. Ho, G. Wei, Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks, Automatica 78 (2017) 231–240.
[26] J. Liu, T. Yin, D. Yue, H.R. Karimi, J. Cao, Event-based secure leader-following consensus control for multi-agent systems with multiple cyber-attacks, IEEE Trans. Cybern.10.1109/TCYB.2020.2970556
[27] Z. Wang, D. Wang, B. Shen, F.E. Alsaadi, Centralized security-guaranteed filtering in multirate-sensor fusion under deception attacks, J. Frankl. Inst. 355 (2018) 406–420.
[28] L. Sun, Y. Wang, G. Feng, Control design for a class of affine nonlinear descriptor systems with actuator saturation, IEEE Trans. Autom. Control 60 (8) (2015) 2195–2200.
[29] C. Peng, E. Tian, J. Zhang, D. Du, Decentralized event-triggering communication scheme for large-scale systems under network environments, Inf. Sci. 380 (2017) 132–144.
[30] Y. Xu, M. Fang, Z.-G. Wu, Y.-J. Pan, M. Chadli, T. Huang, Input-based event-triggering consensus of multiagent systems under denial-of-service attacks, IEEE Trans. Syst. Man Cybern.: Syst.10.1109/TSMC.2018.2875250
[31] Y. Pan, G.H. Yang, Event-driven fault detection for discrete-time interval type-2 fuzzy systems, IEEE Trans. Syst. Man Cybern.: Syst.10.1109/TSMC.2019.2945063
[32] J. Liu, Y. Gu, L. Zha, Y. Liu, J. Cao, Event-triggered h-infinity load frequency control for multi-area power systems under hybrid cyber attacks, IEEE Trans. Syst. Man Cybern.: Syst. 49 (8) (2019) 1665–1678.
[33] L. Cao, H. Li, G. Dong, R. Lu, Event-triggered control for multiagent systems with sensor faults and input saturation, IEEE Trans. Syst. Man Cybern.: Syst.10.1109/TSMC.2019.2938216
[34] J. Liu, M. Yang, X. Xie, C. Peng, H. Yan, Finite-time h_∞ filtering for state-dependent uncertain systems with event-triggered mechanism and multiple attacks, IEEE Trans. Circuits Syst. I: Regul. Pap.10.1109/TCSI.2019.2949014
[35] L. Zha, J.A. Fang, X. Li, J. Liu, Event-triggered output feedback $\mathcal{H}_\infty$ control for networked Markovian jump systems with quantizations, Nonlinear Anal.: Hybrid Syst. 24 (2017) 146–158.
[36] K. Sun, S. Mou, J. Qiu, T. Wang, H. Gao, Adaptive fuzzy control for nontriangular structural stochastic switched nonlinear systems with full state constraints, IEEE Trans. Fuzzy Syst. 29 (8) (2019) 1587–1601.
[37] J. Qiu, K. Sun, I.J. Rudas, H. Gao, Command filter-based adaptive NN control for MIMO nonlinear systems with full-state constraints and actuator hysteresis, IEEE Trans. Cybern.10.1109/TCYB.2019.2944761