ARTICLE IN PRESS

ISA Transactions xxx (xxxx) xxx

Contents lists available at ScienceDirect

ISA Transactions

journal homepage: www.elsevier.com/locate/isatrans

Research article

Event-triggered filter design for nonlinear cyber–physical systems subject to deception attacks

Zhou Gu [a,b,*], Xiaohong Zhou [a], Tao Zhang [b], Fan Yang [a], Mouquan Shen [c]

[a] College of Mechanical & Electronic Engineering, Nanjing Forestry University, Nanjing, China
[b] College of Automation Electronic Engineering, Qingdao University of Science and Technology, Qingdao, China
[c] College of Electrical Engineering and Control Science, Nanjing Technology University, Nanjing, China

HIGHLIGHTS

- The proposed ETM can decrease spurious triggering events during the system with external disturbance.
- The controller can access much information during the system with disturbance under the ETM.
- A deception attack is considered in designing the filter for nonlinear networked systems.
- The problem of mismatched membership functions induced by networked communication is considered.

ARTICLE INFO

Article history:
Received 28 October 2018
Received in revised form 6 February 2019
Accepted 28 February 2019
Available online xxxx

Keywords:
Event-triggered mechanism
Cyber-attacks
Filter design

ABSTRACT

This paper is concerned with an event-triggered filter design for fuzzy-model-based cyber–physical systems with cyber-attacks. Spurious events may be triggered under the conventional event-triggered mechanism (ETM) when the sampling data has a rapid change arising from unpredicted external disturbance. To avoid spurious decisions on data releasing a new ETM is proposed. Furthermore, the communication network is vulnerable to attacks by malicious attackers. Under this scenario, a new resilient filter is designed to ensure the security. Sufficient conditions are established to make the filtering error system asymptotically stable. A numerical example is provided to show the effectiveness of the proposed results.

1. Introduction

On modeling nonlinear behavior, Takagi–Sugeno fuzzy model is an effective approach to represent a class of nonlinear dynamic systems, and has many successful applications in industrial processes [1,2]. In recent years, T–S fuzzy model has been widely applied on filter design for nonlinear systems, and has achieved fruitful theoretical results (see, for instance, [3–5], and the references therein). The authors in [3] investigated a state estimation problem for a class of nonlinear cyber–physical systems (CPSs) which is approximated by a T–S fuzzy model. In [5], a T–S fuzzy model based filter design was developed for nonlinear networked systems with saturation nonlinearities. Due to the advantage of networked framework for control systems, such as low cost, simple installation and maintenance, and high reliability, network-based filter design has received much attention [6–8].

The data transmission using a way of periodical sampling and releasing is called time-triggered mechanism (TTM), which is a popular method in networked control systems(NCSs). This method may result in a poor network quality of service (QoS), especially for the large scaled system with a small sampling period in that more data packets are released into the network per unit of time. Significant efforts have been made to design an event-triggered mechanism (ETM) for improving the network QoS and the control performance of the networked control system [8,9]. In [10], the authors proposed an event-triggered scheme for sampled-data systems with a known controller. By using this event-triggered scheme, the next sampling instant is depended on the event-triggering condition rather than a fixed time period. However, there are two big problems need to be addressed, the one is a Zeno behavior, and the other is that the controller cannot be co-designed with the event-triggered parameters. To overcome these drawbacks, the authors in [6] developed a discrete event-triggered scheme. To get a suitable threshold of the ETM, adaptive thresholds were designed in [11–13]. For the purpose of achieving better performance of both the network and the control system, some other useful information is introduced, for example, the network bandwidth utilization ratio and fault occurrence probability were considered in [14]. To further reduce the communication burden of each channel, a distributed event-triggered mechanism and multiple quantization scheme were put forward

* Corresponding author.
E-mail address: gzh1808@163.com (Z. Gu).

https://doi.org/10.1016/j.isatra.2019.02.036
0019-0578/© 2019 Published by Elsevier Ltd on behalf of ISA.

in [15,16]. Based on event-triggered scheme, a fault detection design method was put forward for discrete-time systems in [17]. In [18], the authors used an event-triggered control method to study the consensus problem for asynchronous distributed multi-agent systems. Borrowing the idea of designing the ETM for continuous-time systems in [6], the authors in [19] designed an ETM for discrete-time Markov jump systems. Under the above ETMs, the data releasing rate can be decreased greatly. The resource of the communication and computation is then saved. It should be noted that some spurious events may be triggered due to rapid change of the state, especially when the system tends to be stable, more spurious events are generated for some state jitter arising from the external disturbance. However, little attention is paid on this situation, which is a main motivation of this study.

Transmitting control signals over the network is vulnerable to attacks by malicious adversaries. When the control signals are modified or blocked by adversaries during the data transmission, such as the system is under deception attack [20–23], denial-of-service (DoS) attack [24,25], the control performance is expected to deteriorate or even result in instability. Therefore, designing a security filter is critical for the system with cyber-attacks, which is another motivation in this study. The hybrid-triggered control for T–S fuzzy model-based nonlinear systems with stochastic cyber-attacks was designed in [26,27], where the probability of attack-launching is governed by a independent Bernoulli variable. Under deception attack, the distributed recursive filtering problem of discrete time-delayed systems was studied in [28]. The estimation problem using distributed information fusion method was investigated in [25] for cyber–physical systems architecture under DoS attacks. In [29], the robust output consensus problem for heterogeneous linear multi-agent systems in presence of aperiodic sampling and random DoS attack was investigated. Periodic DoS jamming attacks, under an assumption that the jamer is partially known, were studied in [24].

In this paper, we aim to design a resilient H_∞ filter for T–S fuzzy model based networked nonlinear systems with a novel ETM under cyber-attacks. The main contributions of this study can be summarized as follows. (1) a new ETM is proposed, under which spurious triggering events may decrease when the sampling data has a rapid change arising from external disturbance. Moreover, under this proposed ETM, the data releasing rate during the system with disturbance is greater than the one during other periods such that the controller can access much information to stabilize the system; (2) a deception attack is considered in designing the filter for networked systems. In order to avoid being detected, it is assumed that the attack is state norm bounded; and (3) by some suitable assumptions, the problem of mismatched membership functions induced by networked communication is considered, and new security criteria are proposed for nonlinear networked filter design under the deception attacks and the proposed ETM.

The rest of the paper is organized as follows. Section 2 presents the system description and problem statement. In Section 3, a fuzzy filter is designed for the system subject to deception attacks with the proposed ETM. A numerical example is given in Section 4 to show the effectiveness of the proposed method.

Notation: $\mathbb{R}^n$ denotes the n-dimensional Euclidean space, $\mathbb{R}^{n\times m}$ is the set of real $n \times m$ matrices. $\|\cdot\|$ stands for the Euclidean vector norm or spectral norm as appropriate. The notation $X > 0$ (respectively, $X < 0$), for $X \in \mathbb{R}^{n\times n}$ means that the matrix X is a real symmetric positive definite (respectively, negative definite). X^T represents the transpose of X. The asterisk $*$ in a matrix is used to denote term that is induced by symmetry. Matrices, if they are not explicitly stated , are assumed to have compatible dimensions.

2. Problem formulation

2.1. Model description

Consider the following nonlinear system described by a T–S fuzzy model with r plant rules.

Plant Rule i: If $\theta_1(t)$ is F_{i1} , ..., $\theta_s(t)$ is F_{is}, then

$$\begin{cases} \dot{x}(t) = (A_i + \Delta A_i)x(t) + B_i\omega(t) \\ z(t) = C_i x(t) \\ y(t) = L_i x(t) \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state vector, $y(t) \in \mathbb{R}^m$ is the measurement output, $\omega(t) \in \mathbb{R}^q$ is exogenous disturbance belongs to $L_2[0,\infty)$, $z(t) \in \mathbb{R}^p$ stands for the output to be estimated, F_{ig} is a fuzzy set ($g = 1, 2, \ldots, s$), $\theta_1(t), \theta_2(t), \ldots, \theta_s(t)$ are the premise variables, A_i, B_i, C_i, and L_i are known real matrices with appropriate dimensions. $\Delta A_i(t)$ denotes the norm-bounded uncertainties, and $\Delta A_i = F_i J(t) E_i$, where F, E_i are known real matrices with appropriate dimensions, and $J(t)$ is a time-varying matrix satisfying $J^T(t)J(t) \leqslant I$.

By using product inference singleton fuzzifier, center-average defuzzifier, the global dynamics of (1) can be inferred as:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{r} h_i(\theta(t))[(A_i + \Delta A_i)x(t) + B_i\omega(t)] \\ z(t) = \sum_{i=1}^{r} h_i(\theta(t))C_i x(t) \\ y(t) = \sum_{i=1}^{r} h_i(\theta(t))L_i x(t) \end{cases} \tag{2}$$

where $F_{ig}(\theta_g(t))$ is the membership function. $h_i(\theta(t)) = \dfrac{\mu_i(\theta(t))}{\sum_{i=1}^{r}\mu_i(\theta(t))}$ satisfying $h_i(\theta(t)) \geqslant 0$ ($i = 1, 2, 3, \ldots$) and $\sum_{i=1}^{r} h_i(\theta(t)) = 1$, $\mu_i(\theta(t)) = \prod_{v=1}^{s} F_{iv}(\theta_v(t))$ denotes the normalized membership function.

2.2. Event-triggered mechanism

A novel ETM will be given in this subsection, by which the data-releasing events are generated according to the current sampling data and the latest releasing data.

Define

$$y(t_k h + \Delta h) = \varrho y(t_k h + lh) + (1-\varrho)y(t_k h) \tag{3}$$

where $\Delta h = \varrho l h$ with $0 \le \varrho \le 1$ and $l \in \varsigma_{t_k} \triangleq \{0, 1, 2, \ldots, l_M\}$. Obviously, $y(t_k h + \Delta h)$ is an arbitrary value between $y(t_k h)$ and $y(t_k h + lh)$. The filter input holds the value of $y(t_k h)$ till it is updated by $y(t_{k+1}h)$ owing to the zero-order-hold (ZOH).

Define

$$\psi(t) = e^T(t)\Theta e(t) - \iota_1 y^T(t_k h)\Theta y(t_k h) + \frac{\iota_2}{2}\left[y^T(t_k h)\Theta e(t) + e^T(t)\Theta y(t_k h)\right] \tag{4}$$

where h is the sampling period, $t_k h$ is the data releasing instant, ι_1, ι_2 are positive scalars, $\Theta > 0$ is a weighting matrix, and $e(t) = y(t_k h) - y(t_k h + \Delta h)$.

The next releasing instant is determined by

$$t_{k+1}h = t_k h + l_M h \tag{5}$$

where $l_M = \max_{l \in \varsigma_{t_k}}\{l \mid \psi(t) < 0\}$, that is, $\psi(t) < 0$ is an event-triggering condition. When the condition is violated, the packet at this instant is needed to release.

Please cite this article as: Z. Gu, X. Zhou, T. Zhang et al., Event-triggered filter design for nonlinear cyber–physical systems subject to deception attacks. ISA Transactions (2019), https://doi.org/10.1016/j.isatra.2019.02.036.

Remark 1. If one sets $\iota_2 = 0$, the event triggering condition $\psi(t) < 0$ reduces to

$$e^T(t)\Theta e(t) < \iota_1 y^T(t_k h)\Theta y(t_k h) \tag{6}$$

The format of (6) is the same as the one in [6] except the definition of $e(t)$. Unlike the existing definition on $e(t)$ that, in this study, is not an error between the value of current sampling packet and the value of latest releasing packet, but an error between the value of current sampling packet and $y(t_k h + \Delta h)$ which is defined in (3). By this new definition, spurious event of data releasing due to the state with a jitter can be avoided greatly. Furthermore, when the system is disturbed, a better control performance can be achieved if the controller with more information from the system. Under the proposed ETM, the second part in (4) makes the ETM be sensitive with the state fluctuation, a bigger data releasing rate may have when the system is disturbed, that is, ι_2 is a weight scalar to regulate the effect of this behavior.

From the above analysis, one can know that the packet at each sampling instant should have a comparison with the one at the latest releasing instant before preparing to transmit. To do so, we partition the interval $[t_k h+\tau_k, t_{k+1}h+\tau_{k+1})$ into l_M+1 segments, where τ_k is the network induce delay at instant t_k. Each segments are denoted by $\chi^l_{t_k} = [t_k h+lh+\tau^l_k, t_k h+lh+h+\tau^{l+1}_{k+1})$. Obviously, $[t_k h+\tau_k, t_{k+1}h+\tau_{k+1}) = \cup^{l_M}_{l=0}\chi^l_{t_k}$ with $\tau^0_k = \tau_k$ and $\tau^{l_M+1}_k = \tau_{k+1}$.

For $t \in \chi^l_{t_k}$, we define $d(t) = t - t_k h - lh$. It yields that

$$\underline{d} \le d_k \le d(t) \le h + \overline{d} = d_M \tag{7}$$

where $\overline{d} = max\{\tau_k\}$, $\underline{d} = min\{\tau_k\}$.

2.3. Deception attacks

The adversary attempts to deteriorate the filtering performance by injecting deception signal into the measurement output through the communication network during the data transmission. The measurement output under deception attacks is modeled by

$$\tilde{y}(t) = y(t) + \sigma(t). \tag{8}$$

where $\sigma(t)$ stands for the signal injected into the output by adversaries, which satisfies $\|\sigma(t)\|_2 \le \|Wx(t)\|_2$, where W is a matrix with appropriate dimension. Thus, we have

$$\begin{aligned}\tilde{y}(t_k h) &= \frac{1}{\varrho}e(t) + \tilde{y}(t-d(t))\\ &= \sum_{i=1}^{r} h_i(\theta(t_k h))[\frac{1}{\varrho}e(t) + \sigma(t-d(t)) + L_i x(t-d(t))]\end{aligned} \tag{9}$$

Remark 2. To avoid being detected, the attack signals commonly has an upper-bound. It is assumed that the injected attack is state norm bounded as in (8). We can also model it as an intermittent attack by borrowing the idea of sojourn probability [30]. For simplicity, we only discuss the case with deterministic injection attack.

We aim to design a resilient fuzzy filter. The j-th rule of the fuzzy filter is described as follows:

Plant Rule j: If $\theta_1(t_k h)$ is $F_{j1}, \ldots, \theta_m(t_k h)$ is F_{jm}, then

$$\begin{cases}\dot{x}_f(t) = A_{fj}x_f(t) + B_{fj}\tilde{y}(t_k h)\\ z_f(t) = C_{fj}x_f(t)\end{cases} \tag{10}$$

where $x_f(t) \in \mathbb{R}^n$ is the filter state vector, $z_f(t) \in \mathbb{R}^p$ is the output of the filter. A_{fj}, B_{fj}, C_{fj} are the filter coefficient matrices to be designed.

The defuzzified output of (10) is represented as follows:

$$\begin{cases}\dot{x}_f(t) = \sum_{j=1}^{r} h_j(\theta(t_k h))[A_{fj}x_f(t) + B_{fj}\tilde{y}(t_k h)]\\ z_f(t) = \sum_{j=1}^{r} h_j(\theta(t_k h))C_{fj}x_f(t)\end{cases} \tag{11}$$

For brevity, we use h_i and g_j to represent $h_i(\theta(t))$ and $h_j(\theta(t_k h))$, respectively, in the subsequent description. It is noticed that the membership functions between h_i and g_j are mismatched due to the network. Borrowing the idea in [31], we do the following reasonable assumption

$$g_j - \kappa_j h_j \geqslant 0 \tag{12}$$

with $(0 < \kappa_j \leqslant 1)$.

2.4. The overall model

Define$\tilde{x}(t) = [x^T(t), x_f^T(t)]^T$ and $e_f(t) = z(t) - z_f(t)$. We can get the following augmented filtering error system:

$$\begin{cases}\dot{\tilde{x}}(t) = \sum_{i=1}^{r}\sum_{j=1}^{r} h_i g_j \left[\overline{A}_{ij}\tilde{x}(t) + \overline{B}_{0j}e(t) + \overline{B}_{1ij}x(t-d(t))\right.\\ \qquad\left. + \overline{B}_{2j}\sigma(t-d(t)) + \overline{B}_{3i}\omega(t)\right]\\ e_f(t) = \sum_{i=1}^{r}\sum_{j=1}^{r} h_i g_j \overline{C}_{0ij}\tilde{x}(t)\end{cases} \tag{13}$$

by combining (2), (9) and (11), where $\overline{A}_{ij} = \overline{A}_{0ij} + \overline{A}_{1ij}$ and

$\overline{A}_{0ij} = \begin{bmatrix}A_i & 0\\ 0 & A_{fj}\end{bmatrix}$, $\overline{A}_{1ij} = \begin{bmatrix}\Delta A_i & 0\\ 0 & 0\end{bmatrix}$, $\overline{B}_{0j} = \begin{bmatrix}0\\ \frac{1}{\varrho}B_{fj}\end{bmatrix}$, $\overline{B}_{1ij} = \begin{bmatrix}0\\ B_{fj}L_i\end{bmatrix}$, $\overline{B}_{2j} = \begin{bmatrix}0\\ B_{fj}\end{bmatrix}$, $\overline{B}_{3i} = \begin{bmatrix}B_i\\ 0\end{bmatrix}$, $\overline{C}_{0ij} = \begin{bmatrix}C_i & -C_{fj}\end{bmatrix}$, $H = \begin{bmatrix}I & 0\end{bmatrix}$

The design problems of H_∞ filter can be summarized as the following conditions:

(1) Ensure that the filtering error system (13) is asymptotically stable when $\omega(t) = 0$.

(2) Under zero initial conditions, making the l_2 norm of the transfer function from disturbance to estimation error smaller than the given constant γ, that is: $\|e_f(t)\|_2 < \gamma\|\omega(t)\|_2$.

Next, we will introduce some lemmas to help us deriving the subsequent theorem.

Lemma 1 ([32]). *Extended Wirtinger's Inequality: For $R = R^T > 0$, we have*

$$\int_a^b \dot{x}^T(s)R\dot{x}(s)ds \ge \frac{1}{b-a}\begin{bmatrix}\Omega_1\\ \Omega_2\end{bmatrix}^T \begin{bmatrix}R & 0\\ 0 & 3R\end{bmatrix}\begin{bmatrix}\Omega_1\\ \Omega_2\end{bmatrix} \tag{14}$$

where $\Omega_1 = x(b) - x(a)$, $\Omega_2 = x(b) + x(a) - \frac{2}{b-a}\int_a^b x(s)ds$

Lemma 2 ([30,33,34]). *Define Υ_1 and Υ_2 as appropriate dimensioned real matrices. Then, for any given scalar $\varepsilon > 0$ and matrix $J(t)$ satisfying $J(t)^T J(t) \le I$, the following inequality holds:*

$$\Upsilon_1 J(t)\Upsilon_2 + \Upsilon_2^T J(t)^T \Upsilon_1^T \le \frac{1}{\varepsilon}\Upsilon_1\Upsilon_1^T + \varepsilon\Upsilon_2^T\Upsilon_2 \tag{15}$$

3. Main results

In this section, sufficient conditions will be developed in Theorem 1 for ensuring asymptotically stable and H_∞ performance of filtering error system with cyber-attacks. The filter design conditions will be presented in Theorem 2.

Theorem 1. *For given positive scalars $\rho, \iota_1, \iota_2, \underline{d}$ and d_M, the system (13) with mismatched membership functions satisfying (12) is asymptotically stable with an H_∞ performance index γ, if there exists positive scalar ε, matrices $P > 0, \Theta > 0, Q_i > 0, R > 0, R_i > 0$ and matrices Υ_i, N_j, M_j $(i = 1, 2, \ldots, r,\ j = 1, 2)$ with appropriate dimensions such that:*

$$\Psi_{ij}^a - \Upsilon_i < 0, (i, j = 1, 2, \ldots, r) \tag{16}$$

$$\kappa_j \Psi_{ij}^a + \kappa_i \Psi_{ji}^a - \kappa_j \Upsilon_i - \kappa_i \Upsilon_j + \Upsilon_i + \Upsilon_j < 0, (i \le j) \tag{17}$$

where

$$\Psi_{ij}^a = \begin{bmatrix} \Psi_{11}^{ij} & * & * \\ \Psi_{21}^{ij} & \Psi_{22} & * \\ \Psi_{31}^a & 0 & -R_2 \end{bmatrix}, (i = 1, 2, \ldots, r;\ a = 1, 2)$$

$$\Psi_{11}^{ij} = \begin{bmatrix} \Psi_{1ij} & * & * & * & * & * & * & * \\ -2R_1H & \Psi_2 & * & * & * & * & * & * \\ 6R_1H & 6R_1 & -12R_1 & * & * & * & * & * \\ 0 & 0 & 0 & \Psi_3 & * & * & * & * \\ \overline{B}_{0j}^TP & 0 & 0 & 0 & -\varpi_1\Theta & * & * & * \\ \overline{B}_{1ij}^TP & N_2 - N_1^T & 0 & M_2^T - M_1 & 0 & \Psi_4 & * & * \\ \overline{B}_{2j}^TP & 0 & 0 & 0 & 0 & 0 & -I & * \\ \overline{B}_{3i}^TP & 0 & 0 & 0 & 0 & 0 & 0 & -\gamma^2 I \end{bmatrix},$$

$\Psi_{1ij} = \overline{A}_{0ij}^TP + H^TQ_1H + P\overline{A}_{0ij} + H^TQ_2H - 4H^TR_1H,$
$\Psi_2 = -Q_1 - 4R_1 + N_1 + N_1^T,$
$\Psi_3 = -Q_2 - M_2 - M_2^T,$
$\Psi_4 = -N_2 - N_2^T + M_1 + M_1^T,$
$\Psi_{21}^{ij} = \begin{bmatrix} \Phi_{1ij}^T & \Phi_{2ij}^T & \Phi_{3i}^T & \Phi_4^T & \Phi_{5i}^T & \Phi_{6i}^T \end{bmatrix}^T,$
$\Psi_{22} = diag\{-2\rho + \rho^2R, -I, -2\rho + \rho^2\Theta, -I, -\varepsilon I, -\varepsilon I\},$
$\Psi_{31}^1 = \begin{bmatrix} 0 & \sqrt{d_M - \underline{d}}N_1^T & 0 & 0 & 0 & \sqrt{d_M - \underline{d}}N_2^T & 0 & 0 \end{bmatrix},$
$\Psi_{31}^2 = \begin{bmatrix} 0 & 0 & 0 & \sqrt{d_M - \underline{d}}M_2^T & 0 & \sqrt{d_M - \underline{d}}M_1^T & 0 & 0 \end{bmatrix},$
$\Phi_{1ij} = \begin{bmatrix} H\overline{A}_{0ij} & 0 & 0 & 0 & H\overline{B}_{0j} & H\overline{B}_{1ij} & H\overline{B}_{2j} & H\overline{B}_{3i} \end{bmatrix},$
$\Phi_{2ij} = \begin{bmatrix} \overline{C}_{0ij} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$
$\Phi_{3i} = \begin{bmatrix} 0 & 0 & 0 & 0 & (\varpi_3 + \frac{\varpi_2}{\varrho})I & \varpi_2L_i & \varpi_2I & 0 \end{bmatrix},$
$\Phi_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & WH & 0 & 0 \end{bmatrix},$
$\Phi_{5i} = \begin{bmatrix} \tilde{F}_i^TP & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$
$\Phi_{6i} = \begin{bmatrix} \varepsilon\tilde{E}_i & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$
$R = \underline{d}^2H^TR_1H + (d_M - \underline{d})H^TR_2H, \tilde{E}_i = \begin{bmatrix} E_i & 0 \end{bmatrix}, \tilde{F} = \begin{bmatrix} F^T & 0 \end{bmatrix}^T,$
$\varpi_1 = 1 + \dfrac{\iota_2^2}{4\iota_1}, \varpi_2 = \sqrt{\iota_1}, \varpi_3 = \dfrac{4\iota_1 + \iota_2}{2\sqrt{\iota_1}}$

Proof. Choose a Lyapunov–Krasovskii candidate as

$$V(t) = V_1(t) + V_2(t) + V_3(t) \tag{18}$$

where

$$V_1(t) = \tilde{x}^T(t)P\tilde{x}(t)$$

$$V_2(t) = \int_{t-\underline{d}}^{t} \tilde{x}^T(s)H^TQ_1H\tilde{x}(s)ds + \int_{t-d_M}^{t} \tilde{x}^T(s)H^TQ_2H\tilde{x}(s)ds$$

$$V_3(t) = \underline{d}\int_{t-\underline{d}}^{t}\int_{s}^{t} \dot{\tilde{x}}^T(v)H^TR_1H\dot{\tilde{x}}(v)dvds + \int_{t-d_M}^{t-\underline{d}}\int_{s}^{t} \dot{\tilde{x}}^T(v)H^TR_2H\dot{\tilde{x}}(v)dvds$$

Taking derivative on $V_i(t)$, for $i = 1, 2, 3$, one can obtain

$$\begin{aligned}
\dot{V}(t) = &\sum_{i=1}^{r}\sum_{j=1}^{r} h_ig_j \Big\{2\dot{\tilde{x}}^T(t)P\tilde{x}(t) + \tilde{x}^T(t)H^TQ_1H\tilde{x}(t) \\
&- \tilde{x}^T(t-\underline{d})H^TQ_1H\tilde{x}(t-\underline{d})\Big\} \\
&+ \sum_{i=1}^{r}\sum_{j=1}^{r} h_ig_j \Big\{\tilde{x}^T(t)H^TQ_2H\tilde{x}(t) \\
&- \tilde{x}^T(t-d_M)H^TQ_2H\tilde{x}(t-d_M)\Big\} \\
&+ \sum_{i=1}^{r}\sum_{j=1}^{r} h_ig_j \Big\{d_1^2\dot{\tilde{x}}^T(t)H^TR_1H\dot{\tilde{x}}(t) \\
&+ (d_M - \underline{d})\dot{\tilde{x}}^T(t)H^TR_2H\dot{\tilde{x}}(t)\Big\} \\
&- \sum_{i=1}^{r}\sum_{j=1}^{r} h_ig_j \Big\{\underline{d}\int_{t-\underline{d}}^{t} \dot{\tilde{x}}^T(s)H^TR_1H\dot{\tilde{x}}(s)ds \\
&- \int_{t-d_M}^{t-\underline{d}} \dot{\tilde{x}}^T(s)H^TR_2H\dot{\tilde{x}}(s)ds\Big\} \\
&+ \sum_{i=1}^{r}\sum_{j=1}^{r} h_ig_j \Big\{2\xi^T(t)N\Big[\tilde{x}(t-\underline{d}) - \tilde{x}(t-d(t)) \\
&- \int_{t-d(t)}^{t-\underline{d}} \dot{\tilde{x}}(s)ds\Big]\Big\} \\
&+ \sum_{i=1}^{r}\sum_{j=1}^{r} h_ig_j \Big\{2\xi^T(t)M\Big[\tilde{x}(t-d(t)) - \tilde{x}(t-d_M) \\
&- \int_{t-d_M}^{t-d(t)} \dot{\tilde{x}}(s)ds\Big]\Big\}
\end{aligned}$$

where $N = \begin{bmatrix} 0 & N_1^T & 0 & 0 & 0 & N_2^T & 0 & 0 & 0 \end{bmatrix}^T$ and $M = \begin{bmatrix} 0 & 0 & 0 & M_2^T & 0 & M_1^T & 0 & 0 & 0 \end{bmatrix}^T$, and $\xi(t) = [\tilde{x}^T(t)\ \tilde{x}^T(t-\underline{d})H^T\ \frac{1}{\underline{d}}\int_{t-\underline{d}}^{t}\tilde{x}^T(t)H^Tds\ \tilde{x}^T(t-d_M)H^T\ e^T(t)\ x^T(t-d(t))\ \sigma^T(t-d(t))\ \omega^T(t)]^T$.

From Lemma 1, we have

$$\begin{aligned}
&-\underline{d}\int_{t-\underline{d}}^{t} \dot{\tilde{x}}^T(s)H^TR_1H\dot{\tilde{x}}(s)ds \\
&\le \begin{bmatrix} \xi(t)T_1 \\ \xi(t)T_2 \end{bmatrix}^T \begin{bmatrix} H^TR_1H & 0 \\ 0 & 3H^TR_1H \end{bmatrix} \begin{bmatrix} \xi(t)T_1 \\ \xi(t)T_2 \end{bmatrix}
\end{aligned} \tag{19}$$

where $T_1 = \begin{bmatrix} I & -I & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$,
$T_2 = \begin{bmatrix} I & I & -2I & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$.

Using Lemma 2 and taking uncertain parameters into account, we have

$$\begin{aligned}
&\tilde{x}^T(t)\overline{A}_{1ij}^TP\tilde{x}(t) + \tilde{x}^T(t)P\overline{A}_{1ij}\tilde{x}(t) \\
&\quad = \tilde{x}^T(t)\tilde{E}_i^TJ^T(t)\tilde{F}_i^TP\tilde{x}(t) + \tilde{x}^T(t)P\tilde{F}_iJ(t)\tilde{E}_i\tilde{x}(t) \\
&\quad \le \varepsilon\tilde{x}^T(t)\tilde{E}_i^T\tilde{E}_i\tilde{x}(t) + \frac{1}{\varepsilon}\tilde{x}^T(t)P\tilde{F}_i\tilde{F}_i^TP\tilde{x}(t)
\end{aligned} \tag{20}$$

It is true that $(\Theta - \rho^{-1}I)\Theta^{-1}(\Theta - \rho^{-1}I) \ge 0$ [35]. Then

$$-\Theta^{-1} \leqslant -2\rho I + \rho^2\Theta \tag{21}$$

Please cite this article as: Z. Gu, X. Zhou, T. Zhang et al., Event-triggered filter design for nonlinear cyber–physical systems subject to deception attacks. ISA Transactions (2019), https://doi.org/10.1016/j.isatra.2019.02.036.

Notice that

$$-2\xi^T(t)N\int_{t-d(t)}^{t-\underline{d}}\dot{\tilde{x}}(s)ds \le (d(t)-\underline{d})\xi^T(t)HR_2^{-1}H^T\xi(t) + \int_{t-d(t)}^{t-\underline{d}}\dot{\tilde{x}}^TH^T(s)R_2H\dot{\tilde{x}}(s)ds$$
$$-2\xi^T(t)M\int_{t-d_M}^{t-d(t)}\dot{\tilde{x}}(s)ds \le (d_M-d(t))\xi^T(t)HR_2^{-1}H^T\xi(t) + \int_{t-d_M}^{t-d(t)}\dot{\tilde{x}}^T(s)H^TR_2H\dot{\tilde{x}}(s)ds \tag{22}$$

The event triggering condition in (4) is equivalent to

$$\varpi_1 e^T(t)\Theta e(t) \le [\varpi_2 y(t_kh)+\varpi_3 e(t)]^T\,\Theta\,[\varpi_2 y(t_kh)+\varpi_3 e(t)] \tag{23}$$

Recalling the definition of deception attacks in Section 2.3, it follows that

$$\sigma^T(t-d(t))\sigma(t-d(t)) \leqslant \tilde{x}^T(t-d(t))H^TW^TWH\tilde{x}(t-d(t)) \tag{24}$$

Combining (19)–(24), one can obtain

$$\dot{V}(t)+e_f^T(t)e_f(t)-\gamma^2\omega^T(t)\omega(t) \leqslant \sum_{i=1}^{r}\sum_{j=1}^{r}h_ig_j\xi^T(t)\hat{\Psi}_{ij}\xi(t) \tag{25}$$

where $\hat{\Psi}_{ij} = \Psi_{11}^{ij} + {\Psi_{21}^{ij}}^T\Psi_{22}^{-1}\Psi_{21}^{ij} + (d(t)-\underline{d})NR_2^{-1}N^T + (d_M - d(t))MR_2^{-1}M^T$.

Taking arbitrary slack matrix Υ_i into account ($\Upsilon_i = \Upsilon_i^T$),

$$\sum_{i=1}^{r}\sum_{j=1}^{r}h_i(h_j-g_j)\Upsilon_i = \sum_{i=1}^{r}h_i(\sum_{j=1}^{r}h_j-\sum_{j=1}^{r}g_j)\Upsilon_i = 0 \tag{26}$$

Then, it follows that

$$\begin{aligned}
&\sum_{i=1}^{r}\sum_{j=1}^{r}h_ig_j\xi^T(t)\hat{\Psi}_{ij}\xi(t)\\
&=\sum_{i=1}^{r}\sum_{j=1}^{r}h_ig_j\xi^T(t)\hat{\Psi}_{ij}\xi(t)\\
&\quad+\sum_{i=1}^{r}\sum_{j=1}^{r}h_i(h_j-g_j+\kappa_jh_j-\kappa_jh_j)\xi^T(t)\Upsilon_i\xi(t)\\
&=\sum_{i=1}^{r}\sum_{j=1}^{r}h_ih_j\xi^T(t)(\kappa_j\hat{\Psi}_{ij}-\kappa_j\Upsilon_i+\Upsilon_i)\xi(t)\\
&\quad+\sum_{i=1}^{r}\sum_{j=1}^{r}h_i(g_j-\kappa_jh_j)\xi^T(t)(\hat{\Psi}_{ij}-\Upsilon_i)\xi(t)\\
&\leqslant\sum_{i=1}^{r}h_i^2\xi^T(t)(\kappa_i\Psi_{ii}^a-\kappa_i\Upsilon_i+\Upsilon_i)\xi(t)\\
&\quad+\sum_{i=1}^{r}h_i(g_j-\kappa_jh_j)\xi^T(t)(\hat{\Psi}_{ij}-\Upsilon_i)\xi(t)\\
&\quad+\sum_{i=1}^{r}\sum_{i<j}\xi^T(t)(\kappa_j\hat{\Psi}_{ij}+\kappa_i\Psi_{ji}^a-\kappa_j\Upsilon_i-\kappa_i\Upsilon_j+\Upsilon_i+\Upsilon_j)\xi(t)
\end{aligned}$$

Using Schur complement to (16) and (17) and the Lemma in [36] for (25), one can know that (16) and (17) are sufficient conditions to guarantee $\sum_{i=1}^{r}\sum_{j=1}^{r}h_ig_j\xi^T(t)\hat{\Psi}_{ij}\xi(t) < 0$, which implies that

$$\dot{V}(t)+e_f^T(t)e_f(t)-\gamma^2\omega^T(t)\omega(t) < 0 \tag{27}$$

Under the zero initial condition, when $\omega(t) \neq 0$, one can obtain $\|e_f(t)\|_2 < \gamma\|\omega(t)\|_2$. Besides, the asymptotic stability of the system is guaranteed with $\omega(t)=0$. The proof is complete.

Based on the results of Theorem 1, we are in position to design the filter next.

Theorem 2. *For given positive scalars $\rho, \iota_1, \iota_2, \underline{d}$ and d_M, the system (13) with mismatched membership functions satisfying (12) is asymptotically stable with an H_∞ performance index γ, if there exists positive scalar ε, matrices $P_1 > 0, Y > 0, \Theta > 0, Q_i > 0, R_i > 0$, and matrices $\bar{A}_{fi}, \bar{B}_{fi}, \bar{C}_{fi}, Y\ \tilde{\Upsilon}_i, N_j, M_j$ $(i = 1, 2, \ldots, r,\ j = 1, 2)$ with appropriate dimensions such that*

$$\tilde{\Psi}_{ij}^a - \tilde{\Upsilon}_i < 0, (i,j = 1,2,\ldots,r) \tag{28}$$
$$\kappa_j\tilde{\Psi}_{ij}^a+\kappa_i\tilde{\Psi}_{ji}^a-\kappa_j\tilde{\Upsilon}_i-\kappa_i\tilde{\Upsilon}_j+\tilde{\Upsilon}_i+\tilde{\Upsilon}_j<0, (i\le j) \tag{29}$$
$$P_1 - Y > 0 \tag{30}$$

where

$$\tilde{\Psi}_{ij}^a = \begin{bmatrix}\tilde{\Psi}_{11}^{ij} & * & *\\ \tilde{\Psi}_{21}^{ij} & \Psi_{22} & *\\ \tilde{\Psi}_{31}^{a} & 0 & -R_2\end{bmatrix}, (i=1,2,\ldots,r, a=1,2),$$

$$\tilde{\Psi}_{11}^{ij} = \begin{bmatrix}
\tilde{\Psi}_{1ij} & * & * & * & * & * & * & * & *\\
\bar{A}_{fj}^T+Y^TA_i & \bar{A}_{fj}^T+\bar{A}_{fj} & * & * & * & * & * & * & *\\
-2R_1 & 0 & \Psi_2 & * & * & * & * & * & *\\
6R_1 & 0 & 6R_1 & -12R_1 & * & * & * & * & *\\
0 & 0 & 0 & 0 & \Psi_3 & * & * & * & *\\
\frac{\bar{B}_{fj}^T}{\varrho} & \frac{\bar{B}_{fj}^T}{\varrho} & 0 & 0 & 0 & -\varpi_1\Theta & * & * & *\\
L^T\bar{B}_{fj}^T & L^T\bar{B}_{fj}^T & N_2-N_1^T & 0 & M_2^T-M_1 & 0 & \Psi_4 & * & *\\
\bar{B}_{fj}^T & \bar{B}_{fj}^T & 0 & 0 & 0 & 0 & 0 & -I & *\\
B_i^TP & B_i^TY & 0 & 0 & 0 & 0 & 0 & 0 & -\gamma^2I
\end{bmatrix},$$

$\tilde{\Psi}_{1ij} = Q_1+Q_2-4R_1+A_1^TP+PA_1,$

$\Psi_2 = -Q_1-4R_1+N_1+N_1^T,$

$\Psi_3 = -Q_2-M_2-M_2^T,$

$\Psi_4 = -N_2-N_2^T+M_1+M_1^T,$

$\tilde{\Psi}_{21}^{ij} = \begin{bmatrix}\tilde{\Phi}_{1ij}^T & \tilde{\Phi}_{2ij}^T & \tilde{\Phi}_{3i}^T & \tilde{\Phi}_{4ij}^T & \tilde{\Phi}_{5i}^T & \tilde{\Phi}_{6i}^T\end{bmatrix}^T,$

$\tilde{\Psi}_{31}^1 = \begin{bmatrix}0 & 0 & \sqrt{d_M-\underline{d}}N_1^T & 0 & 0 & 0 & \sqrt{d_M-\underline{d}}N_2^T & 0 & 0\end{bmatrix},$

$\tilde{\Psi}_{31}^2 = \begin{bmatrix}0 & 0 & 0 & 0 & \sqrt{d_M-\underline{d}}M_2^T & 0 & \sqrt{d_M-\underline{d}}M_1^T & 0 & 0\end{bmatrix},$

$\tilde{\Phi}_{1ij} = \begin{bmatrix}A_i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & B_i\end{bmatrix},$

$\tilde{\Phi}_{2ij} = \begin{bmatrix}C_i & -\bar{C}_{fj} & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix},$

$\tilde{\Phi}_{3i} = \begin{bmatrix}0 & 0 & 0 & 0 & 0 & (\varpi_3+\frac{\varpi_2}{\varrho})I & \varpi_2L_i & \varpi_2I & 0\end{bmatrix},$

$\tilde{\Phi}_4 = \begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0 & WH & 0 & 0\end{bmatrix},$

$\tilde{\Phi}_{5i} = \begin{bmatrix}F_i^TP_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix},$

$\tilde{\Phi}_{6i} = \begin{bmatrix}E_i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix},$

Moreover, the gains of the filter are given by

$$\begin{bmatrix}A_{fj} & B_{fj}\\ C_{fj} & 0\end{bmatrix} = \begin{bmatrix}P_2^{-1}\bar{A}_{fj}P_2^{-T}P_3 & P_2^{-1}\bar{B}_{fj}\\ \bar{C}_{fj}P_2^TP_3 & 0\end{bmatrix}$$

Proof. Partition the matrix P as

$$P = \begin{bmatrix}P_1 & P_2\\ * & P_3\end{bmatrix}$$

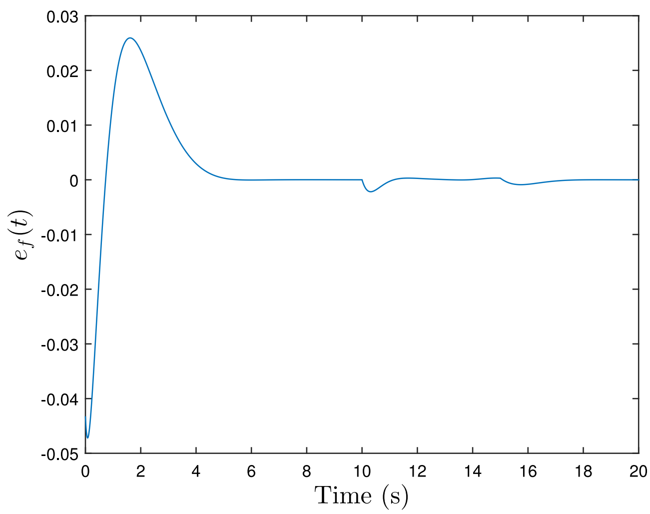

Fig. 1. The filtering error $e_f(t)$.

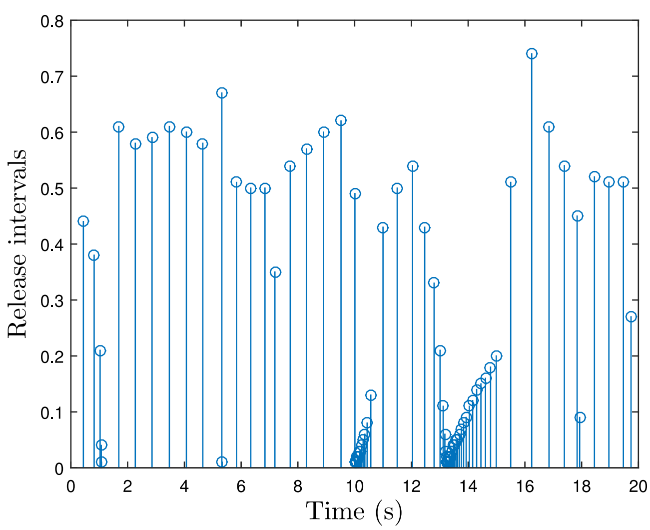

Fig. 2. The releasing instant and its interval.

and define $\exists_1 = \begin{bmatrix} I & 0 \\ 0 & P_2P_3^{-1} \end{bmatrix}$ and $Y = P_2P_3^{-1}P_2^T$.

Since $P > 0$, it follows that $P_1 > 0$ and (30) holds.

Defining $\exists = diag\{\exists_1, I, I, I, I, I, I, I, I, I, I, I, I, I\}$, then pre- and post-multiplying both sides of (16) and (17) by $\exists$ and $\exists^T$, respectively, we have (28) and (29) by defining

$$\begin{cases} \bar{A}_{fj} = P_2A_{fj}P_3^{-1}P_2^T \\ \bar{B}_{fj} = P_2B_{fj} \\ \bar{C}_{fj} = C_{fj}P_3^{-1}P_2^T \end{cases} \quad (31)$$

This completes the proof.

4. Simulation examples

This section aims to demonstrate the effectiveness of the proposed data-releasing scheme and the method of resilient filter design for the system with data injection attacks.

Example 1. Consider the T-S fuzzy-model based nonlinear system with the following parameters:

$$A_1 = \begin{bmatrix} -2.1 & 0.1 \\ 1 & -1 \end{bmatrix}, B_1 = \begin{bmatrix} 1 \\ -0.2 \end{bmatrix}, L_1 = \begin{bmatrix} 1 & 2 \end{bmatrix},$$

$$C_1 = \begin{bmatrix} 0.5 & -2 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} -1.9 & 0.1 \\ -0.2 & -1.1 \end{bmatrix}, B_2 = \begin{bmatrix} 0.3 \\ 0.1 \end{bmatrix}, L_2 = \begin{bmatrix} 0.5 & -0.6 \end{bmatrix},$$

$$C_2 = \begin{bmatrix} -0.2 & 0.3 \end{bmatrix}$$

Suppose H_∞ performance level is $\gamma = 5$, and the bound of time induced delay are $\underline{d} = 4$ ms, $\bar{d} = 20$ ms, the sampling period $h = 0.01$s; Select $\rho = 0.1$, $\kappa = 0.75$, $\varrho = 0.3$ and $F_1 = F_2 = \begin{bmatrix} 0 \\ -0.5 \end{bmatrix}$, $E_1 = E_2 = \begin{bmatrix} 0 & 0.3 \end{bmatrix}$. One can obtain the weight matrices of the proposed ETM in (4) and the filter gains in (11) are

$$\Theta_1 = 9.7551, \Theta_2 = 9.1332,$$

$$A_{f1} = \begin{bmatrix} -7.9469 & 6.9887 \\ 6.8788 & -15.6580 \end{bmatrix}, B_{f1} = \begin{bmatrix} -0.0154 \\ -0.0502 \end{bmatrix},$$

$$C_{f1} = \begin{bmatrix} 0.4494 & 0.3088 \end{bmatrix},$$

$$A_{f2} = \begin{bmatrix} -6.3002 & 0.1960 \\ 0.1920 & -6.7582 \end{bmatrix}, B_{f2} = \begin{bmatrix} -0.0002 \\ -0.0081 \end{bmatrix},$$

$$C_{f2} = \begin{bmatrix} 0.0135 & 0.0039 \end{bmatrix}$$

Suppose the disturbance is

$$\omega(t) = \begin{cases} 0.5e^{-0.03t}\sin(0.05t), & t \in [10, 15] \\ 0, \text{ others} \end{cases}$$

and the membership functions are: $h_1(\theta(t)) = \sin^2 t$, $h_2(\theta(t)) = \cos^2 t$. The initial state are assumed as $x(0) = \begin{bmatrix} 0.1 & -0.2 \end{bmatrix}^T$, $x_f(0) = \begin{bmatrix} -3 & 1 \end{bmatrix}^T$, and the attacks satisfy $\|\sigma(t)\|_2 \le \|Wx(t)\|_2$ with $W = \begin{bmatrix} 0.6 & 0 \\ 0 & 0.4 \end{bmatrix}$.

Fig. 1 shows the filtering error $e_f(t)$, from which one can see that the filter is performed well even when the system is compromised by the cyber-attackers. Fig. 2 depicts the releasing instants and the intervals of ETM. A large amount of "unnecessary" data are discarded due to the designed ETM. The average releasing period is up to 0.2243 s, which is more than 5 times the sampling period $h = 0.01$ second. The communication and computation resources are accordingly saved. It should be noted that the mean data-releasing rate during the attacks or disturbances (10–15 s) is obviously more than the one in other periods owing to the proposed ETM, which can be seen clearly in Fig. 2.

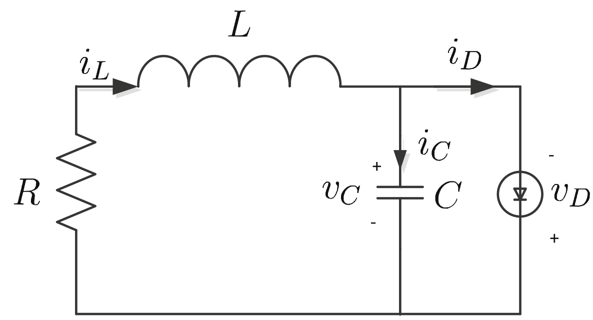

Fig. 3. Tunnel diode circuit.

Example 2. This example considers a tunnel diode circuit shown in Fig. 3, and its dynamic can be described as follows [37,38]:

$$i_D(t) = 0.002v_D(t) + 0.01v_D^3(t) \quad (32)$$

Define $x_1(t) = v_c(t)$ and $x_2(t) = i_L(t)$. Then, the following equation can be obtained:

$$\begin{cases} C\dot{x}_1(t) = -0.002x_1(t) - 0.01x_1^3(t) + x_2(t) \\ L\dot{x}_2(t) = -x_1(t) - Rx_2(t) + \omega(t) \\ y(t) = x_1(t) \\ z(t) = x_1(t) \end{cases} \quad (33)$$

The parameters in the circuit are given as $C = 20$ mF, $L = 1000$ mF, $R = 10\Omega$, $\omega(t)$ is the disturbance noise, $y(t)$ is the measurement output, $z(t)$ is the controlled output. Assume $|x_1| \leq 3$, the nonlinear networked system (33) can be approximated by 2 rules T–S fuzzy model with the format of (2) whose parameters are given by

$$A_1 = \begin{bmatrix} -0.1 & 50 \\ -1 & -10 \end{bmatrix}, B_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, L_1 = \begin{bmatrix} 1 & 0 \end{bmatrix}, C_1 = \begin{bmatrix} 1 & 0 \end{bmatrix},$$
$$A_2 = \begin{bmatrix} -4.6 & 50 \\ -1 & -10 \end{bmatrix}, B_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, L_2 = \begin{bmatrix} 1 & 0 \end{bmatrix}, C_2 = \begin{bmatrix} 1 & 0 \end{bmatrix}.$$

and the membership functions are as follows

$$h_1(\theta(t)) = \begin{cases} \frac{x_1 + 3}{3}, & -3 \leq x_1 \leq 0 \\ \frac{3 - x_1}{3}, & 0 < x_1 \leq 3 \\ 0 & \text{elsewhere} \end{cases}$$
$$h_2(\theta(t)) = 1 - h_1(\theta(t))$$

Let $\gamma = 4$. The other parameters are the same as in Example 1. The event-triggered matrices and the filter parameters can be obtained from Theorem 2 as follows

$$\Theta_1 = 9.3957, \Theta_2 = 9.0878,$$
$$A_{f1} = \begin{bmatrix} -1.0634 & 0.2145 \\ 0.2162 & -106.8381 \end{bmatrix}, B_{f1} = \begin{bmatrix} -0.0254 \\ 0.0002 \end{bmatrix},$$
$$C_{f1} = \begin{bmatrix} -1.0263 & -0.0026 \end{bmatrix},$$
$$A_{f2} = \begin{bmatrix} -3.4760 & 1.2745 \\ 1.2724 & -17.2073 \end{bmatrix}, B_{f2} = \begin{bmatrix} -0.0163 \\ -0.0032 \end{bmatrix},$$
$$C_{f2} = \begin{bmatrix} -0.8982 & -0.0836 \end{bmatrix}$$

We assume the external disturbance is $\omega(t) = 0.2e^{-0.03(t-5)}$ $\sin(0.05t)$, and the initial states are $x(0) = \begin{bmatrix} 0.2 & -0.8 \end{bmatrix}^T$, $x_f(0) = \begin{bmatrix} 0 & 0 \end{bmatrix}^T$. The cyber-attack is shown in Fig. 4, which follows the variation of the state. Using the proposed method yields the response of filtering error shown in Fig. 5. It can be seen that the estimation works well although the network is under the deception attack. 269 of 1000 data packets are released into the network, and the others are discarded. It illustrates that the proposed ETM is effective to reduce the utilization of communication bandwidth, while guaranteeing the performance of the filter.

5. Conclusion

This paper concerned with H_∞ filter design for T–S fuzzy systems with event-triggered mechanism and deception attacks. An novel event-triggered mechanism has been studied. The mean data-releasing rate over the entire simulation period using the proposed ETM can be greatly reduced, compared to the one using TTM. Moreover, the data-releasing rate during the system subject to disturbances and attacks is higher than the one over the other periods. As a result, more information can be achieved to compensate external variations. Sufficient conditions has been proposed to ensure H_∞ performance of filtering error system. In the end, simulation examples are proposed to demonstrate the usefulness of the proposed method.

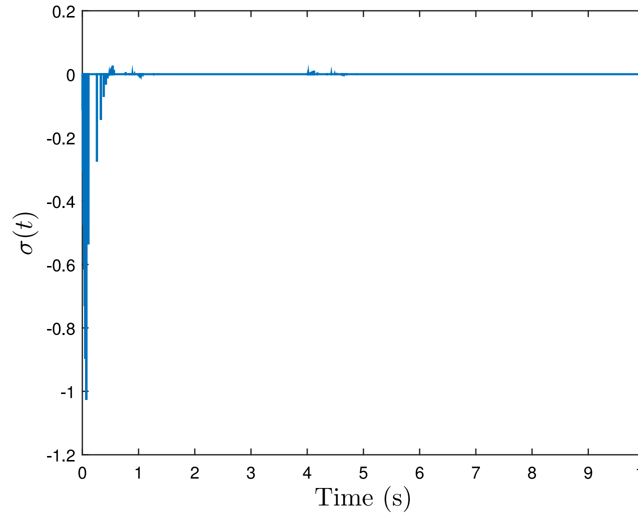

Fig. 4. The deception attack.

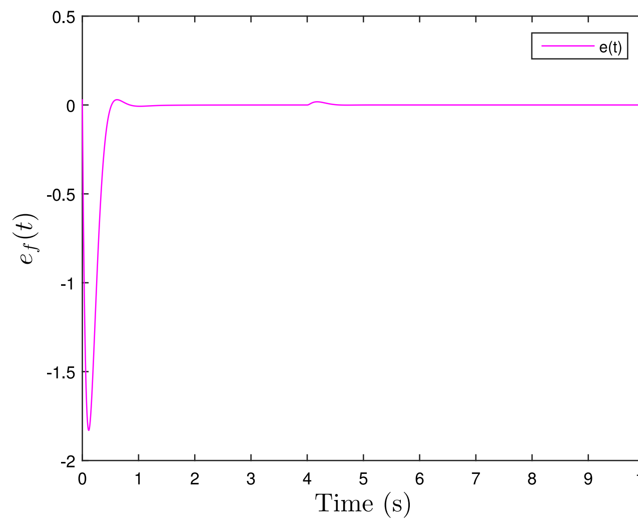

Fig. 5. The filtering error $x_f(t)$.

Acknowledgment

This work was supported by a grant from the National Natural Science Foundation of China No. 61473156.

Conflict of interest

No special conflict of interest.

References

[1] Zhang D, Nguang SK, Srinivasan D, Yu L. Distributed filtering for discrete-time T-S fuzzy systems with incomplete measurements. IEEE Trans Fuzzy Syst 2018;26(3):1459–71.
[2] Zhai D, An LW, Li JH, Zhang QL. Finite frequency fault detection for T-S fuzzy singular multiple time-delay systems. Int J Control Autom Syst 2016;14(4):977–85.
[3] Zhang D, Yang F, Yu C, Srinivasan D, Yu L. Robust fuzzy-model-based filtering for nonlinear networked systems with energy constraints. J Franklin Inst B 2017;354(4):1957–73.
[4] Peng C, Ma S, Xie X. Observer-based non-PDC control for networked T-S fuzzy systems with an event-triggered communication. IEEE Trans Cybern 2017;47(8):2279–87.

[5] Tan Y, Du D, Fei S. Quantized filtering for T-S fuzzy networked systems with saturation nonlinearities: An output-dependent triggering method. ISA Trans 2018;72:122–37.
[6] Dong Y, Tian E, Han QL. A delay system method for designing event-triggered controllers of networked control systems. IEEE Trans Automat Control 2013;58(2):475–81.
[7] Du D, Qi B, Fei M, Peng C. Multiple event-triggered H_2/H_∞ filtering for hybrid wired–wireless networked systems with random network-induced delays. Inform Sci 2015;325:393–408.
[8] Wang YL, Shi P, Lim CC, Liu Y. Event-triggered fault detection filter design for a continuous-time networked control system. IEEE Trans Cybern 2016;46(12):3414–26.
[9] Gu Z, Huan Z, Yue D, Yang F. Event-triggered dynamic output feedback control for networked control systems with probabilistic nonlinearities. Inform Sci 2018;457:99–112.
[10] Wang X, Lemmon M. Technical communique: On event design in event-triggered feedback systems. Automatica 2011;47(10):2319–22.
[11] Gu Z, Shi P, Yue D, Ding Z. Decentralized adaptive event-triggered H_∞ filtering for a class of networked nonlinear interconnected systems. IEEE Trans Cybern 2019;49(2):2168–275.
[12] Tian E, Wang Z, Zou L, Yue D. Probabilistic-constrained filtering for a class of nonlinear systems with improved static event-triggered communication. Internat J Robust Nonlinear Control 2019;29(5):1484–98.
[13] Peng C, Zhang J, Yan H. Adaptive event-triggering H_∞ load frequency control for network-based power systems. IEEE Trans Ind Electron 2018;65(2):1685–94.
[14] Su X, Xia F, Wu L, Chen CLP. Event-triggered fault detector and controller coordinated design of fuzzy systems. IEEE Trans Fuzzy Syst 2018;26(4):2004–16.
[15] Du D, Qi B, Fei M, Wang Z. Quantized control of distributed event-triggered networked control systems with hybrid wired–wireless networks communication constraints. Inform Sci 2017;380:74–91.
[16] Liu J, Wei L, Xie X, Tian E, Fei S. Quantized stabilization for t–s fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks. IEEE Trans Fuzzy Syst 2018;26(6):3820–34.
[17] Zhang C, Hu J. Event-triggered robust H_∞ state estimation for T-S fuzzy systems via piecewise lyapunov functions. In: IEEE International Conference on Control & Automation. 2017, p. 559–64.
[18] Wang A, Mu B, Yang S. Consensus control for a multi-agent system with integral-type event-triggering condition and asynchronous periodic detection. IEEE Trans Ind Electron 2017;64(7):5629–39.
[19] Cheng J, Ahn CK, Karimi HR, Cao J, Qi W. An event-based asynchronous approach to markov jump systems with hidden mode detections and missing measurements. IEEE Trans Syst Man Cybern: Syst 2018. http://dx.doi.org/10.1109/TSMC.2018.2866906.
[20] Liu S, Wei G, Ding D, Mao J. Kalman-type recursive filtering for stochastic nonlinear time-delay systems with randomly occurring deception attacks. In: Chinese Control Conference. 2017, p. 5264–9.
[21] Bu X, Dong H, Han F, Li G. Event-triggered distributed filtering over sensor networks with deception attacks and partial measurements. Int J Gen Syst 2018;47(5):395–407.
[22] Du D, Chen R, Li X, Wu L, Zhou P, Fei M. Malicious data deception attacks against power systems: A new case and its detection method. Trans Inst Meas Control 2018. http://dx.doi.org/10.1177/0142331217740622.
[23] Yuan H, Xia Y. Secure filtering for stochastic non-linear systems under multiple missing measurements and deception attacks. IET Control Theory Appl 2018;12(4):515–23.
[24] Hu S, Yue D, Xie X, Chen X, Yin X. Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. IEEE Trans Cybern PP(99):1–11.
[25] Chen B, Ho DWC, Zhang WA, Yu L. Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks. IEEE Trans Syst Man Cybern Syst 2017;PP(99):1–14.
[26] Liu J, Tian E, Xie X, Hong L. Distributed event-triggered control for networked control systems with stochastic cyber-attacks. J Franklin Inst B 2018. http://dx.doi.org/10.1016/j.jfranklin.2018.01.048.
[27] Liu J, Yin T, Shen M, X, Xie, Cao J. State estimation for cyber-physical systems with limited communication resources, sensor saturation and denial-of-service attacks. ISA Trans 2018. http://dx.doi.org/10.1016/j.isatra.2018.12.032.
[28] Ding D, Wang Z, Ho DWC, Wei G. Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. Automatica 2017;78(C):231–40.
[29] Zhang D, Liu L, Feng G. Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack. IEEE Trans Cybern 2018;PP(99):1–11.
[30] Cheng J, Park JH, Cao J, Zhang D. Quantized H_∞ filtering for switched linear parameter-varying systems with sojourn probabilities and unreliable communication channels. Inform Sci 2018;466:289–302.
[31] Peng C, Wu M, Xie X, Wang Y. Event-triggered predictive control for networked nonlinear systems with imperfect premise matching. IEEE Trans Fuzzy Syst 2018. http://dx.doi.org/10.1109/TFUZZ.2018.2799187.
[32] Zhang CK, He Y, Jiang L, Wu M. Stability analysis for delayed neural networks considering both conservativeness and complexity. IEEE Trans Neural Netw Learn Syst 2017;27(7):1486–501.
[33] Khargonekar PP, Petersen IR, Zhou K. Robust stabilization of uncertain linear systems: Quadratic stability and H_∞ control theory. IEEE Trans Autom Control 1990;35(3):356–61.
[34] Wang Y, Shen H, Karimi HR, Duan D. Dissipativity-based fuzzy integral sliding mode control of continuous-time T-S fuzzy systems. IEEE Trans Fuzzy Syst 2018;26(3):1164–76.
[35] Gu Z, Zhang T, Yang F, Zhao H, Shen M. A novel event-triggered mechanism for networked cascade control system with stochastic nonlinearities and actuator failures. J Franklin Inst B 2019. http://dx.doi.org/10.1016/j.jfranklin.2019.01.021.
[36] Yue D, Tian E, Zhang Y, Peng C. Delay-distribution-dependent stability and stabilization of T-S fuzzy systems with probabilistic interval delay. IEEE Trans Syst Man Cybern 2009;39(2):503–16.
[37] Wang H, Peng S, Zhang J. Event-triggered fuzzy filtering for a class of nonlinear networked control systems. Signal Process 2015;113:159–68.
[38] Gao H, Yan Z, Lam J, Ke C. H_∞ fuzzy filtering of nonlinear systems with intermittent measurements. IEEE Trans Fuzzy Syst 2009;17(2):291–300.