IMPROVED DYNAMIC MEMORY-BASED EVENT-TRIGGERED CONTROL FOR T-S FUZZY SYSTEMS UNDER HYBRID CYBER-ATTACKS

ZIXIAN CHEN[1], HUIYAN ZHANG[2,3,*], YU HUANG[1], JIANGYAN ZOU[3], PENGDA LIU[2], RONGNI YANG[4]

[1]School of Mechanical Engineering, Chongqing Technology and Business University, Chongqing, 400067, China
[2]National Research Base of Intelligent Manufacturing Service, Chongqing Technology and Business University, Chongqing, 400067, China
[3]Chongqing Engineering Laboratory for Detection Control and Integrated Systems, Chongqing Technology and Business University, Chongqing, 400067, China
[4]School of Control Science and Engineering, Shandong University, Jinan, 250100, China
E-MAIL: {chenzixian, huiyanzhang, huangyu, zoujiangyan, liupengda}@ctbu.edu.cn, rnyang@sdu.edu.cn

Abstract:

This paper investigates the robust control problem for Takagi-Sugeno (T-S) fuzzy systems subject to hybrid cyber-attacks, encompassing both Denial-of-Service (DoS) attacks and deception attacks. A novel dynamic memory-based event-triggered mechanism (DMETM) is proposed, which incorporates not only the most recent triggering instant but also multiple historical triggering instants, with the specific number of considered instants being determined by the system's state. Furthermore, a dynamic output feedback controller (DOFC) is designed, and its parameters are derived by solving Linear Matrix Inequalities (LMIs) through the construction of an appropriate Lyapunov function. The method guarantees the closed-loop system's asymptotic stability and meets the predefined H_∞ performance level γ. Finally, a rigorous proof is mentioned to illustrate the absence of Zeno behavior in this control scheme.

Keywords:

Dynamic memory-based event-triggered mechanism, T-S fuzzy system, hybrid cyber-attacks

1 Introduction

In recent years, T-S fuzzy systems have garnered significant attention in the control field due to their remarkable approximation capabilities for complex nonlinear systems. These systems have been extensively applied in various practical engineering domains, including robotic manipulators [1], mechatronic systems [2] and marine vehicles [3]. With the increasing integration of T-S fuzzy systems into networked control systems and their deployment in critical infrastructure as part of cyber-physical systems, the security of these systems has become a paramount concern. In [4], authors propose a resilient event-triggered H_∞ filtering approach for networked switched T-S fuzzy systems under DoS attacks. A switching fuzzy filter is designed to handle asynchronous system-filter modes caused by attacks and ETS. Then, a security-based fuzzy model predictive control approach for discrete-time T-S fuzzy systems subjected to output deception attacks is proposed in [5]. In this approach, dynamic output-feedback control is employed and a worst-case optimization problem is formulated to address system nonlinearity and mitigate the impacts of deception attacks. In [6], the asynchronous event-triggered control problem for switched T-S fuzzy systems subjected to data injection attacks is investigated. The study addresses the asynchronous switching behavior between subsystems and subcontrollers induced by sampled switching signals and sufficient conditions are derived to ensure exponential stability and performance of the system under data injection attacks. It is noteworthy that the aforementioned references primarily focus on individual types of cyber-attacks. The coexistence of different attack types not only exacerbates the complexity of system vulnerabilities but also necessitates the development of advanced control mechanisms that can ensure system stability and maintain desired performance under such ad-

verse conditions.

Communication resources are highly valuable for CPS, over the past decade, researchers have proposed numerous strategies to conserve these resources. Examples include static event-triggered mechanisms [7], dynamic event-triggered mechanisms [8], adaptive event-triggered mechanisms [9], and resilient event-triggered mechanisms [4]. Authors in [10] explore the development of event-triggered controllers for positive T-S fuzzy systems incorporating Markovian stochastic time delays, proposing a controller that switches at different event-triggered instants and deriving design criteria through a Lyapunov function to ensure system positivity and stability. The criteria are solvable via linear programming, guarantee a positive lower bound on inter-execution time to avoid Zeno behavior. Compared to static event-triggered mechanism (SETM) and dynamic event-triggered mechanism (DETM) further conserve communication resources by introducing a non-negative internal dynamic variable, which adaptively adjusts the triggering threshold based on real-time system conditions. Subsequently, a novel DETM is proposed in [11], featuring a specially designed threshold parameter to optimize computational resource utilization. The challenges of data dropouts, time delays, and environmental disturbances are addressed through a hidden Markov model, which is employed to represent the asynchronization between the system and the controller. However, conventional ETM, whether they are static or adaptive, often rely solely on the last triggering instant and the current sampling time and overlook the potential advantages of incorporating multiple previous triggering instants, particularly in scenarios where cyber-attacks may generate numerous false data points. This oversight can lead to inefficient resource utilization and diminished system performance. Consequently, this has prompted us to consider dynamic DMETM. Taking into account all the above factors, the key contributions of this study are outlined as follows:

1. In contrast to the work presented in [4], which exclusively considers DoS attacks, and [5], which solely addresses deception attacks, this paper investigates a more comprehensive scenario where the system is simultaneously subjected to both DoS and deception attacks. The proposed controller demonstrates reduced conservatism compared to existing approaches.

2. Compared to the static ETM employed in [7] and the AETM utilized in [9], this study introduces a novel dynamic memory-based ETM. While the triggering conditions in the aforementioned literatures depend solely on the last triggering instant and the current sampling instant, our proposed dynamic memory-based event-triggering mechanism incorporates multiple previous triggering instants (no fewer than one), thereby enhancing the system's performance and flexibility.

3. By incorporating DETM, the proposed feedback controller can systematically leverage historical triggering information for more informed control decisions. This advanced mechanism demonstrates superior performance in mitigating signal distortions caused by DoS attacks and deception attacks, ensuring robust closed-loop stability under adversarial conditions.

2 Problem Formulation

Consider a class of T-S fuzzy systems subject to hybrid cyber-attacks and external disturbances, described as follows:

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{k} f_i\big(m(t)\big)\big(A_i x(t) + B_i \bar{u}(t) + C_i \omega(t)\big), \\ z(t) = \sum_{i=1}^{k} f_i\big(m(t)\big) D_i x(t), \\ y(t) = \sum_{i=1}^{k} f_i\big(m(t)\big) E_i x(t), \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ denotes the state vector, $\bar{u}(t) \in \mathbb{R}^m$ represents the control input, and $\omega(t) \in \mathbb{R}^p$ means an exogenous disturbance belonging to the space $L_2[0, \infty)$. The system outputs are defined as $y(t) \in \mathbb{R}^q$ for the measured output and $z(t) \in \mathbb{R}^r$ for the controlled output. The T-S fuzzy system dynamics are characterized by constant matrices A_i, B_i, C_i, D_i, and E_i, which govern the relationships between the inputs, states, and outputs. $f_i(m(t)), i \in \mathbb{N}^*$ meets $\sum_{i=1}^{k} f_i(m(t)) = 1, f_i(m(t)) \in [0, 1]$.

In this section, both DoS attacks and deception attacks are taken into consideration. Inspired by [13], these attacks are represented through a Bernoulli process. Consequently, the signal received by the actuator can be described as follows:

$$\bar{u}(t) = \alpha_1(t)u(t) + (1 - \alpha_1(t))\alpha_2(t)\chi(t) \tag{2}$$

where $\chi(t)$ represents the deception attack, which is bounded by $\vartheta > 0$. The variables $\alpha_1(t)$ and $\alpha_2(t)$ follow Bernoulli-distributed processes and are used to model the occurrence of DoS attacks and deception attacks, respectively. Additionally, their expected values are defined as $\mathbb{E}(\alpha_1(t)) = \alpha_1, \mathbb{E}(\alpha_2(t)) = \alpha_2$. Incorporating these considerations, the detailed formulation is presented as follows:

1. If $\alpha_1(t) = 1$ for all $\alpha_2(t)$, no cyber-attack occurs;
2. If $\alpha_1(t) = 0$ and $\alpha_2(t) = 0$, a DoS attack occurs;
3. If $\alpha_1(t) = 0$ and $\alpha_2(t) = 1$, a Deception attack occurs.

Remark 1. This paper presents a more comprehensive approach by simultaneously considering both types of cyber-attacks. This integrated consideration of multiple attack vectors demonstrates reduced conservatism in our security framework.

The structure of the microsensor is illustrated in Figure 1. The sampler operates with a fixed sampling period h. Upon receiving the output signal $y(kh)$, the event generator determines whether to update the control signal. The set of successful triggering instants is defined as $\mathcal{H}_1 = \{t_1, t_2, \ldots, t_k\}, \quad k \in \mathbb{N}^*$. Let the current sampling instant be denoted as $t_k^i = t_k + ih, \quad i \in \mathbb{N}^*$. Based on this, the DMETM is formulated as follows:

$$t_{k+1} = \inf\left\{t > t_k \mid \mathcal{H}\left(y(t_k), y(t_k^i)\right) > 0\right\} \tag{3}$$

where $\mathcal{M}\left(y(t_k), y(t_k^i)\right) = \sum_{j=0}^{[w(t)]-1} u_j\, e_{k-j}^T(t)\, \Phi\, e_{k-j}(t) - \sigma y^T(t_{kj})\Phi y(t_{kj})$. $[w(t)] = \mu_1(1+\frac{2}{\pi}\arctan||y(t_k)-y(t_k^l)||)$, $\mu_1 > 0$. The error vector is $e_{k-j}(t) = y(t_{k-j}) - y(t_k^l)$, $j \in \{0, 1, \ldots, [w(t)]-1\}$, $\mathcal{Y}(t_{kj}) = \frac{1}{[w(t)]}\sum_{j=0}^{[w(t)]-1}\mathcal{Y}(t_{k-j})$, the weighting parameters u_j satisfy $\sum_{j=0}^{[w(t)]-1} u_j = 1$, $\sigma \in (0, 1]$ and $u_0 > u_1 > ... > u_{[w(t)]-1}$, ensuring that recent triggering instants are given greater importance. Here, $\sigma \in (0, 1]$ denotes the event-triggered parameter, $[w(t)]$ denotes the floor function of $w(t)$, which rounds $w(t)$ down to the nearest integer, and Φ represents the event-triggered matrix to be designed.

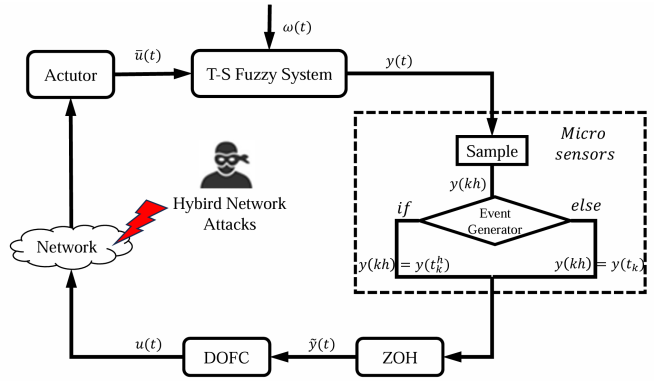

FIGURE 1. The structure of the DMETM.

Next, given the linear segment function $\tau_k(t) = t - t_k^i, \underline{\tau} < \tau_k(t) < \bar{\tau}$, the output signal $\tilde{y}(t_k)$ can be rewritten as

$$\tilde{y}(t_k) = \sum_{j=0}^{[w(t)]-1}\left(y(t-\tau_k(t)) + e_{k-j}(t)\right), \tag{4}$$

with $t \in [t_k + \tau_k,\, t_{k+1} + \tau_{k+1})$.

Remark 2. In contrast to [12], which only considers the current instant and the most recent trigger instant, our proposed DMETM incorporates multiple historical triggering instants. This approach significantly reduces conservatism, particularly in scenarios where the system is subjected to hybrid network attacks. By leveraging a broader range of past triggering instants, the DMETM enhances flexibility and robustness, ensuring more efficient and reliable system performance under complex attack conditions.

In this study, the state vector is assumed to be unmeasurable. To address this, a DOFC is introduced to stabilize the closed-loop system. The signal received by the DOFC is continuous, as it is processed by a zero-order hold that converts the discrete signal transmitted from the event trigger into a continuous one. Under the proposed DMETM, the event-triggered fuzzy DOFC is formulated as follows:

Plant rule j: IF $m_1^j(t_k)$ is M_1^j, ..., and $m_\vartheta(t_k)$ is M_ϑ^j Then

$$\begin{cases} \dot{x}_C(t) = A_{Cj}x_C(t) + B_{Cj}\tilde{y}(t_k), \\ u(t) \;\; = C_{Cj}x_C(t) \end{cases} \tag{5}$$

where $x_C(t) \in \mathbb{R}^p$ represents the state vector, $\tilde{y}(t) \in \mathbb{R}^q$ means the output signal of the event generator, and A_C, B_C, C_C are the controller matrices with approximate dimension to be designed. Then the de-fuzzified output of fuzzy controller rules (4) are obtained as

$$\begin{cases} \dot{x}_C(t) = \sum_{j=1}^{k}\sum_{\nu=0}^{[w(t)]-1} f_j(m(t))\Big\{A_{Cj}x_C(t) \\ \qquad\qquad +B_{Cj}\Big[E_i x\big(t-\tau_k(t)\big) + e_{k-\nu}(t)\Big]\Big\}, \\ u(t) \;\; = \sum_{j=1}^{k} f_j(m(t))\, C_{Cj}x_C(t). \end{cases} \tag{6}$$

For simplicity, $f_i(m(t))$ and $f_j(m(t))$ are abbreviated as f_i and f_j, respectively. By integrating all the aforementioned considerations, the augmented system can be

reformulated as follows.

$$\begin{cases} \dot{\xi}(t) = \sum_{i=1}^{k}\sum_{j=1}^{k}\sum_{\nu=0}^{[w(t)]-1} f_i f_j(\bar{A}\xi(t) + \bar{B}\xi(t-\tau_k(t)) \\ \qquad + \bar{C}\vartheta(t) + \bar{E}e_{k-\nu}(t)), \\ z(t) = \sum_{i=1}^{k}\sum_{j=1}^{k} f_i f_j(\bar{D}\xi(t)), \quad t \in [t_k+\tau_k, t_{k+1}+\tau_{k+1}), \\ \qquad k = 1, 2, \dots \\ \xi(t) = \psi_o, \quad t \in [-\bar{\tau}, 0), \end{cases} \tag{7}$$

where $\xi(t) = [x^T(t)\ x_C^T(t)]^T$, $\vartheta(t) = [\omega^T(t)\ \chi^T(t)]^T$, ψ_o is the initial value, and

$$\bar{A} = A_{0ij} + (\alpha_1(t) - \alpha_1)\bar{A}_{0ij},\ A_{0ij} = \begin{bmatrix} A_i & a_1 B_i C_{Cj} \\ 0 & A_{Cj} \end{bmatrix},$$

$$\bar{A}_{0ij} = \begin{bmatrix} 0 & B_i C_{Cj} \\ 0 & 0 \end{bmatrix},\ \bar{C} = C_{0ij} + ((\alpha_1(t) - \alpha_1)\alpha_2$$

$$+ (1-\alpha_1)(\alpha_2(t) - \alpha_2) - (\alpha_1(t) - \alpha_1)(\alpha_2(t) + \alpha_2))\bar{C}_{0ij},$$

$$C_{0ij} = \begin{bmatrix} C_i & (1-\alpha_1)\alpha_2 B_i \\ 0 & 0 \end{bmatrix},\ \bar{C}_{0ij} = \begin{bmatrix} 0 & B_i \\ 0 & 0 \end{bmatrix},$$

$$\bar{B} = \begin{bmatrix} 0 & 0 \\ B_{Cj}E_i & 0 \end{bmatrix},\ \bar{E} = \begin{bmatrix} 0 \\ B_{Cj} \end{bmatrix},\ \bar{D} = \begin{bmatrix} D_i & 0 \end{bmatrix}.$$

Before deriving the sufficient conditions of the augmented system (7) satisfy the H_∞ performance with index γ, a definition is given as follows.

Definition 1. For non-zero disturbance $\vartheta(t)$, if the augmented system satisfies the following inequality with zero initial conditions,

$$\int_0^{+\infty} z^T(t)z(t)dt < \gamma^2 \int_0^{+\infty} \vartheta^T(t)\vartheta(t)dt, \tag{8}$$

it is said that the closed-loop system meet the H_∞ performance criterion with the prescribed performance level γ.

3 Main Result

Theorem 1 establishes and proves a sufficient condition for the closed-loop system to achieve asymptotic stability and satisfy the H_∞ performance index γ under hybrid cyber-attacks. Theorem 2 provides a method for designing the corresponding DOFC, with the proof omitted due to space constraints. Additionally, a Corollary is presented, which employs a proof by contradiction to demonstrate that the proposed DMETM avoids Zeno behavior.

Theorem 1. For given scalars $\alpha_1, \alpha_2, \mu_1 > 0$, $\sigma \in (0, 1]$, and $u_\nu, \nu \in \{0, 1, ..., [w(t)] - 1\}$, the closed-loop T-S fuzzy system is asymptotically stable with a prescribed performance level, provided that there exist positive definite matrices and with appropriate dimensions satisfying the following linear matrix inequalities:

$$\begin{bmatrix} \Xi_{1ij} & \Xi_{2ij} \\ * & \Xi_{3ij} \end{bmatrix} < 0, \quad i, j = 1, 2, ..., v \in \{0, 1, ..., [w(t)] - 1\},$$

where

$$\Xi_{1ij} = \begin{bmatrix} A_{0ij}^T P + P A_{0ij} + R + \bar{D}^T\bar{D} & P\bar{B} \\ * & E_{1i}^T \Phi E_{1i} - R \end{bmatrix},$$

$$\Xi_{2ij} = \begin{bmatrix} P\bar{E} & PC_{0ij} \end{bmatrix}, \quad \Xi_{3ij} = -\mathrm{diag}\{u, \Phi, \gamma^2 I\}.$$

Proof. The Lyapunov function is constructed as

$$V(t) = \xi^T(t)P\xi(t) + \int_{t-\tau(t)}^{t} \xi^T(s)R\xi(s)ds \tag{9}$$

Following the approach in [13], the infinitesimal generator is utilized to characterize the derivative of the Lyapunov function $V(t)$ along the system's trajectory. Subsequently, we obtain:

$$\mathcal{L}V(t) = \lim_{\Delta\to 0} \frac{\mathbb{E}\{V(\xi(t+\Delta)) \mid \xi(t)\} - V(\xi(t))}{\Delta} \tag{10}$$

where $\Delta > 0$ is defined as a small positive scalar. By taking the expectation of $\bar{A}, \bar{B}, \bar{C}, \bar{D}$, and $\bar{E}$, and leveraging Equation (7), the following result can be derived:

$$\mathbb{E}\{\bar{A} \quad \bar{C}\} = \{A_{0ij} \quad C_{0ij}\}. \tag{11}$$

Next, substituting (10) to (9), it can be derived that

$$\begin{aligned} \mathcal{L}V(t) = &\sum_{j=1}^{k}\sum_{j=1}^{k}\sum_{v=0}^{[w(t)]-1} f_i f_j(\xi^T(t)(\bar{A}^T P + P\bar{A})\xi(t) \\ &+ 2\xi^T(t)P\bar{B}\xi(t-\tau_k(t)) \\ &+ 2\xi^T(t)P\bar{C}\vartheta(t) + 2\xi^T(t)P\bar{E}e_{k-v}(t) \\ &+ \xi^T(t)R\xi(t) - \xi^T(t-\tau_k(t))R\xi(t-\tau_k(t))). \end{aligned}$$

To derive sufficient conditions, the supply rate function $J(t)$ is selected as follows:

$$J(t) = \mathbb{E}\left\{\int_0^\infty \left(z^T(t)z(t) - \gamma^2\vartheta^T(t)\vartheta(t)\right)dt\right\}. \tag{12}$$

By incorporating the DMETM condition (3) into the augmented system (7), the following relationship holds for $t \in [t_k, t_{k+1})$

$$\sum_{\nu=0}^{[w(t)]-1} u_j e_{k-\nu}^T(t)\Phi e_{k-\nu}(t) - \frac{\sigma}{[w(t)]}\xi^T(t-\tau_k(t))E_{1i}^T\Phi E_{1i}\xi(t-\tau_k(t)) < 0$$

where $E_{1i} = \text{diag}\{E_i, 0\}$. Then, it follows that

$$\begin{aligned} J(t) = \mathbb{E}\Big\{ \int_0^\infty \big(z^T(t)z(t) - \gamma^2\vartheta^T(t)\vartheta(t) + \mathcal{L}V(t) \\ + \sum_{\nu=0}^{[w(t)]-1} \frac{\sigma}{[w(t)]}\xi^T(t-\tau_k(t))E_{1i}^T\Phi E_{1i}\xi(t-\tau_k(t)) \\ - \sum_{v=0}^{[w(t)]-1} u_j e_{k-v}^T(t)\Phi e_{k-v}(t)\big)dt\Big\} - V(\infty) \\ \leq \int_0^\infty \sum_{i=1}^{k}\sum_{j=1}^{k}\sum_{v=0}^{[w(t)]-1} \zeta^T(t)\Pi_{ij}\zeta(t)dt \end{aligned}$$

where $\zeta^T(t) = [\xi^T(t) \;\; \xi^T(t-\tau_k(t)) \; e_{k-\nu}^T(t) \;\; \vartheta^T(t)]$, and

$$\Pi_{ij} = \begin{bmatrix} \Pi_{11} & P\bar{B} & P\bar{E} & PC_{0ij} \\ * & \Pi_{22} & 0 & 0 \\ * & * & \Pi_{33} & 0 \\ * & * & * & \Pi_{44} \end{bmatrix}, \tag{13}$$

where

$$\Pi_{11} = A_{0ij}^T P + PA_{0ij} + R + \bar{D}^T\bar{D},\; \Pi_{22} = E_{1i}^T\Phi E_{1i} - R,$$
$$\Pi_{33} = -u_j\Phi,\; \Pi_{44} = -\gamma^2 I.$$

Next, if and only if $\Pi_{ij} < 0$, then

$$\mathcal{L}V(t) + z^T(t)z(t) - \gamma^2\vartheta^T(t)\vartheta(t) < 0$$

when $\vartheta(t) = 0$, it can be readily deduced that $\mathbb{E}\{\mathcal{L}V(t)\} < 0$. This indicates the presence of a positive definite matrix P that guarantees the asymptotic stability of the closed-loop systemy. In other cases, integrating both sides from 0 to $+\infty$ yields:

$$\int_0^{+\infty} z^T(t)z(t)dt - \gamma^2\int_0^{+\infty}\vartheta^T(t)\vartheta(t)dt < 0 \tag{14}$$

which implies H_∞ performance index is satisfied under zero initial condition. □

Theorem 2. For given constants $\alpha_1, \alpha_2, \mu_1 > 0$, $\sigma \in (0, 1]$, and $u_v, v \in \{0, 1, ..., [w(t)] - 1\}$, if there exist matrices $X, Y, R_{11}, R_{12}, R_{22}, \mathcal{A}_{ij}, \mathcal{B}_j, \mathcal{C}_j, j = 1, 2, ...$ with appropriate dimensions such that the following inequalities hold:

$$\begin{bmatrix} \mathcal{N}_{11ij} & \mathcal{N}_{12ij} & \mathcal{N}_{13ij} \\ * & \mathcal{N}_{22ij} & 0_{p\times q} \\ * & * & \mathcal{N}_{33ij} \end{bmatrix} < 0,$$
$$i, j = 1, 2, ..., v \in \{0, 1, ..., [w(t)] - 1\}, \tag{15}$$

where

$$\mathcal{N}_{11ij} = \begin{bmatrix} He(A_iX + \alpha_1 B_i\mathcal{C}_j) + \tilde{R}_{11} & A_i + \mathcal{A}_{ij}^T + \tilde{R}_{12} \\ * & He(YA_i) + \tilde{R}_{22} \end{bmatrix},$$
$$\mathcal{N}_{12ij} = \begin{bmatrix} 0 & 0 \\ B_jE_i & 0 \end{bmatrix},\; \mathcal{N}_{13ij} = \begin{bmatrix} 0 & C_i & (1-\alpha_1)\alpha_2 B_i \\ B_j & YC_i & (1-\alpha_1)\alpha_2 YB_i \end{bmatrix},$$
$$\mathcal{N}_{13ij} = \begin{bmatrix} XD_i^T \\ D_i^T \end{bmatrix},\; \mathcal{N}_{22ij} = \begin{bmatrix} E_i^T\Phi E_i - R_{11} & -R_{12} \\ * & -R_{22} \end{bmatrix},$$
$$\mathcal{N}_{33ij} = -\,\text{diag}\{-u_v\Phi, -\gamma^2 I, -\gamma^2 I, -I\},$$

then the closed-loop T-S fuzzy system under the hybrid cyber-attacks is to be asymptotically stable with the DOFC values $A_{cj}, B_{cj}, C_{Gj}, j = 1, 2, ...$, while satisfying the H_∞ performance with a prescribed gain γ.

Proof. The proof is omitted. □

Corollary 1. The Zeno phenomenon is effectively avoided under the proposed event-triggered mechanism 3.

Proof. Assume that the Zeno phenomenon occurs. This implies the existence of a finite time T, such that $\lim_{k\to\infty} t_k = T < \infty$, and consequently $\lim_{k\to\infty}(t_{k+1} - t_k) = 0$. On the one hand, due to the continuity of the system dynamics, it follows that:

$$\lim_{k\to\infty}(\tilde{y}(t_{k+1}) - \tilde{y}(t_k)) = 0.$$

As a result, the error term satisfies:

$$\begin{aligned} \lim_{k\to\infty} e_{k-j+1}(t^-) &= \lim_{k\to\infty}\big(y_{k-j+1}(t_{k-j}) - y(t_k^i)\big) \\ &= \lim_{k\to\infty}\big(y_{k-j}(t_k) - y(t_k^i)\big) = 0. \end{aligned}$$

On the other hand, based on the event-triggered condition (3) for any $\sigma \in (0, 1]$ and $k \in \mathbb{N}$ the following inequality holds:

$$\sum_{j=0}^{\lceil w(t)\rceil-1} u_j e_{k-j+1}^T(t^-)\Phi e_{k-j+1}(t^-) = \sigma\bar{y}^T(t_{kj}^-)\Phi\bar{y}(t_{kj}^-) > 0,$$

which implies

$$\lim_{k\to\infty} e_{k-j+1}(t^-) \neq 0.$$

Clearly, these two conclusions are contradictory. Therefore, the Zeno phenomenon cannot occur under the proposed event-triggered mechanism (3). This completes the proof. □

4 Conclusions

This work investigates the issue of robust control for T-S fuzzy systems under hybrid cyber-attacks. The hybrid attack scenario follows a Bernoulli probability distribution, and a dynamic memory event-triggered mechanism is developed that fully incorporates state information from multiple triggering instants, thereby enhancing the credibility of the proposed controller while conserving resources. Furthermore, considering the scenario where state signals are unmeasurable, a dynamic output feedback controller is employed to stabilize the closed-loop system. By constructing a Lyapunov function, sufficient conditions for the system to satisfy H_∞ performance are derived. Additionally, the corresponding gain values for the DOFC are obtained by solving LMIs.

Acknowledgements

This work was supported in part by the Science and Technology Research Program of Chongqing Municipal Education Commission under Grant KJZDK202300807; in part by the Chongqing Natural Science Foundation under Grant CSTB2024NSCQ-QCXMX0052; in part by the High-level Talents Research Project of CTBU(2356021); and in part by the Graduate Student Scientific Research Innovation Project of China under Grant yjscxx2024-284-198.

References

[1] Fan Y, An Y, Wang W, C Yang. "T-S Fuzzy Adaptive Control Based on Small Gain Approach for an Uncertain Robot Manipulators", International Journal of Fuzzy Systems, vol. 22, no. 4, pp. 930–942, 2020.

[2] He D, Wang H, Tian Y, Precup R. "Model-Free Global Sliding Mode Control Using Adaptive Fuzzy System Under Constrained Input Amplitude and Rate for Mechatronic Systems Subject to Mismatched Disturbances", Information Sciences, Vol. 697, pp. 121769, 2025.

[3] Hao L Y, Zhang H, Li T S, Lin B, Chen C L P. "Fault Tolerant Control for Dynamic Positioning of Unmanned Marine Vehicles Based on T-S Fuzzy Model With Unknown Membership Functions", IEEE Transactions on Vehicular Technology, vol. 70, no. 1, pp. 146–157, 2021.

[4] Zhao N, Zhao X, Zong G, Xu N. "Resilient Event-Triggered Filtering for Networked Switched T-S Fuzzy Systems Under Denial-of-Service Attacks", IEEE Transactions on Fuzzy Systems, vol. 32, no. 4, pp. 2140–2152, 2024.

[5] Ma J, Song Y, Niu Y, Dong Y. "Security-Based Dynamic Output-Feedback Model Predictive Control for Nonlinear Systems in T-S Fuzzy form Subject to Deception Attacks", Journal of the Franklin Institute, vol. 360, no. 12, pp. 8224–8250, 2023.

[6] Qi Y, Yuan S, Niu B. "Asynchronous Control for Switched T–S Fuzzy Systems Subject to Data Injection Attacks via Adaptive Event-Triggering Schemes", IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 7, pp. 4658–4670, 2022.

[7] Hu S, Yue D, Peng C, Xie X, Yin X. "Event-Triggered Controller Design of Nonlinear Discrete-Time Networked Control Systems in T-S Fuzzy Model", Applied Soft Computing, vol. 30, pp. 400–411, 2015.

[8] Tan Y, Yuan Y, Xie X, Niu B. "Dynamic Event-Triggered Security Control for Networked T-S Fuzzy System with Non-Uniform Sampling", Fuzzy Sets and Systems, vol. 452, pp. 91–109, 2023.

[9] Liu J, Liu Q, Cao J, Zhang Y. "Adaptive Event-Triggered H_∞ Filtering for T-S Fuzzy System with Time Delay", Neurocomputing, vol. 189, pp. 86–94, 2016.

[10] Zhang D, Du B. "Event-Triggered Controller Design for Positive T-S Fuzzy Systems with Random Time-Delay", Journal of the Franklin Institute, vol. 359, no. 15, pp. 7796–7817, 2022.

[11] Liang R, Xiao Z, Wu Z, Tao J, Wang X. "Dynamic Event-Triggered and Asynchronous Sliding Mode Control for T-S Fuzzy Markov Jump Systems", Nonlinear Dynamics, vol. 109, pp. 911–924, 2022.

[12] Nagamani G, Joo Y H, Soundararajan G, Mohajerpoor R. "Robust Event-Triggered Reliable Control for T-S Fuzzy Uncertain Systems via Weighted Based Inequality", Information Sciences, vol. 512, pp. 31–49, 2020.

[13] Zhang H, He X, Minchala L I, Shi P. “Dissipative Output Feedback Control for Semi-Markovian Jump Systems Under Hybrid Cyber-Attacks”, Journal of the Franklin Institute, vol. 358, no. 5, pp. 2683–2702, 2021.