Membership-function-dependent security control for networked T-S fuzzy-model-based systems against DoS attacks

Xiehuan Li¹ | Dan Ye¹,²

¹ College of Information Science and Engineering, Northeastern University, Shenyang, Liaoning, China
² State Key Laboratory of Synthetical Automation of Process Industries, Northeastern University, Shenyang, Liaoning, China

Correspondence
Dan Ye, College of Information Science and Engineering, Northeastern University, Shenyang 110819, Liaoning, China.
Email: yedan@ise.neu.edu.cn

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 61773097, U1813214; Fundamental Research Funds for the Central Universities, Grant/Award Number: N2004027; Liaoning Revitalization Talents Program, Grant/Award Number: XLYC1907035

Abstract
This paper focuses on the observer-based resilient event-triggered security control issue for networked T-S fuzzy-model-based systems suffered from energy-limited Denial-of-Service (DoS) attacks. Firstly, a novel resilient adaptive event-triggered mechanism (AETM) is designed to deal with the packet losses problem induced by energy-limited DoS attacks. Specifically, the resilient AETM threshold is adaptively updated based on the latest available packages. Secondly, according to Lyapunov theory, membership-function-dependent stabilisation criterions are obtained to ensure the control systems are stable with $H_\infty$ performance. Besides, the mismatched premise variables between model and controller are considered, and a slack matrix with the membership functions information is introduced to relax stability conditions. Then, the relationship between allowable duration of DoS attack and resilient AETM parameter is clarified. An algorithm is also presented to derive the resilient AETM parameter and observer-based controller gains simultaneously. Finally, two examples are provided to demonstrate the effectiveness of the proposed method.

1 | INTRODUCTION

In fact, most physical processes are non-linear and difficult to be processed by traditional theories and methods. Fortunately, the fuzzy-model-based (FMB) method can be applied to approximate non-linear systems by connecting multiple local linear systems with non-linear membership functions (MFs) [1, 2]. Due to its strong modeling ability, the FMB control has been widely concerned by scholars in [3–9, 11–14]. In [5], the fault-tolerant controller is designed for a general polynomial FMB system. Then to relax stability conditions, the membership-function-dependent (MFD) stabilisation analysis approach is investigated in [6] for T-S FMB system. For parameter uncertainty IT2 fuzzy systems, the MFD stability analysis has been considered in [7–9]. Besides, the finite-time ET control issue in terms of linear matrix inequalities (LMIs) method [10] has been studied in [11] for Markov jump FMB system. Then, the authors in [12] introduce a new event-based fault detection filter, whose performance is better achieved with MFs information. In addition, for unmeasurable state variables, the observer-based controller is constructed in [13] for discrete time T-S FMB control systems, while the MFs of observer depend on plant state variables. Furthermore, in [14] a novel observer-based controller, whose MFs are related with estimated observer states rather than system ones, is constructed for fuzzy networked control systems (NCSs).

Recently, more and more intelligent devices with sensing, computing, communication, and execution energy appear in physical environment. Although these intelligent devices have many benefits, they also face some challenges in design and implementation, especially security and reliability control [15]. Therefore, the safety problem has achieved extensive research by scholars in recent years, particularly the concern of networked control against cyber attacks [16, 17]. In general, attacks on communication links contain deception attacks and DoS attacks. The former influences data reliability by modifying the information delivered over communication network. DoS attacks can block information transmission, so that the control commands cannot be reached to the controller, resulting in complete loss of data [18, 19]. As described in [20], DoS attacks are more likely to occur in communication network, and correspondingly, they have been widely studied in [21–26]. In [21], the stability analysis is considered for linear discrete-time NCSs under Bernoulli random DoS attacks. Then the risk-sensitive
control problem is investigated in [22] to defense DoS attacks with a known probability distribution. In a specified control range, the optimal control and attack strategy are studied in [23] by assuming the maximum number of jamming. Moreover, a general attack model is discussed in [24], which restricts the attacker’s behavior by limiting the frequency and duration of DoS attacks. In [25], a maximum robust resilient controller is designed to guarantee system stability performance in the presence of DoS attacks. Besides, the authors in [26] propose a unified game approach to achieve resilient control for NCSs against DoS attacks. However, the mentioned results in [21–26] only analyse system performance under DoS attacks, the limited communication bandwidth is not considered.

In practical NCSs, the shared communication network can transmit related signals to realise resource sharing, remote control, and operation [27, 28]. There are also some difficulties in the transmission network, such as access constraints [29], network delay [30], packet dropout [31], and bandwidth limitation [32, 33] etc. Recently, how to construct an effective communication strategy to reduce network bandwidth is getting more and more attention [32–43]. In [34–36], a discrete ET mechanism is designed to make the NCSs satisfy desired performance, which is solved by time-delay system method [37]. Then, an AETM is proposed in [38] to further save network resources. Although the research of ET control has made great progress in [32–38], network security issues are also worth considering. The authors in [39] introduce a hybrid-triggered scheme to improve communication efficiency under stochastic cyber-attacks. In [40], a periodic ET control method is investigated, which can resist DoS attacks with limited frequency and duration. Furthermore, a resilient ET control strategy is discussed in [41] to make the established switching NCSs are globally exponentially stable against periodic DoS attacks. For non-periodic DoS attacks, a distributed state estimation issue is studied in [42]. Moreover, multiple cyber attacks are considered in [43] and [44] for multi-area power systems and multi-agent systems, respectively. Then, a resilient ET mechanism is applied in [45] to tolerate a degree of packets loss against energy-limited DoS attacks. However, the ET communication threshold in [39–45] is a given constant, which can not take full advantage of the information transmitted by packets. Therefore, when researching cyber attacks for FMB control systems, how to change the flexibility of the ET mechanism and further improve resource efficiency is a problem worth studying.

Motivated on the above analysis, the paper investigates the observer-based resilient adaptive ET security control issue for non-linear fuzzy systems subject to energy-limited DoS attacks. Here are the main contributions.

(i) Based on DoS attack characteristics, a new resilient AETM is well designed for observer-based fuzzy systems. Unlike the existing ET mechanism in [32–36, 38, 45], the proposed resilient AETM can improve resource utilisation efficiency and further tolerate data loss caused by cyber-attacks.

(ii) Compared with the recent results in [39–45], the random attacks are handled with a more flexible communication mechanism method. It can fully utilise the adjacent trigger information and further dynamically change the threshold parameters according to the packet loss induced by DoS attacks.

(iii) A quantitative relationship among the resilient AETM parameters under attacks, AETM parameters without attacks, and the number of consecutive packet losses is presented. Furthermore, mismatched premises are considered between fuzzy model and controller, then the slack matrices and characteristics of MFs are well considered in stability analysis.

This paper is organised as follows. The definition of energy-limited DoS attacks and novel resilient AETMs are displayed in Section 2. In Section 3, some basic knowledge about system is stated. Then the main results are presented for observer-based control systems in Section 4. Two examples are shown in Section 5 and the conclusions are given in Section 6.

**Notation.** \( \mathbb{R}^n \) expresses the n-dimensional Euclidean space and the mark * means the symmetric entry. \( L_2[0, \infty) \) stands for the space of square-integrable vector function over \([0, \infty)\).

## 2 RESILIENT AETM WITH DoS ATTACKS

In the section, an energy-limited DoS attack is introduced and a novel resilient AETM is proposed to ensure the control system is stable under attacks.

It is known that DoS attacks can cause network communication interruption, then the packets will be lost during attack duration. As stated in Figure 1, the \( l \)th DoS attack occurs at random instants \( t_{\text{dos}_l} \) with duration \( d_{\text{dos}_l} \). Define \( b_l \) is the number of the consecutive packet losses in the \( l \)th attacks interval, then the maximum one is \( b = \max\{b_1, \ldots, b_l, \ldots\} \). Inspired by [45], we consider an energy-limited DoS attack, whose \( l \)th duration satisfy the following relationship

\[
d_{\text{dos}_l} \leq b b_l,
\]

where \( b \) is the sampling period.

At present, the risk of network communication attacks is increasing day by day in actual system. When the network is affected by DoS attacks, there will be a great probability of data loss, and the traditional ET mechanism will be ineffective. Hence, it is necessary to study a flexible resilient ET communication strategy that is immune to network attacks. First of
all, to make the paper more readable, an AETM is introduced to improve communication efficiency without considering DoS attacks. In what follows, some assumptions are used to simplify the description. Here, \( k \) means the number of transmissions.

**Assumption 1.** The observer state \( \hat{x}(t) \) is sampled at a constant \( b \), and the sampling sequence are denoted as \( \hat{x}(\mathcal{g}(b)) \) with \( \mathcal{g} = \{0, 1, 2, \ldots \} \).

**Assumption 2.** Whether the latest sampled packets \( \hat{x}(\mathcal{g}(b)) \) should be conveyed to wireless network channel are decided by triggered conditions. The transmitted packets are recorded as \( \hat{x}(d_k) \) with \( d_k \subseteq \mathcal{g} \). However, packet losses may exist in wireless network channel due to the occurrence of DoS attacks.

**Assumption 3.** The data packets successfully transmitted to controller are written as \( \hat{x}(t_k) \) with \( t_k \subseteq d_k \).

**Assumption 4.** Network-induced delays from AETM to zero-order-holder (ZOH) is \( \varphi_{b_k} \in (0, \varphi] \), where \( \varphi \) is the upper bound of \( \varphi_{b_k} \).

Remark 1. If \( \mathcal{g} = d_k \), the ET mechanism becomes time-triggered. When \( d_k = t_k \), it implies that there are no DoS attacks in wireless network channel and all the triggered packets are transmitted to controller. If \( t_k < d_k \), it means that there exist DoS attacks and packets loss between wireless network channel and controller.

The diagram of networked T-S FMB control systems with AETM is displayed in Figure 2. Besides, whether the current sampled data \( \hat{x}(\mathcal{g}(b)) \) should be transmitted to wireless network channel is decided by the AETM condition (2). When the obtained signal is conveyed, then the ET threshold is calculated by adaptive rule (3) and stored in Buffer 1. The triggered packet is also placed in Buffer 2 for the later utilisation of ET conditions. Then next release time of AETM under no attacks satisfies the following condition.

\[
t_{k+1}b = t_kb + \min_{a \geq 1} \left\{ a \mathbf{b} | \eta_{k+b}(t) | \right\} \Omega \eta_{k+b}(t) > \rho_1(t_kb) \hat{x}^T(t_kb) \Omega \hat{x}(t_kb),
\]

where \( \Omega > 0 \) is an appropriate dimension matrix to be designed. \( \eta_{k+b}(t) = \hat{x}(t_kb + db) - \hat{x}(t_kb) \) is the error between the current sampled packet \( t_kb + db \) and latest released data \( t_kb \). Furthermore, the ET threshold parameter \( \rho_1(t_kb) \) is decided by the following update rule

\[
\rho_1(t_kb) = \begin{cases} 
\rho_{m1}(t_kb) & \rho_{m2}(t_kb) \leq \rho_{m2} \\
\rho_{m2} & \rho_{m2} < \rho_{m2} 
\end{cases}
\]

where \( \rho_{m1}(t_kb) = \max \left\{ \rho_1(t_kb)(1 - \frac{2d}{\pi} \tan(a)[||\hat{x}(t_kb + db)|| - ||\hat{x}(t_kb)||]) ; \rho_{m2} \right\} \), \( \rho_1(0) \) is the initial value of \( \rho_1(t_kb) \), that is to say, \( \rho_1(0) = \rho_{m2} \). \( 0 \leq \rho_{m1} < \rho_{m2} < 1, a > 0 \) and \( b > 0 \) are known parameters.

**Remark 2.** As we all know, the bounded invert tangent function \( \tan(a) \) satisfies \( \tan(a) \in \left[ \frac{-\pi}{2}, \frac{\pi}{2} \right] \). Then the adaptively updated ET threshold \( \rho_1(t_kb) \) can be obtained from given parameters \( a \) and \( b \). For instance, if \( ||\hat{x}(t_kb + db)|| - ||\hat{x}(t_kb)|| > 0 \), it can be seen that \( \rho_1(t_kb + db) < \rho_1(t_kb) \). Then the update rule (3) uses a smaller \( \rho_1(t_k+1b) \) to permit more transmitted package data to reduce the error between \( ||\hat{x}(t_kb + db)|| \) and \( ||\hat{x}(t_kb)|| \). In contrast, the larger \( \rho_1(t_k+1b) \) can save more communication bandwidth.

Besides, the network-induced delay \( \varphi_{b_k} \) which happens in release time \( t_kb \) is also considered in the paper. Due to the existence of ZOH, the controller receives data \( \hat{x}(t_kb) \) from wireless network channel in the time interval \( [t_kb + \varphi_{b_k}, t_k+1b + \varphi_{b_k+1}] \). Here, \( \varphi_{b_k}, \varphi_{b_k+1} \in (0, \varphi] \). Then, for the mentioned interval we have to consider two cases.

**Case 1:** If \( \varphi_{b_k} + \varphi_{b_k+1} \geq t_k+1b + \varphi_{b_k+1} \), then define

\[
\tau(t) = t - t_kb, \quad t \in [t_kb + \varphi_{b_k}, t_k+1b + \varphi_{b_k+1}].
\]

Obviously, \( \tau(t) \) satisfies \( \tau(t) \leq t_k+1b + \varphi_{b_k+1} - t_kb \leq b + \varphi = \bar{\varphi} \).

**Case 2:** If \( \varphi_{b_k} + \varphi_{b_k+1} < t_k+1b + \varphi_{b_k+1} \), then divide the time interval \( [t_kb + \varphi_{b_k}, t_k+1b + \varphi_{b_k+1}] \) into different sub-intervals. That is

\[
[t_kb + \varphi_{b_k}, t_k+1b + \varphi_{b_k+1}] = \bigcup_{d=1}^{e} \Omega_d
\]

where \( \Omega_d = [(t_kb + d) + \varphi_{b_k+d}, (t_kb + d + 1) + \varphi_{b_k+d+1}] \), \( d = 0, \ldots, e, e = t_k+1 - t_k - 1 \).

\[
\varphi_{b_k+d+1} = \begin{cases} 
\varphi_{b_k} & d = 0, \ldots, t_k+1 - t_k - 2 \\
\varphi_{b_k+1} & d = t_k+1 - t_k - 1
\end{cases}
\]

Define \( \tau(t) = t - t_kb - db, t \in \Omega_d \), one can obtain that \( \tau(t) \) is a differentiable piecewise linear function such that \( 0 \leq \varphi_{b_k} \leq \tau(t) \leq \varphi + b = \bar{\varphi} \), \( t = 1, \ldots, t \in \Omega_d \). Hence, the actual input of the controller can be stated as

\[
\tilde{x}(t) = \hat{x}(t_kb) = \hat{x}(t - \tau(t) - \eta_{b_k}).
\]
In addition, when suffered from DoS attacks, some packets may be lost through the AETM (2). Then the AETM (2) can not be used to decide whether packets are transmitted or not. Therefore, we have to design a novel resilient AETM to eliminate the effect of packet loss induced by DoS attacks.

\[
t_{k+1} = t_{k} + \min_{\beta \geq 1} \{ \beta \beta \|= \eta(t)^T \Omega \eta(t) > \rho \beta \|= \Omega \hat{\varepsilon}(t) \},
\]

(5)

where \( \rho \) is the resilient AETM threshold parameter in triggered interval \([t_k, t_{k+1})\) under attacks, which is related with \( \rho_1(t_k) \).

Remark 3. The resilient AETM (5) is constructed on the basis of AETM (2). Due to the existence of DoS attacks, some packets may be lost in successive trigger intervals \([t_k, t_{k+1})\). In order to ensure system stability, \( \rho \) whose value is lower than \( \rho_1(t_k) \) is designed to allow more data packages to be transmitted. It can improve utilisation efficiency without attack, and the system stability performance is further ensured in the presence of attacks.

Remark 4. According to the following condition (18) satisfied by the resilient parameter \( \rho \), one can conclude that when \( \rho_{a1} \neq 0, a = 0 \), the resilient AETM (5) reduces to ET generators in [34, 45]. If there is no DoS attack in the interval \([t_k, t_{k+1})\), that is the number of successive packet losses \( b_k = 0 \), then the resilient AETM (5) becomes AETM in [38]. When \( b_k = 0, \rho_{a1} \neq 0, a = 0 \), the resilient AETM (5) reduces to traditional fixed threshold ET generators in [32, 33, 35, 36]. Moreover, if \( b_k = 0, \rho_{a1} = 0, a = 0 \), the resilient AETM (5) becomes the time-triggered scheme. In summary, the proposed resilient AETM (5) is more general.

3 | SYSTEM DESCRIPTION AND PRELIMINARIES

3.1 | T-S fuzzy model

Considering a class of non-linear systems which can be represented as T-S fuzzy model with \( j \) fuzzy rules [35].

Rule \( i \): If \( b_1(x(t)) \) is \( K'_i \) and \( b_0(x(t)) \) is \( K'_i \) then

\[
\dot{x}(t) = A_i x(t) + B_i u(t) + D_i \omega(t),
\]

\[
\zeta(t) = C_i x(t) + B_{i1} u(t),
\]

\[
y(t) = C_i x(t),
\]

where \( K'_i \) is the fuzzy term of rule \( i \) corresponding to premise variable \( b_{0}(x(t)), a = 1, 2, \cdots, o, i = 1, 2, \cdots, r \) and \( o \) and \( r \) are positive integers that stand for the number of premise variable and fuzzy rules, respectively. \( x(t) \in \mathbb{R}^n \) and \( y(t) \in \mathbb{R}^r \) are the system state and measurement output, respectively. \( u(t) \in \mathbb{R}^o \) and \( \omega(t) \in \mathbb{R}^o \) are control input and output. \( \omega(t) \in \mathbb{R}^o \) is the unknown external disturbance which belongs to \( L_2[0, \infty) \). \( A_i, B_i, C_i, D_i, C_{i1} \) and \( B_{i1} \) are known system matrices. The system dynamics are of the following format

\[
\dot{x}(t) = \sum_{i=1}^{s} g_i(x(t)) \left( A_i x(t) + B_i u(t) + D_i \omega(t) \right),
\]

\[
\zeta(t) = \sum_{i=1}^{s} g_i(x(t)) \left( C_i x(t) + B_{i1} u(t) \right),
\]

\[
y(t) = \sum_{i=1}^{s} g_i(x(t)) C_i x(t),
\]

(6)

where \( \sum_{i=1}^{s} g_i(x(t)) = 1 \), \( g_i(x(t)) \geq 0 \), \( g_i(x(t)) = \prod_{i=1}^{s} \mu_{K'_i} (b_0(x(t))) / \sum_{i=1}^{s} \prod_{i=1}^{s} \mu_{K'_i} (b_0(x(t))) \) for all \( i \), \( \mu_{K'_i} (b_0(x(t))) \) is the grade of membership corresponding to fuzzy term \( K'_i \).

3.2 | Observer and controller design

The observer and system do not share the same premise variables and the observer premise variables depend on the estimated state variables \( \hat{x}(t) \) [35]. Then the \( j \)th fuzzy rule is obtained as follows.

Rule \( j \): If \( b_1(\hat{x}(t)) \) is \( K'_j \) and \( b_0(\hat{x}(t)) \) is \( K'_j \) then

\[
\dot{\hat{x}}(t) = A_j \hat{x}(t) + B_j u(t) + L_j (y(t) - \hat{y}(t)),
\]

\[
\hat{y}(t) = C_j \hat{x}(t),
\]

where \( \hat{x} \in \mathbb{R}^n \) and \( \hat{y} \in \mathbb{R}^r \) are the estimated state and measurement output, respectively. \( L_j \) is observer gains. The global observer dynamics are shown as follows

\[
\dot{\hat{x}}(t) = \sum_{j=1}^{s} g_j(\hat{x}(t)) \left( A_j \hat{x}(t) + B_j u(t) + L_j (y(t) - \hat{y}(t)) \right),
\]

\[
\hat{y}(t) = \sum_{j=1}^{s} g_j(\hat{x}(t)) C_j \hat{x}(t),
\]

(7)

where \( \sum_{j=1}^{s} g_j(\hat{x}(t)) = 1 \), \( g_j(\hat{x}(t)) \geq 0 \), \( g_j(\hat{x}(t)) = \prod_{j=1}^{s} \mu_{K'_j} (b_0(\hat{x}(t))) / \sum_{j=1}^{s} \prod_{j=1}^{s} \mu_{K'_j} (b_0(\hat{x}(t))) \) for all \( j \), \( \mu_{K'_j} (b_0(\hat{x}(t))) \) is the grade of membership corresponding to fuzzy term \( K'_j \).

Owing to that there exists an AETM between the observer output and controller input, then the premises between observer and controller are asynchronous. Besides, the mismatched premise variables are considered between controller and fuzzy model to improve design flexibility. Then, the \( i \)th fuzzy rule of controller is described as follows.

Rule \( i \): If \( f_i(\hat{x}(t_k) b_i) \) is \( M'_i \) and \( f_i(\hat{x}(t_k) b_i) \) is \( M'_i \) then

\[
u(t) = f_i(\hat{x}(t_k) b_i),
\]

(8)
where $F_l$ are controller parameters. Then the global fuzzy controller is stated as

$$u(t) = \sum_{j=1}^{s} q_j(\hat{x}(t_k)b)F_j\hat{x}(t_k)b,$$

where $M_\beta^l$ is the fuzzy term of rule $l$ corresponding to premise variable $f_\beta(\hat{x}(t))$, $\beta = 1, 2, \cdots, \ell$, $\ell = 1, 2, \cdots, \ell$ is positive integers that means the number of premise variable, $q_j(\hat{x}(t_k)b) = \prod_{\beta=1}^{\ell} \mu_{N_\beta}^j(f_\beta(\hat{x}(t_k)b))/\sum_{l=1}^{\ell} \prod_{\beta=1}^{\ell} \mu_{N_\beta}^j(f_\beta(\hat{x}(t_k)b))$, $\sum_{l=1}^{\ell} q_l(\hat{x}(t_k)b) = 1, q_j(\hat{x}(t_k)b) \geq 0$, for all $l$, $f_\beta(\hat{x}(t_k)b)$ is the normalised grade of membership, $\mu_{N_\beta}^j(f_\beta(\hat{x}(t_k)b))$ is the grade of membership corresponding to fuzzy term $M_\beta^l$.

For simplicity, $g_j(\hat{x}(t))$, $g_j(\hat{x}(t))$ and $q_j(\hat{x}(t_k)b)$ are written as $g_j$, $g_j$ and $q_j$, respectively.

### 3.3 Observer-based error systems

The augmented system is obtained by using the actual control input (4), fuzzy model (6), fuzzy observer (7) and fuzzy controller (9).

$$\dot{\hat{e}}(t) = \sum_{i=1}^{s} \sum_{j=1}^{s} \sum_{k=1}^{s} g_{ij}^k \hat{q}_k^j (A_i \theta(t - \tau(t)) + B_{ij} \hat{\Theta}(t - \tau(t))) + C_{ij} e_{k}(t + D_{ij} \omega(t)),$$

where $\hat{e}(t) = [\hat{x}^T(t), \hat{z}^T(t)]$, $\hat{x}(t) = x(t) - \hat{x}(t), \theta(t - \tau(t)) = [\hat{\xi}^T(t - \tau(t)), \hat{\xi}^T(t - \tau(t))]^T$, $N = [I_{\alpha \times \alpha}, 0_{\alpha \times \alpha}]$.

$$A_{ij} = \left[ \begin{array}{cc} A_j - L_j(C_i - C_j) & L_j C_i \\ A_j - L_j(C_j - C_i) & A_j - L_j C_i \end{array} \right],$$

$$B_{ij} = \left[ \begin{array}{c} B_j F_i \\ (B_j - B_i) F_i \end{array} \right],$$

$$C_{ij} = \left[ \begin{array}{c} -B_j F_i \\ -(B_j - B_i) F_i \end{array} \right],$$

$$D_{ij} = \left[ \begin{array}{c} 0 \\ D_{ij} \end{array} \right].$$

Then, the following lemmas are needed in the stability analysis.

**Lemma 1.** For matrices $H, S > 0$, $\bar{\tau} \in (0, \tau]$, then the inequality $-\bar{\tau} \int_{-\tau}^{0} \dot{\hat{e}}(s) \hat{e}(s) ds \leq \xi^T F \xi$ can be well defined and maintains. Here

$$F = \left[ \begin{array}{ccc} -S & H & -H \\ * & -2S - H - HT & S + H \\ * & * & -S \end{array} \right],$$

$$\xi^T = [\hat{e}(t), \theta(t - \tau(t)), \theta(t - \bar{\tau})].$$

**Lemma 2.** The singular value decomposition for full matrix rank$(C)\epsilon\mathbb{R}$, $C \in \mathbb{R}^{\alpha \times \alpha}$ can be stated as $C = O[\bar{S} \ 0_{(\alpha - r) \times \alpha}] V^T$, where $OO^T = I$ and $VV^T = I$. For matrices $U \in \mathbb{R}^{\alpha \times \alpha} > 0$, $U_1 \in \mathbb{R}^{\alpha \times \alpha}$, $U_2 \in \mathbb{R}^{(\alpha - r) \times (\alpha - r)}$, if the condition $U = V \begin{bmatrix} U_1 & 0 \\ 0 & U_2 \end{bmatrix} V^T$ holds, then there exists a matrix $\hat{C}$, such that $CU = \hat{C}U$.  

## 4 MAIN RESULTS

The $H_\infty$ stability conditions of augmented system (10) under an AETM (2) are presented in Theorem 1. In Theorem 2, a resilient AETM (5) against DoS attacks is proposed and the corresponding $H_\infty$ performance is also guaranteed. Furthermore, in order to derive both observer and controller gains simultaneously, a matrix decoupling technique is provided in Theorem 3. Besides, an algorithm with the consideration of dichotomy method is introduced to describe how to obtain co-designed controller and communication gains.

### 4.1 Stability analysis without DoS attacks

**Theorem 1.** For the given positive scalars $\bar{\tau}, \rho_{m2}, \gamma, \lambda_j$, the augmented system (10) with AETM (2) is stable subject to $H_\infty$ performance, if there exist symmetric matrices $P > 0$, $R > 0$, $\Theta$, and matrices $F_l, \Omega_l, L_j, F_i, j, l = 1, \ldots, s$, such that the following linear matrix inequalities (LMIs) hold with $\hat{q}_k^j - \lambda_j \hat{q}_k^j \geq 0, 0 < \lambda_j \leq 1$

$$\begin{bmatrix} \Theta_1 - \lambda_j \Theta_1 \Theta_1, & \lambda_j \Theta_1 \Theta_1 \end{bmatrix} < 0, \begin{bmatrix} \Theta_2 - \lambda_j \Theta_1 \Theta_2, & \lambda_j \Theta_1 \Theta_2 \end{bmatrix} < 0,$$

where

$$\hat{\Theta}_{ij} = \left[ \begin{array}{ccc} \Psi_{ij} & \Phi_{ij} & \Xi_{ij} \\ * & -I & 0 \\ * & * & -S \end{array} \right],$$

$$\begin{bmatrix} \Psi_{11ij} & \Psi_{12ij} & -N^T H & R_{ij} \\ \Psi_{21ij} & -S + H & \Psi_{24ij} & PD_{ij} \\ * & * & -S & 0 \\ * & * & * & 0 \end{bmatrix} < 0,$$

$$\begin{bmatrix} A_{ij}^T + P + BA_{ij} + N^T R N - N^T S \Theta \end{bmatrix} < 0,$$

$$\begin{bmatrix} \Phi_{ij} & [C_2, B_1 F_1] \ 0 -B_1 F_1 \ 0 \end{bmatrix},$$

$$\Xi_{ij} = \begin{bmatrix} \Sigma_{N4ij} & \Sigma_{SB4ij} & 0 & \Sigma_{NC4ij} & \Sigma_{SN4ij} \end{bmatrix}.$$
Stability analysis with DoS attacks

Proof. Consider the following Lyapunov-Krasovskii functional

\[
V'(t) = \theta^T(t) P \theta(t) + \int_{t-\tau}^t \theta^T(s) N^T R N \theta(s) ds + \bar{\tau} \int_{t-\tau}^t \theta^T(s) S N \theta(s) d\nu(s),
\]

where \( P = P^T > 0 \in \mathbb{R}^{2n}, R = R^T > 0 \in \mathbb{R}^n \) and \( S = S^T > 0 \in \mathbb{R}^n \). Then its derivative follows

\[
\dot{V}'(t) = 2 \dot{\theta}^T(t) P \theta(t) + \dot{\theta}^T(t) N^T R N \theta(t) - \theta^T(t - \tau(t)) N^T R N \theta(t - \tau(t)) + \bar{\tau} \dot{\theta}^T(t) S N \theta(t) d\nu(t)
\]

Integrating both sides of (17) under zero initial condition, one gets \( \|z(t)\|_2 < \gamma \|u(t)\|_2 \) with \( \omega(t) \in [0, \infty) \). Furthermore, when \( \omega(t) = 0 \), it can be obtained that \( \dot{V}'(t) < 0 \) from (12)–(14) in Theorem 1. It implies that the augmented system (10) is stable with \( \omega(t) = 0 \). The proof is completed.

4.2 Stability analysis with DoS attacks

Theorem 2. For the given positive scalars \( \bar{\tau}, \rho_{\omega z}, \gamma, \delta, \lambda_j, \), the augmented system (10) with resilient AETM (5) is stable subject to \( H_{\infty} \) performance \( \gamma \), if there exist symmetric matrices \( P > 0, R > 0, S > 0, \Theta(t), \) and matrices \( H, \Omega, L_j, F_l, i, j = 1, \ldots, n, \) such that the LMIs (11)–(14) hold with \( \bar{\theta}^T - \lambda \bar{\theta} \geq 0, \lambda_j \leq 1 \) and the resilient parameters \( \rho_k \) satisfy

\[
\rho_k \leq \frac{\sqrt{\rho_1} + 1}{1 + \bar{\delta}_k}.
\]

where

\[
\bar{\delta} = |b| (|A_k| + L_k |C_k - C_l|) + |L_k| |C_k| |\lambda_k| + \frac{1 - \sqrt{\rho_1}}{|b|}.
\]

Remark 5. For the known number of successive packet losses \( b_k \) in interval \([t_k, b_k)\), the resilient parameter \( \rho_k \) can be calculated from (18). In reverse, based on given resilient parameter \( \rho_k \), one can obtain the number of successive packet losses \( b_k \) from (18)

\[
b_k \leq \left[ \log_{|1+\Delta|} \left( \frac{1 + \sqrt{\rho_1 (t_k b_k)}}{1 + \sqrt{\rho_k}} \right) \right] h.
\]

where \( |\Delta| \) provides the largest integer smaller than or equal to \( \Delta \). Furthermore, the DoS attacks duration \( d_D^k \) in the interval \([t_k, b_k+1)\) can be derived

\[
d_D^k \leq \left[ \log_{|1+\Delta|} \left( \frac{1 + \sqrt{\rho_1 (t_k b_k)}}{1 + \sqrt{\rho_k}} \right) \right] h.
\]

Then, it is not difficult to obtain the maximum attack duration \( d_D \) = \max \{d_D^1, \ldots, d_D^n\}.

Proof. Consider a successful broadcast release interval \([t_k, t_k+1)\), and assume that there are \( b_k \) unsuccessfully transmitted broadcast packets \( t_k = d_0 < d_1 < d_2 < \ldots < d_k < d_{k+1} = t_{k+1} \). For \( p = 0, 1, \ldots, b_k \), we obtain the following equation from constraint condition (5)

\[
|\tilde{z}(d_{k+1} - b) - \tilde{z}(d_k b)| \leq \sqrt{\rho_k} |\tilde{z}(d_k b)|.
\]
Then
\[
|\hat{x}(d_{p+1} b - b)| \leq |\hat{x}(d_{p+1} b - b) - \hat{x}(d_{p} b)| + |\hat{x}(d_{p} b)|
\]
(22)
\[
\leq (1 + \sqrt{\rho_\varepsilon})|\hat{x}(d_{p} b)|.
\]

Based on (2), it follows
\[
|\hat{x}(t_k b)| = |\hat{x}(d_{p+1} b - b) + \hat{x}(t_k b) - \hat{x}(d_{p+1} b - b)|
\]
(23)
\[
\leq |\hat{x}(d_{p+1} b - b)| + |\hat{x}(d_{p+1} b - b) - \hat{x}(t_k b)|
\]
\[
\leq |\hat{x}(d_{p+1} b - b)| + \sqrt{\rho_1(t_k b)}|\hat{x}(t_k b)|.
\]
That is
\[
|\hat{x}(t_k b)| \leq \frac{1}{(1 - \sqrt{\rho_1(t_k b)})}|\hat{x}(d_{p+1} b - b)|.
\]
(24)

Then assume that there exist positive constants \(\delta_1\) such that
\[
|x(t) - \hat{x}(t)| \leq \delta_1|x(t)|.
\]
We can derive the following inequality from the solution \(x(t)|_{e = d_{p+1} b}\) of (7), (22) and (24)
\[
|\hat{x}(d_{p+1} b - b) - \hat{x}(d_{p+1} b - b)|
\]
\[
\leq \| \delta_1|A\| \hat{x}(d_{p+1} b - b)
\]
\[
+ |\delta_1|A\| \hat{x}(d_{p+1} b - b) + |\delta_1|A\| \hat{x}(d_{p+1} b - b)|
\]
\[
\leq \delta_1|\hat{x}(d_{p+1} b - b)|
\]
\[
\leq \delta_1(1 + \sqrt{\rho_\varepsilon})|\hat{x}(d_{p} b)|,
\]
(25)
where \(\delta\) is defined in Theorem 2.

For \(t \in [d_k b, d_{k+1} b]\), the state error between \(t\) and \(t_k b\) is obtained from (21) and (25)
\[
|\hat{x}(t) - \hat{x}(t_k b)|
\]
\[
\leq |\hat{x}(t) - \hat{x}(d_{k} b)| + \sum_{j=0}^{b_k-1} (\hat{x}(d_{p+1} b - b) - \hat{x}(d_{p} b))
\]
\[
+ \sum_{j=0}^{b_k-1} (\hat{x}(d_{p+1} b - b) - \hat{x}(d_{p} b))
\]
\[
\leq \sum_{j=0}^{b_k} \sqrt{\rho_\varepsilon}|\hat{x}(d_{k} b)| + \sum_{j=0}^{b_k-1} \delta_1(1 + \sqrt{\rho_\varepsilon})|\hat{x}(d_{p} b)|.
\]
(26)

From (21) and (25), it follows
\[
|\hat{x}(d_{p+1} b)| \leq |\hat{x}(d_{p+1} b) - \hat{x}(d_{p+1} b - b) |
\]
\[
+ |\hat{x}(d_{p+1} b - b) - \hat{x}(d_{p} b)| + |\hat{x}(d_{p} b)|
\]
\[
\leq (1 + \delta_1)(1 + \sqrt{\rho_\varepsilon})|\hat{x}(d_{p} b)|
\]
\[
\leq ((1 + \delta_1)(1 + \sqrt{\rho_\varepsilon}))^{b_k}|\hat{x}(t_k b)|.
\]
(27)

Then the following inequality is derived by taking (27) into (26)
\[
|\hat{x}(t) - \hat{x}(t_k b)| \leq \sum_{j=0}^{b_k} \sqrt{\rho_\varepsilon}|\hat{x}(d_{k} b)| + \sum_{j=0}^{b_k-1} \delta_1(1 + \sqrt{\rho_\varepsilon})|\hat{x}(d_{p} b)|
\]
\[
\leq ((1 + \delta_1)^{b_k}(1 + \sqrt{\rho_\varepsilon})^{b_k-1} - 1)|\hat{x}(t_k b)|.
\]
(28)

Based on (18) and (28), we have
\[
|\hat{x}(t) - \hat{x}(t_k b)| \leq \sqrt{\rho_1(t_k b)}|\hat{x}(t_k b)|.
\]
(29)

According to (29), it can be seen that the AETM (2) in Theorem 1 is ensured by the resilient AETM (5). That is to say, if the resilient AETM (5) is applied, then Theorem 2 can be easily proven from Theorem 1. This completes the proof.

4.3 The design of observer-based controller

Theorem 3. For the given positive scalars \(\varepsilon, \rho_\varepsilon, \gamma, \delta_1, \xi_1, \delta_1\) and \(b,\), the augmented system (10) with resilient AETM (5) is stable subject to \(H_\infty\) performance, if there exist symmetric matrices \(U > 0, R > 0, \delta > 0, \Theta,\) and matrices \(\Gamma, \Omega, \Gamma_i,\), such that the following LMIs hold with \(\gamma_0^2 - \lambda_j \delta_j \geq 0, 0 < \lambda_j \leq 1\)
\[
\begin{bmatrix}
\delta & \Gamma_i \\
\Gamma_i & -\delta
\end{bmatrix} \leq 0,
\]
(30)
\[
\Omega_{ij} - \Theta_i < 0,
\]
(31)
\[
\Theta_j - \delta_j \Theta_j + \lambda_j \Omega_{ij} < 0,
\]
(32)
\[
2\Theta_i - \lambda_i \Theta_i + \lambda_j \Omega_{ij} - 2\delta_j \Theta_j < 0, j < l,
\]
(33)
where
\[
\hat{\Theta}_{ij} = \begin{bmatrix}
\Phi_{ij} & \Psi_{ij} \\
* & -I
\end{bmatrix}^T
\]
\[
\begin{bmatrix}
\Psi_{ij} & \Phi_{ij} \\
* & \Psi_{ij}
\end{bmatrix}
\]
\[
= \begin{bmatrix}
\Psi_{11} & \Psi_{12} & \Psi_{13} & -\Gamma_i & -\Gamma_i & D_j \\
* & \Psi_{22} & \Psi_{23} & 0 & \Psi_{25} & 0 \\
* & * & \Psi_{33} & \Psi_{34} & 0 & 0 \\
* & * & * & \Psi_{44} & 0 & 0 \\
* & * & * & * & \Psi_{55} & 0 \\
* & * & * & * & * & \gamma^2 I
\end{bmatrix},
\]
\[
\Phi_{ij} = \begin{bmatrix}
\Psi_{11} & \Psi_{12} & \Psi_{13} & -\Gamma_i & -\Gamma_i & D_j \\
* & \Psi_{22} & \Psi_{23} & 0 & \Psi_{25} & 0 \\
* & * & \Psi_{33} & \Psi_{34} & 0 & 0 \\
* & * & * & \Psi_{44} & 0 & 0 \\
* & * & * & * & \Psi_{55} & 0 \\
* & * & * & * & * & \gamma^2 I
\end{bmatrix},
\]
\[
\Psi_{11} = A_j U + U A_j^T + T_j (C_i - C_j) + (C_i - C_j)^T T_j^T + R - \delta,
\]
\[
\Psi_{12} = T_j C_i + U (A_i - A_j)^T - (C_i - C_j)^T T_j^T,
\]
\[
\Psi_{13} = B_j \hat{F}_i + \hat{H}, \quad \Psi_{23} = T_j C_i + U A_i^T - C_i^T T_j^T,
\]
\[
\Psi_{23} = (B_i - B_j) \hat{F}_i, \quad \Psi_{25} = -(B_i - B_j) \hat{F}_i,
\]
\[\Psi_{33/j} = -\hat{R} - 2\hat{S} - \hat{H} - \hat{H}^T + \rho_{\text{ms2}}\hat{\Omega},\]
\[\Psi_{34/j} = \hat{S} + \hat{H} \Psi_{33/j} = -\rho_{\text{ms2}}\hat{\Omega}, \Psi_{35/j} = (\rho_{\text{ms2}} - 1)\hat{\Omega},\]
\[\Phi_{ij} = [C_{ij} U \ C_{ij} U \ B_i \hat{F}_i \ 0 - B_i \hat{F}_i \ 0],\]
\[\hat{\Xi}_{ij} = \tau[A_{ij} U + T_j(C_i - C_j) \ T_j C_i \ B_i \hat{F}_i \ 0 - B_i \hat{F}_i \ 0 \ 0].\]

Then the observer, controller and AETM gains are obtained as
\[F_j = \hat{F}_j U^{-1}, \ L_j = T_j OSU_1^{-1} S_1^{-1} O^{-1}, \ \Omega = U^{-1} \Omega U^{-1}.\]

**Proof.** Set \(P = \text{diag}(\hat{P}_j, \hat{P}_j), U = \hat{U}^{-1}, \ R = \hat{R} U, \ \hat{S} = \hat{S}_U \ U, \ \Omega = U \hat{\Omega} U, \ \hat{H} = \hat{H} U, \ \hat{F}_j = F_j U, \ T_j = L_j U.\) According to Lemma 2, there exists \(U = OSU_1^{-1} S_1^{-1} O^{-1}\) can make \(CU = UC\) hold. Pre- and post-multiply (12)–(14) by \(\text{diag}(U, U, U, U, I, I, I, S_1^{-1})\) and applying the inequalities \(-U \hat{S}_1 U^{-1} \leq S_1^{-1} \Omega^{-1}\), one can derive (31)–(33). In the same way, (30) can be obtained by pre- and post-multiply (11) \(\text{diag}(U, U)\).

**Remark 6.** The power-constraint DoS attacks in [41, 43] do not happen randomly but are generated periodically, which may be conservative. However, the DoS attacks in the paper are not necessary to occur periodically. It happens randomly which is more practical. In addition, we have assumed that the output matrices have a common one in this work, which is \(C_i = C \in \mathbb{R}^{p \times n}\). Compared with the particle swarm optimisation algorithm in [28] that deals with non-linear coupling problems, the system gain matrix in the paper can be obtained at once by LMIs.

### 4.4 An algorithm to obtain communication and control gains

In Theorem 3, the communication parameters \(\rho_{\text{ms2}}, \Omega\), time delay \(\bar{\tau}\), observer gain \(L_j\) and controller parameter \(F_j\) are coupled together. Besides, the above-mentioned parameters are related to network resource utilisation and control performance. Therefore, an algorithm is necessary to be introduced to calculate these parameters at the same time while ensuring the desired \(H_\infty\) performance and further improving communication efficiency. In addition, the maximum time delay \(\bar{\tau}\) is calculated by a dichotomy method. Then based on network-induced delay upper bound \(\bar{\phi}\), the simulation sample time \(b = \bar{\tau} - \phi\).

### 5 SIMULATION EXAMPLES

This section provides practical and numerical examples to demonstrate the effectiveness of proposed method. All simulations are implemented by using Matlab 8.4.0 (R2014b) running on a PC with 3.40 GHz Intel Core i7 CPU, 8GB RAM, and Windows 7 64-bit Ultimate.

**Algorithm 1** Algorithm to obtain the communication parameter \(\rho_{\text{ms2}}, \rho_b, \Omega\), allowable delay upper bound \(\bar{\tau}\), observer gain \(L_j\) and controller parameter \(F_j\).

**Step 1:** For the given number of consecutive lost packets \(b_k\), network-induced delay upper bound \(\phi\) and ET initial threshold \(\rho_{\text{ms1}}\), set ET threshold upper bound \(\rho_{\text{ms2}} = \rho_{\text{ms1}} - \mu\), where \(\mu\) is the decreased step of \(\rho_{\text{ms2}} \in (0, 1)\).

**Step 2:** If the LMIs (30)–(33) are feasible with the chosen \(\rho_{\text{ms2}}\) in Step 1, go to Step 3. Otherwise, go to Step 1.

**Step 3:** Apply the Matlab LMI toolbox and dichotomy approach to search the maximum delay upper bound \(\tau(\rho_{\text{ms2}})\) and calculate the corresponding parameters \(L_j(\rho_{\text{ms2}}), F_j(\rho_{\text{ms2}})\) and \(\Omega(\rho_{\text{ms2}})\).

**Step 4:** Choose the sampling period \(\delta = \tau(\rho_{\text{ms2}}) - \phi\). If \(\delta \leq 0\), go to Step 1, else set a simulation time \(T\), based on \(L_j(\rho_{\text{ms2}}), F_j(\rho_{\text{ms2}})\) and \(\Omega(\rho_{\text{ms2}})\) in Step 3, obtain the adaptive updated parameters \(\rho_1(b_k)\) from the communication scheme (2).

**Step 5:** Based on the given number of successive packet losses \(b_k\) and adaptive adjusted parameters value \(\rho_1(b_k)\) in Step 4, the maximum resilient AETM threshold \(\rho_2(b_k, \rho_1(b_k))\) can be derived from constraint condition (18). If \(\rho_2(b_k, \rho_1(b_k)) > 0\), set a simulation time \(T\) to validate the proposed resilient AETM (5) method by Matlab, otherwise, go to Step 6.

**Step 6:** Go to Step 1. If \(\rho_{\text{ms2}} < \rho_{\text{ms1}}\), exit.

### 5.1 Mass-spring systems

Consider the following non-linear mass-spring systems [27]
\[
\begin{align*}
\dot{x}_1 &= x_2 \\
\dot{x}_2 &= -0.01x_1 - 0.67x_1^3 + u + 0.1\omega,
\end{align*}
\]
where the MFs are chosen as \(\phi_1 = 1 - x_1^2\) and \(\phi_2 = 1 - \phi_1\), respectively, with \(x_1 \in [-1, 1]\). Then the non-linear mass-spring systems are modeled as the following T-S fuzzy model with two rules.

**Rule 1:** IF \(x_1(t)\) is \(\phi_1\), then
\[
\begin{align*}
\dot{x} &= A_1 x + B_1 u + D_1 \omega \\
\zeta &= C_{11} x + B_{11} u \\
y &= C_1 x,
\end{align*}
\]

**Rule 2:** IF \(x_1(t)\) is \(\phi_2\), then
\[
\begin{align*}
\dot{x} &= A_2 x + B_2 u + D_2 \omega \\
\zeta &= C_{12} x + B_{12} u \\
y &= C_2 x,
\end{align*}
\]
where
\[
\begin{align*}
A_1 &= \begin{bmatrix} 0 & 1 \\ -0.01 & 0 \end{bmatrix}, & A_2 &= \begin{bmatrix} 0 & 1 \\ -0.68 & 0 \end{bmatrix}, \\
B_1 &= B_2 = \begin{bmatrix} 0 & 1 \end{bmatrix}, & D_1 &= D_2 = \begin{bmatrix} 0.1 & 0 \end{bmatrix}, & B_{11} &= B_{12} = 0, \\
C_1 &= C_2 = [0.03 \ 0.2], & C_{11} &= C_{12} = [0 \ 0.1].
\end{align*}
\]
Besides, the MFs of observer and controller are considered as \( \tilde{g}_1 = 1 - \tilde{x}_{ik}^2, \tilde{g}_2 = 1 - \tilde{g}_1 \) and \( \tilde{q}_1 = 1 - \tilde{x}_{ik}^2, \tilde{q}_2 = 1 - \tilde{q}_1 \), respectively. Defining scalars \( \hat{\lambda}_1 = 0.9, \hat{\lambda}_2 = 0.7 \) to ensure \( \tilde{q}_i - \hat{\lambda}_2 \tilde{g}_i \geq 0, i = 1, 2 \). Then, by choosing AETM parameter \( \rho_{m1} = 0.5, L_{\infty} \) performance \( \gamma = 0.9 \), scalar \( \xi = 0.1 \), we obtain the allowable delay upper bound \( \tilde{r} = 0.0283 \), ET parameter matrix \( \Omega \) and co-designed controller gains from LMI conditions (30)–(33)

\[
\Omega = \begin{bmatrix}
0.4905 & 0.7384 \\
0.7391 & 1.1559 \\
\end{bmatrix}, \quad \begin{bmatrix}
L_1 \\
L_2 \\
\end{bmatrix} = \begin{bmatrix}
0.8431 \\
28.8295 \\
\end{bmatrix}, \quad \\
F_1 = [-4.3041 - 6.6487], \\
F_2 = [-4.4165 - 6.8071].
\]

In the simulation, the initial value of the system and estimated states are set to \( x = [0; -0.1] \) and \( \hat{x} = [0.3; -1] \) respectively. Choose the network-induced delay upper bound as \( \rho = 0.0083 \), then the sample time is \( b = 0.02 \). Furthermore, disturbance is assumed to be

\[
\omega(t) = \begin{cases}
1 & 0 \leq t \leq 5, \\
\frac{1}{t^2 + 1} & 8 \leq t \leq 12, \\
0 & \text{otherwise}.
\end{cases}
\]

Setting scalars \( a = 2, b = 1.2 \) and the initial value of AETM \( \rho_{m1} = 0.1 \). When the number of successive packet losses \( b_k = 1 \), the adaptive variation of \( \rho_1(t_k b) \) and \( \rho_k \) are provided in Figure 3, one can see that both them can be dynamically adjusted. Then, Figure 4(a) plots the release instants and release interval of AETM, in which only 64 times are triggered among the total time sampled 1000 times. It can be seen from the figures that the system with AETM can save network resources.

In addition, under no DoS attacks, the number of transmitted packets for different ET schemes is shown in Table 1. One can conclude that the designed AETM has smaller transmitted packets than ET generator with fixed parameters in [32–36] even if different initial values \( \rho_{m1} \) are chosen. For example, when \( \rho_{m1} = 0.2 \), only 5.6% packets are triggered through AETM. On the contrary, the ET generator with fixed parameters in [32–36] can transmit 6.4% packets, which implies that the constructed AETM can improve communication resource utilisation efficiency.

Next, if the wireless network under DoS attacks, then the corresponding AETM becomes the resilient adaptive one (5). Its parameter \( \rho_k \) is related to AETM (2) threshold parameter \( \rho_1(t_k b) \) in trigger interval \([t_k b, t_{k+1} b]\). Therefore, the corresponding ET parameters in each triggered moment are time-varying. To compensate for lost packets caused by DoS attacks, a smaller resilient AETM threshold is required to allow more packets to be transmitted in trigger interval \([t_k b, t_{k+1} b]\). When the number of successive packet losses \( b_k = 1 \), then the release instants and release interval of the resilient AETM are plotted in Figure 4(b), which has 108 trigger times. From Figure 4, one can conclude that the resilient AETM (5) can tolerate 44 times of data loss induced by cyber-attacks. Then, Figure 5 plots the response of estimation error and control input. It is can be seen that

| \( \rho_{m1} \) | 0 | 0.1 | 0.2 | 0.4 |
|---|---|---|---|---|
| In [32–36] | 1000 | 70 | 64 | 53 |
| In this work | 1000 | 64 | 56 | 50 |

| \( \rho_1(t_k b) \) | 0.1 | 0.1458 | 0.1916 | 0.2276 | 0.3653 |
|---|---|---|---|---|---|
| \( b_k = 1, \rho_k \) | 0.0214 | 0.0305 | 0.0394 | 0.0461 | 0.0710 |
| \( b_k = 2, \rho_k \) | 0.0090 | 0.0127 | 0.0163 | 0.0191 | 0.0297 |

![Figure 3](image3.png)  
**FIGURE 3** Adaptive variation of \( \rho_1(t_k b) \) and \( \rho_k \) with \( \rho_{m1} = 0.1 \) in mass-spring systems

![Figure 4](image4.png)  
**FIGURE 4** Release instants and release intervals in mass-spring systems
5.2 | Numerical example

A numerical T-S fuzzy model (6) with 2-rule is considered with the following parameters

\[
A_1 = \begin{bmatrix}
-1.0 & 0.3 & 1.5 \\
0.2 & -1.0 & 0.1 \\
-0.6 & 0.1 & 0.1
\end{bmatrix},
B_1 = \begin{bmatrix}
1.4 \\
1.0 \\
0.9
\end{bmatrix},
\]

\[
A_2 = \begin{bmatrix}
-1.4 & 0.2 & 0.1 \\
0.5 & -2.0 & 0.1 \\
-0.3 & 0.4 & 0.1
\end{bmatrix},
B_2 = \begin{bmatrix}
0.8 \\
0.1 \\
1
\end{bmatrix},
\]

\[
C_1 = C_2 = [0.6, -0.3, 0.5],
B_{11} = 0.1, B_{12} = 0.4,
\]

\[
D_1 = [0.8, 0.4, 0.9],
D_2 = [0.6, 0.2, 0.2],
\]

\[
C_{11} = [0.04, 0.2, 0.3],
C_{12} = [0.02, 0.4, 0.1].
\]

Then, the MFs of model, observer and controller are given as
\[
g_1 = \frac{1}{1 + e^{-2\xi t}},
g_2 = 1 - g_1,\]
\[
\hat{g}_1 = \frac{1}{1 + e^{-2\xi t}},
\hat{g}_2 = 1 - \hat{g}_1
\]
and \[
\hat{g}_1 = \frac{1}{1 + e^{-2\xi t}},
\hat{g}_2 = 1 - \hat{g}_1,\]

respectively. Choosing scalars \( \lambda_1 = 0.85, \lambda_2 = 0.9 \) to ensure \( \dot{\hat{g}}_1 - \lambda_1 \hat{g}_1 \geq 0 \). Setting AETM parameter \( \rho_{a2} = 0.5 \), \( H_\infty \) index \( \gamma = 1.2 \), scalar \( \xi = 0.1 \). Then, base on Algorithm 1, the maximum delay time \( \bar{\tau} = 0.0477 \), ET parameter matrix \( \Omega \) and co-designed controller gains are calculated from LMI conditions (30)–(33)

\[
\Omega = \begin{bmatrix}
0.5785 & 0.2541 & 1.3948 \\
0.2541 & 0.1167 & 0.6226 \\
1.3950 & 0.6225 & 3.3832
\end{bmatrix},
\]

\[
L_1 = \begin{bmatrix}
1.3202 \\
1.4624 \\
1.4746
\end{bmatrix},
L_2 = \begin{bmatrix}
3.1486 \\
-0.8470 \\
2.1195
\end{bmatrix},
\]

In the simulation, the initial value of system and estimation states are set as \( x_0 = [0; 0; -0.1] \) and \( \hat{x}_0 = [0; -0.1; 0] \), respectively. Setting network delay upper bound \( \varphi = 0.0177 \), then the sample time is selected as \( b = 0.035 \). Besides, the disturbance is assumed to be

\[
\omega(t) = \begin{cases}
0.1 \sin(t) & 0 \leq t \leq 8, \\
0 & \text{otherwise}
\end{cases}
\]

Under the consideration of AETM with scalars \( a = 3, b = 2 \) some simulations are presented. When the number of successive packet losses \( b_k = 2 \), the adaptive variation of \( \rho_1(t_k b) \) and \( \rho_k \) are displayed in Figure 6. Under AETM (2), the release instants and release interval is shown in Figure 7(a), which has 74 trigger times among the total time sampled 666 times. Based on the figures, it can conclude that the observer system with AETM can reduce network bandwidth.

Although the AETM (2) saves network resources in the absence of network attacks, it cannot solve data packet loss problem caused by network attacks. Hence, a smaller resilient AETM (5) threshold is needed to allow more packets to be transmitted. If under DoS attacks, the release instants and release interval of the resilient AETM (5) are plotted in

FIGURE 5 | Responses of estimation error and control input for mass-spring systems

FIGURE 6 | Adaptive variation of \( \rho_1(t_k b), \rho_k \) with \( \rho_{a1} = 0.1 \)

FIGURE 7 | Release instants and release intervals

(a) Under AETM | (b) Under resilient AETM
TABLE 3 The number of transmitted packets for different ET mechanisms under DoS attacks

| $\rho_{m1}$ | 0.1 | 0.2 | 0.3 | 0.4 |
|------------|-----|-----|-----|-----|
| In [45]    | 255 | 195 | 172 | 158 |
| In this work| 220 | 178 | 153 | 146 |

Figure 7(b), which has 220 trigger times. Figure 7 implies that the resilient AETM (5) can tolerate 146 times of data loss induced by cyber-attacks. Besides, Table 3 provides the number of transmitted packets for different ET methods under DoS attacks. It is easy to see that when $\rho_{m1}$ takes different values, the resilient AETM (5) has better network resource utilisation than the resilient ET mechanism in [45]. Furthermore, the responses of estimation error and control input are displayed in Figure 8. The above results show that the proposed resilient AETM method can improve resource utilisation efficiency and further tolerate DoS attacks with desired performance.

6 | CONCLUSIONS

This paper solves the observer-based security control issue for T-S FMB systems under energy-limited DoS attacks. The newly designed resilient AETM can not only improve resource utilisation efficiency without DoS attacks but also tolerate data loss caused by cyber-attacks. Then the MFD stability criterions are provided in three theorems to ensure the control systems are stable with desired $H_{\infty}$ performance. In addition, a fuzzy observer is constructed to estimate the unknown states and a slack matrix is introduced with the MFs information. Furthermore, the observer-based controller gains and resilient AETM parameters are derived based on Algorithm 1. Simulations about practical and numerical examples are shown to demonstrate the effectiveness of our method.

ACKNOWLEDGEMENTS

This work was supported in part by the National Natural Science Foundation of China (61773097 and U1813214), the LiaoNing Revitalisation Talents Program (XLYC1907035) and the Fundamental Research Funds for the Central Universities (N2004027).

REFERENCES

1. Tanaka, K., Sugeno, M.: Stability analysis and design of fuzzy control systems. Fuzzy Sets Syst. 45(2), 135–156 (1992)
2. Lam, H.K.: A review on stability analysis of continuous-time fuzzy-model-based control systems: From membership-function-independent to membership-function-dependent analysis. Eng. Appl. Artif. Intell. 67, 390–408 (2018)
3. Shi, K., et al.: Reliable asynchronous sampled-data filtering of T-S fuzzy uncertain delayed neural networks with stochastic switched topologies. Fuzzy Sets Syst. 381, 1–25 (2020)
4. Tanaka, K., et al.: A descriptor system approach to fuzzy control system design via fuzzy Lyapunov functions. IEEE Trans. Fuzzy Syst. 15(3), 333–341 (2007)
5. Ye, D., et al.: Fault-tolerant controller design for general polynomial-fuzzy-model-based systems. IEEE Trans. Fuzzy Syst. 26(2), 1046–1051 (2018)
6. Lam, H.K.: Stability analysis and control synthesis for fuzzy-observer-based controller of nonlinear systems: a fuzzy-model-based control approach. IET Control Theory Appl. 7(5), 663–672 (2013)
7. Xiao, B., et al.: Stabilization of interval type-2 polynomial-fuzzy-model-based control systems. IEEE Trans. Fuzzy Syst. 25(1), 205–217 (2016)
8. Song, G., et al.: Membership-function-dependent stability analysis of interval type-2 polynomial fuzzy-model-base control systems. IET Control Theory Appl. 11(17), 3156–3170 (2017)
9. Xiao, B., et al.: Sampled-data output-feedback tracking control for interval type-2 polynomial fuzzy systems. IEEE Trans. Fuzzy Syst. 28(3), 424–433 (2020)
10. Boyd, S., et al.: Linear Matrix Inequalities in System and Control Theory. SIAM, Philadelphia (1994)
11. Shen, H., et al.: Finite-time event-triggered $H_{\infty}$ control for T-S fuzzy Markov jump systems. IEEE Trans. Fuzzy Syst. 26(5), 3122–3135 (2018)
12. Pan, Y., Yang, G.H.: Event-driven fault detection for discrete-time interval type-2 fuzzy systems. IEEE Trans. Syst., Man, Cybern., Syst., (2019), doi: 10.1109/TSMC.2019.2945065
13. Zhang, J., et al.: A novel observer-based output feedback controller design for discrete-time fuzzy systems. IEEE Trans. Fuzzy Syst. 23(1), 225–229 (2014)
14. Li, H., et al.: Observer-based fuzzy control for nonlinear networked systems under unmeasurable premise variables. IEEE Trans. Fuzzy Syst. 24(5), 1233–1245 (2015)
15. Zhang, T.Y., Ye, D.: False data injection attacks with complete stealthiness in cyber-physical systems: A self-generated approach. Automatica 120, 109117 (2020)
16. Shi, K., et al.: Hybrid-driven finite-time $H_{\infty}$ sampling synchronization control for coupling memory complex networks with stochastic cyber attacks. Neurocomputing 387, 241–254 (2020)
17. Ye, D., Zhang, T.Y.: Summation detector for false data-injection attack in cyber-physical systems. IEEE Trans. Cyber. 50(6), 2338–2345 (2020)
18. Yang, C., et al.: DoS attack in centralised sensor network against state estimation. IET Control Theory Appl. 12(9), 1244–1253 (2018)
19. Zhang, T., Ye, D.: Distributed secure control against denial-of-service attacks in cyber-physical systems based on K-connected communication topology. IEEE Trans. Cyber. 50(7), 3094–3105 (2020)
20. Foroush, H.S., Martinez, S.: On event-triggered control of linear systems under periodic denial-of-service jamming attacks. In: Proceedings of 51st IEEE Annual Conference on Decision and Control, Maui (2012)
21. Niemoczyński, B., et al.: Stability of discrete-time networked control systems under denial of service attacks. In: Resilience Week (RWS), Chicago (2016)
22. Befekadu, G.K., et al.: Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies. IEEE Trans. Autom. Control 60(10), 3299–3304 (2015)
23. Amin, S., et al.: Safe and secure networked control systems under denial-of-service attacks. In: Proceedings of Hybrid Systems: Computation and Control, San Francisco (2009)
24. De Persis, C., Tesi, P.: Input-to-state stabilizing control under denial-of-service. IEEE Trans. Autom. Control 60(11), 2930–2944 (2015)
25. Feng, S., Tesi, P.: Resilient control under denial-of-service: Robust design. Automatica 79, 42–51 (2017)
26. Yuan, Y., et al.: Resilient control of networked control system under DoS attacks: A unified game approach. IEEE Trans. Ind. Inf. 12(5), 1786–1794 (2016)
27. Zhang, H., et al.: Fuzzy model-based robust networked control for a class of nonlinear systems. IEEE Trans. Syst., Man, Cybern. A, Syst., Humans 39(2), 437–447 (2009)
28. Zhang, D., et al.: Network-based modeling and proportional-integral control for direct-drive-wheel systems in wireless network environments. IEEE Trans. Cybern. 50(6), 2462–2474 (2020)
29. Bagzadehnoe, B., et al.: Fuzzy-model-based fault detection for nonlinear networked control systems with periodic access constraints and Bernoulli packet dropouts. Appl. Soft Comput. 80, 465–474 (2019)
30. Yang, F., et al.: Mode-independent fuzzy fault-tolerant variable sampling stabilization of nonlinear networked systems with both time-varying and random delays. Fuzzy Sets Syst. 207, 45–63 (2012)
31. Vali, M.H., et al.: Designing a neuro-sliding mode controller for networked control systems with packet dropout. Int. J. Eng. Trans. A: Basics 29(4), 490–499 (2016)
32. Zhang, X.M., Han, Q.L.: Event-triggered dynamic output feedback control for networked control systems. IET Control Theory Appl. 8(4), 226–234 (2014)
33. Deng, C., et al.: Event-triggered consensus of linear multi-agent systems with time-varying communication delays. IEEE Trans. Cybern. 50(7), 2916–2925 (2020)
34. Peng, C., Yang, T.: Event-triggered communication and $H_{\infty}$ control co-design for networked control systems. Automatica 49, 1326–1332 (2013)
35. Peng, C., et al.: Observer-based non-PDC control for networked T-S fuzzy systems with an event-triggered communication. IEEE Trans. Cybern. 47(8), 2279–2287 (2017)
36. Zhang, D., et al.: Network-based output tracking control for T-S fuzzy systems using an event-triggered communication scheme. Fuzzy Sets Syst. 273, 26–48 (2015)
37. Shi, K., et al.: Some novel approaches on state estimation of delayed neural networks. Inf. Sci. 372, 313–331 (2016)
38. Peng, C., et al.: Adaptive event-triggering $H_{\infty}$ load frequency control for network-based power systems. IEEE Trans. Ind. Electron. 65(2), 1685–1694 (2018)
39. Liu, J., et al.: Quantized stabilization for T-S fuzzy systems with hybrid-triggered mechanism and stochastic cyber-attacks. IEEE Trans. Fuzzy Syst. 26(6), 3820–3834 (2018)
40. Sun, Y., Yang, G.H.: Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks. J. Frankl. Inst. 355(13), 5613–5631 (2018)
41. Hu, S., et al.: Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. IEEE Trans. Cybern. 49(12), 4271–4281 (2019)
42. Liu, J., et al.: Security distributed state estimation for nonlinear networked systems against denial-of-service attacks. Int. J. Robust Nonlinear Control 30(2), 1156–1180 (2020)
43. Liu, J., et al.: Event-triggered $H_{\infty}$ load frequency control for multi-area power systems under hybrid cyber attacks. IEEE Trans. Syst., Man, Cybern., Syst. 49(8), 1665–1678 (2019)
44. Liu, J., et al.: Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks. IEEE Trans. Cybern. (2020), doi: 10.1109/TCYB.2020.2970556
45. Peng, C., et al.: Resilient event-triggered $H_{\infty}$ load frequency control for multi-area power systems with energy-limited DoS attacks. IEEE Trans. Power Syst. 32(5), 4110–4118 (2017)

How to cite this article: Li X, Ye D. Membership-function-dependent security control for networked T-S fuzzy-model-based systems against DoS attacks. IET Control Theory Appl. 2021;15:360–371. https://doi.org/10.1049/cth2.12048