Received: 20 December 2020 | Revised: 12 April 2021 | Accepted: 23 April 2021

DOI: 10.1002/rnc.5570

RESEARCH ARTICLE

WILEY

An event-triggered approach to security control for networked systems using hybrid attack model

Jinliang Liu[1,2] | **Yuda Wang**[1] | **Lijuan Zha**[1,3] | **Xiangpeng Xie**[4] | **Engang Tian**[5]

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

[2]College of Automation Electronic Engineering, Qingdao University of Science and Technology, Qingdao, China

[3]School of Mathematics, Southeast University, Nanjing, China

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

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

Correspondence
Lijuan Zha, College of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210023, China.
Email: zhalijuan@vip.163.com

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 61903182, 61973152; Natural Science Foundation of Jiangsu Province of China, Grant/Award Number: BK20190794; Qinglan Project of Jiangsu Province of China

Abstract

This article presents an event-triggered approach to security control for networked systems by using hybrid attack model. Stochastic deception attacks, replay attacks, and denial of service attacks are assumed to occur in the communication network. The main contribution of the article is that an event-triggered control strategy is presented to stabilize the networked systems based on the hybrid attacks and the network resource limitations. A novel event-based model for networked control systems under hybrid attacks is established. Based on the proposed model, sufficient conditions are acquired to guarantee the closed-loop system stability and the controller design method is developed. Finally, two simulation examples are given to validate the feasibility of the proposed method.

KEYWORDS

deception attacks, denial of service attacks, event-triggered scheme, hybrid attacks, networked control systems, replay attacks

1 | INTRODUCTION

Networked control systems (NCSs) have been an popular research subject in which the controlled plants, sensors, controllers, and actuators[1,2] are connected via communication networks. The components of NCSs can be modularized and independently designed, so that the control system can be maintained by detecting and diagnosing each module, thus reducing the cost of fault diagnosis. In addition, NCSs are superior to traditional control systems, which has widely range of applications in harsh environments involving multiagent systems[3,4] and remote control of teleoperation robots.[5,6] Stability and state estimation problems have been widely investigated for NCSs. For example, for NCSs with probabilistic nonlinearities, the dynamic output feedback control problem is studied in Reference 7. Using the variable sampling approach, the authors of Reference 8 investigate the security stabilization for a kind of wireless NCSs subject

to attacks. The interacting multiple model estimator is designed for the NCSs in Reference 9, where the impact of the control/observation packet arrival rate and the control input on the estimation performance is studied.

The introduction of networks into control system is attractive, which makes NCSs become a research hotspot.[10-13] It is still a challenge problem that how to design a suitable transmission mechanism and use the network resources properly. In the past decades, the mostly used communication mechanism is time-triggered scheme, which transmits all sampled data. However, if the NCS runs smoothly, the signals still transmitted periodically, then the redundant transmissions will result in wasting the limited network resources. To decrease transmission frequency while ensuring the stability of the system, event-triggered scheme was proposed to save the limited network resources, under which the sampled data to be released into the network only when the corresponding event occurs.[14-17] The effectiveness of the event-triggered scheme in getting rid of the redundant data has been illustrated by some researchers. For instance, Yue et al. proposed an event-triggered scheme based on period sampling[14] and discussed the stability of NCS under the developed event-triggered scheme. The event-triggered H_∞ control problem for NCSs with packet losses was investigated in Reference 16. However, the above literature does not consider the influence of network attacks (especially denial of service [DoS] attack). Inspired by this, the design of event-triggered scheme under hybrid attack is studied in this article.

Besides network transmission strategies, network security issue is another major challenge in analysis and design of NCS.[18-20] In practice, communication network is vulnerable to cyberattacks due to its openness, which can be dangerous for stability and normal operation of the system.[21-23] It is very essential to understand the cyberattacks and take preventive measures to avoid dangerous risks. There are several common types of cyberattacks, which are extensively considered,[24,25] such as deception attacks, DoS attacks, and replay attacks. The deception attacks destroy the system by injecting false signals into the true one.[26-29] Replay attacks attempt to record and replay previous normal system data to replace the real data transmitted in the network.[30,31] Different from the deception and replay attacks, the DoS attacks aims to prevent transmitted data from reaching the destination.[32-34]

Inspired by the above literature, this article proposes an event-triggered control approach for NCSs under hybrid attacks. Different from mostly existing literature, the main contributions of this article are as follows:

(1) The control problem is firstly investigated for NCSs subject to hybrid attacks including deception, replay, and DoS attacks at the same time.
(2) Considering the influence of hybrid attacks, a novel event-triggered scheme is proposed to save the limited resources.
(3) A novel system model for NCSs is established for the first time, which takes event-triggered scheme and hybrid attacks into a unified framework.
(4) Sufficient conditions are derived to guarantee the stability of the augmented system and the controller design method is developed.

Notation: Throughout this article, $\mathbb{N}$ denotes the set of natural numbers; $\mathbb{R}_n$ denotes the n-dimensional Euclidean space; $\mathbb{R}_{n\times n}$ denotes the set of $n\times n$ real matrices; M^T denotes the transposition of the matrix M; $M>0$ for $M\in\mathbb{R}_{n\times n}$ means that M is real symmetric and positive definite.

2 | PRELIMINARIES

Consider the networked control system:

$$\dot{x}(t)=Ax(t)+Bu(t), \tag{1}$$

where $x(t)\in\mathbb{R}_n$ is the state vector of the controlled plant and $u(t)\in\mathbb{R}_m$ is the control input. A and B are known constant matrices with appropriate dimensions.

The framework of event-triggered NCSs is shown in Figure 1, where the communication network may suffer from hybrid attacks, including deception, replay, and DoS attacks. In order to make use of network bandwidth properly, an event-triggered scheme is introduced to avoid redundant data transmission in communication networks. If the cyberattacks are absent, the sampled data are transmitted via the network normally. The event-triggered condition is designed as

$$e_k^T(t)\Omega e_k(t)>\rho x^T(t_kh+jh)\Omega x(t_kh+jh), \tag{2}$$

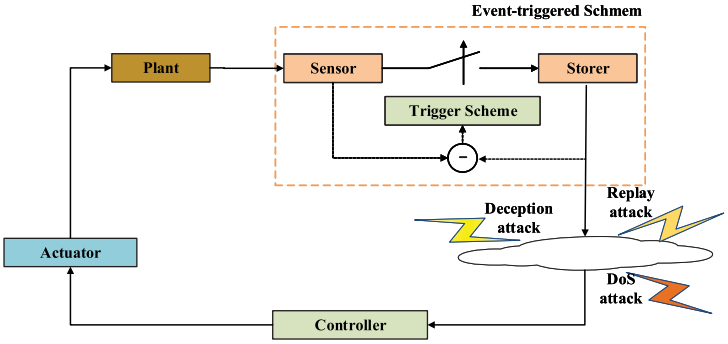

FIGURE 1 Structure of networked control system under event-triggered scheme and hybrid attacks [Colour figure can be viewed at wileyonlinelibrary.com]

where h is the sample period of the smart sensor, $\varrho \in [0,1)$, $\Omega > 0$, $e_k(t) = x(t_k h) - x(t_k h + jh)$, $k, j \in \mathbb{N}$, $x(t_k h)$ is the latest transmission signal, and $x(t_k h + jh)$ represents the current sampling signal.

For simplicity, we use $t_k^j h$ to represent $t_k h + jh$, where $t_k h$ is the latest triggered instant. Then, the next triggering instant is determined by

$$t_{k+1}h = t_k h + \inf_{j \geq 1} \left\{ jh | e_k^T(t) \Omega e_k(t) > \varrho x^T(t_k^j h) \Omega x(t_k^j h) \right\}. \tag{3}$$

Define $v(t) = t - t_k^j h$, then the latest triggering state can be represented as

$$x(t_k h) = x(t - v(t)) + e_k(t). \tag{4}$$

Remark 1. It is noted that communication network resources are often limited. In order to get better system performance, in this article, an event-triggered mechanism is added into the system. Then, the sampled information is transmitted into the network only when it satisfies the condition (2), which greatly reduces the amount of transferred data.

Remark 2. The periodic event-triggered condition applied in this article is dependent on the sampled data of the system state. It should be noted that the minimum time of two consecutive triggering events is at least one sampling period h, which avoids the Zeno effect naturally.

As shown in Figure 1, a hybrid attack includes all three common types of attacks (deception, replay, and DoS ones). It is assumed that the deception and replay attacks occur randomly, and DoS attack appears in a nonperiodic form. In this article, we assume only the network at the sensor-to-controller link may be attacked. The proposed method can be extended to a more general case, where both the sensor-to-controller and controller-to-actuator network links are attacked.

When the sampled information is transmitted into the network, it may encounter deception attack signal which may completely replace normal transmission data. Considering occurrence of the deception attacks, the transmitted data have the following form

$$x_D(t) = \alpha(t) f(x(t)) + (1 - \alpha(t)) x(t_k h), \tag{5}$$

where the nonlinear function $f(\cdot)$ denotes the deception attacks. $\alpha(t)$ satisfying the Bernoulli distribution represents whether or not the deception attack occurs. $\alpha(t) = 1$ denotes deception attack occurs; $\alpha(t) = 0$ denotes the triggered state is transmitted normally.

In this article, we assume the replay attacks occur randomly which aim to deceive the controller. The attackers are assumed to be able to intercepts the networked transmitted signals and record a finite amount of signals. We denote the stored signals are $\mathbb{M} = \{x(t_{r_1} h), x(t_{r_2} h), \ldots, x(t_{r_{m_0}} h)\}$, which will be updated all the time and the oldest one in $\mathbb{M}$ will be replaced by the newly intercepted one. Due to the limitation of storing memory, the attackers cannot send replay attacks all the time.[35] If replay attacks happen, a replay attack $x(t_{r_s} h) \in \mathbb{M}$ will be chosen from $\mathbb{M}$ to replace the normal transmitted signal. We use $\beta(t)$ to represent whether replay attacks occur or not. Then, under the replay attack and deception attacks, the data transmitted is denoted as

$$x_r(t) = \beta(t) x(t_{r_s} h) + (1 - \beta(t)) x_D(t). \tag{6}$$

The replay attack often assumed to occur at a certain time interval in other papers, as a special case, we consider that the replay attack occurs at a certain instant. Once the replay attacks are detected by using time-stamp method, they will be replaced by the last successful transmitted packets $x(t_{k-1}h)$ which are held at the controller. Then, if the replay attacks are detected, the control input (6) can be rewritten as

$$x_r(t) = \beta(t)x(t_{k-1}h) + (1-\beta(t))x_D(t). \tag{7}$$

Define $\eta_r(t) = t - t_{k-1}h$, then, $x(t_{k-1}h)$ can be written as $x(t-\eta_r(t))$, where $0 < \eta_r(t) < \overline{\eta}$. From (5) and (7), we can get the state under deception attacks and replay attacks can be written as

$$x_r(t) = \beta(t)x(t-\eta_r(t)) + (1-\beta(t))[\alpha(t)f(x(t)) + (1-\alpha(t))x(t_kh)]. \tag{8}$$

Assumption 1. In order to facilitate the analysis of this article, we assume that the attack instants can be obtained in real time. In practice, the information related to DoS attack can be obtained online by using attack detection technology.

The occurrence of DoS attack is described as

$$\gamma(t) = \begin{cases} 1, & t \in [h_n, h_n + l_n), \\ 0, & t \in [h_n + l_n, h_{n+1}), \end{cases} \tag{9}$$

where h_n represents the starting instant of the n_{th} sleeping period, and l_n denotes the length of the n_{th} sleeping period. If $\gamma(t) = 1$, the DoS attack is sleeping (i.e., it does not occur), and the data are transmitted normally. Otherwise, the DoS attack is active, and the data transmission is blocked. In addition, the condition $0 \le h_0 < h_1 < h_1 + l_1 < h_2 < \cdots < h_n < h_n + l_n < \cdots$ is satisfied. For the sake of simplicity, define $G_{n,1} \triangleq [h_n, h_n + l_n)$ and $G_{n,2} \triangleq [h_n + l_n, h_{n+1})$.

Then, considering the impacts of the above three types cyberattacks, the real input of the controller is represented as

$$\hat{x}(t) = \gamma(t)\{\beta(t)x(t-\eta_r(t)) + (1-\beta(t))[\alpha(t)f(x(t)) + (1-\alpha(t))x(t_kh)]\}. \tag{10}$$

Remark 3. In (10), if $\alpha(t) = 0$, $\beta(t) = 0$, and $\gamma(t) = 1$, the actual signal $\hat{x}(t)$ transmitted to the controller coincides with $x(t_kh)$, which means that no attack occurs at this moment and the data are transmitted normally. Otherwise, the data transmission process is attacked. In particular, if $\alpha(t) = 1$, $\beta(t) = 1$, and $\gamma(t) = 0$, the actual signal $\hat{x}(t)$ transmitted to the controller is *null*, and all three kinds of attacks occur simultaneously.

Due to the presence of hybrid attack, the original event-triggered scheme is not completely suitable, which leads to redesign of the transmission scheme. By considering the impact of hybrid attack, especially the DoS attack, the transmission instant can be designed as

$$t_{n,k}h = \{t_{k_l}h \ satisfying \ (3) | t_{k_l}h \in G_{n-1,1}\} \cup \{h_n\}, \tag{11}$$

where $k_l, t_{k_l}, n, l \in \mathbb{N}$. k denotes the number of triggering events in n_{th} attack period, and $k \in \{1, \ldots, k(n)\} \triangleq \lambda(n)$, in which $k(n) = \sup\{k \in \mathbb{N} | h_n + l_n \ge t_{n,k}h\}$.

It should be noted that the time sequence $\{t_{n,k}h\}$ in n_{th} action period lies in either interval $G_{n-1,1}$ or right endpoint of interval $[h_{n-1}, h_n)$. That means if there are no data satisfied the condition in the interval $G_{n-1,1}$, in other words, $\{t_{k_l}h \ satisfying (3) | t_{k_l}h \in G_{n-1,1}\} = \emptyset$, then the triggering instant only occurs at h_n.

Define $\epsilon_{n,k} \triangleq \sup\left\{j \in \mathbb{N} | t_{n,k}h + jh < t_{n,k+1}h\right\}$, then the event intervals $C_{n,k}$ can be divided into several intervals.

$$C_{n,k} = \cup_{j=1}^{\epsilon_{n,k}+1} \mathcal{H}_{n,k}^{j}, \tag{12}$$

where the $\mathcal{H}_{n,k}^{j}$ can be presented as:

$$\begin{cases} \mathcal{H}_{n,k}^{j} = \left[t_{n,k}h + (j-1)h, \ t_{n,k}h + jh\right) \\ \mathcal{H}_{n,k}^{\epsilon_{n,k}+1} = \left[t_{n,k}h + \epsilon_{n,k}h, \ t_{n,k+1}h\right) \end{cases}. \tag{13}$$

Note that

$$G_{n,1} = \cup_{k=0}^{k(n)} \left\{C_{n,k} \cap G_{n,1}\right\}. \tag{14}$$

Then combined with the above equations, $G_{n,1}$ can be divided into small intervals.

$$G_{n,1} = \cup_{k=0}^{k(n)} \cup_{j=1}^{\epsilon_{n,k}+1} \Theta_{n,k}^{j}, \tag{15}$$

where $\Theta_{n,k}^{j} = \mathcal{H}_{n,k}^{j} \cap G_{n,1}$.

Thus, for $k \in \lambda(n), n \in \mathbb{N}$, define the following two piecewise-continuous functions

$$\nu_{n,k}(t) = \begin{cases} t - t_{n,k}h, & t \in \Theta_{n,k}^{1} \\ t - t_{n,k}h - h, & t \in \Theta_{n,k}^{2} \\ \vdots & \\ t - t_{n,k}h - \epsilon_{n,k}h, & t \in \Theta_{n,k}^{\epsilon_{n,k}+1} \end{cases} \tag{16}$$

and

$$e_{n,k}(t) = \begin{cases} 0, & t \in \Theta_{n,k}^{1} \\ x\left(t_{n,k}h\right) - x\left(t_{n,k}h + h\right), & t \in \Theta_{n,k}^{2} \\ \vdots & \\ x\left(t_{n,k}h\right) - x\left(t_{n,k}h + \epsilon_{n,k}h\right), & t \in \Theta_{n,k}^{\epsilon_{n,k}+1} \end{cases}, \tag{17}$$

where $\nu_{n,k}(t) \in [0, h), t \in \mathcal{C}_{n,k} \cap G_{n,1}$.

From (11), one can get $\nu_{n,k}(t)$ and $e_{n,k}(t)$ satisfy

$$e_{n,k}^{T}(t)\Omega e_{n,k}(t) < \varrho x^{T}\left(t - \nu_{n,k}(t)\right)\Omega x\left(t - \nu_{n,k}(t)\right). \tag{18}$$

Then, under the event-triggered scheme (11), the triggered state in the nth attack period can be represented as

$$x(t_{n,k}h) = x\left(t - \nu_{n,k}(t)\right) + e_{n,k}(t), t \in \mathcal{C}_{n,k} \cap G_{n,1}. \tag{19}$$

Furthermore, the real input of the controller in (10) under the event-triggered scheme (11) can be written as

$$\hat{x}(t) = \gamma(t)\{\beta(t)x(t - \eta_r(t)) + (1 - \beta(t))[\alpha(t)f(x(t)) + (1 - \alpha(t))x(t_{n,k}h)]\}. \tag{20}$$

Considering the three types of cyberattacks and the event-triggered scheme (11), combine (19) and (20), the controller can be designed as

$$u(t) = \begin{cases} K\left\{\beta(t)x(t - \eta_r(t)) + (1 - \beta(t))\left[x\left(t - \nu_{n,k}(t)\right) + e_{n,k}(t)\right.\right. \\ \left.\left. + \alpha(t)\left(f(x_e(t)) - x\left(t - \nu_{n,k}(t)\right) - e_{n,k}(t)\right)\right]\right\}, \quad t \in G_{n-1,1}, \\ 0, \quad t \in G_{n-1,2}. \end{cases} \tag{21}$$

Then, the system (1) can be modeled as:

$$\begin{cases} \dot{x}(t) = \begin{cases} Ax(t) + BK\left\{\beta(t)x(t - \eta_r(t)) + (1 - \beta(t))\left[x\left(t - \nu_{n,k}(t)\right) + e_{n,k}(t)\right.\right. \\ \left.\left. + \alpha(t)\left(f(x(t)) - x\left(t - \nu_{n,k}(t)\right) - e_{n,k}(t)\right)\right]\right\}, \quad t \in G_{n-1,1}, \\ Ax(t), \quad t \in G_{n-1,2}, \end{cases} \\ x(t) = \varphi(t), \quad t \in [-h, 0), \end{cases} \tag{22}$$

where $\varphi(t)$ is the initial function of $x(t)$.

For the convenience of analysis in the next section, a lemma and some assumptions are introduced as follows.

Assumption 2 (36). For a given real constant matrix F, the deception attack signal $f(x)$ satisfies the following condition:

$$\|f(x)\|_2 \leq \|Fx\|_2. \tag{23}$$

Assumption 3 (37). Assume that there exists a uniform upper bound b_{max} on the lengths of the DoS active periods, as for the DoS active periods, there exists a low bound l_{min}.

$$\begin{cases} b_{max} \geq \sup\limits_{n\in\mathbb{N}}\{h_n - h_{n-1} - l_{n-1}\}, \\ l_{min} \leq \inf\limits_{n\in\mathbb{N}}\{l_n\}. \end{cases} \tag{24}$$

Assumption 4 (37). Let $n(t)$ denote DoS attacks off/on transitions during the interval $[0, t)$. There exist $a_1 \geq 0, a_1 \in \mathbb{R}$ and $\eta_D > h, \eta_D \in \mathbb{R}$, such that

$$n(t) \leq a_1 + \frac{t}{\eta_D}. \tag{25}$$

3 | MAIN RESULTS

Based on (22), we are devoted to give the following two theorems for the sufficient conditions of exponential stability of system (22) and the controller design method.

Theorem 1. *Given scalars $\rho_i > 0, \varsigma_i > 0, \overline{\eta} > 0$, attack probabilities $\overline{\alpha}, \overline{\beta}$, trigger parameter ϱ, sampling period h, DoS parameters a_1, η_D, l_{min}, b_{max}, and matrices F and K, the system (22) is exponentially mean-square stable if there exist matrices $P_i > 0$, $Q_i > 0$, $R_i > 0$, $Z_i > 0$, S_i, $\Omega > 0$, matrices L_i, and N_i with appropriate dimensions, such that for $i = 1, 2$ the following inequalities hold:*

$$\Upsilon_1^1 = \begin{bmatrix} \Gamma_{11}^1 & * & * & * \\ \Gamma_{21}^1 & -I & * & * \\ h\Gamma_{31}^1 & 0 & \Gamma_{33}^1 & * \\ \overline{\eta}\Gamma_{31}^1 & 0 & 0 & \Gamma_{44}^1 \end{bmatrix} < 0, \tag{26}$$

$$\Upsilon_1^2 = \begin{bmatrix} \Gamma_{11}^2 & * & * \\ hP_2A & \Gamma_{33}^2 & * \\ \eta P_2A & 0 & \Gamma_{44}^2 \end{bmatrix} < 0, \tag{27}$$

$$P_1 \leq \varsigma_2 P_2, P_2 \leq \varsigma_1 e^{2(\rho_1+\rho_2)h} P_1, \tag{28}$$

$$Q_i \leq \varsigma_{3-i} Q_{3-i}, \tag{29}$$

$$R_i \leq \varsigma_{3-i} R_{3-i}, \tag{30}$$

$$S_i \leq \varsigma_{3-i} S_{3-i}, \tag{31}$$

$$Z_i \leq \varsigma_{3-i} Z_{3-i}, \tag{32}$$

$$\frac{2\rho_1 l_{min} - 2(\rho_1+\rho_2)h - 2\rho_2 b_{max} - ln\varsigma_1\varsigma_2}{\eta_D} > 0, \tag{33}$$

$$\begin{bmatrix} R_i & * \\ L_i^T & R_i \end{bmatrix} < 0, \quad \begin{bmatrix} Z_i & * \\ N_i^T & Z_i \end{bmatrix} < 0. \tag{34}$$

Other symbol definitions are given in Appendix A.

Proof. See Appendix B ∎

Theorem 2. *For given positive scalars $\rho_i, \varsigma_i, \overline{\eta}, \varepsilon_0, \varepsilon_i, \kappa_i, \mu_i, \nu_i$, attack probabilities $\overline{\alpha}, \overline{\beta}$, trigger parameter ϱ, sampling period h, DoS parameters a_1, η_D, l_{min}, b_{max}, and matrix F, the system (22) is exponentially mean-square stable under the event-triggered scheme (11) and hybrid attacks if there exist matrices $\hat{Q}_i > 0$, $\hat{R}_i > 0$, $\hat{Z}_i > 0$, $\hat{S}_i > 0$, $X_i > 0$, $Y > 0$, $\hat{\Omega} > 0$, and matrices $\hat{L}_i$,*

and $\hat{N}_i$ with appropriate dimensions, such that for $i=1,2$ the following inequalities hold:

$$\hat{\Upsilon}_1^1=\begin{bmatrix}\hat{\Gamma}_{11}^1 & * & * & *\\ \hat{\Gamma}_{21}^1 & -I & * & *\\ h\hat{\Gamma}_{31}^1 & 0 & \hat{\Gamma}_{33}^1 & *\\ \overline{\eta}\hat{\Gamma}_{31}^1 & 0 & 0 & \hat{\Gamma}_{44}^1\end{bmatrix}<0, \tag{35}$$

$$\hat{\Upsilon}_1^2=\begin{bmatrix}\hat{\Gamma}_{11}^2 & * & *\\ hAX_2 & \hat{\Gamma}_{33}^2 & *\\ \eta AX_2 & 0 & \hat{\Gamma}_{44}^2\end{bmatrix}<0, \tag{36}$$

$$\begin{bmatrix}-\varsigma_2 X_2 & *\\ X_2 & -X_1\end{bmatrix}\le 0,\quad \begin{bmatrix}-\varsigma_1 e^{2(\rho_1+\rho_2)h}X_1 & *\\ X_1 & X_2\end{bmatrix}\le 0, \tag{37}$$

$$\begin{bmatrix}-\varsigma_{3-i}\hat{Q}_{3-i} & *\\ X_{3-i} & -2\mu_i X_i+\mu_i^2\hat{Q}_i\end{bmatrix}\le 0, \tag{38}$$

$$\begin{bmatrix}-\varsigma_{3-i}\hat{S}_{3-i} & *\\ X_{3-i} & -2\varepsilon_i X_i+\varepsilon_i^2\hat{S}_i\end{bmatrix}\le 0, \tag{39}$$

$$\begin{bmatrix}-\varsigma_{3-i}\hat{R}_{3-i} & *\\ X_{3-i} & -2\nu_i X_i+\nu_i^2\hat{R}_i\end{bmatrix}\le 0, \tag{40}$$

$$\begin{bmatrix}-\varsigma_{3-i}\hat{Z}_{3-i} & *\\ X_{3-i} & -2\kappa_i X_i+\kappa_i^2\hat{Z}_i\end{bmatrix}\le 0, \tag{41}$$

$$\begin{bmatrix}\hat{R}_i & *\\ \hat{L}_i^T & \hat{R}_i\end{bmatrix}<0,\quad \begin{bmatrix}\hat{Z}_i & *\\ \hat{N}_i^T & \hat{Z}_i\end{bmatrix}<0. \tag{42}$$

Other symbols are defined in Appendix C.

Moreover, the designed controller gain can be given by

$$K=YX_1^{-1}. \tag{43}$$

Proof. Appendix D ∎

Remark 4. Notice that one of the main difficulties in deriving the main results of this article is how to deal with the nonlinear terms $-P_iR_i^{-1}P_i$ and $-P_iZ_i^{-1}P_i,(i=1,2)$. However, we can tackle with the nonlinear terms using the cone complementary linearization algorithm or use the inequalities in (D1). Although the cone complementary linearization algorithm[38] can cut conservativeness down, but it will need more auxiliary variables to obtain a feasible solution set. In this article, we use the inequalities in (D1) to linearize the nonlinear terms. Then, by directly applying the MATLAB/LMI Toolbox, the feasible solution set can be obtained solving matrix inequalities.

Remark 5. In this article, we devote to the controller design problem for event-triggered NCSs under three kinds of cyber-attacks, which has not been discussed yet and still be a challenging issue. Based on the established model, sufficient conditions are proposed to guarantee the stability of system (22). By applying the MATLAB/LMI Toolbox, the feasible solution set of LMIs (33) and (35)–(42) in Theorem 2 can be obtained. Then the desired controller K can be derived from (43).

4 | SIMULATION EXAMPLES

Example 1. Consider the networked control system (22) with the parameters

$$A=\begin{bmatrix}-1 & 0 & -2\\ -1 & -0.5 & 0\\ 2 & -1 & -0.5\end{bmatrix},\quad B=\begin{bmatrix}2\\ -1\\ -1\end{bmatrix}.$$

The deception attack signal is selected as

$$f(x(t)) = \begin{bmatrix} -\tanh(0.15x(t)) \\ -\tanh(0.10x(t)) \\ -\tanh(0.05x(t)) \end{bmatrix}.$$

According to Assumption 2, we can obtain that if the nonlinearity upper bound is given by $F = diag\{0.05, 0.10, 0.15\}$, the condition (23) is satisfied.

We assume $\rho_1 = 0.05$, $\rho_1 = 0.3$, $\varsigma_1 = \varsigma_2 = 1.01$, $\overline{\eta} = 0.2$, $\varepsilon_0 = 10$, $\varepsilon_i = 10$, $\kappa_i = 10$, $\mu_i = 10$, $\nu_i = 10$, attack probabilities $\overline{\alpha} = 0.2$, $\overline{\beta} = 0.1$, trigger parameter $\varrho = 0.02$, sampling period $h = 0.06$, DoS parameters $\eta_D = 1$, $l_{min} = 1.78$, $b_{max} = 0.2$. The initial condition is $x_0 = \begin{bmatrix} -1.8 & 1.2 & -0.1 \end{bmatrix}^T$. Set $\overline{\alpha} = 0.08$, $\overline{\beta} = 0.05$, $b_{max} = 0.2$, $l_{min} = 1.78$. This means that the networked control system is under all three types of network attacks.

Solving the LMIs of Theorem 2 with MATLAB, one can obtain:

$$K = \begin{bmatrix} -0.0559 & 0.0226 & 0.0244 \end{bmatrix}, \quad \Omega = \begin{bmatrix} 0.0173 & -0.0058 & -0.0025 \\ -0.0058 & 0.0142 & 0.0050 \\ -0.0025 & 0.0050 & 0.0112 \end{bmatrix}. \tag{44}$$

As shown in Table 1, the number of transmission packets under the event-triggered scheme proposed in this article is recorded with different trigger parameters and the number of data transmission packets under time-triggered scheme is also recorded. From the data in Table 1, one can see that the amount of the triggered dada is dependent on the sampling period h and the triggering parameter ϱ. The larger of h and ϱ, the less amount of the triggered packets. Figure 3 shows the release instants and intervals of the event generator. Figure 2 presents the state response under an event-triggered scheme and hybrid attacks, validating that the system is exponentially stable while the transmission of data packets is reduced. Obviously, the above simulation results illustrate the effectiveness of the designed controller.

Example 2. Considering the following mass spring system

$$\begin{cases} \dot{x}_1(t) = x_2(t) \\ \dot{x}_2(t) = -\frac{k}{m}x_1(t) - \frac{c}{m}x_2(t) + \frac{1}{m}u(t) \end{cases}. \tag{45}$$

Choose $x^T(t) = \begin{bmatrix} x_1^T(t) & x_2^T(t) \end{bmatrix}$, $m = 1, k = c = 2$, system (45) can be described as (1) with

$$A = \begin{bmatrix} 0 & 1 \\ -2 & -2 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

The deception attacks are

$$f(x(t)) = \begin{bmatrix} -\tanh(0.05x(t)) \\ -\tanh(0.10x(t)) \end{bmatrix}.$$

with $F = diag\{0.05, 0.05\}$.

TABLE 1 The number of data packet transmitted with different sampling periods ($T = 10$ s)

Sampling period	0.02	0.06
Time-triggered	500	166
Event-triggered scheme with $\varrho = 0.1$	72	69
Event-triggered scheme with $\varrho = 0.3$	43	41
Event-triggered scheme with $\varrho = 0.5$	34	32

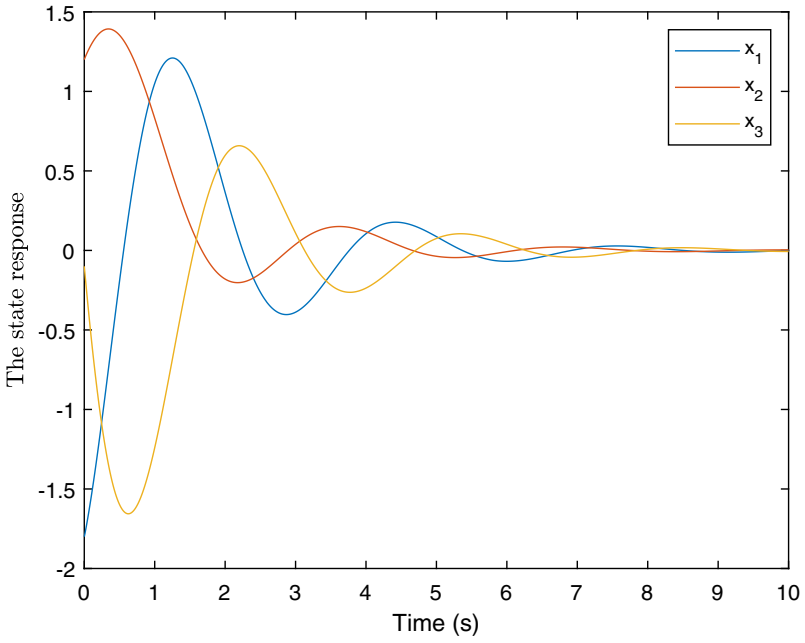

FIGURE 2 State response under K and Ω in (44) [Colour figure can be viewed at wileyonlinelibrary.com]

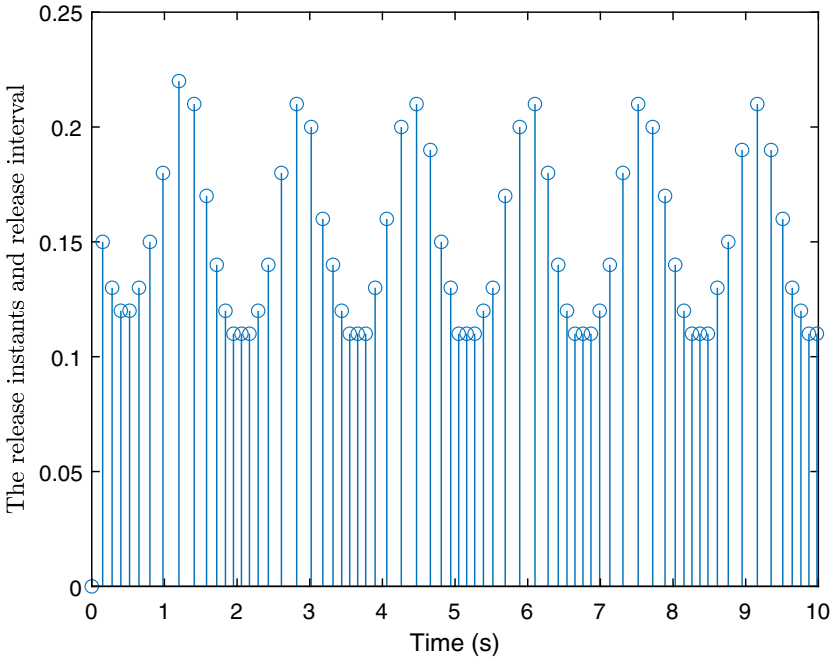

FIGURE 3 Release instants and intervals under K and Ω in (44) [Colour figure can be viewed at wileyonlinelibrary.com]

Choosing $\rho_1 = 0.0005$, $\rho_1 = 0.0003$, $\varsigma_1 = \varsigma_2 = 2$, $\overline{\eta} = 0.2$, $\varepsilon_0 = 10$, $\varepsilon_i = 10$, $\kappa_i = 10$, $\mu_i = 10$, $\nu_i = 10$, attack probabilities $\overline{\alpha} = 0.2$, $\overline{\beta} = 0.1$, trigger parameter $\varrho = 0.02$, sampling period $h = 0.1$, DoS parameters $\eta_D = 1$, $l_{min} = 1.88$, $b_{max} = 0.2$. The initial state is $x(0) = \begin{bmatrix} -1 & 0.5 \end{bmatrix}^T$.

By applying Theorem 2, we obtain the feedback gain K and the event triggering matrix Ω are

$$K = \begin{bmatrix} 0.0512 & 0.0225 \\ 0.0225 & 0.0402 \end{bmatrix}, \quad \Omega = \begin{bmatrix} 0.2480 & -0.2268 \end{bmatrix}. \tag{46}$$

The system state response with the feedback gain K and the event triggering matrix Ω in (46) are shown in Figures 4 and 5. From these simulation results, we can see that the designed controller can eliminate the effects of the cyberattacks and ensure the stability of the mass-spring system while reducing the amount of transmissions.

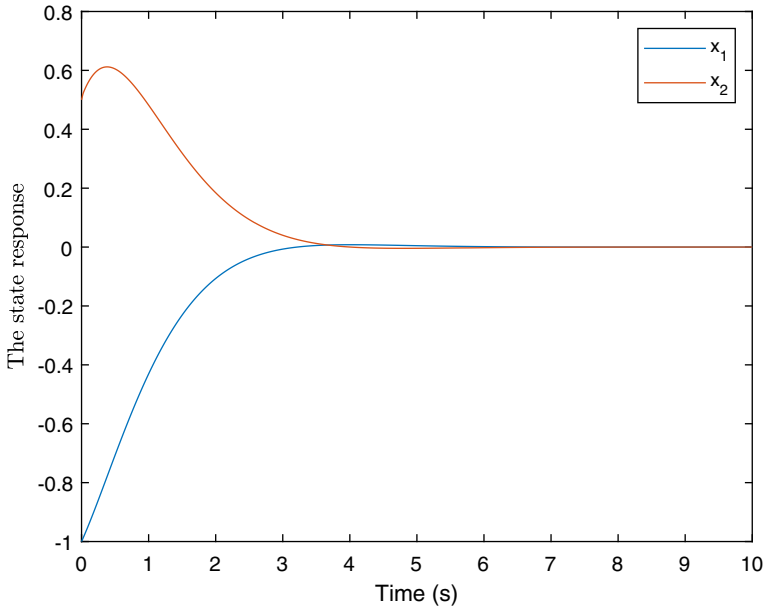

FIGURE 4 State response under K and Ω in (46) [Colour figure can be viewed at wileyonlinelibrary.com]

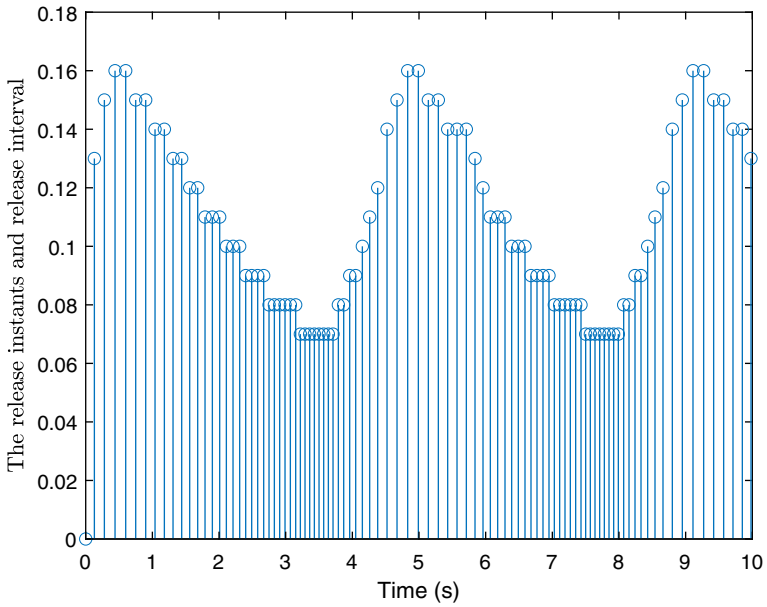

FIGURE 5 The release instants and release interval under K and Ω in (46) [Colour figure can be viewed at wileyonlinelibrary.com]

5 | CONCLUSIONS

The event-based security control problem is studied for networked systems subjected to hybrid attacks. A hybrid attack, including deception, replay, and DoS attacks, is considered for the first time. To save the limited network resources, a novel event-triggered scheme is proposed with the consideration of hybrid attacks. Then, an event-based model for NCSs under hybrid attacks is proposed. By applying the Lyapunov stability theory, sufficient conditions are obtained in LMI terms to guarantee the system stability and determine the controller gain. In the future, we will focus on more complex systems against hybrid-attacks, such as multiagent systems and discrete systems with missing sensor measurements.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grant 61973152 and Grant 61903182, in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20190794, and in part by the Qing Lan Project.

CONFLICT OF INTEREST

There is no conflict of interest about this article.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

REFERENCES

1. Shi Y, Tian E, Shen S, Zhao X. Adaptive memory-event-triggered H_∞ control for network-based T-S fuzzy systems with asynchronous premise constraints. *IET Control Theory Appl*. 2021;15:534-544.
2. Liu J, Wang Y, Cao J, Yue D, Xie X. Secure adaptive-event-triggered filter design with input constraint and hybrid cyber-attack. *IEEE Trans Cybern*. 2019. https://doi.org/10.1109/TCYB.2020.3003752.
3. Li X, Chen MZQ, Su H. Quantized consensus of multi-agent networks with sampled data and Markovian interaction links. *IEEE Trans Cybern*. 2019;49(5):1816-1825.
4. Liu J, Yin T, Yue D, Karimi HR, Cao J. Event-based secure leader-following consensus control for multi-agent systems with multiple cyber-attacks. *IEEE Trans Cybern*. 2021;51(1):162-173.
5. Sun D, Liao Q, Gu X, Li C, Ren H. Multilateral teleoperation with new cooperative structure based on reconfigurable robots and type-2 fuzzy logic. *IEEE Trans Cybern*. 2019;49(8):2845-2859.
6. Li Y, Shi L, Cheng P, Chen J, Quevedo DE. Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach. *IEEE Trans Automat Contr*. 2015;60(10):2831-2836.
7. Gu Z, Zhao H, Yue D, Yang F. Event-triggered dynamic output feedback control for networked control systems with probabilistic nonlinearities. *Inf Sci*. 2018;457-458:99-112.
8. Yang H, Shi M, Xia Y, Zhang P. Security research on wireless networked control systems subject to jamming attacks. *IEEE Trans Cybern*. 2019;49(6):2022-2031.
9. Lin H, Lam J, Chen MZQ, Shu Z, Wu Z. Interacting multiple model estimator for networked control systems: stability, convergence, and performance. *IEEE Trans Automat Contr*. 2019;64(3):928-943.
10. Li J, Niu Y, Song J. Finite-time boundedness of sliding mode control under periodic event-triggered strategy. *Int J Robust Nonlinear Control*. 2020;31(2):623-639.
11. Zhang T, Deng F, Shi P. Event-triggered H_∞ filtering for nonlinear discrete-time stochastic systems with application to vehicle roll stability control. *Int J Robust Nonlinear Control*. 2020;30(18):8430-8448.
12. Guo G, Ding L, Han QL. A distributed event-triggered transmission strategy for sampled-data consensus of multi-agent systems. *Automatica*. 2014;50(5):1489-1496.
13. Hu S, Yue D, Xie X, Ma Y, Yin X. Stabilization of neural-network-based control systems via event-triggered control with nonperiodic sampled data. *IEEE Trans Neural Netw Learn Syst*. 2018;29(3):573-585.
14. Yue D, Tian E, Han Q. A delay system method for designing event-triggered controllers of networked control systems. *IEEE Trans Automat Contr*. 2013;58(2):475-481.
15. Liu J, Suo W, Xie X, Yue D, Cao J. Quantized control for a class of neural networks with adaptive event-triggered scheme and complex cyber-attacks. *Int J Robust Nonlinear Control*. https://doi.org/10.1002/rnc.5500.
16. Peng C, Yang TC. Event-triggered communication and H_∞ control co-design for networked control systems. *Automatica*. 2013;49(5):1326-1332.
17. Ding D, Wang Z, Han Q-L. A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks. *IEEE Trans Automat Contr*. 2020;65(4):1792-1799.
18. Liu J, Wu Z, Yue D, Park JH. Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber-attacks. *IEEE Trans Syst Man Cybern Syst*. 2021;51(2):943-953.
19. Gu Z, Shi P, Yue D, Yan S, Xie X. Memory-based continuous event-triggered control for networked T-S fuzzy systems against cyber-attacks. *IEEE Trans Fuzzy Syst*. 2020. https://doi.org/10.1109/TFUZZ.2020.3012771.
20. Wang Y, Wang H, Xiao J, Guan Z. Synchronization of complex dynamical networks under recoverable attacks. *Automatica*. 2010;46(1):197-203.
21. Ma R, Shi P, Wu L. Active resilient control for two-dimensional systems under denial-of-service attacks. *Int J Robust Nonlinear Control*. https://doi.org/10.1002/rnc.5310.
22. Liu J, Suo W, Zha L, Tian E, Xie X. Security distributed state estimation for nonlinear networked systems against denial-of-service attacks. *Int J Robust Nonlinear Control*. 2020;30(3):1156-1180.
23. Wang K, Tian E, Liu J, Wei L, Yue D. Resilient control of networked control systems under deception attacks: a memory-event-triggered communication scheme. *Int J Robust Nonlinear Control*. 2020;30(4):1534-1548.
24. Hu S, Yue D, Han Q, Xie X, Chen X, Dou C. Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. *IEEE Trans Cybern*. 2020;50(5):1952-1964.
25. Liu J, Yin T, Cao J, Yue D, Karimi HR. Security control for T-S fuzzy systems with adaptive event-triggered mechanism and multiple cyber-attacks. *IEEE Trans Syst Man Cybern-Syst*. 2019. https://doi.org/10.1109/TSMC.2019.2963143.

26. Cao J, Ding D, Liu J, Tian E, Hu S, Xie X. Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks. *Inf Sci*. 2021;548:69-84.
27. Zha L, Tian E, Xie X, Gu Z, Cao J. Decentralized event-triggered H_∞ control for neural networks subject to cyber-attacks. *Inf Sci*. 2018;457-458:141-155.
28. Ding D, Wang Z, Han Q, Wei G. Security control for discrete-time stochastic nonlinear systems subject to deception attacks. *IEEE Trans Syst Man Cybern Syst*. 2018;48(5):779-789.
29. Ding D, Wang Z, Ho DW, Wei G. Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. *Automatica*. 2017;78:231-240.
30. Ye D, Zhang TY, Guo G. Stochastic coding detection scheme in cyber-physical systems against replay attack. *Inf Sci*. 2019;481:432-444.
31. Zhu M, Martínez S. On the performance analysis of resilient networked control systems under replay attacks. *IEEE Trans Automat Contr*. 2014;59(3):804-808.
32. Gu Z, Ahn CK, Yue D, Xie X. Event-triggered H_∞ filtering for T–S fuzzy-model-based nonlinear networked systems with multi-sensors against DoS attacks. *IEEE Trans Cybern*. 2020. https://doi.org/10.1109/TCYB.2020.3030028.
33. Song J, Ding D, Xiang Y, Liu J, Wang X. Non-fragile distributed state estimation over sensor networks subject to DoS attacks: the almost sure stability. *Int J Syst Sci*. 2020;51(6):1119-1132.
34. Chen X, Wang Y, Hu S. Event-based robust stabilization of uncertain networked control systems under quantization and denial-of-service attacks. *Inf Sci*. 2018;459:369-386.
35. Chen B, Ho DWC, Hu G, Yu L. Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. *IEEE Trans Cybern*. 2018;48(6):1862-1876.
36. Liu J, Yang M, Xie X, Peng C, Yan H. Finite-time H_∞ filtering for state-dependent uncertain systems with event-triggered mechanism and multiple attacks. *IEEE Trans Circuits Syst I Reg Pap*. 2020;67(3):1021-1034.
37. Persis CD, Tesi P. Input-to-state stabilizing control under denial-of-service. *IEEE Trans Automat Contr*. 2015;60(11):2930-2944.
38. El Ghaoui L, Oustry F, AitRami M. A cone complementarity linearization algorithm for static output-feedback and related problems. *IEEE Trans Automat Contr*. 1997;42:1171-1176.

How to cite this article: Liu J, Wang Y, Zha L, Xie X, Tian E. An event-triggered approach to security control for networked systems using hybrid attack model. *Int J Robust Nonlinear Control*. 2021;31:5796–5812. https://doi.org/10.1002/rnc.5570

APPENDIX A

$$\Gamma_{11}^1 = \begin{bmatrix} \Phi_{11}^1 & * & * & * & * & * & * \\ \Phi_{21}^1 & \Phi_{22}^1 & * & * & * & * & * \\ L_1^T & R_1 - L_1^T & \Phi_{33}^1 & * & * & * & * \\ \Phi_{41}^1 & 0 & 0 & -\Omega & * & * & * \\ \Phi_{51}^1 & \Phi_{52}^1 & \Phi_{53}^1 & 0 & \Phi_{55}^1 & * & * \\ N_1 & 0 & 0 & 0 & Z_1 - N_1^T & \Phi_{66}^1 & * \\ \overline{\alpha}\overline{\beta}_1 K^T B^T P_1 & 0 & 0 & 0 & 0 & 0 & -I \end{bmatrix},$$

$$\overline{\alpha}_1 = 1 - \overline{\alpha}, \quad \overline{\beta}_1 = 1 - \overline{\beta}, \quad \delta_1 = \sqrt{\overline{\alpha}\,\overline{\alpha}_1}, \quad \delta_2 = \sqrt{\overline{\beta}\,\overline{\beta}_1},$$

$$\Phi_{11}^1 = 2\rho_1 P_1 + P_1 A + A^T P_1 + Q_1 + S_1 - R_1 - Z_1,$$

$$\Phi_{21}^1 = \overline{\alpha}_1\overline{\beta}_1 K^T B^T P_1 + R_1 - L_1, \quad \Phi_{22}^1 = \varrho\Omega - 2R_1 + L_1 + L_1^T,$$

$$\Phi_{33}^1 = -e^{-2\rho_1 h} Q_1 - R_1, \quad \Phi_{41}^1 = \overline{\alpha}_1\overline{\beta}_1 K^T B^T P_1,$$

$$\Phi_{51}^1 = \overline{\beta}_1 K^T B^T P_1 + Z_1 - N_1,$$

$$\Phi_{55}^1 = -2Z_1 + N_1 + N_1^T, \quad \Phi_{66}^1 = -e^{-2\rho_1\overline{\eta}} S_1 - Z_1,$$

$$\Gamma_{21}^1 = \begin{bmatrix} F & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\Gamma_{31}^1 = \begin{bmatrix} \Pi_1 & \Pi_2 & 0 & \Pi_2 & \Pi_3 & 0 & \Pi_4 \end{bmatrix},$$

$$\Pi_1 = \begin{bmatrix} P_1A \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \Pi_2 = \begin{bmatrix} (\Phi_{41}^1)^T \\ -\delta_1\overline{\beta}_1P_1BK \\ -\delta_2\overline{\alpha}_1P_1BK \\ \delta_1\delta_2P_1BK \end{bmatrix}, \quad \Pi_3 = \begin{bmatrix} \overline{\beta}P_1BK \\ 0 \\ \delta_2P_1BK \\ 0 \end{bmatrix}, \quad \Pi_4 \begin{bmatrix} \overline{\alpha}\overline{\beta}_1P_1BK \\ \delta_1\overline{\beta}_1P_1BK \\ -\delta_2\overline{\alpha}P_1BK \\ -\delta_1\delta_2P_1BK \end{bmatrix},$$

$$\Gamma_{33}^1 = diag\{-P_1R_1^{-1}P_1, -P_1R_1^{-1}P_1, -P_1R_1^{-1}P_1, -P_1R_1^{-1}P_1\},$$

$$\Gamma_{44}^1 = diag\{-P_1Z_1^{-1}P_1, -P_1Z_1^{-1}P_1, -P_1Z_1^{-1}P_1, -P_1Z_1^{-1}P_1\},$$

$$\Gamma_{11}^2 = \begin{bmatrix} \Phi_{11}^2 & * & * & * & * \\ R_1 - L_1 & \Phi_{22}^2 & * & * & * \\ L_2^T & R_2 - L_2^T & \Phi_{33}^2 & * & * \\ Z_2 - N_2^T & 0 & 0 & \Phi_{44}^2 & * \\ N_2^T & 0 & 0 & Z_2 - N_2^T & \Phi_{55}^2 \end{bmatrix},$$

$$\Phi_{11}^2 = 2\rho_2P_2 + P_2A + A^TP_2 + Q_2 + S_2 - R_2 - Z_2, \quad \Phi_{22}^2 = -2R_2 + L_2 + L_2^T,$$

$$\Phi_{33}^2 = -e^{-2\rho_2h}Q_2 - R_2, \quad \Phi_{44}^2 = -2Z_2 + N_2 + N_2^T, \quad \Phi_{55}^2 = -e^{-2\rho_2\overline{\eta}}S_2 - Z_2,$$

$$\Gamma_{33}^2 = -P_2R_2^{-1}P_2, \quad \Gamma_{44}^2 = -P_2Z_2^{-1}P_2.$$

APPENDIX B

Proof of Theorem 1. Choose the following Lyapunov functional for system (22):

$$\begin{aligned} V_{\phi(t)}(t) = {} & x^T(t)P_{\phi(t)}x(t) + \int_{t-h}^{t} x^T(s)exp(\cdot)Q_{\phi(t)}x(s)ds + \int_{t-\overline{\eta}}^{t} x^T(s)exp(\cdot)S_{\phi(t)}x(s)ds \\ & + h\int_{-h}^{0}\int_{t+v}^{t} \dot{x}^T(s)exp(\cdot)R_{\phi(t)}\dot{x}(s)dsdv + \overline{\eta}\int_{-\overline{\eta}}^{0}\int_{t+v}^{t} \dot{x}^T(s)exp(\cdot)Z_{\phi(t)}\dot{x}(s)dsdv, \end{aligned} \tag{B1}$$

where $P_{\phi(t)} > 0$, $Q_{\phi(t)} > 0$, $R_{\phi(t)} > 0$, $S_{\phi(t)} > 0$, $Z_{\phi(t)} > 0$, $exp(\cdot) = e^{2(-1)^{\phi(t)}\rho_{\phi(t)}(t-s)}$, $\rho_{\phi(t)} > 0$, and

$$\phi(t) = \begin{cases} 1, & t \in [-h, 0] \cup (\underset{n\in\mathbb{N}}{\cup} G_{n,1}), \\ 2, & t \in \underset{n\in\mathbb{N}}{\cup} G_{n,2}. \end{cases}$$

When $\phi(t) = 1$, by taking the derivative and mathematical expectation of equations (B1), one obtains:

$$\begin{aligned} \mathbb{E}\{\dot{V}_1(t)\} \le {} & -2\rho_1V_1(t) + 2\rho_1x^T(t)P_1x(t) + 2\mathbb{E}\{x^T(t)P_1\dot{x}(t)\} + x^T(t)(Q_1 + S_1)x(t) \\ & - x^T(t-h)e^{-2\rho_1h}Q_1x(t-h) + h^2\mathbb{E}\{\dot{x}^T(t)R_1\dot{x}(t)\} + \overline{\eta}^2\mathbb{E}\{\dot{x}^T(t)Z_1\dot{x}(t)\} \\ & - h\int_{t-h}^{t} \dot{x}^T(s)e^{-2\rho_1h}R_1\dot{x}(s)ds - x^T(t-\overline{\eta})e^{-2\rho_1\overline{\eta}}Q_1x(t-\overline{\eta}) \\ & - \overline{\eta}\int_{t-\overline{\eta}}^{t} \dot{x}^T(s)e^{-2\rho_1\overline{\eta}}Z_1\dot{x}(s)ds. \end{aligned} \tag{B2}$$

Using the lemma 1 in Reference 27, For L_1 and N_1 satisfying (35), the following equalities hold

$$\begin{aligned} & -h\int_{t-h}^{t} \dot{x}^T(s)e^{-2\rho_1h}R_1\dot{x}(s)ds \le \theta_1^T(t)U_1\theta_1(t), \\ & -\overline{\eta}\int_{t-\overline{\eta}}^{t} \dot{x}^T(s)e^{-2\rho_1\overline{\eta}}Z_1\dot{x}(s)ds \le \theta_2^T(t)U_2\theta_2(t), \end{aligned} \tag{B3}$$

where $\theta_1^T(t) = \begin{bmatrix} x^T(t) & x^T(t-\nu_{n,k}(t)) & x^T(t-h) \end{bmatrix}$, $\theta_2^T(t) = \begin{bmatrix} x^T(t) & x^T(t-\eta_r(t)) & x^T(t-\overline{\eta}) \end{bmatrix}$.

$$U_1 = \begin{bmatrix} -R_1 & * & * \\ R_1 - L1^T & -2R_1 + L_1 + L_1^T & * \\ L_1^T & R_1 - L_1^T & -R_1 \end{bmatrix}, U_2 = \begin{bmatrix} -Z_1 & * & * \\ Z_1 - N1^T & -2Z_1 + N_1 + N_1^T & * \\ N_1^T & Z_1 - N_1^T & -Z_1 \end{bmatrix}.$$

Note that

$$\mathbb{E}\{\dot{x}^T(t)R_1\dot{x}(t)\} = \mathcal{A}^T R_1 \mathcal{A} + \delta_1^2 \mathcal{A}_\alpha^T R_1 \mathcal{A}_\alpha + \delta_2^2 \mathcal{A}_\beta^T R_1 \mathcal{A}_\beta + \delta_1^2\delta_2^2 \mathcal{A}_{\alpha\beta}^T R_1 \mathcal{A}_{\alpha\beta}, \tag{B4}$$

$$\mathbb{E}\{\dot{x}^T(t)Z_1\dot{x}(t)\} = \mathcal{A}^T Z_1 \mathcal{A} + \delta_1^2 \mathcal{A}_\alpha^T Z_1 \mathcal{A}_\alpha + \delta_2^2 \mathcal{A}_\beta^T Z_1 \mathcal{A}_\beta + \delta_1^2\delta_2^2 \mathcal{A}_{\alpha\beta}^T Z_1 \mathcal{A}_{\alpha\beta}, \tag{B5}$$

where

$$\begin{aligned}
\mathcal{A} &= Ax(t) + \overline{\beta}BKx(t-\eta_r(t)) + \overline{\alpha}(1-\overline{\beta})BKf(x(t)) + (1-\overline{\alpha})(1-\overline{\beta})BK\left[(x(t-\nu_{n,k}(t))) + e_{n,k}(t)\right], \\
\mathcal{A}_\alpha &= (1-\overline{\beta})BKf(x(t)) - (1-\overline{\beta})BK\left[(x(t-\nu_{n,k}(t))) + e_{n,k}(t)\right], \\
\mathcal{A}_\beta &= BKx(t-\eta_r(t)) - \overline{\alpha}BKf(x(t)) - (1-\overline{\alpha})BK\left[x(t-\nu_{n,k}(t)) + e_{n,k}(t)\right], \\
\mathcal{A}_{\alpha\beta} &= BK\left[(x(t-\nu_{n,k}(t))) + e_{n,k}(t)\right] - BKf(x(t).
\end{aligned} \tag{B6}$$

Taking into account the condition (18), one obtains:

$$\varrho x^T(t-\nu_{n,k}(t))\Omega x(t-\nu_{n,k}(t)) - e_{n,k}^T(t)\Omega e_{n,k}(t) > 0. \tag{B7}$$

In addition, from Assumption 2, the following inequality can be derived:

$$x^T(t)F^TFx(t) - f^T(x(t))f(x(t)) \geq 0. \tag{B8}$$

Combining (B2)–(B8), it can be yields by using the free weighting matrix method and the Schur complement:

$$\mathbb{E}\{\dot{V}_1(t)\} \leq -2\rho_1 V_1(t) + \theta^T(t)\Gamma_{11}^1\theta(t) + h^2\mathbb{E}\{\dot{x}^T(t)R_1\dot{x}(t)\} + \overline{\eta}^2\mathbb{E}\{\dot{x}^T(t)Z_1\dot{x}(t)\} + x^T(t)F^TFx(t), \tag{B9}$$

in which $\theta^T(t) = \begin{bmatrix} \theta_1^T(t) & e_{n,k}(t) & x^T(t-\eta_r(t)) & x^T(t-\overline{\eta}) & f(x(t)) \end{bmatrix}$.

Using (26), it can be obtained that $\mathbb{E}\{\dot{V}_1(t)\} \leq -2\rho_1 V_1(t)$.

Processing $V_2(t)$ in the same way, one obtains:

$$\mathbb{E}\{\dot{V}_2(t)\} \leq 2\rho_2 V_2(t) + \hat{\theta}^T(t)\Gamma_{11}^2\hat{\theta}(t) + h^2\mathbb{E}\{\dot{x}^T(t)R_2\dot{x}(t)\} + \overline{\eta}^2\mathbb{E}\{\dot{x}^T(t)Z_2\dot{x}(t)\} \tag{B10}$$

and $\mathbb{E}\{\dot{V}_2(t)\} \leq -2\rho_2 V_2(t)$, where $\hat{\theta}^T(t) = \begin{bmatrix} \theta_1^T(t) & x^T(t-\eta_r(t)) & x^T(t-\overline{\eta}) \end{bmatrix}$

Hence, one can see that

$$\begin{cases} \mathbb{E}\{V_1(t)\} \leq e^{-2\rho_1(t-t_{n,1})}\mathbb{E}\{V_1(t)\}, & t \in [t_{n,1}, t_{n,2}) \\ \mathbb{E}\{V_2(t)\} \leq e^{2\rho_2(t-t_{n,2})}\mathbb{E}\{V_2(t)\}, & t \in [t_{n,2}, t_{n+1,1}) \end{cases}. \tag{B11}$$

Choose

$$V(t) = \begin{cases} V_1(t), & t \in C_{n-1,k} \cap G_{n-1,1} \\ V_2(t), & t \in G_{n-1,2} \end{cases}. \tag{B12}$$

Using the inequalities (28)–(32), it yields

$$\begin{cases} \mathbb{E}\{V_1(t_{n,1})\} \leq \varsigma_2\mathbb{E}\{V_2(t_{n,1}^-)\}, \\ \mathbb{E}\{V_2(t_{n,2})\} \leq \varsigma_1 e^{2(\rho_1+\rho_2)h}\mathbb{E}\{V_2(t)\}. \end{cases} \tag{B13}$$

For $t \in [t_{n,1}, t_{n,2})$, from (B11) and (B13), it can be derived that

$$\begin{aligned}\mathbb{E}\{V_1(t)\} &\le \varsigma_2 e^{-2\rho_1(t-t_{n,1})}\mathbb{E}\{V_2(t_{n,1}^-)\}\\ &\le \varsigma_2 e^{-2\rho_1(t-t_{n,1})}e^{2\rho_2(t_{n,1}-t_{n-1,2})}\mathbb{E}\{V_2(t_{n-1,2})\}\\ &\quad\vdots\\ &\le e^{c_1(t)}\mathbb{E}\{V_1(0)\},\end{aligned} \tag{B14}$$

where $c_1(t) = \left(a_1 + \frac{t}{\eta_D}\right)\left[2(\rho_1+\rho_2)h + 2\rho_2 b_{max} - 2\rho_1 l_{min} + ln(\varsigma_1\varsigma_2)\right]$.

According to (33),

$$\mathbb{E}\{V_1(t)\} \le e^{m_1}e^{-dt}\mathbb{E}\{V_1(0)\}, \tag{B15}$$

where $m_1 = a_1\left[2(\rho_1+\rho_2)h + 2\rho_2 b_{max} - 2\rho_1 l_{min} + ln(\varsigma_1\varsigma_2)\right]$, $d = \frac{\rho_1 l_{min} - (\rho_1+\rho_2)h - \rho_2 b_{max} - 1/2 ln\varsigma_1\varsigma_2}{\eta_D}$.

Similarly,

$$\mathbb{E}\{V_2(t)\} \le \frac{1}{\varsigma_2}e^{m_2}e^{-dt}\mathbb{E}\{V_1(0)\}, \tag{B16}$$

where $m_2 = (a_1+1)[2(\rho_1+\rho_2)h + 2\rho_2 b_{max} - 2\rho_1 l_{min} + ln(\varsigma_1\varsigma_2)]$.

Defining $M = max\{e^{m_1}, \frac{1}{\varsigma_2}e^{m_2}\}$,

$$\mathbb{E}\{V(t)\} \le Me^{-dt}\mathbb{E}\{V_1(0)\}. \tag{B17}$$

According to the definition of V(t), we can obtain:

$$\mathbb{E}\{V(t)\} \ge c_1\|x(t)\|^2, \mathbb{E}\{V_1(0)\} \le c_2\|\varphi\|_h^2, \tag{B18}$$

where $c_1 = min\{d_{min}(P_i)\}$, $c_2 = max\{d_{max}(P_i) + hd_{max}(Q_1) + d_{max}(R_1 + Z_1)\}$.

Then, combining (B17) with (B18), one obtains:

$$\|x(t)\| \le \sqrt{\frac{Mc_2}{c_1}}e^{-\frac{d}{2}t}|\varphi\|_h. \tag{B19}$$

That is to say, under the conditions (27)–(33), the exponentially mean-square stability of system (22) is ensured. This completes the proof. ∎

APPENDIX C

Symbol definitions in Theorem 2:

$$\hat{\Gamma}_{11}^1 = \begin{bmatrix} \hat{\Phi}_{11}^1 & * & * & * & * & * & * \\ \hat{\Phi}_{21}^1 & \hat{\Phi}_{22}^1 & * & * & * & * & * \\ \hat{L}_1^T & \hat{R}_1 - \hat{L}_1^T & \hat{\Phi}_{33}^1 & * & * & * & * \\ \hat{\Phi}_{41}^1 & 0 & 0 & -\hat{\Omega} & * & * & * \\ \hat{\Phi}_{51}^1 & \hat{\Phi}_{52}^1 & \hat{\Phi}_{53}^1 & 0 & \hat{\Phi}_{55}^1 & * & * \\ \hat{N}_1 & 0 & 0 & 0 & \hat{Z}_1 - \hat{N}_1^T & \hat{\Phi}_{66}^1 & * \\ \overline{\alpha}\overline{\beta}_1 Y^T B^T & 0 & 0 & 0 & 0 & 0 & -2\varepsilon_0 X_1 + \varepsilon_0^2 I \end{bmatrix},$$

$$\overline{\alpha}_1 = 1 - \overline{\alpha}, \quad \overline{\beta}_1 = 1 - \overline{\beta}, \quad \delta_1 = \sqrt{\overline{\alpha}\,\overline{\alpha}_1}, \quad \delta_2 = \sqrt{\overline{\beta}\,\overline{\beta}_1},$$

$$\hat{\Phi}_{11}^1 = 2\rho_1 X_1 + AX_1 + X_1 A^T + \hat{Q}_1 + \hat{S}_1 - \hat{R}_1 - \hat{Z}_1,$$

$$\hat{\Phi}_{21}^1 = \overline{\alpha}_1\overline{\beta}_1 Y^T B^T + \hat{R}_1 - \hat{L}_1, \quad \hat{\Phi}_{22}^1 = \rho\hat{\Omega} - 2\hat{R}_1 + \hat{L}_1 + \hat{L}_1^T,$$

$$\hat{\Phi}_{33}^{1} = -e^{-2\rho_1 h}\hat{Q}_1 - \hat{R}_1, \quad \hat{\Phi}_{41}^{1} = \overline{\alpha}_1\overline{\beta}_1 Y^T B^T,$$
$$\hat{\Phi}_{51}^{1} = \overline{\beta}_1 Y^T B^T + \hat{Z}_1 - \hat{N}_1,$$
$$\hat{\Phi}_{55}^{1} = -2\hat{Z}_1 + \hat{N}_1 + \hat{N}_1^T, \quad \hat{\Phi}_{66}^{1} = -e^{-2\rho_1\overline{\eta}}\hat{S}_1 - \hat{Z}_1,$$
$$\hat{\Gamma}_{21}^{1} = \begin{bmatrix} FX_1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$
$$\hat{\Gamma}_{31}^{1} = \begin{bmatrix} \hat{\Pi}_1 & \hat{\Pi}_2 & 0 & \hat{\Pi}_2 & \hat{\Pi}_3 & 0 & \hat{\Pi}_4 \end{bmatrix},$$
$$\hat{\Pi}_1 = \begin{bmatrix} AX_1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \hat{\Pi}_2 = \begin{bmatrix} \overline{\beta}_1\overline{\alpha}_1 BY \\ -\delta_1\overline{\beta}_1 BY \\ -\delta_2\overline{\alpha}_1 BY \\ \delta_1\delta_2 BY \end{bmatrix}, \quad \hat{\Pi}_3 = \begin{bmatrix} \overline{\beta} BY \\ 0 \\ \delta_2 BY \\ 0 \end{bmatrix}, \quad \Pi_4 \begin{bmatrix} \overline{\alpha}\overline{\beta}_1 BY \\ \delta_1\overline{\beta}_1 BY \\ -\delta_2\overline{\alpha} BY \\ -\delta_1\delta_2 BY \end{bmatrix},$$
$$\hat{\Gamma}_{33}^{1} = diag\{-2\nu_1 X_1 + \nu_1^2\hat{R}_1, -2\nu_1 X_1 + \nu_1^2\hat{R}_1, -2\nu_1 X_1 + \nu_1^2\hat{R}_1, -2\nu_1 X_1 + \nu_1^2\hat{R}_1\},$$
$$\hat{\Gamma}_{44}^{1} = diag\{-2\kappa_1 X_1 + \kappa_1^2\hat{Z}_1, -2\kappa_1 X_1 + \kappa_1^2\hat{Z}_1, -2\kappa_1 X_1 + \kappa_1^2\hat{Z}_1, -2\kappa_1 X_1 + \kappa_1^2\hat{Z}_1\},$$
$$\hat{\Gamma}_{11}^{2} = \begin{bmatrix} \hat{\Phi}_{11}^{2} & * & * & * & * \\ \hat{R}_1 - \hat{L}_1 & \Phi_{22}^{2} & * & * & * \\ \hat{L}_2^T & \hat{R}_2 - \hat{L}_2^T & \hat{\Phi}_{33}^{2} & * & * \\ \hat{Z}_2 - \hat{N}_2^T & 0 & 0 & \hat{\Phi}_{44}^{2} & * \\ \hat{N}_2^T & 0 & 0 & \hat{Z}_2 - \hat{N}_2^T & \hat{\Phi}_{55}^{2} \end{bmatrix},$$
$$\hat{\Phi}_{11}^{2} = 2\rho_2 X_2 + AX_2 + X_2 A^T + \hat{Q}_2 + \hat{S}_2 - \hat{R}_2 - \hat{Z}_2, \quad \hat{\Phi}_{22}^{2} = -2\hat{R}_2 + \hat{L}_2 + \hat{L}_2^T,$$
$$\hat{\Phi}_{33}^{2} = -e^{-2\rho_2 h}\hat{Q}_2 - \hat{R}_2, \quad \hat{\Phi}_{44}^{2} = -2\hat{Z}_2 + \hat{N}_2 + \hat{N}_2^T, \quad \hat{\Phi}_{55}^{2} = -e^{-2\rho_2\overline{\eta}}\hat{S}_2 - \hat{Z}_2,$$
$$\hat{\Gamma}_{33}^{2} = -2\nu_2 X_2 + \nu_2^2\hat{R}_2, \hat{\Gamma}_{44}^{2} = -2\kappa_2 X_2 + \kappa_2^2\hat{Z}_2.$$

APPENDIX D

Proof of Theorem 2. The proof of Theorem 2 is as follows. Since

$$\begin{cases} -P_i Z_i^{-1} P_i \le -2\kappa_i P_i + \kappa_i^2 Z_i, \\ -P_i R_i^{-1} P_i \le -2\nu_i P_i + \nu_2^2 R_i. \end{cases} \tag{D1}$$

Replace $-P_1R_1^{-1}P_1$ and $-P_1Z_1^{-1}P_1$ in (26) with $-2\nu_1P_1 + \nu_1^2R_1$ and $-2\kappa_1P_1 + \kappa_1^2Z_1$, and replace $-P_2R_2^{-2}P_2$ and $-P_2Z_1^{-2}P_2$ in (27) with $-2\nu_2P_2 + \nu_2^2R_2$ and $-2\kappa_2P_2 + \kappa_2^2Z_2$, respectively, one can obtain (26) and (27) can be ensured by

$$\overline{\Upsilon}_1^1 = \begin{bmatrix} \Gamma_{11}^1 & * & * & * \\ \Gamma_{21}^1 & -I & * & * \\ h\Gamma_{31}^1 & 0 & \overline{\Gamma}_{33}^1 & * \\ \overline{\eta}\Gamma_{31}^1 & 0 & 0 & \overline{\Gamma}_{44}^1 \end{bmatrix} < 0, \tag{D2}$$

$$\overline{\Upsilon}_1^2 = \begin{bmatrix} \Gamma_{11}^2 & * & * \\ hP_2A & \overline{\Gamma}_{33}^2 & * \\ \eta P_2A & 0 & \overline{\Gamma}_{44}^2 \end{bmatrix} < 0, \tag{D3}$$

where $\overline{\Gamma}_{33}^1 = diag\{-2\nu_1P_1 + \nu_1^2R_1, -2\nu_1P_1 + \nu_1^2R_1, -2\nu_1P_1 + \nu_1^2R_1, -2\nu_1P_1 + \nu_1^2R_1\}$, $\overline{\Gamma}_{44}^1 = diag\{-2\kappa_1P_1 + \kappa_1^2Z_1, -2\kappa_1P_1 + \kappa_1^2Z_1, -2\kappa_1P_1 + \kappa_1^2Z_1, -2\kappa_1P_1 + \kappa_1^2Z_1\}$, $\overline{\Gamma}_{33}^2 = -2\nu_2P_2 + \nu_2^2R_2$, and $\overline{\Gamma}_{44}^2 = -2\kappa_2P_2 + \kappa_2^2Z_2$.

Define $X_i = P_1^{-i}$, $Y = KX_1$, $\hat{\Omega} = X_1\Omega X_1$, $\hat{Q}_i = X_iQ_iX_i$, $\hat{R}_i = X_iR_iX_i$, and $\hat{Z}_i = X_iZ_iX_i$, $\hat{L}_i = X_iL_iX_i$, $\hat{N}_i = X_iN_iX_i$, $\hat{S}_i = X_iS_iX_i(i = 1, 2, \dots, 7)$, $J_1 = diag\{\underbrace{X_1, \dots, X_1}_{7}, I, X_1, X_1, X_1, X_1\}$, $J_2 = diag\{\underbrace{X_2, \dots, X_2}_{5}, I, X_2, X_2\}$. Pre- and postmultiplying

both sides of $\overline{\Upsilon}_1^1$ in (D2) with J_1 and its transposition, pre- and postmultiplying both sides of $\overline{\Upsilon}_1^2$ in (D3) with J_2 and its transposition, one can obtain (D2) and (D3) can be guaranteed by the following (D4) and (42).

$$\tilde{\Upsilon}_1^1 = \begin{bmatrix} \hat{\Gamma}_{11}^1 & * & * & * \\ \hat{\Gamma}_{21}^1 & -X_1X_1 & * & * \\ h\hat{\Gamma}_{31}^1 & 0 & \hat{\Gamma}_{33}^1 & * \\ \overline{\eta}\hat{\Gamma}_{31}^1 & 0 & 0 & \hat{\Gamma}_{44}^1 \end{bmatrix} < 0. \tag{D4}$$

Recalling that $-X_1X_1 \leq -2\varepsilon_0 X_1 + \varepsilon_0^2 I$. Replace $-X_1X_1$ in (D4) by $-2\varepsilon_0 X_1 + \varepsilon_0^2 I$, we derive (D4) can be ensured by (35). Pre- and postmultiplying the first inequality and the second inequality in (28), respectively, one can obtain that (37) can ensure (28) holds by applying Schur complement. Similarly, one can get (38)–(41) from (29)–(32). Pre- and postmultiplying (35) by $\{X_i, X_i\}$ and its transposition, one can get (42). This completes the proof. ■