Security-based Fuzzy Control for Nonlinear Networked Control Systems with DoS Attacks via a Resilient Event-Triggered Scheme

Yingnan Pan, Yanmin Wu, and Hak-Keung Lam, Fellow, IEEE

Abstract—This paper studies the issue of resilient event-triggered (RET) based security controller design for nonlinear networked control systems (NCSs) described by interval type-2 (IT2) fuzzy models subject to non-periodic denial of service (DoS) attacks. Under the non-periodic DoS attacks, the state error caused by the packets loss phenomenon is transformed into an uncertain variable in the designed event-triggered condition. Then, an RET strategy based on the uncertain event-triggered variable is firstly proposed for the nonlinear NCSs. The existing results that utilized the hybrid triggered scheme have the defect of complex control structure, and most of the security compensation methods for handling the impacts caused by DoS attacks need to transmit some compensation data when the DoS attacks disappear, which may lead to large performance loss of the systems. Different from these existing results, the proposed RET strategy can transmit the necessary packets to the controller under non-periodic DoS attacks to reduce the performance loss of the systems and a new security controller subject to the RET scheme and mismatched membership functions is designed to simplify the control structure under DoS attacks. Finally, some simulation results are utilized to testify the advantages of the presented approach.

Index Terms—Interval type-2 (IT2) fuzzy models, denial of service (DoS) attacks, resilient event-triggered (RET) strategy, mismatched membership functions.

I. INTRODUCTION

URING the last few decades, due to the advantages of network communication and remote control, networked control systems (NCSs) were extensively used in actual projects, and lots of significant results were presented by using fuzzy control and neural network approaches [1]–[9]. However, the problem of limited network bandwidth cannot be disregarded in the NCSs. By considering the limited network bandwidth issue, P. Tabuada firstly proposed an event-triggered (ET) scheme for achieving control tasks in [10]. Different from the time-triggered mechanism, the ET control scheme [11] can reduce unnecessary packets transmission and select some packets that satisfy ET conditions to be transmitted into the network. Owing to this feature, the ET control scheme has been widely applied such as [12]–[17]. A model-based networked predictive strategy was studied by combining ET schemes in [12]. Zhang et al. studied the issue of sampled-data-based ET filtering in [13]. An ET and $H_{\infty}$ control co-design approach for NCSs subject to packet loss was provided in [17]. It is worth noting that these mentioned results can only be applied for linear NCSs.

As a powerful nonlinear approximation tool, the Takagi-Sugeno (T-S) fuzzy modeling technique was employed in many fields. In recent ten years, some significant works by combining T-S fuzzy model and ET scheme have been reported. To name a few, an ET fault detection filter was designed for NCSs with biased sensor faults in [18]. In [19], the authors investigated a new ET controller with varying gains, and an online iteration algorithm was designed to obtain the newly updated gains. The issue of fault detector combined with controller design was solved in [20]. In addition, considering the uncertain parameters in the system, an interval type-2 (IT2) fuzzy modeling and control method under the fuzzy-model-based framework was proposed for the first time in [21], [22] that the imperfect premise matching concept and membership-function-dependent techniques were proposed to support the system analysis and control design. Some significant ET-based literatures about IT2 fuzzy NCSs were presented in [23]–[25]. Pan et al. solved the issue of fault detection filter design based on ET scheme for nonlinear NCSs in [23]. In [24], a dynamic output feedback (DOF) control strategy was studied under the structure of IT2 fuzzy systems. Tang et al. studied the issue of ET predictive control based on DOF model in [25]. However, the above works only considered the network bandwidth limitation situation of the NCSs.

From the aspect of network security, although the utilization of ET communication scheme reduces unnecessary data transmission, the corresponding network security issue still may occur. The cause of network security problems mainly results from malicious network attacks. In the actual project, malicious network attacks will cause system paralysis and serious security accidents. Therefore, the investigations on the attack and defense of cyber attacks have become an important field, recently. In general, malicious attacks for communication networks are divided into two common attack types: deception attacks [26]–[28] and denial of service (DoS) attacks [29], [30]. The method of deception attacks is to intercept data and tamper with the content to make the NCSs breakdown. The DoS attacks can hinder the transmission of data in the communication network and cause NCSs cannot work.
properly. Recently, many excellent works about the security control under DoS attacks have been published [31]–[36]. A decentralized ET strategy was proposed for cyber-physical systems subject to DoS attacks in [31]. A state-feedback controller was designed for NCSs with DoS attacks satisfying the Bernoulli distribution in [32]. Hu et al. [32] designed a new $H_\infty$ filter for NCSs with nonperiodic DoS attacks in [33].

For confronting the influences of DoS attacks, resilient state feedback controllers were designed for NCSs in [34]. Although the works mentioned above have proposed corresponding security control schemes, these works only were considered for linear systems. For considering the security control problem of nonlinear NCSs, Tang et al. [35] proposed a hybrid ET (HET) scheme to guarantee the security of formation control for nonlinear MASs with DoS attacks. In addition, resilient fixed-time observers were designed for high-order MASs against DoS attacks in [36]. In most of the existing works, the proposed methods can recompense the impacts caused by DoS attacks when the DoS attacks disappear. Although the HET scheme [37] was proposed in order to protect system operation under DoS attacks, the approach has the disadvantages of complex control structure and high cost. Up to present, under the authors’ knowledge, few works addressed the intractable problem of security control for IT2 fuzzy systems. Considering the simple control structure and low cost, how to design a new controller to counter the effects of non-periodic DoS attacks for IT2 fuzzy NCSs is a challenging issue that needs to be handled, which inspires this work.

In this paper, considering non-periodic DoS attacks, a new controller based on RET scheme is designed for IT2 fuzzy NCSs. The major contributions are given below:

1) An RET communication scheme based on the resilient control scheme and ET mechanism is proposed firstly for the IT2 fuzzy NCSs. Compared with the existing results, the RET communication scheme can provide the necessary data transmission for the controller under non-periodic DoS attacks and simplify the network control structure.

2) A novel RET based security controller for nonlinear NCSs is designed to effectively reduce the performance loss of the systems in the presence of non-periodic DoS attacks.

3) By considering the parameter uncertainties, mismatched membership functions and non-periodic DoS attacks, a new method to obtain the conditions of guaranteeing systems stability and designing the security controller is provided for the IT2 fuzzy NCSs.

The structure is arranged below. Problem formulation is introduced in Section II. Section III describes the main results. Simulation verification and the conclusion are given, respectively, in Sections IV and V.

II. Problem Formulation

A. IT2 T-S Fuzzy Models

The nonlinear continuous-time systems can be modeled by the following IT2 T-S fuzzy models:

\[
\dot{x}(t) = A_i x(t) + B_i u(t) + B_{w_1} w(t),
\]

\[
z(t) = C_i x(t) + D_i u(t),
\]

where $i = 1, 2, \ldots, r$ ($r$ denotes the number of inference rules), $A_i$, $B_i$, $B_{w_1}$, $C_i$, and $D_i$ stand for appropriate parameter matrices. The MFs of IT2 fuzzy systems can be defined below [21]:

\[
m_i(x(t)) = \prod_{b=1}^{p} \bar{\mu}_{v_b}^i(\phi_b(x(t))) \geq 0,
\]

\[
\tilde{m}_i(x(t)) = \prod_{b=1}^{p} \tilde{\bar{\mu}}_{v_b}^i(\phi_b(x(t))) \geq 0,
\]

\[
\tilde{\bar{\mu}}_{v_b}^i(\phi_b(x(t))) \geq \bar{\mu}_{v_b}^i(\phi_b(x(t))) \geq 0,
\]

\[
\bar{m}_i(x(t)) \geq \tilde{m}_i(x(t)) \geq 0,
\]

where $\bar{\mu}_{v_b}^i(\phi_b(x(t)))$ is the lower grade of membership, and $\tilde{\bar{\mu}}_{v_b}^i(\phi_b(x(t)))$ is the upper grade of membership, $\bar{m}_i(x(t))$ and $\tilde{m}_i(x(t))$ denote lower and upper MFs.

Thus, the global dynamics model can be obtained by

\[
\dot{x}(t) = \sum_{i=1}^{r} m_i(x(t)) [A_i x(t) + B_i u(t) + B_{w_1} w(t)],
\]

\[
z(t) = \sum_{i=1}^{r} m_i(x(t)) [C_i x(t) + D_i u(t)],
\]

where

\[
m_i(x(t)) = \frac{\bar{m}_i(x(t))}{\sum_{i=1}^{r} \bar{m}_i(x(t))}, \quad m_i(x(t)) \geq 0,
\]

\[
\tilde{m}_i(x(t)) = \tilde{\bar{\mu}}_{i}^i(x(t)) m_i(x(t)) + \tilde{\bar{\mu}}_{i}^i(x(t)) \bar{m}_i(x(t)),
\]

\[
0 \leq \tilde{\bar{\mu}}_{i}^i(x(t)) \leq 1, \quad 0 \leq \tilde{\bar{\mu}}_{i}^i(x(t)) \leq 1,
\]

\[
\sum_{i=1}^{r} m_i(x(t)) = 1, \quad \bar{\mu}_{i}^i(x(t)) + \bar{\mu}_{i}^i(x(t)) = 1,
\]

\[
m_i(x(t)) \text{ is the normalized MF.} \quad \bar{\mu}_{i}^i(x(t)) \text{ and } \tilde{\bar{\mu}}_{i}^i(x(t)) \text{ are the weighting functions.}
\]

B. Energy-Limited DoS Attacks

The structure of the NCSs with DoS attacks is plotted in Fig. 1. The data packets cannot transmit normally under DoS attacks. As a result, the controller cannot acquire the triggering data packet at the corresponding instance. DoS attacks will cause serious system errors and wreck the system performance.

**Assumption 1:** The energy of each DoS attack is limited, and the attacker cannot re-attack during a malicious intrusion period.
To express the sequence of DoS attacks from on to off, the expression is described as follows:

$$H_n = \{h_n\} \cup [h_n, h_n + \xi_n],$$  \hspace{1cm} (3)

where $h_n > 0$, and $\xi_n \in \mathbb{R}$ $\geq 0$ stands for the duration of DoS attacks. In this paper, we assume that $\xi_n > 0$ in order to better reflect the effect of DoS attacks. In addition, all single attack ranges are expressed as follows:

$$T(0,t) = \bigcup_{n \in \mathbb{N}} H_n.$$  \hspace{1cm} (4)

### C. Resilient Event-Triggered Scheme

We will analyze the effect of DoS attacks on ET condition in this subsection. Assumptions 2 and 3 are provided below.

**Assumption 2:** The sampling period is $h$. The sensor and the controller are time-triggered and ET, respectively. In addition, the sampling sequence of the sensor is given as $S_1 = \{0, h, 2h, \ldots, i_k h\}$, $i_k \in \mathbb{N}$. The triggered sampling sequence is defined as $S_2 = \{0, t_1 h, t_2 h, \ldots, t_k h\}$, $t_k \in \mathbb{N}$. And, we have $S_2 \subset S_1$.

**Assumption 3:** DoS attacks may occur at arbitrary instants, but they cannot occur when $i_k h = 0$ to ensure that the controller can obtain the initial data. $\zeta(i_k h)$ in (5) is provided to represent whether there are DoS attacks at the current instant. Furthermore, we consider the limit duration of DoS attacks $\Delta_{t_{k+1} h}^{\text{dos}} \neq 0$, and the limit duration meets (6) and (7).

$$\zeta(i_k h) = \begin{cases} 1, & \text{DoS attack,} \\ 0, & \text{no DoS attack,} \end{cases}$$  \hspace{1cm} (5)

$$\Delta_{t_{k+1} h}^{\text{dos}} = t_{k+1} h - t_k h,$$  \hspace{1cm} (6)

$$\Delta_{t_{k+1} h}^{\text{dos}} \leq \Delta_{\text{dos}},$$  \hspace{1cm} (7)

where $t_{k+1}^{\text{dos}} h$ represents that the DoS attacks start at $t_{k+1} h$ and end at $t_{k+1}^{\text{dos}} h$, $\Delta_{\text{dos}}$ stands for the maximum time of DoS attacks. And, we define

$$e(i_k h) = x(i_k h) - x(t_k h),$$  \hspace{1cm} (8)

where $i_k h = t_k h + l h$ ($l \in \mathbb{N}$), $e(i_k h)$ is the error between the sampling packet $x(i_k h)$ and the last successfully transmitted packet $x(t_k h)$.

Additionally, under DoS attacks, the error can be written as follows:

$$e^{\text{dos}}(i_k h) = x(i_k h)_{\text{dos}} - x(t_{k+1} h),$$  \hspace{1cm} (9)

where $x(i_k h)_{\text{dos}}$ is the sampling state vector under DoS attacks.

An RET communication mechanism is introduced in this paper, and the RET condition is given as follows:

$$t_{k+1}^{\text{dos}} h = t_k h + \min_{l \geq 1} \{h|\delta x^T(t_k h) \Phi x(t_k h) - e^T(i_k h) \Phi e(i_k h) + \zeta(i_k h) \Upsilon(\Delta_{t_{k+1} h}^{\text{dos}}) \leq 0\},$$  \hspace{1cm} (10)

and

$$\Upsilon(\Delta_{t_{k+1} h}^{\text{dos}}) \leq \Upsilon,$$  \hspace{1cm} (11)

where $\delta \in (0, 1)$ represents the threshold of RET scheme, and $\Phi > 0$ is the weight matrix. $\Upsilon(\Delta_{t_{k+1} h}^{\text{dos}}) = (e^{\text{dos}}(i_k h))^T \Phi e^{\text{dos}}(i_k h)$ denotes the variation of the RET condition caused by DoS attacks. $\Upsilon$ represents the maximum variation of the RET condition under DoS attacks.

**Remark 1:** Under DoS attacks, the maximum performance loss value is introduced in the ET condition such that a great number of packets loss. Thereupon, the phenomenon of continuous packets loss caused by DoS attacks can be transformed into the RET condition (10) in the procedure of DoS attacks launched by the attacker. The RET condition (10) will revert to the normal ET condition when there are no DoS attacks.

**Remark 2:** Different from the existing literature [32] which considered DoS attacks with point attack method that satisfies the Bernoulli distribution, this paper considers the non-periodic DoS attacks method with indefinite time interval. The attacking approach considered in this paper can better reflect the authenticity of DoS attacks. Owing to that the initial sampling packet should be transmitted to the fuzzy controller, thus, the DoS attacks cannot occur when $i_k h = 0$.

**Remark 3:** Different from the existing literature [38] which employed secure adaptive ET communication scheme to recommend the impacts caused by DoS attacks when the DoS attacks disappear, this paper uses the RET communication scheme that can provide the necessary data transmission for the controller under non-periodic DoS attacks to effectively reduce the performance loss of the systems. By combining the ET scheme and the scheme of resilient control, three work patterns are depicted in Fig. 2.

a. Stability region. The ET condition will not change in the absence of DoS attacks.

b. Resilient region. The ET condition is converted to the RET condition under DoS attacks. In addition, the error is within the tolerance of NCSs.

c. Un-safety region. The ET condition is converted to the RET condition in the presence of DoS attacks. However, the error is beyond the tolerance of NCSs.

### D. IT2 T-S Fuzzy Controller

**Controller Rule f:** IF $\varphi_1(x(t_k h))$ is $n_1^f$, and $\varphi_2(x(t_k h))$ is $n_2^f$, and $\ldots$, and $\varphi_r(x(t_k h))$ is $n_r^f$, THEN:

$$u(t) = K_j x(t_k h),$$  \hspace{1cm} (12)

where $K_j$ ($j = 1, \ldots, r$) denote the controller gains to be determined. The MFs of the RET based controller are given.
as follows:

\[
\bar{w}_j(x(t_k h)) = \prod_{q=1}^{\rho} g_{n_q}(\varphi_q(x(t_k h))) \geq 0,
\]

\[
\bar{\omega}_j(x(t_k h)) = \prod_{q=1}^{\rho} g_{n_q}(\varphi_q(x(t_k h))) \geq 0,
\]

\[
\bar{g}_{n_q}(\varphi_q(x(t_k h))) \geq g_{n_q}(\varphi_q(x(t_k h))) \geq 0,
\]

\[
\bar{w}_j(x(t_k h)) \geq w_j(x(t_k h)) \geq 0,
\]

where \( g_{n_q}(\varphi_q(x(t_k h))) \) and \( g_{n_q}(\varphi_q(x(t_k h))) \) are the upper and lower grades of membership. \( \bar{w}_j(x(t_k h)) \) and \( \bar{w}_j(x(t_k h)) \) denote upper and lower MFs (ULMFs). Thus, the controller (12) is rewritten by

\[
u(t) = \sum_{j=1}^{r} w_j(x(t_k h)) [K_j x(t_k h)], \tag{13}
\]

where

\[
w_j(x(t_k h)) = \bar{w}_j(x(t_k h)) - \sum_{j=1}^{r} \bar{\omega}_j(x(t_k h)) \geq 0,
\]

\[
\bar{\omega}_j(x(t_k h)) = \frac{\bar{w}_j(x(t_k h))}{\sum_{j=1}^{r} \bar{w}_j(x(t_k h))} \geq 0,
\]

\[
\bar{g}_{n_q}(\varphi_q(x(t_k h))) \geq g_{n_q}(\varphi_q(x(t_k h))) \geq 0,
\]

\[
\bar{w}_j(x(t_k h)) \geq w_j(x(t_k h)) \geq 0,
\]

\[
\bar{w}_j(x(t_k h)) \text{ is the normalized MFs,} \bar{w}_j(x(t_k h)) \text{ and} \bar{w}_j(x(t_k h)) \text{ are non-linear weighting functions. In what follows,} m_i \triangleq m_i(x(t)), w_j \triangleq w_j(x(t_k h)).
\]

\section{E. Actuator Failure Model}

During the system long-term operation, actuator failure is considered and its model is described as follows:

\[
u_f(k) = fu(k), \tag{14}
\]

\section{F. The Closed-Loop System}

Similar to [17], we introduce the communication delays \( \tau_k \).

\[
\tau_k = [t_k h + \tau_k, t_k h + \tau_k + 1]
\]

with \( \Pi = \cup \Pi_k \). Define \( \eta(t) = t - t_k h \). The input \( u(t) \) of the systems can be rewritten as follows:

\[
u(t) = \sum_{j=1}^{r} w_j(K_j [x(t - \eta(t)) - e(i_k h)]), \tag{15}
\]

By combining (2), (14) and (15), the closed-loop system can be described by

\[
\dot{x}(t) = \sum_{i=1}^{r} m_i w_j(A_{ij} x(t) + B_{ij} x(t - \eta(t)) - \bar{B}_{ij} e(i_k h) + \bar{B}_{w_i} w(t)), \tag{16}
\]

\[
z(t) = \sum_{i=1}^{r} m_i w_j(\tilde{C}_{ij} x(t) + \tilde{D}_{ij} x(t - \eta(t)) - \tilde{D}_{ij} e(i_k h)),
\]

where \( A_{ij} = A_i, B_{ij} = fB_i K_j, \bar{B}_{w_i} = B_{w_i}, \tilde{D}_{ij} = fD_i K_j. \)

The main control objectives of this paper can be summed below:

1) In the absence of DoS attacks, the closed-loop system (16) is asymptotically stable and meets the following \( H_\infty \) performance:

\[
||z(t)||^2_2 \leq \beta^2 ||w(t)||^2_2.
\]

2) In the presence of DoS attacks, the closed-loop system (16) achieves the security performance that satisfies uniformly ultimately bounded. And, the performance loss satisfies \( ||L(x(t))|| \leq G \), where \( ||L(x(t))|| \) denotes the performance loss under DoS attacks. \( G \) is the upper bound of the performance loss.

\section{III. Main Results}

In this part, we will verify that the system (16) is asymptotically stable when \( \zeta(i_k h) = 0 \) and \( w(t) = 0 \) and analyze the security performance of NCSs with DoS attacks. In addition, sufficient conditions of the controller design are provided.

\textbf{Theorem 1}: Given known parameters \( \delta > 0, \eta_M > 0 \) and \( \beta > 0 \), by considering the RET, if there exist matrices \( P > 0, R > 0, Q > 0 \) and \( M \) containing (1 \leq i, j \leq r)

\[
\sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \Xi_{ij} < 0, \tag{17}
\]

\[
\sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \Xi_{ij} < 0, \tag{18}
\]

\[
\begin{bmatrix} Q & M \end{bmatrix} \geq 0, \tag{19}
\]

\section{IV. Conclusion}

In this paper, the security issues due to DoS attacks in NCSs are studied. The main results are as follows:

1) The closed-loop system (16) is asymptotically stable when \( \zeta(i_k h) = 0 \) and \( w(t) = 0 \) and the security performance of NCSs with DoS attacks is analyzed.

2) The sufficient conditions of controller design are provided.

3) The control objectives of this paper can be summed below:

\[
||z(t)||^2_2 \leq \beta^2 ||w(t)||^2_2.
\]
where

\[ \Xi_{ij} = \begin{bmatrix} \Sigma_1 & \Sigma_2 & -M^T & \Sigma_3 & \Sigma_4 \\ * & \Sigma_5 & Q + M^T & \Sigma_6 & \eta^2_M B_{ij}^T Q B_{wi} \\ * & * & -R - Q & 0 & 0 \\ * & * & * & \Sigma_7 & -\eta^2_M B_{ij}^T Q B_{wi} \\ * & * & * & * & \Sigma_8 \end{bmatrix}, \]

\[ \Sigma_1 = H e(P A_{ij} + R - Q + \bar{C}_{ij} \bar{D}_{ij} + \eta^2_M \bar{A}_{ij}^T \bar{Q} \bar{A}_{ij}), \]

\[ \Sigma_2 = P \bar{B}_{ij} + Q + M^T + \bar{C}_{ij} \bar{D}_{ij} + \eta^2_M \bar{A}_{ij}^T \bar{Q} \bar{B}_{ij}, \]

\[ \Sigma_3 = -P \bar{B}_{ij} - \bar{C}_{ij} \bar{D}_{ij} - \eta^2_M \bar{A}_{ij}^T \bar{Q} \bar{B}_{ij}, \]

\[ \Sigma_4 = P \bar{B}_{wi} + \eta^2_M \bar{A}_{ij} Q B_{wi}, \]

\[ \Sigma_5 = -2Q - M - M^T + \eta^2_M B_{ij}^T Q B_{ij} - \bar{D}_{ij}^T \bar{D}_{ij}, \]

\[ \Sigma_6 = -\eta^2_M B_{ij}^T Q B_{ij} - \bar{D}_{ij}^T \bar{D}_{ij}, \]

\[ \Sigma_7 = -\beta^2 I + \eta^2_M B_{ij}^T Q B_{wi}, \]

\[ \Sigma_8 = \bar{D}_{ij}^T \bar{D}_{ij}, \]

and then, the system (16) contains the control objectives below:

S.1: In the absence of DoS attacks, the system (16) is asymptotically stable and meets $H_{\infty}$ performance.

S.2: In the presence of DoS attacks, the closed-loop system contains the security performance which satisfies uniformly ultimately bounded $||x(t)|| \leq \sqrt{\frac{\zeta(i_k) \gamma(\Delta_{d+1})}{\lambda(P)^2}}$. The performance loss satisfies

\[ G = \{||L(x(t))|| \leq \sqrt{\frac{\zeta(i_k) \gamma(\Delta_{d+1})}{\rho \lambda(P)^2}}\}, \]

where $\rho$ denotes a positive scalar and $\lambda(P)$ stands for the minimum eigenvalue of $P$.

**Proof:** Choose the Lyapunov-Krasovskii functional as follows:

\[ \mathcal{V}(t) = \mathcal{V}_1(t) + \mathcal{V}_2(t) + \mathcal{V}_3(t), \]

where

\[ \mathcal{V}_1(t) = x^T(t) P x(t), \]

\[ \mathcal{V}_2(t) = \int_{t-\eta_M}^{t} x^T(s) R x(s) ds, \]

\[ \mathcal{V}_3(t) = \eta_M \int_{t+\theta}^{t} \int_{t-\eta_M}^{t} \dot{x}^T(s) Q \dot{x}(s) ds d\theta. \]

By computing the time derivative of $\mathcal{V}(t)$, one obtains

\[ \dot{\mathcal{V}}_1(t) = 2x^T(t) \dot{x}(t) \]

\[ = \sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j 2x^T(t) P [\bar{A}_{ij} x(t) + \bar{B}_{ij} x(t - \eta_M) - \bar{B}_{ij} e(i_k h) + \bar{B}_{wi} w(t)], \]

\[ \dot{\mathcal{V}}_2(t) = x^T(t) Rx(t) - x^T(t - \eta_M) Rx(t - \eta_M), \]

\[ \dot{\mathcal{V}}_3(t) = \eta^2_M \dot{x}^T(t) Q \dot{x}(t) - \eta_M \int_{t-\eta_M}^{t} \dot{x}^T(s) Q \dot{x}(s) ds. \]

Since \[ \begin{bmatrix} Q & M \end{bmatrix} \geq 0, \]

and \[ -\eta_M \int_{t-\eta_M}^{t} \dot{x}^T(s) Q \dot{x}(s) ds \]

\[ \leq -[x(t - \eta_M) - x(t - \eta_M)]^T Q[x(t - \eta_M) - x(t - \eta_M)] - [x(t - x(t - \eta_M))]^T Q[x(t - x(t - \eta_M))] + 2|x(t - \eta_M) - x(t - \eta_M)|^T M[x(t - x(t - \eta_M))]. \]

Then, we can obtain

\[ J(t) = \dot{\mathcal{V}}(t) + z(t)^T z(t) - \beta^2 w(t)^T w(t) \]

\[ \leq \sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \xi^T(t) [\Xi_{ij}] \xi(t), \]

where $\xi^T(t) = [x^T(t), x^T(t - \eta_M), e^T(i_k h), w(t)^T]$. Based on (17), we can get

\[ J(t) = \dot{\mathcal{V}}(t) + z(t)^T z(t) - \beta^2 w(t)^T w(t) \leq 0. \]

Therefore, we know that the system (16) is asymptotically stable and possesses $H_{\infty}$ performance without DoS attacks.

Next, we will further analyze the security performance of the system. By considering the RET condition (10), then, one obtains

\[ \mathcal{V}(t) \leq \dot{\mathcal{V}}(t) + \zeta(i_k h) \gamma(\Delta_{d+1}) + \delta x^T(t) \dot{x}(t) \Phi x(t) + e^T(i_k h) \Phi e(i_k h) \]

\[ = \sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \xi^T(t) [\Theta_{1ij} + \Theta_{2ij} \xi(t)], \]

\[ + \Theta_{3ij} Q \Theta_{3ij}^T \xi(t) + \zeta(i_k h) \gamma(\Delta_{d+1}) \]

\[ = \sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \xi^T(t) \Xi_{ij} \xi(t) + \zeta(i_k h) \gamma(\Delta_{d+1}) \gamma(\Delta_{d+1}). \]

According to \[ \sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \Xi_{ij} < 0, \] we have

\[ \sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \xi^T(t) \Xi_{ij} \xi(t) \leq 0. \]

Moreover, there should exist a suitable parameter $\rho > 0$ such that \[ \sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \xi^T(t) \Xi_{ij} \xi(t) \leq -\rho \mathcal{V}(t) \]

holds.

From (24), one has

\[ \mathcal{V}(t) \leq -\rho \mathcal{V}(t) + \zeta(i_k h) \gamma(\Delta_{d+1}). \]
By multiplying $e^{-pt}$ and integrating on both sides of (25), it yields
\[ \mathcal{V}(t) = e^{-pt}\mathcal{V}(0) + \frac{\zeta(ikh)\Upsilon(\Delta_{t+1}^{dos})}{\rho} (1 - e^{-pt}) \]
\[ \leq \mathcal{V}(0) + \frac{\zeta(ikh)\Upsilon(\Delta_{t+1}^{dos})}{\rho}, \]
Furthermore, one can get
\[ x^T(t)Px(t) \leq \mathcal{V}(t) \leq \mathcal{V}(0) + \frac{\zeta(ikh)}{\rho} \Upsilon(\Delta_{t+1}^{dos}), \]
\[ \|x(t)\| \leq \sqrt{\frac{\mathcal{V}(0) + \frac{\zeta(ikh)}{\rho} \Upsilon(\Delta_{t+1}^{dos})}{\lambda(P)}}, \]
where $\lambda(P)$ stands for the minimum eigenvalue of $P$.

We further express the performance loss by the following expression:
\[ G \in \{L(x(t)) : |L(x(t))| \leq \sqrt{\frac{\zeta(ikh)\Upsilon(\Delta_{t+1}^{dos})}{\rho\lambda(P)}}\}, \]
where $G = \sqrt{\frac{\zeta(ikh)\Upsilon(\Delta_{t+1}^{dos})}{\rho\lambda(P)}}$. The analysis of security performance is completed.

Taking the issues of the asynchronous premise variables and mismatched MFs into account, in Theorem 2, to obtain more relaxed results, the information of MFs and slack matrices are employed.

**Theorem 2:** Given scalars $\delta > 0$, $\eta_M > 0$, $\delta_j > 0$, by considering the RET scheme (10), if the MFs satisfy $w_j - \delta_j m_j \geq 0$ ($0 < \delta_j \leq 1$), and there exist matrices $P > 0$, $R > 0$, $Q > 0$, and $M$ contending ($1 \leq i, j \leq r$)
\[ \Xi_{ij} - A_i < 0, \quad (26) \]
\[ \dot{\rho}_i \Xi_{ii} - \dot{\rho}_j A_i + \dot{\rho}_j A_i < 0, \quad (27) \]
\[ \dot{\rho}_i \Xi_{ij} - \dot{\rho}_j A_i + \dot{\rho}_j \Xi_{ji} - \dot{\rho}_j A_j + \dot{\Lambda}_j < 0, \quad (28) \]
\[ \begin{bmatrix} Q & M \\ M & Q \end{bmatrix} \geq 0, \quad \text{(29)} \]
where
\[ \Xi_{ij} = \begin{bmatrix} \Theta_{1ij} & \Theta_{2ij} & \Theta_{3ij} \\ * & -I & 0 \\ * & -Q^{-1} & \end{bmatrix}, \]
\[ \Theta_{1ij} = \begin{bmatrix} \Sigma_{11} & \Sigma_{12} & -MT \\ * & \Sigma_{13} & Q + MT \end{bmatrix}, \]
\[ \Theta_{2ij} = \begin{bmatrix} \tilde{C}_{ij} & \tilde{D}_{ij} & 0 & -\tilde{D}_{ij} & 0 \end{bmatrix}^T, \]
\[ \Theta_{3ij} = \begin{bmatrix} \eta_M \tilde{A}_{ij} & \tilde{B}_{ij} & 0 & -\tilde{B}_{ij} & \tilde{B}_{wi} \end{bmatrix}^T, \]
\[ \Sigma_{11} = H \varepsilon(A_i \lambda_i) + R - \tilde{Q}, \]
\[ \Sigma_{12} = P \varepsilon B_i \lambda_j + Q + MT, \]
\[ \Sigma_{13} = -2Q - M - MT + \delta \Phi, \]
\[ \Sigma_{21} = \Sigma_{22} - \tilde{M}^T - \tilde{f} B_i Y_j - \tilde{B}_{wi}, \]
\[ \tilde{\Omega} = \begin{bmatrix} \Sigma_{21} & \Sigma_{22} & -\tilde{M}^T & -\tilde{f} B_i Y_j & \tilde{B}_{wi} \\ * & \Sigma_{23} & \tilde{Q} + \tilde{M}^T & -\delta \Phi & 0 \\ * & * & -\tilde{R} - \tilde{Q} & 0 & 0 \\ \tilde{\Xi}_{ij} & \tilde{\Xi}_{ji} & \tilde{\Xi}_{ij} & \tilde{\Xi}_{ji} & \tilde{\Xi}_{ij} \end{bmatrix}, \]
\[ \tilde{\Xi}_{ij} = \begin{bmatrix} \tilde{\Omega} & \tilde{\Theta}_{2ij} & \tilde{\Theta}_{3ij} \\ * & -I & 0 \\ * & * & -\tilde{Q} - 2\chi \end{bmatrix}, \]
\[ \tilde{\Theta}_{2ij} = \begin{bmatrix} \tilde{C}_{ij} & \tilde{D}_{ij} & 0 & -\tilde{D}_{ij} & 0 \end{bmatrix}^T, \]
\[ \tilde{\Theta}_{3ij} = \begin{bmatrix} \eta_M [\tilde{A}_{ij} & \tilde{B}_{ij} & 0 & -\tilde{B}_{ij} & \tilde{B}_{wi} \end{bmatrix}^T, \]
\[ \Sigma_{11} = H \varepsilon(PA_i \lambda_i) + R - Q, \]
\[ \Sigma_{12} = P \varepsilon B_i \lambda_j + Q + MT, \]
\[ \Sigma_{13} = -2Q - M - MT + \delta \Phi, \]
and then, the closed-loop system (16) satisfies (S.1) and (S.2).

**Proof:** Since $\sum_{i=1}^{r} \sum_{j=1}^{r} m_i (m_j - w_j) \Lambda_i = \sum_{i=1}^{r} \sum_{j=1}^{r} m_i (\sum_{j=1}^{r} m_j - w_j) \Lambda_i = 0$, in which $\Lambda_i = \Lambda_i^T$ is an arbitrary matrix with appropriate dimensions, then, one has
\[ \sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j = \sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \Xi_{ij}, \]
\[ = \sum_{i=1}^{r} m_i^2 (\rho_i \Xi_{ii} - \rho_i \Lambda_i + \Lambda_i) + \sum_{i=1}^{r} \sum_{j=i+1}^{r} m_i m_j \]
\[ \times (\rho_i \Xi_{ij} - \rho_i \Lambda_i + \rho_i \Xi_{ji} - \rho_i \Lambda_j + \Lambda_j) + \sum_{i=1}^{r} \sum_{j=1}^{r} m_i (w_j - \delta_j m_j)(\Xi_{ij} - \Lambda_i). \]

Under $w_j - \delta_j m_j \geq 0$, according to (26), (27) and (28), we get $\sum_{i=1}^{r} \sum_{j=1}^{r} m_i w_j \Xi_{ij} < 0$, which indicates that the closed-loop system (16) achieves (S.1) and (S.2).

According to Theorem 2, the conditions of the controller design are given in Theorem 3.

**Theorem 3:** Given constants $\delta > 0$, $\eta_M > 0$, $\delta_j > 0$, by considering the RET scheme (10), if the MFs satisfy $w_j - \delta_j m_j \geq 0$ ($0 < \delta_j \leq 1$), and there exist matrices $\tilde{P} > 0$, $\tilde{R} > 0$, $\tilde{Q} > 0$, $\tilde{M}$, $\tilde{K}_j$, and $\tilde{Y}_j$ contending ($1 \leq i, j \leq r$)
\[ \Xi_{ij} - \tilde{\Lambda}_i < 0, \quad (30) \]
\[ \dot{\rho}_i \Xi_{ii} - \dot{\rho}_j \tilde{\Lambda}_i + \tilde{\Lambda}_i < 0, \quad (31) \]
\[ \dot{\rho}_i \Xi_{ij} - \dot{\rho}_j \tilde{\Lambda}_i + \dot{\rho}_j \Xi_{ji} - \dot{\rho}_j \tilde{\Lambda}_j + \tilde{\Lambda}_j < 0, \quad i < j, \quad (32) \]
\[ \begin{bmatrix} \tilde{Q} & \tilde{M} \\ \tilde{M} & \tilde{Q} \end{bmatrix} \geq 0, \quad (33) \]
where
\[ \tilde{\Xi}_{ij} = \begin{bmatrix} \tilde{\Omega} & \tilde{\Theta}_{2ij} & \tilde{\Theta}_{3ij} \\ * & -I & 0 \\ * & * & -\tilde{Q} - 2\chi \end{bmatrix}, \]
\[ \tilde{\Theta}_{2ij} = \begin{bmatrix} \tilde{C}_{ij} & \tilde{D}_{ij} & 0 & -\tilde{D}_{ij} & 0 \end{bmatrix}^T, \]
\[ \tilde{\Theta}_{3ij} = \eta_M \begin{bmatrix} \tilde{\Lambda}_i & \tilde{\Phi} & \tilde{\Phi} & -\beta^2 I \end{bmatrix}, \]
then, the closed-loop system (16) satisfies (S.1) and (S.2).

**Proof:** We define $\chi = P^{-1}$, $\lambda^T Q \chi' = \tilde{Q}$, $\lambda^T M \chi = \tilde{M}$, $\chi^T \Phi \chi = \tilde{\Phi}$, $\chi^T \lambda \chi = \tilde{\Lambda}_i$ and $K_j = Y_j X^{-1}$. Pre- and post-multiplying $[\lambda', \chi']^T$ and $[\lambda', \chi']$ for (29), the inequality (33) can be obtained. In addition, pre- and post-multiplying (26)-(28) via $\mathcal{R}^T$ and $\mathcal{R} = [\lambda', \chi', \chi, \lambda', I, I]$, respectively, we can have (30)-(32) by utilizing the fact $-S Z^{-1} S \leq Z - 2 S$.

Then, the proof is finished. ■
According to the controller design method, the procedure of the proposed scheme can be described in Algorithm 1.

**Algorithm 1**: Security-based fuzzy control under RET communication mechanism.

**Step 1**: By solving LMIs (30)-(33), the gains of controllers $K_1$ and $K_2$ can be obtained.

**Step 2**: Set $x(0) = x_0$. Then, by performing the equation (13), the control input $u(t)$ is obtained, which will be utilized to control the system (2).

**Step 3**: Detect the state $x(t)$ of the closed-loop system (16) and DoS attacks under the given sampling period $h$.

**Step 4**: Implement the RET scheme (10). If $x(i_kh)$ is transmitted to the network between the system and the controller, the control input of the system can be got by executing the equation (13). Otherwise, the actuator keeps the value of the last transmission instant. Go to **Step 3**.

### IV. Simulation Results

In this part, the effectiveness and advantage of the proposed RET based control approach are verified by the example of mass-spring-damping system, and its physical model [40] is drawn in Fig. 3. Based on the Newton’s law of motion, the corresponding physical formula is represented below.

\[
F_f + F_s + m\ddot{x} = u(t),
\]

in which $F_f$ and $F_s$ stand for the friction and the restoring force of the spring, respectively. $m$ is the mass. $x$ and $u(t)$ denote the displacement and the control input, respectively. We assume that $F_f = cx$, in which $c > 0$, and $F_s = k(1+b^2x^2)x$. Thus, the following equation is obtained:

\[
m\ddot{x} + c\dot{x} + kx + kb^2x^3 = u(t).
\]

Let $x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} = \begin{bmatrix} x \\ \dot{x} \end{bmatrix}$ and $\phi(t) = -\frac{k-kt^2}{m}x_2(t)$.

Assume that $x_1(t) \in [-5, 5]$, $m = 1.1kg$, $c = 0.4N \cdot m/s$, $k = 4.7N/m$, $b = 0.3m^{-1}$, and the uncertain parameter $k \in [4, 7]$. Thereupon, we obtain $\phi_{\max} = -3.64$ ($k = 4$ and $x_1(t) = 0$) and $\phi_{\min} = -20.68$ ($k = 7$ and $x_1(t) = \pm 5$).

Based on $m_1(x_1(t)) + m_2(x_1(t)) = 1$, $\phi$ is described by the following equation:

\[
\phi = m_1(x_1(t))\phi_{\min} + m_2(x_1(t))\phi_{\max},
\]

where

\[
m_1(x_1(t)) = \frac{-\phi + \phi_{\max}}{\phi_{\max} - \phi_{\min}},
m_2(x_1(t)) = \frac{\phi - \phi_{\min}}{\phi_{\max} - \phi_{\min}}.
\]

And, the following ULMFs of the system are given:

\[
m_1(x_1(t)) = \frac{-\phi + \phi_{\max}}{\phi_{\max} - \phi_{\min}}, \quad \text{with } k = 4,
m_2(x_1(t)) = \frac{\phi - \phi_{\min}}{\phi_{\max} - \phi_{\min}}, \quad \text{with } k = 4,
m_1(x_1(t)) = \frac{-\phi + \phi_{\max}}{\phi_{\max} - \phi_{\min}}, \quad \text{with } k = 7,
m_2(x_1(t)) = \frac{\phi - \phi_{\min}}{\phi_{\max} - \phi_{\min}}, \quad \text{with } k = 7.
\]

Then, the mass-spring-damping system is modeled as the following form via the IT2 fuzzy system:

\[
\dot{x}(t) = \sum_{i=1}^{2} m_i(x_1(t))\left[A_i x(t) + B_i u(t)\right],
\]

where

\[
A_1 = \begin{bmatrix} 0 \\ \phi_{\min} - \frac{c}{m} \end{bmatrix}, \quad B_1 = \begin{bmatrix} 0 \\ \frac{1}{m} \end{bmatrix},
\]

\[
A_2 = \begin{bmatrix} 0 \\ \phi_{\max} - \frac{c}{m} \end{bmatrix}, \quad B_2 = \begin{bmatrix} 0 \\ \frac{1}{m} \end{bmatrix}.
\]

Other related system matrices are defined as follows:

\[
B_{w1} = \begin{bmatrix} 0.1 \\ 0.5 \end{bmatrix}, \quad C_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad D_1 = 0.0010,
\]

\[
B_{w2} = \begin{bmatrix} -0.4 \\ -1.15 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad D_2 = -0.0020.
\]

The corresponding ULMFs of the controller are provided in Table I.

<table>
<thead>
<tr>
<th>Lower membership functions</th>
<th>Upper membership functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_1(x_1(t)) = 0.3 \times e^{-x_1^2}$</td>
<td>$m_1(x_1(t)) = 0.1 \times e^{-x_1^2}$</td>
</tr>
<tr>
<td>$m_2(x_1(t)) = 1 - m_1(x_1(t))$</td>
<td>$m_2(x_1(t)) = 0.9 \times e^{-x_1^2}$</td>
</tr>
</tbody>
</table>

To ensure $m_j - \vartheta_j w_j \geq 0$, we set $\vartheta_1 = 0.8$ and $\vartheta_2 = 0.7$. Assume the external disturbance $w(t) = \begin{cases} -2\cos(1.2t)e^{-0.1t}, & 0.1 \leq t \leq 11.6 \\ \text{else} \end{cases}$. By solving Theorem 3 with the parameters $\delta = 0.15$, $\beta = 0.6351$, then, we get the following controller gains:

\[
K_1 = \begin{bmatrix} -0.2720 \\ -0.5646 \end{bmatrix},
\]

\[
K_2 = \begin{bmatrix} -0.2278 \\ -0.4098 \end{bmatrix}.
\]

In this simulation part, we select the periodic sampling $h = 0.002$. The initial state of the system is set to $x(0) = [1.6, 0.6]^T$. Based on the above descriptions, the corresponding simulation results are described in Figs. 4-7. Assume that there are no DoS attacks when the initial data is transferred to ensure that the controller can obtain the initial data. The non-periodic DoS attacks are depicted in Fig. 4. From Fig. 5, compared with the related result [38] which employed the secure adaptive ET, we can clearly see that the performance
of the mass-spring-damping system can be well protected due to the application of the RET scheme.  Fig. 6 and Fig. 7 show release instants and release intervals of the RET scheme and the secure adaptive ET strategy. By comparing Fig. 6 and Fig. 7, it can be observed that the state data violated the RET condition can be transmitted to the controller under non-periodic DoS attacks. Finally, according to these simulation figures, we know that the proposed RET based control policy in this work can better reduce the performance loss of the system in the presence of non-periodic DoS attacks by providing the necessary data transmission compared with the control method with the secure adaptive ET in [38].

Remark 5: The DoS attack is a malicious network attack method, which may cause the fault and collapse of the NCSs in some practical applications. In this paper, we present a security-based fuzzy control approach to handle the problem of DoS attacks for NCSs. In the simulation results, we can know that the proposed control strategy can effectively reduce the performance loss of the system in the presence of non-periodic DoS attacks by applying a mass-spring-damping system. And, the system can reach a stable state.

Remark 6: In the procedure of simulation, we need to select initial variable parameters and state values of the system. Some of the parameters should meet the design conditions such as the given conditions in Theorem 3, and we need to adjust the other parameters based on the experience and the physical meaning of different system models.

V. CONCLUSIONS

In this paper, a new RET based security control problem for IT2 fuzzy NCSs under DoS attacks has been settled. The parameter uncertainties have been handled by employing the ULMFs. The packets loss phenomenon caused by DoS attacks has been transformed into the RET condition. Considering the RET communication mechanism, the asynchronous issue of premise variables and actuator failure, existence conditions of the RET based security controller have been obtained. The security controller can ensure the asymptotical stability of NCSs when there are no DoS attacks and better reduce the performance loss of the system when there are DoS attacks. Finally, the simulation example has been provided to prove the effectiveness and advantages of the proposed approach. However, when the communication networks of nonlinear NCSs [41], [42] subject to time-varying delay are attacked by DoS attacks and deception attacks at the same time, the proposed control strategy may fail. Therefore, how to design an effective secure control technique for nonlinear NCSs with DoS attacks and deception attacks is our future work.

REFERENCES


