Hindawi
Discrete Dynamics in Nature and Society
Volume 2022, Article ID 4167304, 10 pages
https://doi.org/10.1155/2022/4167304

Research Article

Secure Event-Triggered Mechanism for Networked Control Systems under Injection Cyber-Attacks

Xiao Cai,[1] **Jian Kang**,[2] **and Kaibo Shi**[3]

[1]*School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China*
[2]*Sichuan Provincial Big Data Technology Services Center, Chengdu, Sichuan 610041, China*
[3]*School of Information Science and Engineering, Chengdu University, Chengdu, Sichuan 611731, China*

Correspondence should be addressed to Jian Kang; kangjian_spbdtsc@sina.com

Received 17 February 2022; Revised 14 March 2022; Accepted 19 March 2022; Published 25 April 2022

Academic Editor: Zi-Peng Wang

Copyright © 2022 Xiao Cai et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This study focuses on the secure stability issue of networked control systems (NCSs) under injection cyber-attacks (ICAs), which have important research value of applications for network security. Firstly, a more general Lyapunov–Krasovskii functional (LKF) is constructed based on the time-delay phenomenon in systems. Secondly, a novel boundary looped function (BLF) is developed depending on the sampling period, fully considering delay and sampling information, and the initial constraints of the criteria on the matrices are effectively relaxed. In addition, appropriate integral inequalities are used, making the obtained criteria less conservative in this paper. Then, a new event-trigger mechanism (ETM) controller under ICAs is designed to control the asymptotical stability (AS) of NCSs. Finally, a numerical experiment verifies the correctness and feasibility of the theory.

1. Introduction

As one of the greatest inventions in the 21st century, the popularity of the Internet has brought significant changes and influences on people's production and lives. With the further development of the Internet, the emergence of big data better reflects the advantages of the Internet. Better handling of big data and better transmission of data have become a hot direction for future research [1, 2]. Data transmission is ultimately reflected in network communication applications (see Figure 1). Thus, network communication technology has been widely used in industrial and military fields. It is a current trend to add components of control systems to these applications through the Internet [3–5].

However, in control theory, signal transmission usually relies on network communication techniques. Therefore, this brings the control system into contact with the Internet [6, 7]. Signal transmission between the components of NCSs can be carried out through the network. When we design and implement the corresponding control system, we can reduce the influence of the signal transmission between the components of NCSs through the network [8]. This approach allows NCSs to reduce their complexity and overall cost-effectiveness. Unnecessary wiring between components is eliminated, which effectively reduces the NCS complexity and overall cost. Therefore, NCSs have become one of the hot issues of current research [9, 10]. In [8], Zhang proposed a novel robust event-triggered fault-tolerant automatic steering control strategy for autonomous land vehicles to achieve path tracking and vehicle lateral motion control under in-vehicle network delay. In [9], the problem of fault-tolerant sampled-data control for an NCS with random time delays and actuator faults was investigated. In [10], the authors studied the application of NCSs to high-speed trains.

On the one hand, the data on the NCS can be effectively shared, which facilitates the fusion of all the information in an ample actual physical space. This way, if the system needs to be upgraded or changed, sensors, controllers, and actuators will need to be added or removed without significant changes to the system architecture [11]. Most importantly, connecting cyber-space to physical space makes real-time control feasible. Therefore, this makes the NCSs gradually

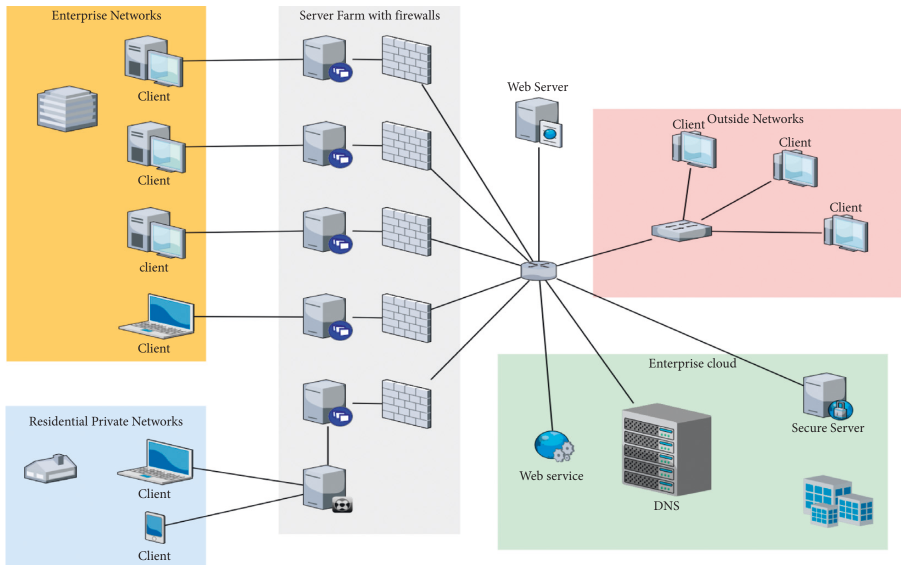

Figure 1: Internet communication topology.

tend to control artificial intelligence and the arrival of the era when everything is connected [12]. On the other hand, the transmission of signals in the communication process of the network is not always secure. Normal loss or delay of signals in network communications is a common phenomenon. We think this phenomenon is acceptable and can be controlled. There has been a malicious attack or sabotage of communication equipment or control systems. We believe this behavior is a cyber-attack, and the person that launched the cyber-attack is a hacker [13]. At present, common cyber-attacks are mainly divided into the following categories: random cyber-attacks [14–16], deception cyber-attacks [17–19], jamming attacks [20, 21], and DoS attacks [22–24]. Thus, effectively countering and defending against hacker attacks is also one of the hot topics. In [15], Liu focused on the controller design problem of NCSs, and a hybrid-triggering communication strategy was employed to save the limited communication resources. In [18], the authors investigated the H_∞ memory sample-data control issue of the T-S fuzzy NCSs with multiple asynchronous deception attacks. In [21], the event-based controller synthesis problem of NCSs under resilient event-triggering communication schemes and periodic DoS jamming attacks was studied. In [24], Feng aimed to explore the tradeoffs between system resilience and network bandwidth capacity.

Based on the above discussion, this paper mainly studies the security issues of NCSs. When hackers attack the system, the ETM controller we designed can effectively ensure the stability of the system. Compared with existing works [25–27], the main contributions of this paper are as follows:

(1) According to the advent of the Internet and the big data era, the security issues of NCSs are being studied. A new ICA is proposed to study the communication security of the system.

(2) A more general LKF is constructed by utilizing the time-delay phenomenon inside the system. According to the characteristics of the sampling period, the constructed LKF contains more sampling information. In addition, the positive definiteness constraint on the initial matrices is further relaxed.

(3) For ICAs launched by hackers, we designed an ETM controller to ensure the AS of the NCS.

2. Preliminaries

In this article, we research the following NCSs:

$$\dot{x}(t) = Ax(t) + B\tilde{u}(t), \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the current state vector of the system; $\tilde{u}(t) \in \mathbb{R}^m$ is the signal to control the input; and A and B are constant matrices.

The control signals are represented as follows:

$$\tilde{u}(t) = u(t) + f(t), \tag{2}$$

where $f(t)$ is the injection attack function.

Remark 1. The popularity of the Internet has made the processing of big data more efficient and faster. Therefore, studying the control of the system based on network communication has become a hot topic of research. There are always some signal fluctuations in the communication process of the control signal. Normal signal fluctuations of the control signal are acceptable. However, some abnormal signals are often injected into the system to destroy the systems' performance, which we call ICAs. As shown in Figure 2, the sensor communicates with the actuator through network communication with signal transmission. During this process, the system may be maliciously attacked by hackers. Therefore, this paper designs a suitable ETM controller for the communication security of NCSs to ensure the system's regular operation.

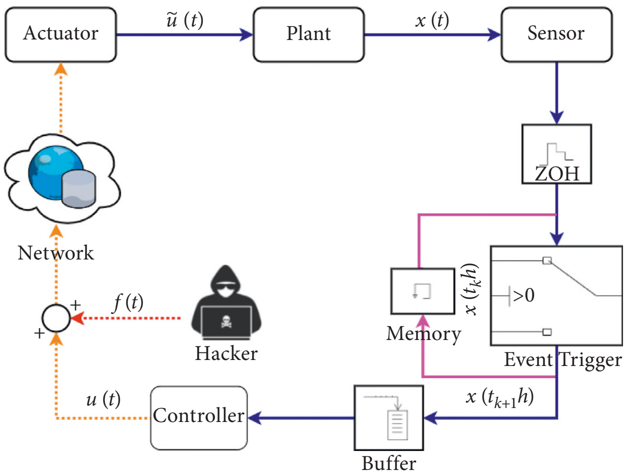

Figure 2: Networked control system under injection attack.

Then, the controller can be designed as

$$u(t) = Kx(t_k h), \quad t \in (t_k h, t_{k+1} h], \tag{3}$$

where K is a controller gain matrix.

In this framework, the sensor is time-triggered while the controller, the zero-order hold (ZOH), and the actuator are event-triggered.

We will illustrate our proposed security-orient resilient triggering strategy as follows:

$$t_{k+1}h = t_k h + \min_{\ell}\{\ell h | e(t_k)\Phi e(t_k) - \delta x^T(t_k h)\Phi x(t_k h) > 0\}, \tag{4}$$

where $e(t_k) = x(t_k h + \ell h) - x(t_k h)$ and $\Phi > 0$. $x(t_k h)$ is the latest transmitted signal at the latest triggering time $t_k h$. The sampling interval is divided into $[t_k h + \eta_{t_k}, t_{k+1}h + \eta_{t_{k+1}})$. η satisfies $[t_k h + \eta_{t_k}, t_{k+1}h + \eta_{t_{k+1}}) = \cup_{\ell=0}^{\eta}\Omega_\ell$, where $\Omega_\ell = [t_k h + \ell h + \eta_{t_{k+\ell}}, t_k h + \ell h + h + \eta_{t_k} + \ell + 1]$, $\ell = 0, 1, \ldots, \eta$, and $\eta = t_{k+1} - t_k - 1$. We define $d(t) = t - t_k h - \ell h$ and $0 \leq \eta_{t_k+\ell} \leq \rho(t) \leq \rho$, in which $\rho \triangleq h + \eta_{t_k+\ell+1}$. From the definitions of $\rho(t)$ and $e(t_k)$, we can obtain $x(t_k h) = x(t - \rho(t)) + e(t_k)$.

Then, we can obtain

$$\tilde{u}(t) = K[x(t - \rho(t)) - e(t_k) + f(t)]. \tag{5}$$

From equations (1) and (5), the closed-loop system as follows:

$$\dot{x}(t) = Ax(t) + BK[x(t - \rho(t)) - e(t_k) + f(t)]. \tag{6}$$

Assumption 1. ([19]). Any $u_1(t)$ and $u_2(t) \in \mathbb{R}^{n_2}$ meets the Lipschitz condition with the following form:

$$f^T(t)f(t) \leq x^T(t)F^T F x(t), \tag{7}$$

where F is the upper bound of $f(\cdot)$.

Lemma 1 (see [28]). *Given $\Omega > 0$ and integrate $e(s)$ over the interval $[a, b] \longrightarrow \mathbb{R}^{n\times n}$, we know the matrix inequality holds:*

$$-(b-a)\int_a^b \dot{e}(s)\Omega\dot{e}(s)\mathrm{d}s \geq -\zeta^T\Omega\zeta - 3\varpi^T\Omega\varpi, \tag{8}$$

where $\zeta = x(b) - x(a)$ and $\varpi = x(b) + x(a) - 2\int_a^b x(s)/b - a$.

3. Main Results

Theorem 1. *Given positive scalars ε, ν, α, h_m, and h_M, system (6) is AS; if there exist symmetric matrices P_1, $P_2 > 0$ and $M_1 > 0$, M_2, then any matrices R_1, R_2, and Y_i $(i = 1, 2, 3)$ with appropriate dimensions satisfy the following LMIs:*

$$\begin{aligned} P_1 + \rho P_2 &> 0, \\ M_1 + \rho M_2 &> 0, \end{aligned} \tag{9}$$

$$\begin{bmatrix} \Xi_{\rho(t)}^{h_k} & \Pi_1 & \Pi_2^T \\ * & -\varepsilon_1 I & 0 \\ * & * & -\varepsilon_2^{-1} I \end{bmatrix} < 0, \tag{10}$$

$$\begin{aligned} \rho(t) &\in \{0, \rho\}, \\ h_k &\in \{h_m, h_M\}, \end{aligned} \tag{11}$$

where other symbols and associated equations are expressed in Appendix B.

Proof. Construct a suitable LKF as follows:

$$V(x_t) = \sum_i^4 V_i(x_t), \quad t \in [t_k h, t_{k+1} h), \tag{12}$$

where

$$\begin{aligned} V_1(x_t) &= \alpha^T(t)P_{\rho(t)}\alpha(t), \\ V_2(x_t) &= \overline{h}_k \underline{h}_k \delta^T(t) M_{\rho(t)}\delta(t), \\ V_3(x_t) &= \overline{h}_k h_M \int_{t_k h - \rho}^{t-\rho} \dot{x}^T(s)R_1\dot{x}(s)\mathrm{d}s, \\ V_4(x_t) &= \underline{h}_k h_M \int_{t-\rho}^{t_{k+1}h-\rho} \dot{x}^T(s)R_2\dot{x}(s)\mathrm{d}s, \end{aligned}$$

$P_{\rho(t)}$, $M_{\rho(t)}$, $\alpha(t)$, $\delta(t)$, $\overline{h}_k$, $\underline{h}_k$, and $\xi(t)$ are listed in Appendix A.

Then, we can obtain the derivative of $V(x_t)$ as follows:

$$\begin{aligned} \frac{\mathrm{d}V(x_t)}{\mathrm{d}t} &= \sum_i^4 \frac{\mathrm{d}V_i(x_t)}{\mathrm{d}t}, \quad t \in [t_k h, t_{k+1} h), \\ \frac{\mathrm{d}V(x_t)}{\mathrm{d}t} &= 2\alpha^T(t)P_{\rho(t)}\dot{\alpha}(t) - \dot{\rho}(t)\alpha^T(t)P_2\alpha(t), \\ &= -\dot{\rho}(t)\alpha^T(t)P_2\alpha(t) + 2\alpha^T(t)P_{\rho(t)}\begin{bmatrix} \dot{x}(t) \\ -x(t-\rho) \\ x(t-\rho) \end{bmatrix}, \\ &= \xi^T(t)\Xi_1\xi(t), \end{aligned} \tag{13}$$

$$\begin{aligned}\frac{\mathrm{d}V_2(x_t)}{\mathrm{d}t} &= \left(\overline{h}_k - \underline{h}_k\right)\delta^T(t)M_{\rho(t)}\delta(t) - \dot{\rho}(t)\overline{h}_k\underline{h}_k \\ &\quad\times \delta^T(t)M_2\delta(t) + 2\delta^T(t)M_{\rho(t)}\dot{\delta}(t), \\ &= \left(\overline{h}_k - \underline{h}_k\right)\delta^T(t)M_{\rho(t)}\delta(t) - \dot{\rho}(t)\overline{h}_k\underline{h}_k \\ &\quad\times \delta^T(t)M_2\delta(t) + 2\delta(t)M_{\rho(t)}\begin{bmatrix} x(t-\rho) \\ 0 \\ 0 \end{bmatrix}, \\ &= \xi^T(t)\Xi_2\xi(t),\end{aligned} \tag{14}$$

$$\begin{aligned}\frac{\mathrm{d}V_3(x_t)}{\mathrm{d}t} &= -\overline{h}_k h_M \dot{x}^T(t-\rho)R_1\dot{x}(t-\rho) \\ &\quad - h_M\int_{t_{k+1}h-\rho}^{t-\rho}\dot{x}(s)R_1\dot{x}(s)\mathrm{d}s,\end{aligned} \tag{15}$$

$$\begin{aligned}\frac{\mathrm{d}V_4(x_t)}{\mathrm{d}t} &= -\overline{h}_k h_M \dot{x}^T(t-\rho)R_1\dot{x}(t-\rho) \\ &\quad - h_M\int_{t_{k+1}h-\rho}^{t-\rho}\dot{x}(s)R_1\dot{x}(s)\mathrm{d}s.\end{aligned} \tag{16}$$

By using Lemma 1, we have

$$\begin{aligned}-h_M\int_{t-\rho}^{t_kh-\rho}\dot{x}^T(s)R_1x(s)\mathrm{d}s &\leq \frac{h_M}{\underline{h}_k\left[x(t_kh-\rho) - x(t-\rho)/x(t_kh-\rho) + x(t-\rho) - 2\int_{t-\rho}^{t_{kh}h-\rho}x(s)/\underline{h}_k ds\right]^T} \\ &\quad\times\begin{bmatrix} R_1 & 0 \\ 0 & 3R_1\end{bmatrix}\left[x(t_kh-\rho) - x(t-\rho)x(t_kh-\rho) + x(t-\rho) - 2\int_{t-\rho}^{t_{kh}h-\rho}x(s)/\underline{h}_k ds\right] \\ &\leq \frac{h_M}{h_m\xi^T(t)\Omega_a^T\overline{R}\Omega_a\xi(t)},\end{aligned} \tag{17}$$

$$\begin{aligned}-h_M\int_{t-\rho}^{t_{k+1}h-\rho}\dot{x}^T(s)R_2x(s)\mathrm{d}s &\leq \frac{h_M}{\overline{h}_k\left[x(t_{k+1}h-\rho) - x(t-\rho)/x(t_{k+1}h-\rho) + x(t-\rho) - 2\int_{t-\rho}^{t_{kh+1}h-\rho}x(s)/\overline{h}_k \mathrm{d}s\right]^T} \\ &\quad\times\begin{bmatrix} R_2 & 0 \\ 0 & 3R_2\end{bmatrix}\left[x(t_{k+1}h-\rho) - x(t-\rho)x(t_{k+1}h-\rho) + x(t-\rho) - 2\int_{t-\rho}^{t_{kh+1}h-\rho}x(s)/\overline{h}_k \mathrm{d}s\right] \\ &\leq \frac{h_M}{h_m\xi^T(t)\Omega_b^T\overline{R}\Omega_b\xi(t)}.\end{aligned} \tag{18}$$

Thus, we know that the following inequality holds:

$$\frac{\mathrm{d}V_3(x_t)}{\mathrm{d}t} + \frac{\mathrm{d}V_4(x_t)}{\mathrm{d}t} \leq \xi^T(t)\left(h_M e^T\left(\underline{h}_k R_2 - \overline{h}_k R_1\right)e_7 + \frac{h_M}{\underline{h}_k\Omega_a\overline{R}_1\Omega_a} + \frac{h_M}{\overline{h}_k\Omega_b\overline{R}_2\Omega_b}\right)\xi(t) = \xi^T(t)\Xi_3\xi(t). \tag{19}$$

Based on system (6), for any matrices Y_1, Y_2, and Y_3, we have the following equation:

$$\begin{aligned}0 &= 2\left[e^T(t_k)Y_1 + x^T(t_kh)Y_2 + x^T(t-\rho(t))Y\right]_3 \\ &\quad\times[Ax(t) + BKx(t-\rho(t)) + BKf(t)], \\ &= \xi^T(t)\mathrm{Sym}\{L\phi\}\xi(t) + 2LBKf(t).\end{aligned} \tag{20}$$

According to Assumption 1, we have the following equation:

$$2LBKf(t) \leq \xi^T(t)\left(\varepsilon\Pi_1\Pi_1^T + \varepsilon^{-1}\Pi_2^T\Pi_2\right)\xi(t). \tag{21}$$

Considering the rules of the designed event-triggered schemes, the following equation holds:

$$e(t_k)\Phi e(t_k) - \delta x^T(t_kh)\Phi x(t_kh) = \xi^T(t)\Theta\xi(t). \tag{22}$$

According to equations (13)–(22), the following equation hold:

$$\begin{aligned}&\frac{\mathrm{d}V(x_t)}{\mathrm{d}t} \\ &\leq \xi^T(t)\left(\sum_{i=1}^{3}\Xi_i + \mathrm{Sym}\{L\phi\} + \varepsilon\times\Pi_1\Pi_1^T + \varepsilon^{-1}\Pi_2^T\Pi_2 + \Theta\right) \\ &\quad\cdot\xi(t).\end{aligned} \tag{23}$$

By using the LCCM, for all, $\mathrm{d}V(x_t)/\mathrm{d}t < 0$ are established. Then, using the Schur complement lemma, we know that (23) is equivalent to

$$\begin{bmatrix} \Xi_{\rho(t)}^{h_k} & \Pi_1 & \Pi_2^T \\ * & -\varepsilon_1 I & 0 \\ * & * & -\varepsilon_2^{-1} I \end{bmatrix} < 0. \tag{24}$$

Therefore, it follows $\sum_i^4 \mathrm{d}V_i(x_t)/\mathrm{d}t < 0$. Finally, system (6) tends to AS. □

Remark 2. Compared with existing works [26, 27, 29], this paper constructs a more general LKF for the time-delay phenomenon in systems: (1) when $\rho(t) = \rho$, the constructed LKF will degenerate into being independent of time delay and (2) when $\rho(t) = 0$, the LKF contains correct time-delay information and time-delay derivative information. This method can introduce more information storage and reduce the conservativeness of the criterion.

Remark 3. Different from the traditional BLFs, $V_2(x_t)$ constructed in this paper contains more sampling moments information $\overline{h}_k$ and $\underline{h}_k$. When $\lim_{t\longrightarrow t_{k+1}^+}\overline{h}_k = \lim_{t\longrightarrow t_k^+}\underline{h}_k = 0$ holds, there is no constraint on the matrices $M_{\rho(t)}$. The BLF constructed in this paper is a promotion and enhancement of the BLF in [30].

Remark 4. In this paper, we construct $V_3(x_t)$ and $V_4(x_t)$. Compared with the LKF in reference [30], $V_3(x_t)$ and $V_4(x_t)$ contain the sampling period h_M information and time-delay ρ information. Then, we obtain tighter upper bounds by scaling with appropriate integral inequalities, which ensures that the criterion is less conservative.

Remark 5. This paper analyzes the performance of the computer in the process of solving the LMIs. The computational complexity of Theorem 1 is $7n^2 + 2n$. Then, based on Intel(R) Core(TM) i7-8700 CPU@3.20 GHz 3.19 GHz, pairs of large-scale LMIs are calculated.

Theorem 2. *Given scalars ε, ν, α, ψ_1, ψ_2, h_m, and h_M, system (6) is AS; if there exist symmetric matrices P_1, $P_2 > 0$, $M_1 > 0$, and M_2, any matrices R_1, R_2, and N with appropriate dimensions satisfy the following LMIs:*

$$\begin{cases} \tilde{P}_1 + \rho\tilde{P}_2 > 0, \\ \tilde{M}_1 + \rho\tilde{M}_2 > 0, \end{cases} \tag{25}$$

$$\begin{bmatrix} \tilde{\Xi}_{\rho(t)}^{h_k} & \tilde{\Pi}_1 & \tilde{\Pi}_2^T \\ * & -\varepsilon_1 I & 0 \\ * & * & -\varepsilon_2^{-1} I \end{bmatrix} < 0, \tag{26}$$

$$\begin{aligned} \rho(t) &\in \{0, \rho\}, \\ h_k &\in \{h_m, h_M\}, \end{aligned} \tag{27}$$

where other symbols and associated equations are expressed in Appendix C.

Table 1: MASPs h_M for different δ's.

δ	[25]	Theorem 2	Improvement (%)
0	1.6982	1.9601	13.3609
0.1	1.1596	1.4927	14.9496
0.2	0.9346	1.0854	13.8935
0.3	0.7621	1.0061	24.2521
0.4	0.6169	0.9592	35.6860
0.5	0.4894	0.6813	28.1667

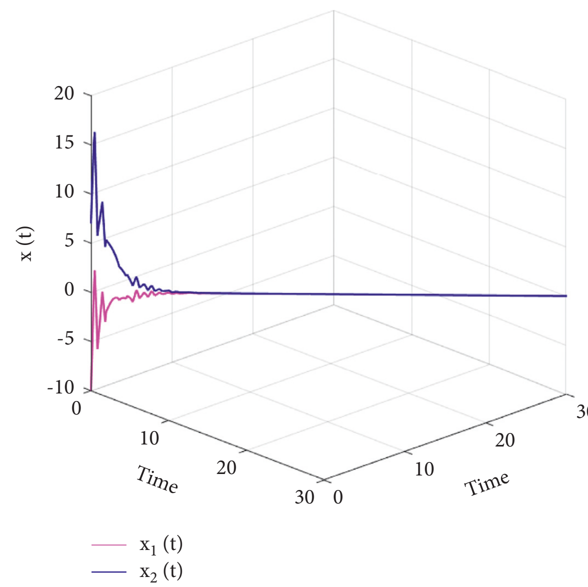

Figure 3: State responses of the original system with control.

Proof. the matrices are defined as $K = NX^{-1}$ and $\tilde{\Phi} = X^{-T}\Phi X^{-1}$.

Then, other matrices are defined as follows:

$$\begin{aligned} Y_1 &= X^{-1}, \\ Y_2 &= \psi_1 X^{-1}, \\ Y_3 &= \psi_2 X^{-1}, \\ \tilde{P}_{\delta(t)} &= \operatorname{diag}\{X^T, X^T, X^T\} P_{\delta(t)} \operatorname{diag}\{X, X, X\}, \\ \tilde{M}_{\delta(t)} &= \operatorname{diag}\{X^T, X^T, X^T\} M_{\delta(t)} \operatorname{diag}\{X, X, X\}, \\ \tilde{R}_1 &= X^T R_1 X, \\ \tilde{R}_1 &= X^T R_1 X. \end{aligned} \tag{28}$$

Premultiplying and postmultiplying (9) and (10) by $\operatorname{diag}\{X^T, X^T, X^T\}$ and $\operatorname{diag}\{X, X, X\}$, then according to Schur complement, we can derive the LMIs (25) and (26). The proof process is consistent with Theorem 1. □

4. Illustrative Example

Example 1. Consider a NCS, the parameters are as follows [25]:

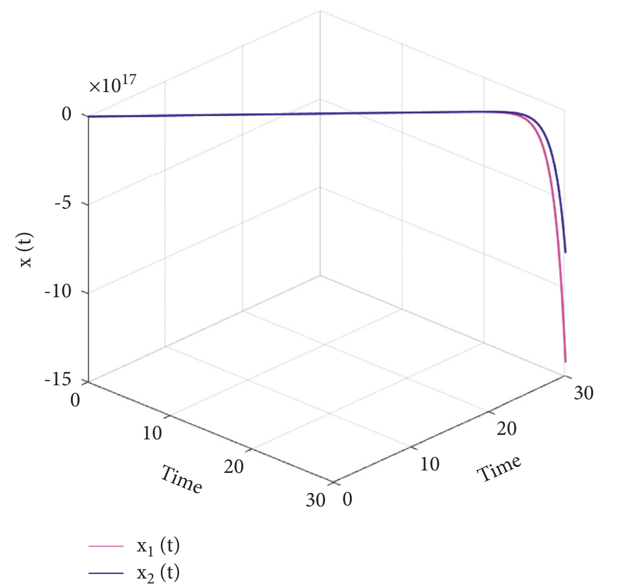

Figure 4: State responses of the original system without control.

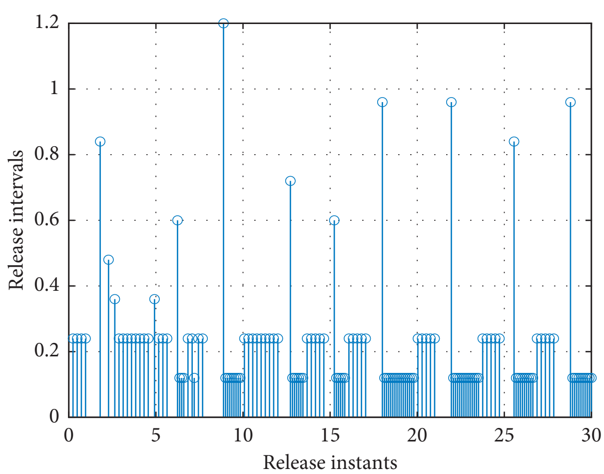

Figure 5: Release instants and time intervals.

$$A = \begin{bmatrix} 0 & 1 \\ 0 & -0.1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0.1 \end{bmatrix}. \tag{29}$$

4.1. Case A: The System Is in Normal State. In this case, our research system is operating normally in a safe state. When $\rho = 0$, $F = 0$, and $h_m = 0.1$, we solve for maximum acceptable sampling periods (MASPs) by using Theorem 2. It can be seen from Table 1 that the MASPs h_M under different δ are better than reference [25]. When $\delta = 0.3$, the $h_M = 1.0061$ solved in this paper is 24.2521% higher than the result of reference [25].

To verify the validity of the criterion, we solve the controller gain matrix is $K = [50.4168 - 17.8803]$ by using the Yalmip toolbox in Matlab. Then, we set $h_m = h_M = 0.01$, $\delta = 0.3$, and $x(0) = [-10, 7]^T$; furthermore, the stability of the system is verified by plotting the state trajectory images of the system.

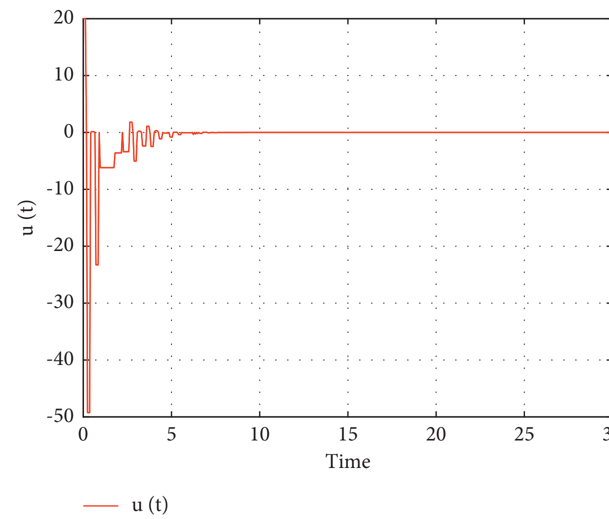

Figure 6: Control input signal $u(t)$.

Table 2: MASPs h_M for different δ's under ICA.

δ	[25]	Case A	Case B	Reduction (%)
0	1.6982	1.9601	1.5039	23.2743
0.1	1.1596	1.4927	1.1725	21.4511
0.2	0.9346	1.0854	0.9967	8.1721
0.3	0.7621	1.0061	0.8916	11.3806
0.4	0.6169	0.9592	0.7109	25.8861
0.5	0.4894	0.6813	0.4593	32.5845

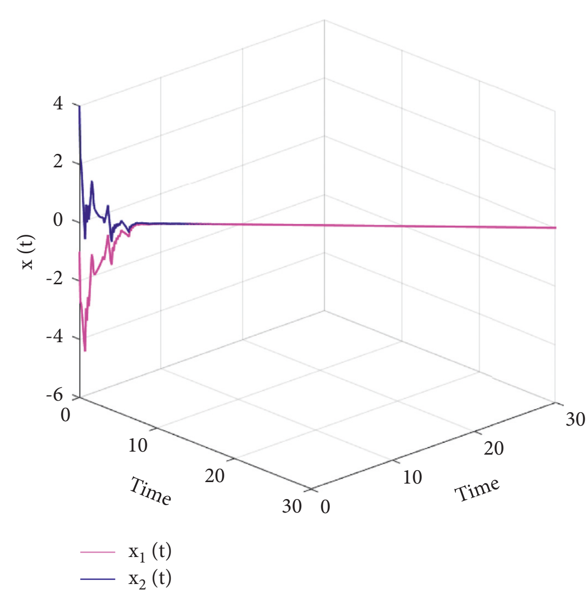

Figure 7: State responses of the original system with control.

In Figure 3, we can see that with the increase in time, the running trajectory of the system will fluctuate. But it eventually converges on a steady state. This means that the controller we designed is suitable. In order to more intuitively reflect the effect of the controller designed in this paper, we also draw Figure 4 of the running trajectory of the system when the controller fails.

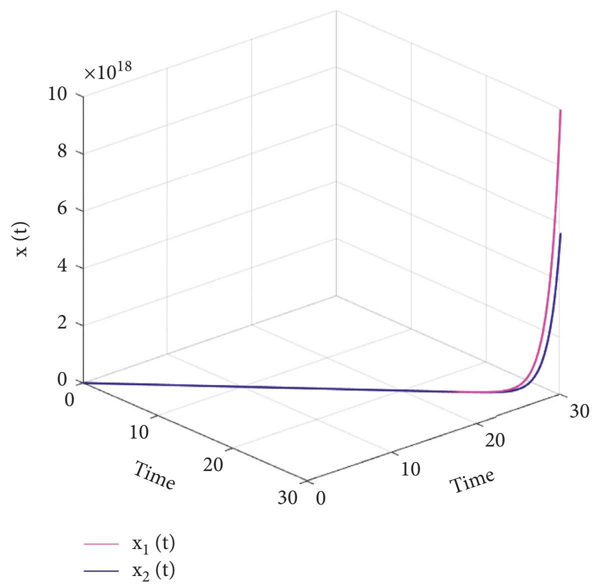

Figure 8: State responses of the original system without control.

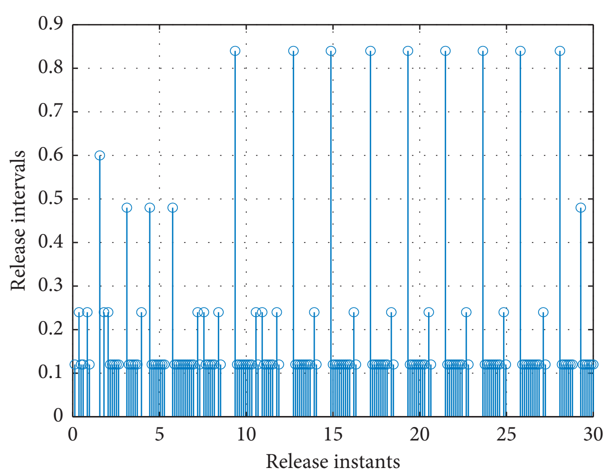

Figure 9: Release instants and time intervals.

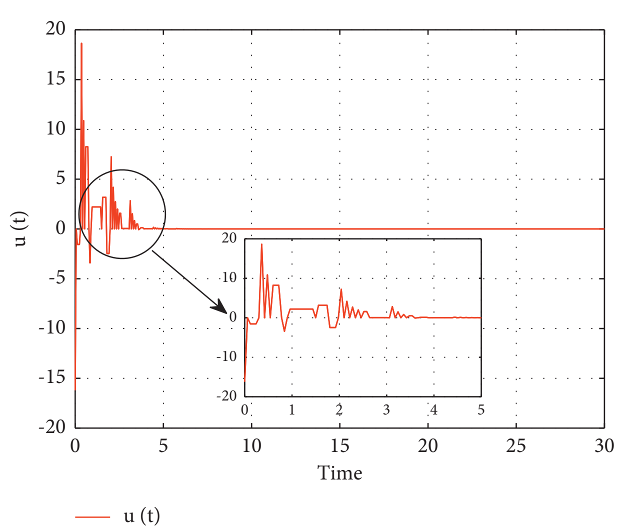

Figure 10: Control input signal $u(t)$.

In addition, the release time distribution and control signal input are shown in Figures 5 and 6, respectively.

4.2. Case B: The System Is in Abnormal State. In this case, we conducted a simulation experiment, as in Case A. When $\rho = 0$, $h_m = 0.1$, $F_1 = 0.1$, and $F_2 = 0.1$, the MASPs solved by using Matlab are shown in Table 2. Table 2 shows that the performance of the system is reduced when the system is attacked. However, the method proposed in this paper can still ensure the stability of the system. Assuming $\delta = 0.3$, we solve $h_M = 1.0061$ when the system is running normally. However, solve for $h_M = 0.8916$ when ICAs constrain the system. By comparing the results, we know that although 11.3806% reduces the performance, our criterion is still less conservative than the results in reference [25].

Then, when $\psi_1 = \psi_2 = 1$ the controller gain is $K = [27.8726 - 10.5776]$. Setting $\rho = 0$, $h_m = h_M = 0.01$, and $\delta = 0.3$, the initial condition is $x(0) = [4, -1]^T$. We assume that the attack function injected by the hacker is $f(t) = [-\tanh(0.5x(t)), -\tanh(0.25x(t))]^T$. When the system is subjected to ICAs, we plot the state trajectory of the system in Figure 7. Compared with the normal running trajectory in Figure 3, we can see that the system oscillates more obviously and can still reach a stable state eventually. Furthermore, the trajectory of the system in the case of controller failure is plotted in Figure 8.

Finally, we plot the release time distribution of the system in Figure 9 and the control signal input in Figure 10.

5. Conclusion

This paper has considered the secure stability issue of NCSs under ICAs, which have important research value of applications for network security. Firstly, a more general LKF has been constructed based on the time-delay phenomenon in the system. Secondly, a novel BLF has been developed depending on the sampling period, fully considering time delay and sampling information, and the initial constraints on the criterion on the matrices have been effectively relaxed. In addition, appropriate integral inequalities have been used, making the criteria less conservative in this paper. Then, a new ETM controller under ICAs has been designed to control the AS of NCSs. Finally, a numerical experiment has verified the correctness and feasibility of the theory. In the future, we extend this method and safety control strategy to T-S fuzzy systems, switching systems, Markov hopping systems, and some other systems.

Notations

R^n:	n-Dimensional Euclidean space
$\mathbf{Z}^{n\times n}$:	$n\times n$ real matrices
I:	Identity matrix
$\mathbf{Q}^n$:	$n\times n$ real symmetric matrices
$\mathscr{H} > 0$:	Denote that $\mathscr{H}$ is a real positive definite matrix
Sym $= X^T + X$, and diag $\{\cdots\}$:	Block diagonal matrix.

Appendix

A

$$\alpha(t)=\mathrm{col}\left\{x(t),\int_{t-\rho}^{t_kh-\rho}x(s)\mathrm{d}s,\int_{t_{k+1}h-\rho}^{t-\rho}x(s)\mathrm{d}s\right\},$$
$$\delta(t)=\mathrm{col}\left\{x(t-\rho),x(t_kh-\rho),x\left(t_{k+1h-\rho}\right)\right\},$$
$$P_{\rho(t)}=P_1+(\rho-\rho(t))P_2,$$
$$M_{\rho(t)}=M_1+(\rho-\rho(t))M_2,$$
$$\overline{h}_k=t_{k+1}h-t,$$
$$\underline{h}_k=t-t_kh,$$
$$\xi(t)=\mathrm{col}\left\{\begin{array}{c}x(t),x(t-\rho),\\ x(t_kh-\rho),x(t_{k+1}h-\rho),x(t_kh),\dot{x}(t),\dot{x}(t-\rho)\\ \int_{t-\rho}^{t_kh-\rho}\frac{x(s)}{\underline{h}_k}\mathrm{d}s,\int_{t-\rho}^{t_{k+1}h-\rho}\frac{x(s)}{\overline{h}_k}\mathrm{d}s,x(t-\rho(t)),e(t_k)\end{array}\right\}. \tag{A.1}$$

B

$$\widetilde{\Xi}_{\rho(t)}^{h_k}=\sum_{i=1}^{3}\widetilde{\Xi}_i+\mathrm{Sym}\left\{\widetilde{L}\widetilde{\phi}\right\}+\widetilde{\Theta},$$
$$\widetilde{\Xi}_1=\mathrm{Sym}\left\{\Phi_1^T\widetilde{P}_{\rho(t)}\Phi_2\right\}-\mu_1\Phi_1^T\widetilde{P}_2\Phi_1,$$
$$\widetilde{\Xi}_2=-\underline{h}_k\Phi_3^T\widetilde{M}_{\rho(t)}\Phi_3+\overline{h}_k\Phi_3^T\widetilde{M}_{\rho(t)}\Phi_3-\mu_1\overline{h}_k\underline{h}_k\Phi_3^T\widetilde{M}_2\Phi_3,$$
$$\widetilde{\Xi}_3=h_Me_7^T\left(\underline{h}_k\widetilde{R}_2-\overline{h}_k\widetilde{R}_1\right)e_7+\frac{h_M}{h_m\Omega_a^T\widetilde{\overline{R}}_1\Omega_a}+\frac{h_M}{h_m\Omega_b^T\widetilde{\overline{R}}_2\Omega_b},$$
$$\widetilde{L}=e_{11}^T+\psi_1e_5^T+\psi_2e_{10}^T,$$
$$\widetilde{\varphi}=AXe_1+BNe_{10},$$
$$\Theta=e_{11}^T\Phi e_{11}-\delta e_5^T\Phi e_5,$$
$$\Pi_1=LBK,$$
$$\Pi_2=Fe_3,$$
$$\Omega_a=\mathrm{col}\{e_3-e_2,e_3+e_2-2e_8\},$$

(HTML translation failed)

$$\Phi_1=\mathrm{col}\left\{e_1,\underline{h}_ke_8,\overline{h}_ke_9\right\},$$
$$\Phi_2=\mathrm{col}\{e_6,-e_2,e_2\},$$
$$\Phi_3=\mathrm{col}\{e_2,e_3,e_4\},$$
$$\Phi_4=\mathrm{col}\{e_7,0,0\},$$
$$\overline{R}_1=\begin{bmatrix}R_1&0\\0&3R_1\end{bmatrix},$$
$$\overline{R}_2=\begin{bmatrix}R_2&0\\0&3R_2\end{bmatrix}, \tag{A.2}$$

C

$$\Xi_{\rho(t)}^{h_k}=\sum_{i=1}^{3}\Xi_i+\mathrm{Sym}\{L\phi\}+\Theta,$$
$$\Xi_1=\mathrm{Sym}\left\{\Phi_1^TP_{\rho(t)}\Phi_2\right\}-\mu_1\Phi_1^TP_2\Phi_1,$$
$$\Xi_2=-\underline{h}_k\Phi_3^TM_{\rho(t)}\Phi_3+\overline{h}_k\Phi_3^TM_{\rho(t)}\Phi_3-\mu_1\overline{h}_k\underline{h}_k\Phi_3^TM_2\Phi_3,$$
$$\Xi_3=h_Me_7^T\left(\underline{h}_kR_2-\overline{h}_kR_1\right)e_7+\frac{h_M}{h_m\Omega_a^T\overline{R}_1\Omega_a}+\frac{h_M}{h_m\Omega_b^T\overline{R}_2\Omega_b},$$
$$L=e_{11}^TY_1+e_5^TY_2+e_{10}^TN_3,$$
$$\varphi=Ae_1+BKe_{10},$$
$$\Theta=e_{11}^T\Phi e_{11}-\delta e_5^T\Phi e_5,$$
$$\Pi_1=LBK,$$
$$\Pi_2=Fe_3,$$
$$\Omega_a=\mathrm{col}\{e_3-e_2,e_3+e_2-2e_8\},$$
$$\Omega_b=\mathrm{col}\{e_4-e_2,e_4+e_2+2e_9\},$$
$$\Phi_1=\mathrm{col}\left\{e_1,\underline{h}_ke_8,\overline{h}_ke_9\right\},$$
$$\Phi_2=\mathrm{col}\{e_6,-e_2,e_2\},$$
$$\Phi_3=\mathrm{col}\{e_2,e_3,e_4\},$$
$$\Phi_4=\mathrm{col}\{e_7,0,0\},$$
$$\overline{R}_1=\begin{bmatrix}R_1&0\\0&3R_1\end{bmatrix},$$
$$\overline{R}_2=\begin{bmatrix}R_2&0\\0&3R_2\end{bmatrix}. \tag{A.3}$$

Data Availability

The data used to support this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (n61703060, 12061088, 61802036, and 61873305), the Sichuan Science and Technology Program (21YYJC0469), the Project funded by the China Postdoctoral Science Foundation (2020M683274 and 2021T140092), the Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China (ICT2021B38), and Guangdong Basic and Applied Basic Research Foundation (2021A1515011692). This study was supported by a grant from the Science and Technology Department of Sichuan Province (2020YFG0300) and an open project fund of Intelligent Terminal Key Laboratory of Sichuan Province (2019–2020)+SCITLAB-0002.

References

[1] M. G. H. Bangui and B. B. Uhnova, "Big data for Internet of things: a survey," *Future Generation Computer Systems*, vol. 87, pp. 601–614, 2018.

[2] S. Shadroo and A. M. Rahmani, "Systematic survey of big data and data mining in internet of things," *Computer Networks*, vol. 139, no. 5, pp. 19–47, 2018.

[3] R. M. Murray, "Future directions in control, dynamics, and systems: overview, grand challenges and new courses," *RM Murray European Journal of Control*, vol. 9, no. 2, pp. 144–158, 2003.

[4] L. Zhang, H. Gao, and O. Kaynak, "Network-induced constraints in networked control systems-A survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 403–416, 2013.

[5] W. Zhang, M. S. Branicky, and S. M. Phillips, "Reachable set estimation for neural network control systems: a simulation-guided approach," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 5, pp. 1821–1830, 2021.

[6] A. L. S. N. Bharathi, A. B. Ganesh, and T. K. Radhakrishnan, "Particle swarm optimization tuned cascade control system in an Internet of Things (IoT) environment," *Measurement*, vol. 117, pp. 80–89, 2018.

[7] Z. L. Ning, K. Y. Zhang, X. J. Wang et al., "Joint computing and caching in 5G-envisioned Internet of vehicles: a deep reinforcement learning-based traffic control system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 5201–5212, 2021.

[8] J. Zhang, B. Zhang, N. Zhang, C. Wang, and Y. Chen, "A novel robust event-triggered fault tolerant automatic steering control approach of autonomous land vehicles under in-vehicle network delay," *International Journal of Robust and Nonlinear Control*, vol. 31, no. 7, pp. 2436–2464, 2021.

[9] F. Fang, H. Ding, Y. Liu, and J. H. Park, "Fault tolerant sampled-data H∞ control for networked control systems with probabilistic time-varying delay," *Information Sciences*, vol. 544, no. 12, pp. 395–414, 2021.

[10] X. Cai, K. Shi, S. Zhong, and X. Pang, "Dissipative sampled-data control for high-speed train systems with q_m," *IEEE Transactions on Intelligent Transportation Systems*, vol. 6, no. 429, pp. 1–12, 2021.

[11] Z. Zhang, S. Shu, F. Lin, and S. Li, "Online supervisory control of networked discrete-event systems with control delays," *IEEE Transactions on Automatic Control*, vol. 1, 2021.

[12] J. P. Farwell and R. Rohozinski, "Extended dissipative sliding mode control for nonlinear networked control systems via event-triggered mechanism with random uncertain measurement," *Applied Mathematics and Computation*, vol. 396, no. 1, Article ID 125901, 2021.

[13] X.-M. Zhang, Q.-L. Han, X. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3616–3626, 2020.

[14] X. Cai, S. Zhong, J. Wang, and K. Shi, "Robust H∞ control for uncertain delayed T-S fuzzy systems with stochastic packet dropouts," *Applied Mathematics and Computation*, vol. 385, Article ID 125432, 2020.

[15] J. Liu, Z.-G. Wu, D. Yue, and J. H. Park, "Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 2, pp. 943–953, 2021.

[16] A. Y. Lu and G. H. Yang, "Hybrid-driven-based H_∞ control for networked cascade control systems with actuator saturations and stochastic cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 12, pp. 2452–2463, 2019.

[17] K. Wang, E. Tian, J. Liu, L. Wei, and D. Yue, "Resilient control of networked control systems under deception attacks: a memory-event-triggered communication scheme," *International Journal of Robust and Nonlinear Control*, vol. 30, no. 4, pp. 1534–1548, 2020.

[18] X. Cai, K. Shi, K. She, and S. Zhong, "H_∞ memory sample-data control for T-S fuzzy network control system with multiple asynchronous deception attacks," in *Proceedings of the International Conference on Applied Nonlinear Dynamics*, pp. 801–811, Springer, Hong Kong, China, August 2021.

[19] Z. Gu, X. Zhou, T. Zhang, F. Yang, and M. Shen, "Event-triggered filter design for nonlinear cyber-physical systems subject to deception attacks," *ISA Transactions*, vol. 104, pp. 130–137, 2020.

[20] H. Yang, M. Shi, Y. Xia, and P. Zhang, "Security research on wireless networked control systems subject to jamming attacks," *IEEE Transactions on Cybernetics*, vol. 49, no. 6, pp. 2022–2031, 2019.

[21] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Transactions on Cybernetics*, vol. 49, no. 12, pp. 4271–4281, 2019.

[22] Y. Deng, X. Yin, and S. Hu, "Event-triggered predictive control for networked control systems with DoS attacks," *Information Sciences*, vol. 542, no. 4, pp. 71–91, 2021.

[23] N. Zhao, P. Shi, W. Xing, and J. Chambers, "Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks," *IEEE Transactions on Control of Network Systems*, vol. 8, no. 1, pp. 158–167, 2020.

[24] S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, and C. D. Persis, "Networked control under DoS attacks: tradeoffs between resilience and data rate," *IEEE Transactions on Automatic Control*, vol. 66, no. 1, pp. 460–467, 2020.

[25] Y. Guan and C. Peng, "A hybrid transmission scheme for networked control systems," *ISA Transactions*, vol. 96, pp. 155–162, 2020.

[26] X. Cai, K. B. Shi, K. She, S. M. Zhong, J. Wang, and H. C. Yan, "New results for t-s fuzzy systems with hybrid communication delays," *Fuzzy Sets and Systems*, vol. 438, 2021.

[27] F. Long, C. K. Zhang, L. Jiang, Y. He, and M. Wu, "Stability analysis of systems with time-varying delay via improved Lyapunov-Krasovskii functional," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 4, pp. 1–10, 2019.

[28] A. Seuret and F. Gouaisbaut, "Wirtinger-based integral inequality: application to time-delay systems," *Automatica*, vol. 49, no. 8, pp. 2860–2866, 2013.

[29] C.-K. Zhang, Y. He, L. Jiang, M. Wu, and Q.-G. Wang, "An extended reciprocally convex matrix inequality for stability analysis of systems with time-varying delay," *Automatica*, vol. 85, pp. 481–485, 2017.

[30] X. Cai, K. Shi, S. Zhong, and Y. Q. Tang, "Dissipative analysis for high speed train systems via looped-functional and relaxed condition methods," *Applied Mathematical Modelling*, vol. 96, pp. 570–583, 2021.