Received: 7 April 2023 | Revised: 15 June 2023 | Accepted: 20 July 2023

DOI: 10.1002/rnc.6919

RESEARCH ARTICLE

WILEY

Outlier-resistant quantized control for T-S fuzzy systems under multi-channel-enabled round-robin protocol and deception attacks

Lijuan Zha[1] | Tao Huang[1] | JinLiang Liu[2] | Xiangpeng Xie[3] | Engang Tian[4]

[1]College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, China

[2]School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, China

[3]Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China

[4]School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, China

Correspondence
Jinliang Liu, School of Computer Science, Nanjing University of Information Science and Technology, Nanjing 210044, China.
Email: liujinliang@vip.163.com

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 62273174, 61973152, 61903182; Natural Science Foundation of Jiangsu Province of China, Grant/Award Number: BK20211290; Qinglan Project of Jiangsu Province of China

Abstract

In this study, the security quantized control problem is investigated for discrete-time Takagi-Sugeno (T-S) fuzzy systems with deception attacks based on the multi-channel-enabled round-robin (MCERR) protocol. The MCERR protocol breaks through the limitation in the well-known RR protocol where only one signal can be transmitted at every turn. Under MCERR protocol, multiple transmission channels are put to use and a set of sensor nodes can gain access to network. Considering the random deception attacks and the measurement outliers, a new system model is established and a sufficient condition is derived to ensure the stability of the discussed system. Furthermore, an outlier resistant observer-based controller which can mitigate the impact of deception attacks is developed. Besides, the concrete expressions of observer gains and controller gains are obtained. Finally, the effectiveness of the proposed method can be validated by simulation results.

KEYWORDS

deception attacks, multi-channel-enabled round-robin protocol, outlier-resistant observer-based control, T-S fuzzy systems

1 | INTRODUCTION

Recent years have observed extensive attention in modeling and controlling the nonlinear complex systems by Takagi–Sugeno (T–S) fuzzy model.[1,2] The basic idea of T–S fuzzy model is to describe nonlinear complex systems by a finite number of linear subsystems, which are fused with membership functions (MFs) by if-then rules.[3] With the method of the T–S fuzzy model, the nonlinear factors of control systems can be dealt with effectively. In the past few years, great progress has been made in the study of T-S fuzzy system.[4-7] For some nonlinear complex systems, such was the case with the availability of state information to the controlled system may not be guaranteed. In view of this case, the appraisal to the state variables is indispensable by employing fuzzy observers. Nowadays, observer-based output feedback control problem has caused more widespread concern and fruitful results can be found by considerable research recently.[8,9]

For networked systems, the shared communication network is used as the transmission medium to realize the signal transmission from sensor to controller and controller to actuator. With the widely application of network technologies, networked communication has exhibited distinctive merits such as low installation, high flexibility and easy maintenance. However, a key obstacle of the networked communication is the limited networked bandwidth, which may induce data collision and network congestion, and also can make significant degradation for system performance and even result in system instability.[10,11] In view of this, it is of vital importance to make rational and efficient use of limited network resources. As such, various communication protocols have been used to manage information transmission. Common communication protocols include RR protocol,[12,13] stochastic communication protocol[14] and weighted try-once-discard (WTOD) protocol.[15] Among them, RR protocol has received the most attention in practice due to its easy implementation and predictability. Specifically, only one node is authorized to access the network in a fixed circular order at each time under it. It should be mentioned that most of the existing results assume the signal transmissions based on RR protocol are carried out over one transmission channel at each time instant.[16-19] Multi-channel-enabled round-robin (MCERR) protocol has not gained any attention yet in the investigation of networked systems, which motivates this work.

Besides of the constraint network-bandwidth in networked systems, the network security is another important issue worthy of attention.[20-22] The network openness and vulnerabilities make the networked system expose to malicious attacks, which interfere the integrity and authenticity of the transmitted data during transmission aiming to destroy the target system. With the hope of eliminating the negative impacts inducing by malicious attacks, several types of malicious attacks to networked systems have been studied in depth including denial-of-service (DoS) attacks[23-25] and deception attacks.[26-29] Compared with other attacks, deception attacks are difficult to detect because of their strong concealment, which are launched to modify the transmitted signal intermittently and corrupt the real signal value. So far, ever-increasing interest has been evoked on how to protect the networked system from the adverse impacts of deception attacks. For example, robust asynchronous filtering method was been proposed in Reference 30 for discrete-time T-S fuzzy complex dynamical networks with random coupling delays and deception attacks.[30] In Reference 31, in the case of spoofing attack and continuous packet loss, a security controller for sampled data fuzzy system is developed.[31]

In actual engineering, the sudden or large disturbances on the measurement output may be unavoidable, which are called measurement outliers. These measurement outliers may be induced by multiple reasons, including operation errors, sensor aging, sensor failures and unpredictable environmental disturbances. So far, the outlier detection methods and anti-outlier control scheme have attracted increasing attention.[32] In comparison with measurement noises, the unexpected measurement outliers may result in anomalous amplitude changes and degrade the performance of the observer.[33] As a consequence, it is of enormous significance to checkout anti-outlier state estimation by eliminating/suppressing the side effects induced by measurement outliers. Aiming at ease up the impact of measuring outliers and improve the accuracy of data, an effective approach is to introduce a particular saturation function into the design of the observers-based controller.[34,35] Such as, to mitigate the negative effects on estimation error for a class of T-S fuzzy delayed neural networks with reaction-diffusion terms, a state estimator scheme is presented by introducing a saturation function.[36] In Reference 37, a certain confidence dependent saturation function is used to reduce the side effects of measurement outliers on the estimation error dynamics.[37] In the case of measured outliers, the saturation function in Reference 38 is used in the Tobit Kalman filter structure to constrain innovations contaminated by measured outliers.[38] However, up to now, there are few related reference results, and there is still a lot of research space for the outlier-resistant observer-based control for T-S fuzzy systems, which also inspires our research.

In this paper, motivated by the above analysis, the outlier resistant observer-based security controller is devised for one-class T-S fuzzy systems under the network constraints. The challenges to deal with the problem are as follows: First, how to tackle the communication constraints and the fragile communication network? Second, how to scheme the outlier resistant observer-based controller of the considered system subject to quantization, MCERR protocol and deception attacks? These two challenges will be addressed in this paper. The main contributions can be summarized as follows:

1. The MCERR protocol and signal quantization are presented to reduce the networked transmission burden and improve the performance of the augmented system. The quantized measurement outputs will be scheduled by the MCERR protocol. under which a group of sensor nodes can be connected to the network simultaneously.
2. The quantization, MCERR protocol and the deception attacks are taking into consideration in establishing the addressed closed-loop system model. A new outlier-resistant observer-based controller is designed to ensure the stability of the addressed networked systems with communication constraints and deception attacks.

The reminder of this paper is organized as follows. Section 2 describes the outlier-resistant observer-based control problem for one-class T-S fuzzy systems with network constraints and deception attacks. The main results of the paper are presented in Section 3. Sections 4 and 5 give the simulation results and the conclusion to this paper, respectively.

Notation: $\mathbb{R}^m$ stands for the m-dimensional Euclidean space, I is the identity matrix of appropriate dimensions and 0 represents the zero matrix of compatible dimensions. The superscript T stands for matrix transposition. The symbol $diag\{\dots\}$ represents a block-diagonal matrix and $*$ stands for the symmetric term in a symmetric block matrix. $||\cdot||$ is the Euclidean norm of a vector and its induced norm of a matrix. $mod(a,b)$ means the nonnegative remainder on division of the integer a by the positive integer b.

2 | PROBLEM DESCRIPTION

2.1 | The T-S fuzzy system

Consider the following discrete-time networked T-S fuzzy system with s rules, and the ith rule is

Plant Rule i :

IF $\vartheta_1(k)$ is M_{i1}, $\vartheta_2(k)$ is M_{i2}, $\dots$, $\vartheta_l(k)$ is M_{il},

THEN

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

where $\vartheta(k) = [\vartheta_1(k), \vartheta_2(k), \dots, \vartheta_l(k)]^T$ is the premise variable vector. $M_{ij}(j = 1, 2, \dots, l)$ is the fuzzy set. $x(k) \in \mathbb{R}^{n_x}$ is the state vector, $u(k) \in \mathbb{R}^{n_u}$ is control input vector and $y(k) \in \mathbb{R}^{n_y}$ is the measurement output, respectively. A_i, B_i and C_i are known constant matrices with appropriate dimensions.

By operating the method of center-average defuzzifier, product inference, and singleton fuzzifier, the T-S fuzzy system (1) can be represented as:

$$\begin{cases} x(k+1) = \sum_{i=1}^{s} h_i(\vartheta(k))[A_i x(k) + B_i u(k)] \\ y(k) = \sum_{i=1}^{s} h_i(\vartheta(k)) C_i x(k), i = 1, \dots, s \end{cases} \tag{2}$$

where $h_i(\vartheta(k))$ is the normalized membership which satisfies:

$$h_i(\vartheta(k)) = \frac{\prod_{j=1}^{l} \varrho_{ij}(\vartheta_j(k))}{\sum_{i=1}^{s} \prod_{j=1}^{l} \varrho_{ij}(\vartheta_j(k))}$$

with $h_i(\vartheta(k)) \geq 0$, $\sum_{i=1}^{s} h_i(\vartheta(k)) = 1$ and $\varrho_{ij}(\vartheta_j(k))$ is the grade of membership of $\vartheta_j(k)$ in M_{ij}.

Definition 1. The nonlinearity $\varphi(\cdot)\mathbb{R}^n \to \mathbb{R}^n$ satisfies the sector interval $[\Omega_1, \Omega_2]$ if

$$(\varphi(\varepsilon) - \Omega_1 \varepsilon)^T (\varphi(\varepsilon) - \Omega_2 \varepsilon) \leq 0, \forall \varepsilon \in \mathbb{R}^n \tag{3}$$

where $\Omega_1, \Omega_2 \in \mathbb{R}^n$ are real matrices, and positive-definite matrix $\Omega = \Omega_2 - \Omega_1$ is true.

Assumption 1. The matrix B_i is column full-rank.

2.2 | Logarithmic quantization

For networked systems with limited communication capacity, the quantization of sensor measurements is required before transmission. It is evident that the system performance is significantly influenced by the quantization, which should be taken into account. Similar to Reference 38, the logarithmic quantizer $q(\cdot)$ is modeled by Reference 39

$$q(y(k)) = [q_1(y_1(k)), q_2(y_2(k)), \dots, q_{n_y}(y_{n_y}(k))]^T$$

the quantization levels for each $q_\ell(\cdot)(1 \le \ell \le n_y)$ is given as follows

$$\mho_\ell := \left\{ \pm\epsilon_{\ell(i)} : \epsilon_{\ell(i)} = \rho_\ell^i \epsilon_{\ell(0)}, \quad i = 0, \pm 1, \pm 2, \ldots \right\} \cup \{0\}(\epsilon_{\ell(0)} > 0) \tag{4}$$

where $\epsilon_{\ell(0)}$ is a scaling constant. The logarithmic quantizer $q_\ell(\cdot)$ is formulated as

$$q_\ell(y_\ell(k)) = \begin{cases} \epsilon_{\ell(i)}, & \frac{1+\rho_\ell}{2}\epsilon_{\ell(i)} \le y_\ell(k) \le \frac{1+\rho_\ell}{2\rho_\ell}\epsilon_{\ell(i)} \\ 0, & y_\ell(k) = 0 \\ -q_\ell(-y_\ell(k)), & y_\ell(k) < 0. \end{cases} \tag{5}$$

where $\rho_\ell \in (0, 1)$ is quantization density.

Using quantization approach in Reference 39, the signal $q(y(k))$ satisfies[40]

$$(q(y(k)) - H_1 y(k))^T (q(y(k)) - H_2 y(k)) \le 0. \tag{6}$$

Denoting $H_1 = diag_{n_y}\{2\rho_\ell/(1+\rho_\ell)\}$ and $H_2 = diag_{n_y}\{2/(1+\rho_\ell)\}$. Since $0 < \rho_\ell < 1$, one can get that $0 \le H_1 \le I \le H_2$. Then, $q(y(k))$ can be formulated as

$$q(y(k)) = H_1 y(k) + \varphi(y(k)) \tag{7}$$

where $\varphi(y(k))$ is a nonlinear vector-valued function (see Definition 1) satisfying

$$\varphi(y(k))^T (\varphi(y(k)) - Hy(k)) \le 0 \tag{8}$$

with $H = H_2 - H_1$.

2.3 | The description of communication network

In the considered nonlinear networked system, the quantized signal $q(y(k))$ will be transmitted through the channels of the communication network. A MCERR protocol is implemented to avoid data collisions in signal transmission. Under the MCERR protocol, more than one sensor data can access to the communication channel at each time, which improves the utilization of network bandwidth resources and reduces the cost. In this mechanism, each sensor is assigned to several sets and transmit all sensor measurements in a set equally at a time. Let $F(k)$ be one of the sets, N be the number of sensor nodes and $F(k) \subseteq \{1, 2, \ldots, N\}$ be the group of active nodes which obtain the token at the instant k. That is to say, the value of $F(k)$ chooses which sensor nodes to be authorized to release packets. We assume that the number of sensor nodes able to access the communication network at one instant is m and t is the least common multiple of N and m, that is, $t = \frac{[N,m]}{m}$.

$$F(k) = F(k+t) = \{mod((k-1) * m, N) + 1, \ldots, mod((k-1) * m + (m-1), N) + 1\} \tag{9}$$

where $mod(a, b)$ refers to the nonnegative remainder on division of the integer a by the positive integer b.

In practice, the communication network in control systems is prone to attacks, which makes the signal $q(y(k))$ probable to be attacked in the transmission process. The attacker can destroy the data authenticity by injecting some deception signals maliciously. Specifically, there exists a certain possibility that the wrong signal will be injected by the attacker. For safety purposes, the deception attacks on sensor measurements should be taken onto account and eliminate the negative effects on the controlled system.

Then, $\bar{y}_i(k)$ subject to MCERR protocol and deception attacks can be modeled as

$$\bar{y}_i(k) = \begin{cases} q_i(y_i(k)) + \alpha(k) g(x(k)), & i \in F(k) \\ \bar{y}_i(k-1), & otherwise \end{cases} \tag{10}$$

where $g(x(k))$ is the erroneous data denoted the injected deception attacks, which satisfies:

$$||g(x(k))||^2 \leq ||S \cdot x(k)||^2 \tag{11}$$

where S is a given matrix of constants with appropriate dimensions.

The parameter $\alpha(k)$ is a random variable, it is assumed that $\alpha(k)$ satisfies:

$$\begin{cases} Pr\{\alpha(k) = 1\} = \overline{\alpha} \\ Pr\{\alpha(k) = 0\} = 1 - \overline{\alpha} \end{cases} \tag{12}$$

where $\overline{\alpha} \in [0,1)$ is a given constant and $Prob(\alpha(k) - \overline{\alpha})^2 = \overline{\alpha}(1 - \overline{\alpha})$, obviously.

Define the following update matrix:

$$\Phi_{\hbar(k)} = \sum_{i \in F(k)} \psi_i \tag{13}$$

in which

$$\psi_i = diag\{\delta(i-1)I, \delta(i-2)I, \ldots, \delta(i-n_y)I\} \tag{14}$$

where $\delta(\cdot) \in \{0, 1\}$ is the Kronecker delta function and $\hbar(k) \in \{1, 2, \ldots, n\}$. Then, the update strategy of the controller input can be presented as:

$$\overline{y}(k) = \Phi_{\hbar(k)}(q(y(k)) + \alpha(k)g(x(k))) + (I - \Phi_{\hbar(k)})\overline{y}(k-1) \tag{15}$$

Remark 1. In (15), $\alpha(k) = 1$ donates the erroneous $g(x(k))$ is successfully injected into $\overline{y}(k)$, which means deception attacks occur. When $\alpha(k) = 0$, it represents that the controller input $\overline{y}(k)$ is normal.

Remark 2. In the light of the characteristic of original RR protocol, the MCERR protocol is employed in this article, which is a generalization formula of the original one. Specifically, under the implemented RR protocol, the number of the transmitted signals are according to (9), which has made a breakthrough in the conventional RR protocol that only one node can be accessable to the network. Therefore, the results we obtained will be more general.

2.4 | Outlier-resistant observed-based controller

For diminishing the adverse effect of abnormal innovation caused by measurement outliers, we employ a saturation function in the observer-based controller structure, in which the saturation level can be decided based on the range of the innovation. In this paper, a kind of outlier-resistant control strategy will be designed for networked system (1) under the influence of the MCERR protocol and logarithmic quantization. The proposed outlier-resistant observer-based controller is as follows:

Plant Rule i :
IF $\vartheta_1(k)$ is M_{i1}, $\vartheta_2(k)$ is M_{i2}, $\ldots$, $\vartheta_l(k)$ is M_{il},
THEN

$$\begin{cases} \hat{x}(k+1) = A_i\hat{x}(k) + B_iu(k) + L_{i,\hbar(k)}\upsilon(\overline{y}(k) - \hat{y}(k)) \\ \hat{y}(k) = C_i\hat{x}(k) \\ u(k) = K_{i,\hbar(k)}\hat{x}(k), i = 1, \ldots, s, \hbar(k) = 1, 2, \ldots, n_y \end{cases} \tag{16}$$

where $\hat{x}(k)$ is the state estimate, $L_{i,\hbar(k)}$ and $K_{i,\hbar(k)}$ are the observer gain and controller gain to be designed, respectively.

Define the saturation function $\upsilon(\cdot)$: $\mathbb{R}^{n_y} \rightarrow \mathbb{R}^{n_y}$ as $\upsilon(\kappa) = \left[\upsilon_1^T(\kappa_1) \quad \upsilon_2^T(\kappa_2) \cdots \upsilon_{n_y}^T(\kappa_{n_y})\right]^T$ and $\upsilon_\iota(\kappa_\iota) \triangleq$ sign (κ_ι) min $\{\kappa_{\iota,max}, |\kappa_\iota|\}$, $\iota = 1, 2, \ldots, n_y$, where $\kappa_{\iota,max}$ is the ιth element of κ_{max} which is used to represent the saturation level.

Obviously, the defuzzied overall observer-based control law can be formulated as:

$$\begin{cases} \hat{x}(k+1) = \sum_{i=1}^{s} h_i(\vartheta(k))[A_i\hat{x}(k) + B_i u(k) + L_{i,\hbar(k)}\upsilon(\bar{y}(k) \\ \qquad -\hat{y}(k))] \\ \hat{y}(k) = \sum_{i=1}^{s} h_i(\vartheta(k))C_i\hat{x}(k) \\ u(k) = \sum_{i=1}^{s} h_i(\vartheta(k))K_{i,\hbar(k)}\hat{x}(k) \end{cases} \tag{17}$$

Denote $e(k) \triangleq x(k) - \hat{x}(k)$ as observation error. The dynamics of the error $e(k)$ is easily derived:

$$e(k+1) = \sum_{i=1}^{s}\sum_{j=1}^{s} h_i(\vartheta(k))h_j(\vartheta(k))\{A_i e(k) - L_{i,\hbar(k)}\upsilon(\bar{y}(k) - \hat{y}(k))\} \tag{18}$$

The linear part and the nonlinear part compose of the saturation function $\upsilon(\bar{y}(k) - \hat{y}(k))$ in (17), that is,

$$\upsilon(\bar{y}(k) - \hat{y}(k)) = N_1(\bar{y}(k) - \hat{y}(k)) + \phi(\bar{y}(k) - \hat{y}(k)) \tag{19}$$

for the diagonal matrices $N_1 \in \mathbb{R}^{n_y \times n_y}$ and $N_2 \in \mathbb{R}^{n_y \times n_y}$ satisfying $0 \le N_1 < I \le N_2$. For the nonlinear vector-valued function $\phi(\cdot)$ above, it satisfies:

$$\phi^T(\bar{y}(k) - \hat{y}(k))[\phi(\bar{y}(k) - \hat{y}(k)) - N(\bar{y}(k) - \hat{y}(k))] \le 0 \tag{20}$$

where $N = N_2 - N_1$.

Remark 3. The measurement outliers refers to the contaminated sensor measurements which are induced by multiple causes such as equipment damage, operation error and so on. The measurement outliers may lead to abnormal updates and adversely make an negative impact on the system stability. As to the observer in this paper, if the measurement outliers are in presence, the innovations will deviate from the normal ones and affect the accuracy of the observer. As such, we try to design a new outlier-resistant observer-based controller so as to block the outliers interference and ensure the accuracy of the estimation.

Remark 4. The specific saturation function $\upsilon(\cdot)$, which is adopted to tackle with anomalous data impact caused by the measurement outliers, is introduced to offset the deviation and make the innovation constrained in a controllable range. The outlier-resistant observer-based controller we designed is capable of reducing the interference of outliers.

Remark 5. Although some secure control method for T-S fuzzy systems with limited networked resources and cyber attacks can be found in the existing literature, the discussed problem in this paper is distinct from these publications.[16,23,30] In Reference 16, a secure control method for T-S fuzzy systems is proposed under consideration of quantization and RR protocol. In References 23 and 30, for T–S fuzzy systems, the authors discussed the secure control problem against cyber-attacks by introducing event-triggered schemes to avoid waste of network resources. However, these existing methods can not be applicable when the measurement outliers are in presence and multiple transmission channels are put to use. Different from these references, in this paper, the multi-channel-enabled round-robin (MCERR) protocol is employed to deal with the communication constraints and a new security outlier-resistant quantized control method is presented for T-S fuzzy systems under the MCERR protocol, which makes up for the shortcomings of previous studies.

Let $\eta(k) = [x^T(k) \quad \bar{y}^T(k-1) \quad e^T(k)]^T$, the augmented system can be presented as following:

$$\begin{aligned} \eta(k+1) = \sum_{i=1}^{s}\sum_{j=1}^{s} h_i(\vartheta(k))h_j(\vartheta(k))\big\{&\vec{A}_{ij,\hbar(k)}\eta(k) + \vec{B}_{i,\hbar(k)}\varphi(y(k)) + \bar{\alpha}\vec{B}_{i,\hbar(k)}g(x(k)) \\ &+ (\alpha(k) - \bar{\alpha})\vec{B}_{i,\hbar(k)}g(x(k)) + \vec{D}_{i,\hbar(k)}\phi(\bar{y}(k) - \hat{y}(k))\big\} \end{aligned} \tag{21}$$

where

$$\vec{A}_{ij,\hbar(k)}=\begin{bmatrix} A_i+B_iK_{j,\hbar(k)} & 0 & -B_iK_{j,\hbar(k)} \\ \Phi_{\hbar(k)}H_1C_i & \Gamma(k) & 0 \\ \Pi_{31} & \Pi_{32} & \Pi_{33}\end{bmatrix},\quad \vec{B}_{i,\hbar(k)}=\begin{bmatrix} 0 \\ \Phi_{\hbar(k)} \\ -L_{i,\hbar(k)}N_1\Phi_{\hbar(k)}\end{bmatrix},\quad \vec{D}_{i,\hbar(k)}=\begin{bmatrix} 0 \\ 0 \\ -L_{i,\hbar(k)}\end{bmatrix},$$

$$\Pi_{31}=L_{i,\hbar(k)}N_1(C_j-\Phi_{\hbar(k)}H_1C_j), \Pi_{32}=-L_{i,\hbar(k)}N_1\Gamma(k), \Pi_{33}=A_i-L_{i,\hbar(k)}N_1C_j, \Gamma(k)=I-\Phi_{\hbar(k)}.$$

3 | MAIN RESULTS

In this section, the sufficient condition for the asymptotic stability of the addressed T-S fuzzy systems will be analyzed in Theorem 1. The proposed co-design method of controller gains and the observer gains will be shown in Theorem 2 which can guarantee the desired system performance.

Theorem 1. *For given scalars $\mu_0>0$, $\mu_1>0$ and $\overline{\alpha}\in[0,1)$, controller gain matrices $L_{i,r}$ and $K_{j,r}$, the asymptotic stability of the overall fuzzy system (21) can be achieved if there exist $P_r>0$ for any $r=1,2,\ldots,n$, such that*

$$\Xi_{ij,r}=\begin{bmatrix} \Xi_{11}^{r} & * & * & * & * & * \\ \Xi_{21}^{i} & -\mu_1 I & * & * & * & * \\ 0 & 0 & -I & * & * & * \\ \Xi_{41}^{j,r} & \Xi_{42}^{r} & \Xi_{43}^{r} & -\mu_0 I & * & * \\ \Xi_{51}^{ij,r} & \Xi_{52}^{i,r} & \Xi_{53}^{i,r} & \Xi_{54}^{i,r} & -P_{r+1} & * \\ 0 & 0 & \Xi_{63}^{i,r} & 0 & 0 & -P_{r+1}\end{bmatrix}<0 \tag{22}$$

where

$$\begin{aligned}
\Xi_{11}^{r}&=-P_r+\theta^TS^TS\theta, \Xi_{21}^{i}=\mu_1\frac{HC_i\theta}{2}, \Xi_{41}^{j,r}=\mu_0\frac{NG_{j,r}}{2},\\
\Xi_{42}^{r}&=\mu_0\frac{N\Phi_r}{2}, \Xi_{43}^{r}=\mu_0\overline{\alpha}\frac{N\Phi_r}{2}, \Xi_{51}^{ij,r}=P_{r+1}\vec{A}_{ij,r}, \Xi_{52}^{i,r}=P_{r+1}\vec{B}_{i,r},\\
\Xi_{53}^{i,r}&=\overline{\alpha}P_{r+1}\vec{B}_{ij,r}, \Xi_{54}^{i,r}=P_{r+1}\vec{D}_{i,r}, \Xi_{63}^{i,r}=\sqrt{\overline{\alpha}(1-\overline{\alpha})}P_{r+1}\vec{B}_{i,r},\\
\theta&=\begin{bmatrix} I & 0 & 0\end{bmatrix}, G_{j,r}=\begin{bmatrix}\Phi_rH_1C_j-C_j & \Gamma(k) & C_j\end{bmatrix}, r=\hbar(k).
\end{aligned}$$

Proof. See Appendix A.1. ∎

By reason of some nonlinear terms existing in (22), the nonlinear matrix inequality need to be converted to linear matrix inequality (LMI). In the following, we will devote to overcome this issue and give the observer and controller gains design method in Theorem 2.

Theorem 2. *For given scalars $\mu_0>0$, $\mu_1>0$ and $\overline{\alpha}\in(0,1)$, the asymptotic stability of the overall fuzzy system (21) can be achieved if there exist $P_r>0$ for any $r=1,2,\ldots,n$, such that*

$$\tilde{\Xi}_{ij,r}=\begin{bmatrix} \Psi_{11}^{r} & * & * & * & * & * \\ \Psi_{21}^{i} & -\mu_1 I & * & * & * & * \\ 0 & 0 & -I & * & * & * \\ \Psi_{41}^{j,r} & \Xi_{42}^{r} & \Xi_{43}^{r} & -\mu_0 I & * & * \\ \overline{\Psi}_{51}^{ij,r} & \overline{\Psi}_{52}^{i,r} & \overline{\Psi}_{53}^{i,r} & \overline{\Psi}_{54}^{i,r} & -P_{i+1} & * \\ 0 & 0 & \overline{\Psi}_{63}^{i,r} & 0 & 0 & -P_{i+1}\end{bmatrix}<0 \tag{23}$$

where

$$\Psi_{11}^{r}=\begin{bmatrix}-\overline{P}_r+S^TS & * & * \\ 0 & -\tilde{P}_r & * \\ 0 & 0 & -\overline{P}_r\end{bmatrix},\quad \Psi_{21}^{i}=\begin{bmatrix}\mu_1\frac{HC_i}{2} & 0 & 0\end{bmatrix},$$

$$\overline{\Psi}_{52}^{i,r}=\begin{bmatrix}0 \\ \tilde{P}_{i+1}\Phi_r \\ -Y_{i,r}N_1\Phi_r\end{bmatrix},\Psi_{41}^{i,r}=\begin{bmatrix}\mu_0\frac{N(\Phi_rH_1C_j-C_j)}{2} & \mu_0\frac{N\Gamma(k)}{2} & \mu_0\frac{NC_j}{2}\end{bmatrix},$$

$$\overline{\Psi}_{51}^{ij,r}=\begin{bmatrix}\overline{\Upsilon}_{11}^{ij,r} & 0 & -B_iX_{j,r} \\ \Upsilon_{21}^{i,r} & \tilde{P}_{i+1}\Gamma(k) & 0 \\ \overline{\Upsilon}_{31}^{ij,r} & \overline{\Upsilon}_{32}^{i,r} & \overline{\Upsilon}_{33}^{ij,r}\end{bmatrix},\quad \overline{\Psi}_{53}^{i,r}=\begin{bmatrix}0 \\ \overline{\alpha}\tilde{P}_{r+1}\Phi_r \\ -\overline{\alpha}Y_{i,r}N_1\Phi_r\end{bmatrix},$$

$$\overline{\Psi}_{54}^{i,r}=\begin{bmatrix}0 \\ 0 \\ -Y_{i,r}\end{bmatrix},\quad \overline{\Psi}_{63}^{i,r}=\begin{bmatrix}0 \\ \sqrt{\overline{\alpha}(1-\overline{\alpha})}\tilde{P}_{r+1}\Phi_r \\ -\sqrt{\overline{\alpha}(1-\overline{\alpha})}Y_{i,r}N_1\Phi_r\end{bmatrix},$$

$$\overline{\Upsilon}_{11}^{ij,r}=\overline{P}_{r+1}A_i+B_iX_{j,r},\Upsilon_{21}^{i,r}=\tilde{P}_{r+1}\Phi_rH_1C_i,\overline{\Upsilon}_{31}^{ij,r}=Y_{i,r}N_1(C_j-\Phi_rH_1C_j),$$
$$\overline{\Upsilon}_{32}^{i,r}=-Y_{i,r}N_1\Gamma(k),\overline{\Upsilon}_{33}^{ij,r}=\overline{P}_{r+1}A_i-Y_{i,r}N_1C_j.$$

Moreover, the parameters of the controller in the form of (17) are

$$L_{i,r}=(\overline{P}_{r+1}^{1})^{-1}Y_{i,r},K_{i,r}=(\overline{P}_{r+1}^{1})^{-1}X_{j,r},\overline{P}_{r+1}^{1}=V_iQ_i^{-1}U_iQ_iV_i^T \tag{24}$$

Proof. : See Appendix A.2. ∎

4 | NUMERICAL SIMULATION

A tangible example will be pursued to illustrate the validity of the designed controller of the networked system under the impact of the MCERR protocol and logarithmic quantization. Consider one-class nonlinear systems as described in (1), and the corresponding system parameters are:

$$A_1=\begin{bmatrix}-0.31 & 0.22 & -0.32 \\ -0.36 & -0.51 & 0.14 \\ 0.26 & 0.36 & 0.11\end{bmatrix},\quad A_2=\begin{bmatrix}-0.22 & 0.21 & -0.22 \\ -0.35 & -0.61 & 0.16 \\ 0.16 & 0.21 & 0.12\end{bmatrix},\quad B_1=\begin{bmatrix}1.8 & 1 & 0.5 \\ -0.3 & 1 & 0.2 \\ -0.4 & -0.3 & 1\end{bmatrix},$$

$$B_2=\begin{bmatrix}2 & 0.4 & 0.2 \\ -0.2 & 1.3 & 0.3 \\ -0.3 & -0.5 & 1\end{bmatrix},\quad C_1=\begin{bmatrix}0.6 & 0.4 & 0.4 \\ 0.3 & 1.8 & 0.4 \\ 0.3 & 0.3 & 0.7\end{bmatrix},\quad C_2=\begin{bmatrix}0.6 & 0.4 & 0.4 \\ 0.3 & 0.7 & 0.4 \\ 0.3 & 0.3 & 0.7\end{bmatrix},\quad S=\begin{bmatrix}0.5 & 0 & 0 \\ 0 & 0.1 & 0 \\ 0 & 0 & 0.1\end{bmatrix},$$

$$H_1=\begin{bmatrix}0.23 & 0 & 0 \\ 0 & 0.63 & 0 \\ 0 & 0 & 0.83\end{bmatrix},\quad H_2=\begin{bmatrix}1.33 & 0 & 0 \\ 0 & 1.3 & 0 \\ 0 & 0 & 1.33\end{bmatrix},\quad N_1=\begin{bmatrix}1 & 2.02 & 2.99 \\ 1.03 & 1 & 2.97 \\ 0.98 & 4.01 & 1\end{bmatrix},$$

$$N_2=\begin{bmatrix}-0.2 & 0.6 & 2.7 \\ 1 & 0 & 2.9 \\ 0 & 3 & 0\end{bmatrix},\quad h_1(\vartheta(k))=\frac{1-sin^2(||x_1(k)||_2)}{2},h_2(\vartheta(k))=1-h_1(\vartheta(k)).$$

The nonlinear function g(·) is given by:

$$g(x(k)) = 0.1sin(2x(k))\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^T.$$

The saturation function $\upsilon(\overline{y}(k) - \hat{y}(k))$ is described as follows.

$$\upsilon(\overline{y}(k) - \hat{y}(k)) = |\overline{y}(k) - \hat{y}(k)|$$

The initial auxiliary offset variable of the deception attacks is given by $\overline{\alpha} = 0.2$.

Then, by solving LMI conditions in Theorem 2, observer gain $L_{i,r}$ and controller gain $K_{j,r}$ can be calculated as

$$L_{11} = \begin{bmatrix} 0.0232 & -0.0100 & -0.0048 \\ -0.0107 & 0.0174 & -0.0072 \\ -0.0055 & -0.0073 & 0.0242 \end{bmatrix}, \quad L_{21} = \begin{bmatrix} 0.0124 & -0.0053 & -0.0044 \\ -0.0053 & 0.0091 & -0.0006 \\ -0.0054 & -0.0021 & 0.0115 \end{bmatrix},$$

$$L_{12} = \begin{bmatrix} 0.0231 & -0.0096 & -0.0046 \\ -0.0104 & 0.0176 & -0.0066 \\ -0.0053 & -0.0068 & 0.0239 \end{bmatrix}, \quad L_{22} = \begin{bmatrix} 0.0231 & -0.0096 & -0.0046 \\ -0.0104 & 0.0176 & -0.0066 \\ -0.0053 & -0.0068 & 0.0239 \end{bmatrix},$$

$$L_{13} = \begin{bmatrix} 0.0232 & -0.0099 & -0.0043 \\ -0.0105 & 0.0175 & -0.0068 \\ -0.0051 & -0.0073 & 0.0246 \end{bmatrix}, \quad L_{23} = \begin{bmatrix} 0.0232 & -0.0099 & -0.0043 \\ -0.0105 & 0.0175 & -0.0068 \\ -0.0051 & -0.0073 & 0.0246 \end{bmatrix},$$

$$K_{11} = \begin{bmatrix} 0.1030 & -0.0288 & 0.0206 \\ -0.0288 & 0.1645 & -0.0092 \\ 0.0206 & -0.0092 & 0.1363 \end{bmatrix}, \quad K_{21} = \begin{bmatrix} 0.1073 & 0.0060 & 0.0361 \\ 0.0060 & 0.1308 & 0.0190 \\ 0.0361 & 0.0190 & 0.1611 \end{bmatrix},$$

$$K_{12} = \begin{bmatrix} 0.0993 & -0.0446 & 0.0112 \\ -0.0446 & 0.1577 & -0.0119 \\ 0.0112 & -0.0119 & 0.1267 \end{bmatrix}, \quad K_{22} = \begin{bmatrix} 0.0917 & 0.0008 & 0.0191 \\ 0.0008 & 0.1515 & 0.0148 \\ 0.0191 & 0.0148 & 0.1452 \end{bmatrix},$$

$$K_{13} = \begin{bmatrix} 0.0978 & -0.0343 & 0.0190 \\ -0.0343 & 0.1899 & 0.0060 \\ 0.0190 & 0.0060 & 0.1293 \end{bmatrix}, \quad K_{23} = \begin{bmatrix} 0.0972 & -0.0063 & 0.0276 \\ -0.0063 & 0.1515 & 0.0180 \\ 0.0276 & 0.0180 & 0.1435 \end{bmatrix}.$$

Assume there exist three sensors and two different ones of them are picked every time which means they are divided into three groups. Under the MCERR protocol, only one set will be authorized to transmit information through the communication network at every moment in Table 1. The simulation results are given in Figures 1–5. From Figure 1, it can be seen that the system state converges to zero, which indicates that the controller designed can stabilize the discussed system. In Figures 2–4, three groups of system states and their observations are plotted. Finally, the errors between system state and observer state are shown in Figure 5, which implies the observer has received wrong signals under deception attacks and generated fluctuation partly. However, even though the errors stray from the original path slightly, it will reach stability gradually.

TABLE 1 Scheduling signal $F(k)$ under the MCERR protocol.

***k*(*time*)**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**...**
*Sensor*1	1	1	0	1	1	0	1	1	0	...
*Sensor*2	1	0	1	1	0	1	1	0	1	...
*Sensor*3	0	1	1	0	1	1	0	1	1	...

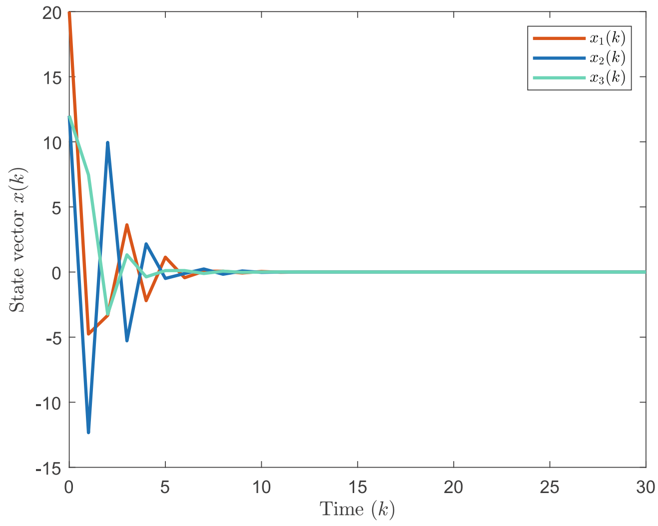

FIGURE 1 State responses.

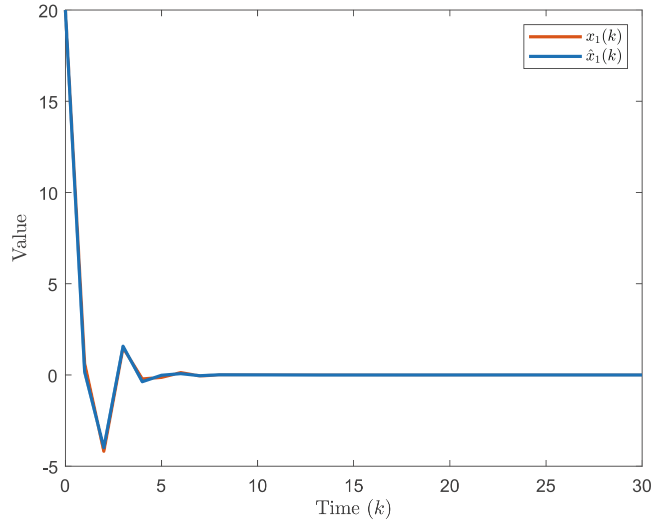

FIGURE 2 Trajectories of state $x_1(k)$ and its observation.

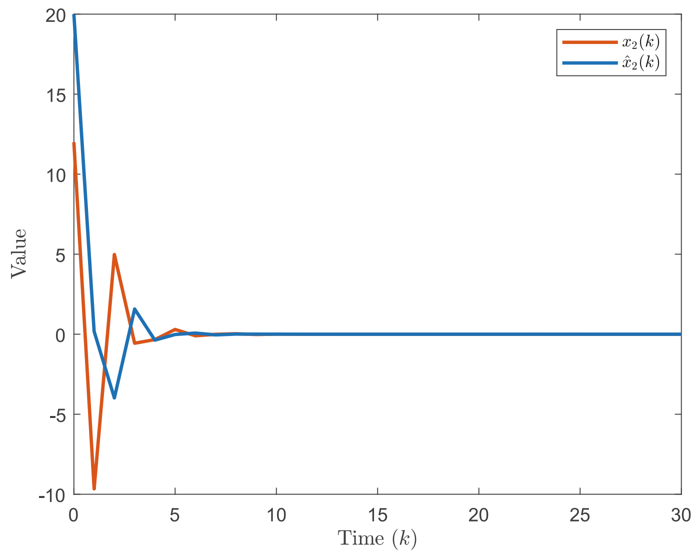

FIGURE 3 Trajectories of state $x_2(k)$ and its observation.

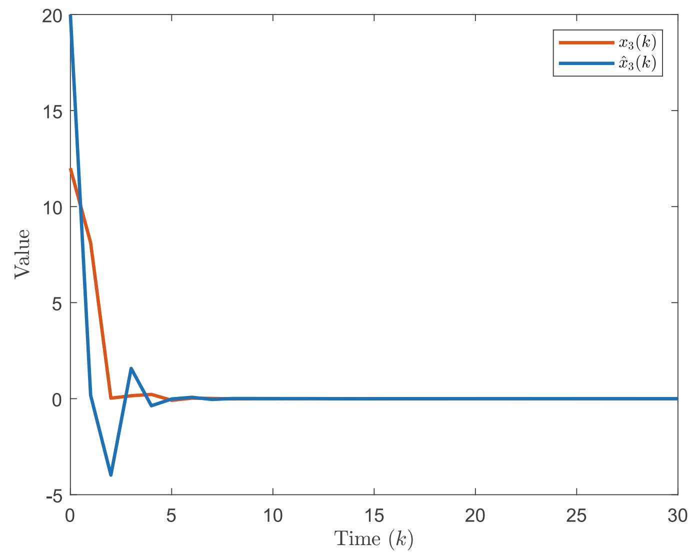

FIGURE 4 Trajectories of state $x_3(k)$ and its observation.

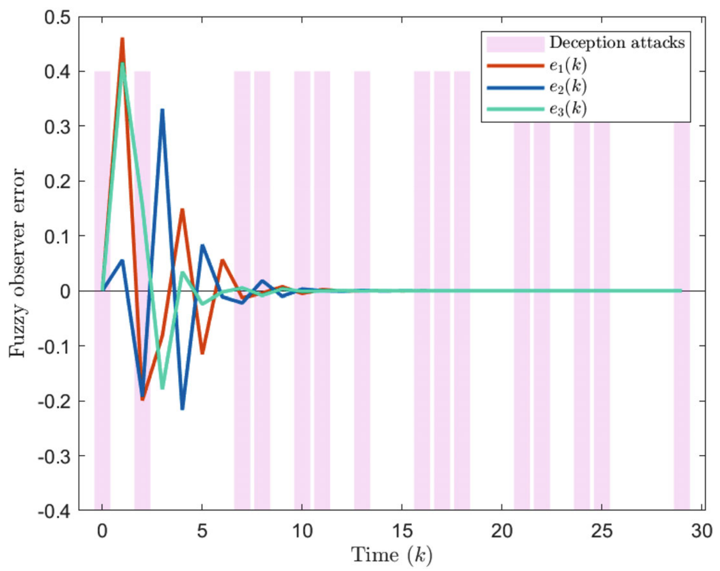

FIGURE 5 Trajectories of error responses $e(k)$.

From the above simulation results, it is clear to see the closed-loop system can be stabilized effectively by the proposed observer-based controller and the unmeasurable states can also be estimated by the observer at the same time. According to these simulation results, the effectiveness and feasibility of the proposed method are illustrated.

5 | CONCLUSION

In this paper, the outlier-resistant observer-based control problem for one-class T-S fuzzy systems under logarithmic quantization, the MCERR protocol and deception attacks has been investigated. Relying on the quantization technique, the data compression has been realized, which reduces the communication resource occupation. Based on the MCERR protocol and deception attacks, an observer-based control scheme is put forward for the discrete-time T-S fuzzy systems. By introducing a special saturation function into the state observer, the influence of measurement outliers on measurement accuracy is effectively alleviated. A sufficient condition and the outlier-resistant control method have been developed for the stability of the argument system. Finally, a tangible example has been pursued to check the validity of the proposed approach.

The future research direction includes designing a state estimator for nonlinear systems under new dynamic event triggering mechanisms and scheduling protocols, as well as the influences of various factors such as network attacks, signal saturation, and sensor failures.

ACKNOWLEDGMENTS

This research was supported by the National Natural Science Foundation of China under grants 62273174, 61973152, and 61903182, in part by the Natural Science Foundation of Jiangsu Province of China under grant BK20211290, and in part by the Qing Lan Project.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Research data are not shared.

ORCID

Lijuan Zha https://orcid.org/0000-0003-0475-8866
JinLiang Liu https://orcid.org/0000-0001-5489-0246
Xiangpeng Xie https://orcid.org/0000-0003-4822-3134
Engang Tian https://orcid.org/0000-0002-8169-5347

REFERENCES

1. Kang Y, Yao L, Zhou J, Wang H. Fault isolation and fault-tolerant control for nonlinear stochastic distribution control systems with multiplicative faults. *Int J Robust Nonlinear Control*. 2023;33(11):6070-6086.
2. Wang Y, Wang Z, Zou L, Dong H. H_∞ PID control for discrete-time fuzzy systems with infinite-distributed delays under round-robin communication protocol. *IEEE Trans Fuzzy Syst*. 2022;30(6):1875-1888.
3. Zhang J, Shi P, Qiu J, Nguang SK. A novel observer-based output feedback controller design for discrete-time fuzzy systems. *IEEE Trans Fuzzy Syst*. 2015;23(1):223-229.
4. Chekakta I, Jabri D, Motchon KMD, Guelton K, Belkhiat DEC. Design of asynchronous switched Takagi–Sugeno model-based $H\infty$ filters with nonlinear consequent parts for switched nonlinear systems. *Int J Adapt Control Signal Process*. 2023;37(6):1511-1535.
5. Li G, Peng C, Xie X, Xie S. On stability and stabilization of T–S fuzzy systems with time-varying delays via quadratic fuzzy Lyapunov matrix. *IEEE Trans Fuzzy Syst*. 2022;30(9):3762-3773.
6. Zhang X, Wang H, Stojanovic V, et al. Asynchronous fault detection for interval Type-2 fuzzy nonhomogeneous higher level Markov jump systems with uncertain transition probabilities. *IEEE Trans Fuzzy Syst*. 2022;30(7):2487-2499.
7. Cheng P, He S, Stojanovic V, Luan X, Liu F. Fuzzy fault detection for Markov jump systems with partly accessible hidden information: an event-triggered approach. *IEEE Trans Cybern*. 2022;52(8):7352-7361.
8. 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):2279-2287.
9. Zhang W, Wang Z, Raïssi T, Shen Y. Fault detection for Takagi–Sugeno fuzzy systems using multiple observers and ellipsoidal analysis. *Int J Robust Nonlinear Control*. 2023;33(4):2811-2839.
10. Dong Y, Song Y, Wei G. Efficient model-predictive control for nonlinear systems in interval type-2 T-S fuzzy form under round-robin protocol. *IEEE Trans Fuzzy Syst*. 2022;30(1):63-74.
11. Zhang Z, Niu Y, Lam HK. Sliding-mode control of T–S fuzzy systems under weighted try-once-discard protocol. *IEEE Trans Cybern*. 2020;50(12):4972-4982.
12. Yuan Y, Zhang P, Wang Z, Chen Y. Noncooperative event-triggered control strategy design with round-robin protocol: applications to load frequency control of circuit systems. *IEEE Trans Ind Electron*. 2020;67(3):2155-2166.
13. Geng H, Wang Z, Zou L, Mousavi A, Cheng Y. Protocol-based tobit Kalman filter under integral measurements and probabilistic sensor failures. *IEEE Trans Signal Process*. 2021;69:546-559.
14. Luo Y, Wang Z, Chen Y, Yi X. H_∞ state estimation for coupled stochastic complex networks with periodical communication protocol and intermittent nonlinearity switching. *IEEE Trans Netw Sci Eng*. 2021;8(2):1414-1425.
15. Liu J, Gong E, Zha L, Tian E, Xie X. Observer-based security fuzzy control for nonlinear networked systems under weighted try-once-discard protocol. *IEEE Trans Fuzzy Syst*. doi:10.1109/TFUZZ.2023.3269786
16. Wu B, Chang XH. Security control for nonlinear systems under quantization and round-robin protocol subject to deception attacks. *ISA Trans*. 2022;130:25-34.
17. Dong Y, Song Y, Zhang B. Model predictive control for nonlinear systems in Takagi-Sugeno's form under round-robin protocol. *J Franklin Inst*. 2020;357(12):7597-7616.
18. Gao M, Zhang W, Sheng L, Zhou D. Distributed fault estimation for delayed complex networks with round-robin protocol based on unknown input observer. *J Franklin Inst*. 2020;357(13):8678-8702.

19. Shen H, Men Y, Cao J, Park JH. H_∞ filtering for fuzzy jumping genetic regulatory networks with round-robin protocol: a hidden-Markov-model-based approach. *IEEE Trans Fuzzy Syst*. 2020;28(1):112-121.
20. Zha L, Liao R, Liu J, Xie X, Cao J, Xiong L. Finite-time adaptive event-triggered asynchronous state estimation for Markov jump systems with cyber-attacks. *Int J Robust Nonlinear Control*. 2022;32(2):583-599.
21. Zha L, Liao R, Liu J, Xie X, Tian E, Cao J. Dynamic event-triggered output feedback control for networked systems subject to multiple cyber attacks. *IEEE Trans Cybern*. 2022;52(12):13800-13808.
22. Gu Z, Shi P, Yue D, Yan S, Xie X. Memory-based continuous event-triggered control for networked T–S fuzzy systems against cyberattacks. *IEEE Trans Fuzzy Syst*. 2021;29(10):3118-3129.
23. Fan M, Tian E, Xp X, Yue D, Cao T. Stochastic data-based denial-of-service attack strategy design against remote state estimation in interval type-2 T–S fuzzy systems. *IEEE Trans Fuzzy Syst*. 2023;31(3):825-834.
24. Zhao D, Wang Z, Ho DWC, Wei G. Observer-based PID security control for discrete time-delay systems under cyber-attacks. *IEEE Trans Syst Man Cybern: Syst*. 2021;51(6):3926-3938.
25. Li Y, Song F, Liu J, Xie X, Tian E. Decentralized event-triggered synchronization control for complex networks with nonperiodic DoS attacks. *Int J Robust Nonlinear Control*. 2022;32(3):1633-1653.
26. Qu F, Tian E, Zhao X. Chance-constrained H_∞ state estimation for recursive neural networks under deception attacks and energy constraints: the finite-horizon case. *IEEE Trans Neural Netw Learn Syst*. 2022;1-12.
27. Han F, Wang Z, Dong H, Alsaadi FE, Alharbi KH. A local approach to distributed H_∞-consensus state estimation over sensor networks under hybrid attacks: dynamic event-triggered scheme. *IEEE Trans Signal Inf Process Netw*. 2022;8:556-570.
28. Geng H, Wang Z, Alsaadi FE, Alharbi KH, Cheng Y. Protocol-based fusion estimator design for state-saturated systems with dead-zone-like censoring under deception attacks. *IEEE Trans Signal Inf Process Netw*. 2022;8:37-48.
29. Liu J, Yin T, Cao J, Yue D, Karimi HR. Security control for T–S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks. *IEEE Trans Syst Man Cybern: Syst*. 2021;51(10):6544-6554.
30. Sakthivel R, Kwon OM, Park MJ, Choi SG, Sakthivel R. Robust asynchronous filtering for discrete-time T-S fuzzy complex dynamical networks against deception attacks. *IEEE Trans Fuzzy Syst*. 2022;30(8):3257-3269.
31. Sun HY, Han HG, Sun J, Yang HY, Qiao JF. Security control of sampled-data T–S fuzzy systems subject to cyberattacks and successive packet losses. *IEEE Trans Fuzzy Syst*. 2023;31(4):1178-1188.
32. Jiang Y, Yin S. Recent advances in key-performance-indicator oriented prognosis and diagnosis with a MATLAB toolbox: DB-KIT. *IEEE Trans Industr Inform*. 2019;15(5):2849-2858.
33. Wei B, Tian E, Zhang T, Zhao X. Probabilistic-constrained H_∞ tracking control for a class of stochastic nonlinear systems subject to dos attacks and measurement outliers. *IEEE Trans Circuits Syst I: Regul Pap*. 2021;68(10):4381-4392.
34. Nguyen AT, Campos V, Guerra TM, Pan J, Xie W. Takagi–Sugeno fuzzy observer design for nonlinear descriptor systems with unmeasured premise variables and unknown inputs. *Int J Robust Nonlinear Control*. 2021;31(17):8353-8372.
35. Liu J, Gong E, Zha L, Xie X, Tian E. Outlier-resistant recursive security filtering for multirate networked systems under fading measurements and round-robin protocol. *IEEE Trans Control Netw Syst*. doi:10.1109/TCNS.2023.3256299
36. Fang F, Liu Y, Park JH, Liu Y. Outlier-resistant non-fragile control of T-S fuzzy neural networks with reaction-diffusion terms and its application in image secure communication. *IEEE Trans Fuzzy Syst*. doi:10.1109/TFUZZ.2023.3239732
37. Li J, Wang Z, Dong H, Ghinea G. Outlier-resistant remote state estimation for recurrent neural networks with mixed time-delays. *IEEE Trans Neural Netw Learn Syst*. 2021;32(5):2266-2273.
38. Geng H, Wang Z, Mousavi A, Alsaadi FE, Cheng Y. Outlier-resistant filtering with dead-zone-like censoring under try-once-discard protocol. *IEEE Trans Signal Process*. 2022;70:714-728.
39. Mousavinejad E, Ge X, Han QL, Yang F, Vlacic L. Resilient tracking control of networked control systems under cyber attacks. *IEEE Trans Cybern*. 2021;51(4):2107-2119.
40. Fu M, Xie L. The sector bound approach to quantized feedback control. *IEEE Trans Automat Contr*. 2005;50(11):1698-1711.

How to cite this article: Zha L, Huang T, Liu JL, Xie X, Tian E. Outlier-resistant quantized control for T-S fuzzy systems under multi-channel-enabled round-robin protocol and deception attacks. *Int J Robust Nonlinear Control*. 2023;33(18):10916-10931. doi: 10.1002/rnc.6919

APPENDIX A

A.1 Proof of Theorem 1

Construct a Lyapunov–Krasovskii function as

$$V(k) = \eta^T(k)P_r\eta(k) \tag{A1}$$

Given that $\mathbb{E}\{\alpha(k)-\overline{\alpha}\}=0$, $\mathbb{E}\{(\alpha(k)-\overline{\alpha})^2\}=\overline{\alpha}(1-\overline{\alpha})$, take expectations of the difference $\Delta V(k)=V(k+1)-V(k)$, we get

$$
\begin{aligned}
\mathbb{E}\{\Delta V(k)\} &= \mathbb{E}\{\eta^T(k+1)P_{r+1}\eta(k+1)-\eta^T(k)P_r\eta(k)\} \\
&= \mathbb{E}\Bigg\{\sum_{i=1}^{s}\sum_{j=1}^{s}h_i(\vartheta(k))h_j(\vartheta(k))\Big[\vec{A}_{ij,r}\eta(k)+\vec{B}_{i,r}\varphi(y(k)) \\
&\quad +(\alpha(k)-\overline{\alpha}+\overline{\alpha})\vec{B}_{i,r}g(x(k)+\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big]^T \\
&\quad P_{r+1}\Big[\vec{A}_{ij,r}\eta(k)+\vec{B}_{i,r}\varphi(y(k))+(\alpha(k)-\overline{\alpha}+\overline{\alpha})\vec{B}_{i,r}g(x(k)) \\
&\quad +\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big]-\eta^T(k)P_r\eta(k)\Bigg\} \\
&= \mathbb{E}\Bigg\{\sum_{i=1}^{s}\sum_{j=1}^{s}h_i(\vartheta(k))h_j(\vartheta(k))\Big[\vec{A}_{ij,r}\eta(k)+\vec{B}_{i,r}\varphi(y(k)) \\
&\quad +\overline{\alpha}\vec{B}_{i,r}g(x(k)+\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big]^T P_{r+1}\Big[\vec{A}_{ij,r}\eta(k) \\
&\quad +\vec{B}_{i,r}\varphi(y(k))+\overline{\alpha}\vec{B}_{i,r}g(x(k))+\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big] \\
&\quad +(\alpha(k)-\overline{\alpha})^2(\vec{B}_{i,r}g(x(k))^T P_{r+1}\vec{B}_{i,r}g(x(k))-\eta^T(k)P_r\eta(k)\Bigg\} \\
&= \mathbb{E}\Bigg\{\sum_{i=1}^{s}\sum_{j=1}^{s}h_i(\vartheta(k))h_j(\vartheta(k))\Big[\vec{A}_{ij,r}\eta(k)+\vec{B}_{i,r}\varphi(y(k)) \\
&\quad +\overline{\alpha}\vec{B}_{i,r}g(x(k)+\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big]^T P_{r+1}\Big[\vec{A}_{ij,r}\eta(k) \\
&\quad +\vec{B}_{i,r}\varphi(y(k))+\overline{\alpha}\vec{B}_{i,r}g(x(k))+\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big] \\
&\quad +\overline{\alpha}(1-\overline{\alpha})(\vec{B}_{i,r}g(x(k))^T P_{r+1}\vec{B}_{i,r}g(x(k))-\eta^T(k)P_r\eta(k)\Bigg\}
\end{aligned}
$$

In light of (8), (20), (21), (A1), and (A2), we can further derive that

$$
\begin{aligned}
\mathbb{E}\{\Delta V(k)\} \le{}& \mathbb{E}\Bigg\{\sum_{i=1}^{s}\sum_{j=1}^{s}h_i(\vartheta(k))h_j(\vartheta(k))\Big[\vec{A}_{ij,r}\eta(k)+\vec{B}_{i,r}\varphi(y(k)) \\
&+\overline{\alpha}\vec{B}_{i,r}g(x(k))+\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big]^T P_{r+1}\Big[\vec{A}_{ij,r}\eta(k) \\
&+\vec{B}_{i,r}\varphi(y(k))+\overline{\alpha}\vec{B}_{i,r}g(x(k))+\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big] \\
&+\overline{\alpha}(1-\overline{\alpha})(\vec{B}_{i,r}g(x(k))^T P_{r+1}\vec{B}_{i,r}g(x(k))-\eta^T(k)P_r\eta(k) \\
&-\mu_0\phi^T(\overline{y}(k)-\hat{y}(k))\phi(\overline{y}(k)-\hat{y}(k))+\mu_0\phi^T(\overline{y}(k)-\hat{y}(k)) \\
&N(\overline{y}(k)-\hat{y}(k))-\mu_1\varphi^T(y(k))\varphi(y(k))+\mu_1\varphi^T(y(k))Hy(k) \\
&-g^T(x(k))g(x(k))+x^T(k)S^TSx(k)\Bigg\} \\
={}& \mathbb{E}\Bigg\{\sum_{i=1}^{s}\sum_{j=1}^{s}h_i(\vartheta(k))h_j(\vartheta(k))\Big[\vec{A}_{ij,r}\eta(k)+\vec{B}_{i,r}\varphi(y(k)) \\
&+\overline{\alpha}\vec{B}_{i,r}g(x(k))+\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big]^T P_{r+1}\Big[\vec{A}_{ij,r}\eta(k) \\
&+\vec{B}_{i,r}\varphi(y(k))+\overline{\alpha}\vec{B}_{i,r}g(x(k))+\vec{D}_{i,r}\phi(\overline{y}(k)-\hat{y}(k))\Big]
\end{aligned}
$$

$$
\begin{aligned}
&+\overline{\alpha}(1-\overline{\alpha})g^T(x(k)\vec{B}_{i,r}^TP_{r+1}\vec{B}_{i,r}g(x(k))-\eta^T(k)P_r\eta(k)\\
&-\mu_0\phi^T(\overline{y}(k)-\hat{y}(k))\phi(\overline{y}(k)-\hat{y}(k))+\mu_0\phi^T(\overline{y}(k)-\hat{y}(k))\\
&N(G_{j,r}\eta(k)+\Phi_r\varphi(y(k))+\overline{\alpha}\Phi_r g(x(k)))\\
&-\mu_1\varphi^T(y(k))\varphi(y(k))+\mu_1\varphi^T(y(k))HC_i\theta\eta(k)\\
&\left.-g^T(x(k))g(x(k))+\eta^T(k)\theta^TS^TS\theta\eta(k)\right\}
\end{aligned} \tag{A2}
$$

According to schur complement, it can be concluded that

$$
\mathbb{E}\{\Delta V(k)\}\le\xi^T(k)\left(\Sigma_{ij,r}+\Xi_5^{ij,r\,T}P_{r+1}^{-1}\Xi_5^{ij,r}+\Xi_6^{i,r\,T}P_{r+1}^{-1}\Xi_6^{i,r}\right)\xi(k)<0 \tag{A3}
$$

where

$$
\Sigma_{ij,r}=\begin{bmatrix}\Xi_{11}^r & * & * & *\\ \Xi_{21}^i & -\mu_1 I & * & *\\ 0 & 0 & -I & *\\ \Xi_{41}^{j,r} & \Xi_{42}^r & \Xi_{43}^r & -\mu_0 I\end{bmatrix},
$$

$$
\Xi_5^{ij,r}=\begin{bmatrix}\Xi_{51}^{ij,r} & \Xi_{52}^{i,r} & \Xi_{53}^{i,r} & \Xi_{54}^{i,r}\end{bmatrix},\Xi_6^{i,r}=\begin{bmatrix}0 & 0 & \Xi_{63}^{i,r} & 0\end{bmatrix},
$$

$$
\xi^T(k)=\begin{bmatrix}\eta^T(k) & \varphi^T(y(k)) & g^T(x(k)) & \phi^T(\overline{y}(k)-\hat{y}(k))\end{bmatrix}.
$$

Obviously, $\Delta V(k)<0$ holds from (22). This completes the proof.

A.2 Proof of Theorem 2

Set $P_r=diag\{\overline{P}_r,\tilde{P}_r,\overline{P}_r\}$. Then, (22) is equivalent to the following inequality:

$$
\Xi_{ij,r}=\begin{bmatrix}\Xi_{11}^r & * & * & * & * & *\\ \Xi_{21}^i & -\mu_1 I & * & * & * & *\\ 0 & 0 & -I & * & * & *\\ \Xi_{41}^{j,r} & \Xi_{42}^r & \Xi_{43}^r & -\mu_0 I & * & *\\ \Psi_{51}^{ij,r} & \Psi_{52}^{i,r} & \Psi_{53}^{i,r} & \Psi_{54}^{i,r} & -P_{r+1} & *\\ 0 & 0 & \Psi_{63}^{i,r} & 0 & 0 & -P_{r+1}\end{bmatrix}<0 \tag{A4}
$$

where

$$
\Psi_{51}^{ij,r}=\begin{bmatrix}\Upsilon_{11}^{ij,r} & 0 & -\overline{P}_{i+1}B_iK_{j,r}\\ \Upsilon_{21}^{i,r} & \tilde{P}_{i+1}\Gamma(k) & 0\\ \Upsilon_{31}^{ij,r} & \Upsilon_{32}^{i,r} & \Upsilon_{33}^{ij,r}\end{bmatrix},\quad \Psi_{52}^{i,r}=\begin{bmatrix}0\\ \tilde{P}_{i+1}\Phi_r\\ -\overline{P}_{i+1}L_{i,r}N_1\Phi_r\end{bmatrix},
$$

$$
\Psi_{53}^{i,r}=\begin{bmatrix}0\\ \overline{\alpha}\tilde{P}_{r+1}\Phi_r\\ -\overline{\alpha}\overline{P}_{i+1}L_{i,r}N_1\Phi_r\end{bmatrix},\quad \Psi_{54}^{i,r}=\begin{bmatrix}0\\ 0\\ -\overline{P}_{i+1}L_{i,r}\end{bmatrix},
$$

$$
\Psi_{63}^{i,r}=\begin{bmatrix}0\\ \sqrt{\overline{\alpha}(1-\overline{\alpha})}\tilde{P}_{r+1}\Phi_r\\ -\sqrt{\overline{\alpha}(1-\overline{\alpha})}\overline{P}_{i+1}L_{i,r}N_1\Phi_r\end{bmatrix},\quad \Upsilon_{11}^{ij,r}=\overline{P}_{r+1}A_i+\overline{P}_{r+1}B_iK_{j,r},
$$

$$
\Upsilon_{21}^{i,r}=\tilde{P}_{r+1}\Phi_rH_1C_i,\ \Upsilon_{31}^{ij,r}=\overline{P}_{i+1}L_{i,r}N_1(C_j-\Phi_rH_1C_j),
$$

$$\Upsilon_{32}^{i,r} = -\overline{P}_{i+1} L_{i,r} N_1 \Gamma(k), \Upsilon_{33}^{ij,r} = \overline{P}_{r+1} A_i - \overline{P}_{i+1} L_{i,r} N_1 C_j.$$

Note that the singular value decomposition (SVD) for $B_i \in \mathbb{R}^{m\times n}$ with the full rank matrix is $B_i = O_i \begin{bmatrix} Q_i \\ 0 \end{bmatrix} V_i^T$, in which $O_i^T O_i = I$ and $V_i^T V_i = I$. By using lemma 1 in Reference 22, one can get that there exists $\overline{P}_{r+1}^{1} = V_i Q_i^{-1} U_i Q_i V_i^T$ satisfying $\overline{P}_{r+1} B_i = B_i \overline{P}_{r+1}^{1}$, where $\overline{P}_{r+1} = O_i \begin{bmatrix} U_i & 0 \\ 0 & W_i \end{bmatrix} O_i^T$.

Replace $\overline{P}_{r+1} B_i$ with $B_i \overline{P}_{r+1}^{1}$ and define $Y_{i,r} \triangleq \overline{P}_{r+1} L_{i,r}$ and $X_{j,r} \triangleq \overline{P}_{r+1}^{1} K_{j,r}$, then (23) can be derived from (A4). This concludes the proof.