applied sciences

MDPI

Article

Event-Based Security Control for Markov Jump Cyber–Physical Systems under Denial-of-Service Attacks: A Dual-Mode Switching Strategy

Mingke Gao [1], Zhiqiang Li [1,*], Tao Pang [1], Hong Xu [1,2] and Siji Chen [1,3]

[1] The 32nd Research Institute of China Electronics Technology Group Corporation (CETC 32), Shanghai 201800, China; michaelgar@foxmail.com (M.G.); t_pang@126.com (T.P.); xuhong1990@hdu.edu.cn (H.X.); cqchensj@foxmail.com (S.C.)
[2] School of Computer Science, Hangzhou Dianzi University, Hangzhou 310018, China
[3] School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
* Correspondence: zhiqiangli1030@163.com

Abstract: This paper studies the design of dual-mode resilient event-triggered control strategy for Markov jump cyber–physical systems (MJCPSs) under denial-of-service (DoS) attacks. Firstly, a novel resilient event-triggering scheme dependent on the DoS signal is developed to select the corresponding control protocol based on the current network quality of services. Particularly, the potential relationship between the triggering signal and system mode under DoS attacks is discussed, aiming to eliminate both Zeno behavior and singular triggering behavior by calculating the minimum and maximum data update rates. Then, we design an event-based dual-mode security controller to ensure that the closed-loop system has stochastic stability and good robust H_∞ performance under DoS attacks. By constructing a Lyapunov–Krasovskii functional which depends on the lower and upper bounds of time delay, sufficient conditions for the existence of dual-mode security controller gains and resilient triggering parameters are presented with the LMI form. Finally, simulation results show that the proposed security control strategy has good robustness against DoS attacks.

Keywords: Markov jump cyber–physical systems (MJCPSs); denial-of-service (DoS) attacks; event-triggered control; resilient control; dual-mode switching strategy

Citation: Gao, M.; Li, Z.; Pang, T.; Xu, H.; Chen, S. Event-Based Security Control for Markov Jump Cyber–Physical Systems under Denial-of-Service Attacks: A Dual-Mode Switching Strategy. *Appl. Sci.* **2023**, *13*, 11815. https://doi.org/10.3390/app132111815

Academic Editor: Luis Javier García Villalba

Received: 25 August 2023
Revised: 26 October 2023
Accepted: 26 October 2023
Published: 29 October 2023

1. Introduction

With the rapid development of artificial intelligence and other technologies, cyber–physical systems (CPSs) that can highly integrate computation, communication, and control have emerged and been widely used in critical infrastructures, such as smart grids [1], intelligent transportation [2], industrial internet [3], and so on. In essence, CPSs are a class of complex networked control systems with a cyclic feedback mechanism, and the ubiquitous interconnection features make the openness increasingly enhanced [4]. This means that the deep interaction between the information world and physical plant has achieved global autonomy and collaboration. However, the influence of cyber security threats and physical safety issues has brought great challenges to the integrated protection of CPSs. Once the security defense mechanism deployed on the information layer fails, malicious adversaries can covertly invade the information systems, causing CPS-induced failures to spread rapidly in the communication media, thereby making the serious non-contact damage to the physical process. Since physical systems operate in a relatively isolated environment, there is a lack of in-depth understanding of external network threats and internal security vulnerabilities [5]. Thus, it is of great value to design advanced security control strategies to ensure the safe operation of plants in an unreliable network environment. Recently, security issues for CPSs have attracted widespread attention, such as intrusion identification [6–8], secure state estimation [9–11], stability analysis [12–15], and resilient control [16–19].

In CPSs, malicious attackers have developed various remote intrusion modes by destroying the security requirements of physical systems, such as denial-of-service (DoS) attacks, false data injection (FDI) attacks, and deception attacks [20], where DoS attacks force system service interruption by occupying the limited communication bandwidth. In addition, DoS attacks do not need to acquire any prior system knowledge, which implies that DoS attacks can be easily launched without regard for privacy protection [21]. In this attack scenario, the abnormal behaviors caused by DoS attacks can be quickly perceived. However, the access to control and measurement signals will be lost, making it impossible to effectively deal with this attack behavior. Thus, it is necessary to develop an advanced security control strategy with robustness and intrusion tolerance to ensure that CPSs can operate smoothly in a degraded manner under DoS attacks. The authors in [12] have proposed the concept of "*resilient control*" to characterize the basic ability of CPSs to defend against DoS attacks. In [13], the authors developed an observer-based security control strategy for linear CPSs with multiple parallel transmission channels. The maximum operational duty cycle tolerated by CPSs under DoS attacks was obtained. To ensure both steady-state accuracy and transient security, the authors in [22] designed an active security control policy, where DoS attacks are assumed to occur in both control and measurement channels. The relationship between the resilience and communication bandwidth was studied in [23], where the bit rate condition under DoS attacks depends on the attack parameters and system matrices. The issue of secure consensus for interconnected CPSs under DoS attacks was discussed in [24–28], where the authors in [25] developed a time-varying resilient control scheme to ensure the secure consensus of the agent team. In [28], the authors discussed the co-design of the fault detection algorithm and consensus control protocol for interconnected CPSs under hidden DoS attacks. Since CPSs are susceptible to environmental mutations or random failures of physical components, they may consist of multiple subsystems with different structures and parameters. However, the above achievements are research on the security of deterministic CPSs, ignoring the research on CPSs with random jumps under cyber attacks.

Generally, it is difficult for the system to obtain measurement or control signals in a continuous manner. In order to overcome persistent communication, many sampled-data control policies based on a time-triggered communication mechanism have been widely investigated, see [29–32]. However, due to the limited communication bandwidth, this implies that the time-triggered sampling strategies can generate unnecessary consumption and computing resources. Consequently, the oversampling problem needs to be eliminated. As an effective solution to alleviate the communication burden, the event-triggered mechanism (ETM) regarded as "*on-demand communication*" was reported in [33–37], where the authors in [33] proposed a co-design method for the resilient event-triggered control (ETC) strategy to tolerate DoS attacks as much as possible. To obtain a higher communication efficiency, a novel switching-like ETC strategy for continuous CPSs was developed in [34] to balance the desired communication rate and security performance. In [35], a fully distributed secure cooperative control protocol for CPSs was developed to guarantee asymptotic consensus against distributed DoS attacks from multiple adversaries. The authors in [36] formulated a stochastic ETC scheme to overcome the stochastic DoS attacks by fully using the dynamic features of communication in the open network. Particularly, CPSs are vulnerable to environmental mutations or random failures of physical components, resulting in their potential to be composed of multiple subsystems with different structures and parameters. Therefore, it is necessary to develop appropriate security control strategies to ensure that jump CPSs still have an acceptable level of operation under cyber attacks. In addition, the authors in [37] developed a finite-time ETC strategy for nonlinear semi-Markov jump CPS to quickly defend against FDI attacks in finite time. Note that most ETC schemes adjust their event-triggering parameters in advance to counter the negative impact of DoS attacks on data transmission. This indicates that the traditional strategies have certain limitations when dealing with unpredictable DoS jamming attacks. Recently,

the impact of DoS attacks was transformed into the uncertainty in triggering rule reported in [38], which plays a positive role in solving the mentioned problem.

However, very few works are available to solve similar topics for stochastic CPSs under DoS attacks and Markovian switching, to our knowledge. These facts inspire us to proceed with the present work.

This paper proposes a novel dual-mode resilient event-triggered control strategy for MJCPSs under DoS attacks. The salient contributions are as follows:

(1) A novel resilient event-triggering rule that relies on DoS signals is designed to select corresponding control strategies on demand based on the current network service quality.
(2) By analyzing the inner relationship between the system mode and the triggering instant under DoS attacks, the minimum and maximum inter-execution intervals are calculated to avoid Zeno behavior and singular triggering.
(3) Based on the LMI method and Lyapunov stability theory, sufficient conditions for the existence of security controller gains and resilient triggering parameters are given in the form of concise LMIs simultaneously.

The outline of this paper is organized as follows. Section 2 presents preliminaries and problem formulation. In Section 3, stability analysis under resilient event-triggered rule and DoS attacks is investigated in detail. The dual-mode security controller is designed in Section 4. In Section 5, a simulation example is presented to illustrate the effectiveness of the proposed method. Finally, Section 6 summarizes this paper.

2. Preliminaries and Problem Formulation

2.1. System Framework

Consider MJCPSs defined on a complete probability space $(\Omega, \mathcal{F}, \mathbb{P})$, whose dynamics can be captured by

$$\begin{cases} \dot{x}(t) = A_{r(t)}x(t) + B^u_{r(t)}u(t) + B^\omega_{r(t)}\omega(t) \\ z(t) = C_{r(t)}x(t) + D^u_{r(t)}u(t) \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^{n_x}$, $u(t) \in \mathbb{R}^{n_u}$, and $z(t) \in \mathbb{R}^{n_z}$ are the system state, control input, and regulated output variables, respectively. $\omega(t) \in \mathbb{R}^{n_\omega}$ represents an exogenous disturbance belonging to $\mathcal{L}_2[0, +\infty)$. $A_{r(t)}$, $B^u_{r(t)}$, $B^\omega_{r(t)}$, $C_{r(t)}$, and $D^u_{r(t)}$ denote known matrices of compatible dimensions.

Let $\{r(t), t \geq 0\}$ represent a right-continuous Markov process taking values in a finite set $\mathbb{S} \triangleq \{1, 2, \ldots, S\}$, whose stationary mode transition rate matrix (TRM) $\Pi \triangleq [\pi_{ij}] \in \mathbb{R}^{S\times S}$ can be given by

$$\begin{aligned} &\Pr\{r(t+\Delta t) = j | r(t) = i\} \\ &\qquad = \begin{cases} \pi_{ij}\Delta t + o(\Delta t), & i \neq j \\ 1 + \pi_{ii}\Delta t + o(\Delta t), & i = j \end{cases} \end{aligned} \tag{2}$$

where $\Delta t > 0$, $\lim_{\Delta t \to 0}(o(\Delta t)/\Delta t) = 0$, and TRs from i to j satisfy two conditions, that is, if $i \neq j$ then $\pi_{ij} > 0$; otherwise, $\pi_{ii} = -\sum_{i \neq j} \pi_{ij}$ for any $i, j \in \mathbb{S}$.

On the other hand, Figure 1 presents an advanced event-based control architecture for MJCPSs subject to energy-limited DoS attacks, where the virtual sensor system determined by a novel resilient event-triggered rule is developed to alleviate the heavy communication burden generated by using traditional sampled-data schemes, see refs. [29–31] and the references therein. For clarity, let $e_s(t) = x(t_{k+1}) - x(t_k)$ represent the sampled error, then we review a general event-triggered scheme mentioned in [38] as follows:

$$t_{k+1} = \inf\Big\{ t \in \mathbb{R}_{>t_k} | e_s^T(t)\Theta_a e_s(t) > \sigma x^T(t)\Theta_b x(t) \Big\}, \tag{3}$$

where $\sigma \in (0, 1)$ is a given triggering parameter, Θ_a and Θ_b are the unknown weighting matrices to be designed, and $\{t_k\}_{k\in\mathbb{N}_0}$ denotes the triggering sequence determined by (3).

In this way, the control input applied to the control layer in the absence of DoS attacks can be described as

$$u(t) = K_{r(t)}x(t_k),\ t \in [t_k, t_{k+1}) \tag{4}$$

where $K_{r(t)}$ denotes the unknown control gain to be designed. Notice that the packets are transmitted on the sensor–controller (S-C) and controller–actuator (C-A) channels over the open and secure communication networks, respectively. This means that the S-C channel is vulnerable to remote intrusion by malicious attackers. From the perspective of system control performance, malicious intrusion on the S-C channel may cause information mismatch between the S-C and C-A channels. That is, the actuator may maintain historical control actions for a long time, which is enough to pose a serious threat to physical security. In order to ensure safe operation in an unreliable network environment, we will redesign an improved resilient event-triggered scheme and related security control protocol for MJCPSs in the sequel.

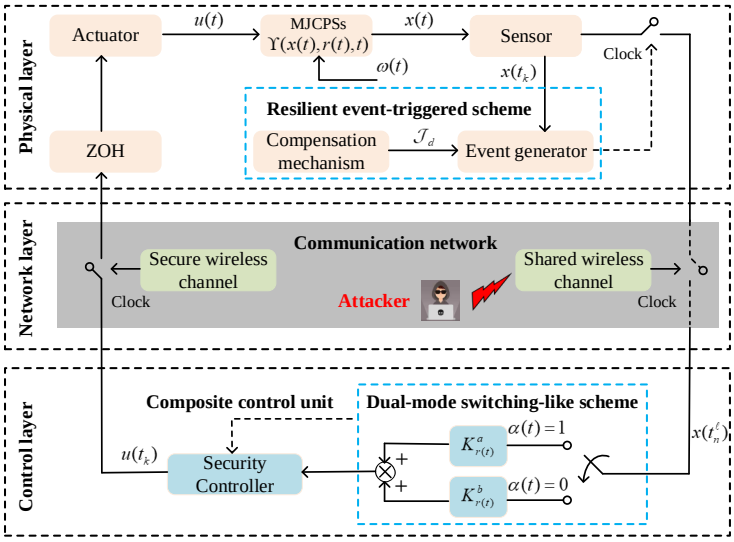

Figure 1. Control architecture of MJCPSs under DoS attacks.

2.2. Dual-Mode Security Control Scheme

In general, the purpose of designing event-based data update strategy is to improve communication utilization. However, the malicious attackers always launch DoS attacks on the S-C channel covertly to destroy information interaction. This will inevitably lead to the accumulation of actual error between the historical update state and the current operation state such that the event-triggered condition is violated for a long time because the state error cannot be reset to zero. These facts motivates us to design a resilience margin for the event-triggered condition (3), which aims to be more robust against DoS attacks. From this, for any aperiodic interval $[\mathcal{T}_n, \mathcal{T}_{n+1})$, let $\mathcal{H}_n = \{\mathcal{T}_n^{\text{on}}\} \cup [\mathcal{T}_n^{\text{on}}, \mathcal{T}_{n+1})$ be the nth DoS active interval shown in Figure 2, where $\{\mathcal{T}_n^{\text{on}}\}_{n\in\mathbb{N}_0}$ represents an injected DoS sequence. Then, for any $t \in [t_a, t_b]$, we define

$$\mathcal{D}_1(t_a, t_b) = \bigcup_{n\in\mathbb{N}_0} \mathcal{H}_n \bigcap [t_a, t_b] \tag{5}$$

and

$$\mathcal{D}_2(t_a, t_b) = [t_a, t_b] \backslash \mathcal{D}_1(t_a, t_b) \tag{6}$$

as the union and relative complement of DoS subintervals over interval $[t_a, t_b]$, respectively. Clearly, once the intermittent DoS attacks are successfully launched over a shared communication network, certain packets determined by the event-triggered rule (3) will be lost during the transmission. This implies that these criteria for stability analysis and controller synthesis presented in [24,25,27] may no longer be valid. Moreover, these packets that

cannot be updated successfully are also considered redundant. In this case, we need to develop an improved event-triggered rule with a resilience margin according to (3). Firstly, the actual state error caused by DoS attacks can be defined as

$$e_a(t) = x(t) - x(t_k),\ t \in \left[t_n^{\ell}, t_n^{\ell+1}\right) \tag{7}$$

where $\{t_n^{\ell}\}_{\ell\in\mathbb{N}_0} \subseteq \{t_k\}_{k\in\mathbb{N}_0}$ denotes a successful transmission sequence during the interval $[\mathcal{T}_n, \mathcal{T}_{n+1})$. Note that $e_a(t) = e_s(t)$ holds if DoS attacks do not exist; otherwise, DoS attacks cause an additional state error that can degrade security performance, i.e., $e_a(t) > e_s(t)$ holds. Then, a novel event-triggered rule with a resilience margin can be designed as

$$\begin{aligned}\mathfrak{T}_* = \max\Big\{t_k + \Delta, \inf\Big\{t \in \mathbb{R}_{>t_k} \wedge t_n^{\ell} | e_a^T(t)\Theta_a e_a(t) \\ -\sigma x^T(t_k)\Theta_b x(t_k) - (1-\alpha(t))\mathcal{J}_d > 0\Big\}\Big\},\end{aligned} \tag{8}$$

where $\mathfrak{T}_*$ represents the latest update instant when DoS attacks are no longer injected, $\Delta \in \mathbb{R}_{>0}$ denotes an unknown constant to be calculated, $\mathcal{J}_d \leq \mathcal{J}_{\max}$ is the performance compensation for condition (3), and $\mathcal{J}_{\max}$ is the maximum resilience margin. Furthermore, $\alpha(t) \in \{0, 1\}$ is a Dirac measure used to describe DoS on/off properties, and its mathematical expectation can be characterized as

$$\begin{cases}\text{Prob}\{\alpha(t) = 1\} = \mathbb{E}\{\alpha(t)\} = \alpha \\ \text{Prob}\{\alpha(t) = 0\} = 1 - \alpha\end{cases} \tag{9}$$

where $\alpha \in [0, 1]$ is a positive scalar. In this way, we can design a novel dual-mode security controller under the resilient event-triggered rule (8) as follows:

$$u(t) = \alpha(t)K_{r(t)}^a x(t_k) + (1-\alpha(t))\xi_{r(t)}K_{r(t)}^b x(t_k) \tag{10}$$

where $\xi_{r(t)} \in \mathbb{R}_{>0}$ denotes a given regulated parameters, $K_{r(t)}^a$ and $K_{r(t)}^b$ represent the unknown control gains without or with DoS attacks, respectively. Let $\tau(t) \triangleq t - t_n^{\ell}$ denote the time delay, then the control protocol (10) can be further rewritten as

$$\begin{aligned}u(t) = \alpha(t)K_{r(t)}^a(x(t-\tau(t)) - e_a(t)) + (1-\alpha(t)) \\ \times \xi_{r(t)}K_{r(t)}^b(x(t-\tau(t)) - e_a(t)),\ t \in \left[t_n^{\ell}, t_n^{\ell+1}\right)\end{aligned} \tag{11}$$

where $\tau_{\min}$ and $\tau_{\max}$ denote the minimum and maximum time delays, respectively.

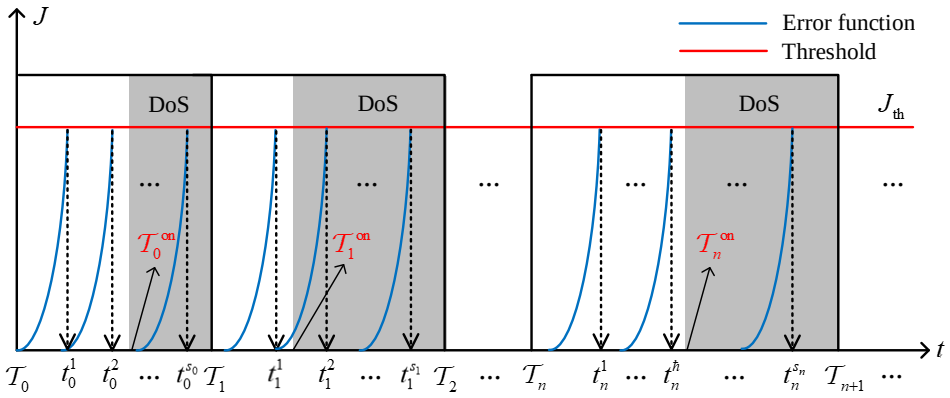

Figure 2. Evolution of update data in the presence of DoS attacks.

In view of the designed resilient event-triggered rule (8) and dual-mode security control protocol (11), the resulting closed-loop systems can be described as

$$\begin{cases} \dot{x}(t) = A_{r(t)}x(t) + \left[\bar{B}^u_{r(t)} + (\alpha(t)-\alpha)\tilde{B}^u_{r(t)}\right]\bar{K}_{r(t)} \\ \qquad \times (x(t-\tau(t)) - e_a(t)) + B^{\omega}_{r(t)}\omega(t) \\ z(t) = C_{r(t)}x(t) + \left[\bar{D}^u_{r(t)} + (\alpha(t)-\alpha)\tilde{D}^u_{r(t)}\right]\bar{K}_{r(t)} \\ \qquad \times (x(t-\tau(t)) - e_a(t)) \end{cases} \tag{12}$$

where $\bar{\alpha} = 1-\alpha$, $\bar{K}_{r(t)} = \mathrm{col}\{K^a_{r(t)}, K^b_{r(t)}\}$, and

$$\bar{B}^u_{r(t)} = \begin{bmatrix} \alpha & \bar{\alpha}\xi_{r(t)} \end{bmatrix} \otimes B^u_{r(t)}, \tilde{B}^u_{r(t)} = \begin{bmatrix} 1 & -\xi_{r(t)} \end{bmatrix} \otimes B^u_{r(t)},$$
$$\bar{D}^u_{r(t)} = \begin{bmatrix} \alpha & \bar{\alpha}\xi_{r(t)} \end{bmatrix} \otimes D^u_{r(t)}, \tilde{D}^u_{r(t)} = \begin{bmatrix} 1 & -\xi_{r(t)} \end{bmatrix} \otimes D^u_{r(t)}.$$

In general, malicious attackers can launch three different types of DoS attacks on the CPS communication network, including periodic DoS attacks, stochastic DoS attacks, and time-constrained DoS attacks as shown in Figure 3. From the perspective of attack concealment, we consider time-constrained DoS attacks, whose properties can be characterized by frequency and duration.

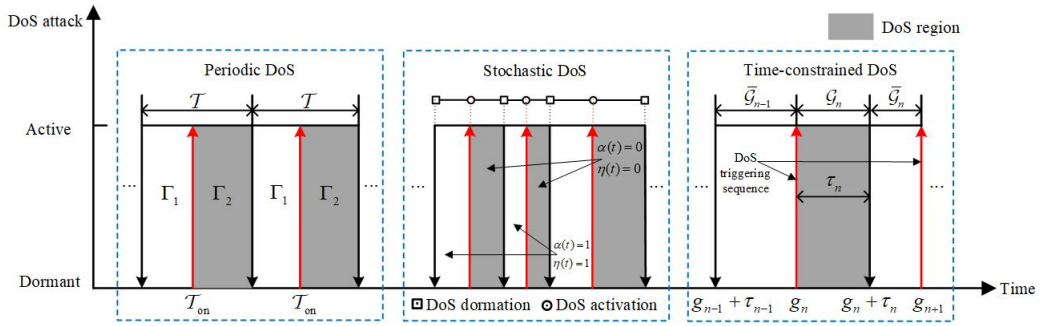

Figure 3. Typical DoS attack models.

Assumption 1 (DoS Frequency [12]). *There exist scalars $\eta \in \mathbb{R}_{\geq 0}$ and $\tau_D \in \mathbb{R}_{\geq \Delta}$ such that*

$$n(t_s, t_f) \leq \eta + \frac{t_f - t_s}{\tau_D}$$

for any $0 \leq t_s < t_f$.

Assumption 2 (DoS Duration [12]). *There exist scalars $\xi \in \mathbb{R}_{\geq 0}$ and $T \in \mathbb{R}_{\geq 1}$ such that*

$$|\mathcal{H}(t_s, t_f)| \leq \xi + \frac{t_f - t_s}{T}$$

for any $0 \leq t_s < t_f$.

2.3. Control Objective

For MJCPSs under DoS attacks, the control objective of this article is to develop the advanced resilient event-triggered rule and dual-mode security control protocol, which aims to ensure the safe operation of physical system in an unreliable network environment. Some useful definitions are given as follows.

Definition 1 ([38]). *For any initial condition* $(x(0), r(0))$*, MJCPSs (1) can be said to be stochastically stable if they have a positive parameter* $\mathcal{M}(x(0), r(0))$ *such that*

$$\mathbb{E}\left\{\int_0^\infty x^T(t)x(t)\mathrm{d}t \mid (x(0), r(0))\right\} \leq \mathcal{M}(x(0), r(0)).$$

Definition 2 ([38]). *Given a positive parameter* $\gamma \in \mathbb{R}_{>0}$*, MJCPSs (1) can be considered stochastically stable and to have an* H_∞ *disturbance attenuation level* γ *if this condition is met:*

$$\mathbb{E}\left\{\int_0^\infty z^T(t)z(t)\mathrm{d}t\right\} \leq \gamma^2 \int_0^\infty \omega^T(t)\omega(t)\mathrm{d}t.$$

Definition 3 ([13]). *The transmission sequence* $\{t_k\}_{k\in\mathbb{N}_0}$ *is said to have a finite update rate if there are two positive scalars* $\Delta_{\min}$ *and* $\Delta_{\max} \in \mathbb{R}_{>0}$ *such that*

$$\Delta_{\min} \leq t_{k+1} - t_k = \Delta_k \leq \Delta_{\max},$$

where $\Delta_{\min}$ *and* $\Delta_{\max}$ *are the minimum and maximum update rates, respectively.*

Remark 1. *Generally, DoS behaviors launched by malicious attackers have a certain concealment, which makes it difficult for defenders to predict attack intentions. Under such an unreliable communication network, the packets to be updated determined by ETM may be lost during the transmission, thereby reducing the security performance of the physical system. To defend against DoS attacks, several popular resilient ETC strategies have been proposed, which can adjust the triggering parameters online or in advance according to changes in the system state, see [34,35,39–42] and the references therein. However, the invisibility of DoS attacks makes it difficult to adjust triggering parameters in real time, which leads to certain limitations of such methods. In contrast, setting a certain resilience margin for ETM to cope with the transmission failures caused by DoS attacks can break through the barriers of traditional control schemes. In addition, the triggering parameters do not need to be adjusted depending on whether DoS attacks occur. Hence, the method of designing a reasonable resilience margin for ETM in a unified framework may facilitate system analysis under DoS attacks.*

Remark 2. *The control behavior in response to DoS attacks can be divided into two cases: one is to force the control signal to zero as mentioned in [12,13], and the other is to maintain the historical control input by using a zero-order holder (ZOH), see [34,38] and the references therein. Obviously, the former is an extremely conservative way to defend against DoS attacks because the controlled system may be in an open-loop unstable status for a long time. Conversely, the latter allows the physical system to obtain relatively satisfactory security performance in a degraded manner. That is, it can be concluded that the second way is more suitable as the core idea of the intrusion tolerance control scheme. On this basis, we can design a DoS-based dual-mode security controller by introducing a Dirac measure* $\alpha(t)$ *[43], which is independent of the system mode* $r(t)$*. The composite control scheme that includes two different control protocols is similar to hybrid control, but both protocols cannot take effect simultaneously. It should be noted that the event-triggered rules corresponding to the above control protocols are selected based on whether DoS attacks occur.*

3. Stability Analysis under Resilient Event-Triggered Rule and DoS Attacks

3.1. Stability Criterion

Firstly, the primary goal of this subsection is to find the stability criteria for MJCPSs (1) under resilient event-triggered rule (8) and DoS attack. Then, we perform a comprehensive feasibility analysis on condition (8) to demonstrate the theoretical validity.

Theorem 1. *Given positive scalars* σ*,* α*,* τ_p*,* τ_q*, and* γ*,* $\xi_i \in \mathbb{R}_{>0}$*, and the dual-mode security controller gains* K_i^a *and* K_i^b*. Under the proposed resilient event-triggered rule (8), MJCPSs (1) are stochastically stable in the presence of intermittent DoS attacks and have an* H_∞ *disturbance*

attenuation level γ *if there exist the positive definite matrices* $P_i > 0$, $Q_i^a > 0$, $Q_i^b > 0$, $S_a > 0$, $S_b > 0$, $R_a > 0$, $R_b > 0$, $\Theta_a > 0$, $\Theta_b > 0$, *and the real matrix* $\tilde{R}_b$ *such that the following conditions are satisfied:*

$$\Omega = \begin{bmatrix} \Omega_c & \Omega_1 & \Omega_2 \\ * & \Omega_3 & 0 \\ * & * & \Omega_4 \end{bmatrix}, \ \mathcal{R} = \begin{bmatrix} R_b & \tilde{R}_b \\ * & R_b \end{bmatrix} > 0, \tag{13}$$

$$\sum_{j=1}^{S} \pi_{ij} Q_j^a < S_a, \ \sum_{j=1}^{S} \pi_{ij} Q_j^b < S_b, \tag{14}$$

where $\mathrm{diag}\{\Omega_3, \Omega_4\} = -\mathrm{diag}\{\bar{\tau}R_a, \tilde{\tau}R_b, \hat{\alpha}\bar{\tau}R_a, \hat{\alpha}\tilde{\tau}R_b, I, \hat{\alpha}I\}$,

$$\Omega_c = \begin{bmatrix} \varphi_{11} & \bar{\tau}R_a & \varphi_{13} & 0 & \varphi_{15} & \varphi_{16} \\ * & \varphi_{22} & \varphi_{23} & \tilde{\tau}\tilde{R}_b & 0 & 0 \\ * & * & \tilde{\varphi}_{33} & \varphi_{34} & -\sigma\Theta_b & 0 \\ * & * & * & \varphi_{44} & 0 & 0 \\ * & * & * & * & \sigma\Theta_b - \Theta_a & 0 \\ * & * & * & * & * & -\gamma^2 I \end{bmatrix},$$

$$\Omega_1 = \begin{bmatrix} A_i^T R_a & A_i^T R_b & 0 \\ 0 & 0 & 0 \\ \bar{K}_i^T \bar{B}_i^{uT} R_a & \bar{K}_i^T \bar{B}_i^{uT} R_b & \bar{K}_i^T \tilde{B}_i^{uT} R_a \\ 0 & 0 & 0 \\ -\bar{K}_i^T \bar{B}_i^{uT} R_a & -\bar{K}_i^T \bar{B}_i^{uT} R_b & -\bar{K}_i^T \tilde{B}_i^{uT} R_a \\ B_i^{\omega T} R_a & B_i^{\omega T} R_b & 0 \end{bmatrix},$$

$$\Omega_2 = \begin{bmatrix} 0 & C_i^T & 0 \\ 0 & 0 & 0 \\ \bar{K}_i^T \tilde{B}_i^{uT} R_b & \bar{K}_i^T \bar{D}_i^{uT} & \bar{K}_i^T \tilde{D}_i^{uT} \\ 0 & 0 & 0 \\ -\bar{K}_i^T \tilde{B}_i^{uT} R_b & -\bar{K}_i^T \bar{D}_i^{uT} & -\bar{K}_i^T \tilde{D}_i^{uT} \\ 0 & 0 & 0 \end{bmatrix},$$

with

$$\begin{aligned} \varphi_{11} &= Q_i^a + \tau_p S_a + \hat{\tau} S_b + A_i^T P_i + P_i A_i + \sum_{j=1}^{S} \pi_{ij} P_j \\ &\quad - \bar{\tau} R_a, \ \tilde{\varphi}_{33} = -2\varphi_{23} + \sigma\Theta_b, \ \tilde{\alpha} = \hat{\alpha}^{-1} = \alpha\bar{\alpha}, \\ \varphi_{13} &= -\varphi_{15} = P_i \bar{B}_i^u \bar{K}_i, \ \varphi_{16} = P_i B_i^{\omega}, \ \hat{\tau} = \tau_q - \tau_p, \\ \varphi_{22} &= Q_i^b - Q_i^a - \bar{\tau} R_a - \tilde{\tau} R_b, \ \tilde{\tau} = \hat{\tau}^{-1}, \ \bar{\tau} = \tau_p^{-1}, \\ \varphi_{23} &= \varphi_{34} = \tilde{\tau} R_b - \tilde{\tau} \tilde{R}_b, \ \varphi_{44} = -Q_i^b - \tilde{\tau} R_b. \end{aligned}$$

Proof. Firstly, consider a stochastic Lyapunov–Krasovskii functional as follows:

$$\begin{aligned} V(x(t), r(t)) &= V_1(x(t), r(t)) + V_2(x(t), r(t)) \\ &\quad + V_3(x(t), r(t)) + V_4(x(t), r(t)), \end{aligned} \tag{15}$$

where

$$\begin{aligned}
V_1(x(t), r(t)) &= x^T(t) P_{r(t)} x(t), \\
V_2(x(t), r(t)) &= \int_{t-\tau_p}^{t} x^T(s) Q^a_{r(t)} x(s) \mathrm{ds} \\
&\quad + \int_{t-\tau_q}^{t-\tau_p} x^T(s) Q^b_{r(t)} x(s) \mathrm{ds}, \\
V_3(x(t), r(t)) &= \int_{-\tau_p}^{0} \int_{t+\theta}^{t} x^T(s) S_a x(s) \mathrm{dsd}\grave{} \\
&\quad + \int_{-\tau_q}^{-\tau_p} \int_{t+\theta}^{t} x^T(s) S_b x(s) \mathrm{dsd}\grave{}, \\
V_4(x(t), r(t)) &= \int_{-\tau_p}^{0} \int_{t+\theta}^{t} \dot{x}^T(s) R_a \dot{x}(s) \mathrm{dsd}\grave{} \\
&\quad + \int_{-\tau_q}^{-\tau_p} \int_{t+\theta}^{t} \dot{x}^T(s) R_b \dot{x}(s) \mathrm{dsd}\grave{}.
\end{aligned}$$

For $r(t) = i \in \mathbb{S}$, let $\mathfrak{L}$ be the weak infinitesimal generator, which is computed along the state trajectory of MJCPSs (1) as

$$\begin{aligned}
&\mathfrak{L}V_1(x(t), r(t)) \\
&= 2x^T(t) P_i \big[A_i x(t) + B^{\omega}_i \omega(t) - \bar{B}^u_i \bar{K}_i e_a(t) \\
&\quad + \bar{B}^u_i \bar{K}_i x(t - \tau(t)) \big] + x^T(t) \sum_{j=1}^{S} \pi_{ij} P_j x(t),
\end{aligned} \tag{16}$$

$$\begin{aligned}
&\mathfrak{L}V_2(x(t), r(t)) \\
&= x^T(t) Q^a_i x(t) - x^T(t - \tau_q) Q^b_i x(t - \tau_q) \\
&\quad + x^T(t - \tau_p)(Q^b_i - Q^a_i) x(t - \tau_p) \\
&\quad + \int_{t-\tau_q}^{t-\tau_p} x^T(s) \sum_{j=1}^{S} \pi_{ij} Q^b_j x(s) \mathrm{ds} \\
&\quad + \int_{t-\tau_p}^{t} x^T(s) \sum_{j=1}^{S} \pi_{ij} Q^a_j x(s) \mathrm{ds},
\end{aligned} \tag{17}$$

$$\begin{aligned}
&\mathfrak{L}V_3(x(t), r(t)) \\
&= \tau_p x^T(t) S_a x(t) - \int_{t-\tau_p}^{t} x^T(s) S_a x(s) \mathrm{ds} \\
&\quad + \hat{\tau} x^T(t) S_b x(t) - \int_{t-\tau_q}^{t-\tau_p} x^T(s) S_b x(s) \mathrm{ds},
\end{aligned} \tag{18}$$

$$\begin{aligned}
&\mathfrak{L}V_4(x(t), r(t)) \\
&= \tau_p \mathbb{E}\{\dot{x}^T(t) R_a \dot{x}(t)\} - \int_{t-\tau_p}^{t} \dot{x}^T(s) R_a \dot{x}(s) \mathrm{ds} \\
&\quad + \hat{\tau} \mathbb{E}\{\dot{x}^T(t) R_b \dot{x}(t)\} - \int_{t-\tau_q}^{t-\tau_p} \dot{x}^T(s) R_b \dot{x}(s) \mathrm{ds},
\end{aligned} \tag{19}$$

where $\hat{\tau} \in \mathbb{R}_{>0}$ is defined in Theorem 1. For clarity, let $\eta(t) := \mathrm{col}\{x(t), x(t - \tau_p), x(t - \tau(t)), x(t - \tau_q), e_a(t), \omega(t)\}$ represent the augmented vector. Then, in view of the mathematical nature of $\alpha(t)$, one can obtain that

$$\begin{aligned}
&\mathbb{E}\{\dot{x}^T(t) R_\phi \dot{x}(t)\} \\
&= \eta^T(t) \big[\zeta_1^T R_\phi \zeta_1 + \tilde{\alpha} \zeta_2^T R_\phi \zeta_2 \big] \eta(t), \ \phi \in \{a, b\}
\end{aligned} \tag{20}$$

where $\tilde{\alpha} \in \mathbb{R}_{>0}$, $\zeta_1 = \left[A_i, 0, \bar{B}_i^u \bar{K}_i, 0, -\bar{B}_i^u \bar{K}_i, B_i^\omega\right]$, and $\zeta_2 = \left[0, 0, \tilde{B}_i^u \bar{K}_i, 0, -\tilde{B}_i^u \bar{K}_i, 0\right]$. By virtue of the Jessen's inequality, the integral terms in (19) are calculated as

$$\begin{aligned} &-\int_{t-\tau_p}^{t} \dot{x}^T(s) R_a \dot{x}(s) \mathrm{d}s \\ &\leq -\bar{\tau}\left[x(t) - x(t-\tau_p)\right]^T R_a \left[x(t) - x(t-\tau_p)\right], \end{aligned} \tag{21}$$

$$\begin{aligned} &-\int_{t-\tau_q}^{t-\tau_p} \dot{x}^T(s) R_b \dot{x}(s) \mathrm{d}s \\ &\leq -\tilde{\tau}\left[x(t-\tau_p) - x(t-\tau(t))\right]^T R_b \left[x(t-\tau_p)\right. \\ &\quad \left. - x(t-\tau(t))\right] - \tilde{\tau}\left[x(t-\tau(t)) - x(t-\tau_q)\right]^T \\ &\quad \times R_b \left[x(t-\tau(t)) - x(t-\tau_q)\right] - 2\tilde{\tau}\left[x(t-\tau_p)\right. \\ &\quad \left. - x(t-\tau(t))\right]^T \tilde{R}_b \left[x(t-\tau(t)) - x(t-\tau_q)\right], \end{aligned} \tag{22}$$

where $\bar{\tau}$ and $\tilde{\tau} \in \mathbb{R}_{>0}$ are defined in Theorem 1, respectively.

Combining condition (14), it follows from (16)–(22) that

$$\begin{aligned} \mathfrak{L}V(x(t), r(t)) \leq \eta^T(t) \big[&\Omega_a + \zeta_1^T (\tau_p R_a + \hat{\tau} R_b) \zeta_1 \\ &+ \zeta_2^T (\tilde{\alpha} \tau_p R_a + \tilde{\alpha} \hat{\tau} R_b) \zeta_2 \big] \eta(t), \end{aligned} \tag{23}$$

where

$$\Omega_a = \begin{bmatrix} \varphi_{11} & \bar{\tau} R_a & \varphi_{13} & 0 & \varphi_{15} & \varphi_{16} \\ * & \varphi_{22} & \varphi_{23} & \tilde{\tau} \tilde{R}_b & 0 & 0 \\ * & * & \varphi_{33} & \varphi_{34} & 0 & 0 \\ * & * & * & \varphi_{44} & 0 & 0 \\ * & * & * & * & 0 & 0 \\ * & * & * & * & * & 0 \end{bmatrix}$$

with $\varphi_{33} = -2\varphi_{23} = 2\tilde{\tau}\tilde{R}_b - 2\tilde{\tau} R_b$ and other parameters, which are given in Theorem 1.

Then, we will show that MJCPSs (1) have an H_∞ disturbance attenuation level γ for any non-zero $\omega(t) \in \mathcal{L}_2[0, +\infty)$. Define $\Lambda(t) := \mathfrak{L}V(x(t), r(t)) + \mathbb{E}\{z^T(t) z(t) - \gamma^2 \omega^T(t) \omega(t)\}$. Based on Definition 2, it can be derived that

$$\begin{aligned} \Lambda(t) \leq \eta^T(t) \big[&\Omega_b + \zeta_1^T (\tau_p R_a + \hat{\tau} R_b) \zeta_1 + \zeta_3^T \zeta_3 \\ &+ \zeta_2^T (\tilde{\alpha} \tau_p R_a + \tilde{\alpha} \hat{\tau} R_b) \zeta_2 + \tilde{\alpha} \zeta_4^T \zeta_4 \big] \eta(t), \end{aligned} \tag{24}$$

where $\zeta_3 = \left[C_i, 0, \bar{D}_i^u \bar{K}_i, 0, -\bar{D}_i^u \bar{K}_i, 0\right]$, $\zeta_4 = \left[0, 0, \tilde{D}_i^u \bar{K}_i, 0, -\tilde{D}_i^u \bar{K}_i, 0\right]$, and

$$\Omega_b = \begin{bmatrix} \varphi_{11} & \bar{\tau} R_a & \varphi_{13} & 0 & \varphi_{15} & \varphi_{16} \\ * & \varphi_{22} & \varphi_{23} & \tilde{\tau} \tilde{R}_b & 0 & 0 \\ * & * & \varphi_{33} & \varphi_{34} & 0 & 0 \\ * & * & * & \varphi_{44} & 0 & 0 \\ * & * & * & * & 0 & 0 \\ * & * & * & * & * & -\gamma^2 I \end{bmatrix},$$

which implies that $\zeta_1^T (\tau_p R_a + \hat{\tau} R_b) \zeta_1 + \zeta_2^T (\tilde{\alpha} \tau_p R_a + \tilde{\alpha} \hat{\tau} R_b) \zeta_2 + \zeta_3^T \zeta_3 + \tilde{\alpha} \zeta_4^T \zeta_4 + \Omega_b < 0$ is established. In this way, we obtain that $\Lambda(t) \leq -\|\eta(t)\|^2 < -\lambda \|x(t)\|^2$, where $\lambda \in \mathbb{R}_{>0}$. From this, we can conclude that MJCPSs (1) are stochastically stable and have an H_∞ disturbance attenuation level γ.

Finally, based on the developed resilient event-triggered rule (8), it follows from condition (24) that

$$\begin{aligned}\Lambda(t) &\leq \tilde{\Lambda}(t) + \alpha(t)\mathcal{J}_d \\ &= \eta^T(t)\big[\Omega_c + \zeta_1^T(\tau_p R_a + \hat{\tau} R_b)\zeta_1 + \zeta_2^T(\tilde{\alpha}\tau_p R_a \\ &+ \tilde{\alpha}\hat{\tau} R_b)\zeta_2 + \zeta_3^T\zeta_3 + \tilde{\alpha}\zeta_4^T\zeta_4\big]\eta(t) + (1-\alpha(t))\mathcal{J}_d,\end{aligned} \tag{25}$$

where $\tilde{\Lambda}(t) = \Lambda(t) + \sigma x^T(t_k)\Theta_b x(t_k) - e_a^T(t)\Theta_a e_a(t)$ and Ω_c is given in condition (13). By Schur's complement lemma, it is concluded that the objective term $\tilde{\Lambda}(t)$ in (25) is equivalent to Ω in (13). Thus, it is derived that $\tilde{\Lambda}(t) \leq -\tilde{\lambda}\|x(t)\|^2$, where $\tilde{\lambda} \in \mathbb{R}_{>0}$. This implies that $\mathfrak{L}V(x(t), r(t)) \leq -\hat{\lambda}V(x(t), r(t))$ is established, where $\hat{\lambda} = \tilde{\lambda}/\lambda_{\max}(P_i)$ represents the decay rate and $\lambda_{\max}(P_i)$ represents the maximum eigenvalue of P_i. From this, we can obtain that

$$\mathfrak{L}V(x(t), r(t)) \leq -\hat{\lambda}V(x(t), r(t)) + (1-\alpha(t_n^\ell))\mathcal{J}_d, \tag{26}$$

where $t \in [t_n^\ell, t_n^{\ell+1})$. Then, it follows from condition (26) that

$$\mathbb{E}[V(x(t), r(t))] \leq \mathbb{E}[V(x(0), r(0))] + \frac{(1-\alpha(t_n^\ell))\mathcal{J}_d}{\hat{\lambda}}, \tag{27}$$

which implies that

$$\begin{aligned}&\mathbb{E}\left\{\int_0^\infty x^T(t)x(t)\mathrm{dt} \mid (x(0), r(0))\right\} \\ &\leq \hbar\mathbb{E}[V(x(0), r(0))] + \frac{(1-\alpha(t_n^\ell))\hbar\mathcal{J}_d}{\hat{\lambda}} \\ &= \mathcal{M}(x(0), r(0)),\end{aligned} \tag{28}$$

where $\hbar = \lambda_{\min}^{-1}(P_i)$ and $\lambda_{\min}(P_i)$ is the minimum eigenvalue of P_i. In this case, it can be concluded that $\|x(t)\|^2$ is bounded by $\mathcal{M}(x(0), r(0))$. Meanwhile, the maximum performance loss induced by DoS attacks is calculated as $\mathcal{J}_{\max} = \hbar\lambda_d\mathcal{J}_d$, where $\lambda_d = 1/\hat{\lambda}$. This completes the proof. □

3.2. Feasibility Criterion

In this subsection, the main objective is to find the minimum update rate, which aims to avoid Zeno behavior with an unlimited number of transmission instants in a finite time period. The maximum downtime of (8) under DoS attacks is calculated.

Theorem 2. *For the closed-loop MJCPSs (12) with resilient event-triggered rule (8) and dual-mode security controller (10), Zeno behavior is strictly excluded if the inter-execution interval Δ_k, $k \in \mathbb{N}_0$ is greater than or equal to*

$$\Delta_{\min} = \min\left\{\Delta_{\min}^1, \Delta_{\min}^2\right\}, \tag{29}$$

where

$$\Delta_{\min}^1 = \frac{1}{\vartheta_1}\ln\left[\frac{\mu_1}{\mu_2} + 1\right],\ \Delta_{\min}^2 = \frac{1}{\vartheta_1}\ln\left[\frac{\mu_3}{\mu_4} + 1\right],$$

with $\mu_1 = \vartheta_1 \min\{\varsigma_1, \varsigma_2\}$, $\mu_2 = \max\{\vartheta_2(\varsigma_1+1), (\vartheta_2\varsigma_2 + \vartheta_3)\}$, $\mu_3 = \vartheta_1 \min\{\varsigma_3, \varsigma_4, \varsigma_5, \varsigma_6\}$, $\mu_4 = \max\{\theta_1(\varsigma_3+1), (\theta_1\varsigma_4 + \vartheta_3), (\theta_1\varsigma_5 + \vartheta_4), \theta_1\varsigma_6\}$, $\varsigma_1 = (\sqrt{2\sigma}\varrho_2)/(2\varrho_1)$, $\varsigma_2 = \varpi/(\sqrt{2}\varrho_1)$, $\varsigma_3 = (\sqrt{\sigma}\varrho_2)/(2\varrho_1)$, $\varsigma_4 = \varpi/(2\varrho_1)$, $\varsigma_5 = \hat{\omega}/(2\varrho_1)$, $\varsigma_6 = \tilde{\omega}/(2\varrho_1)$, $\hat{\Theta}_a^2 = \Theta_a$, $\hat{\Theta}_b^2 = \Theta_b$, $\varrho_1 = \lambda_{\max}(\hat{\Theta}_a)$, $\varrho_2 = \lambda_{\min}(\hat{\Theta}_b)$, $\hat{A}_i = A_i + B_i^u K_i^a$, $\hat{B}_i^u = \xi_i \times B_i^u K_i^b$, $\vartheta_1 = \max_{i\in\mathbb{S}}\{\|A_i\|\}$, $\vartheta_2 = \max_{i\in\mathbb{S}}\{\|\hat{A}_i\|\}$, $\vartheta_3 = \max_{i\in\mathbb{S}}\{\|B_i^\omega\|\}$, $\vartheta_4 = \max_{i\in\mathbb{S}}\{\|\hat{B}_i^u\|\}$, *and* ξ_i, σ, ϖ, $\hat{\omega}$, *and* $\tilde{\omega} \in \mathbb{R}_{>0}$ *represent the given positive parameters. Moreover, the maximum downtime caused by DoS attacks can be calculated as* $\Delta_{\max} = \vartheta_1^{-1}\ln[(\mu_5\Gamma)/\mu_6 + 1]$ *with* $\mu_5 = \max\{\tilde{\varsigma}_3, \tilde{\varsigma}_4, \tilde{\varsigma}_5, \tilde{\varsigma}_6\}$, $\mu_6 = \min\{\vartheta_1\hat{\varsigma}_3, (\vartheta_1\tilde{\varsigma}_4 + \vartheta_3), (\vartheta_1\tilde{\varsigma}_5 + \vartheta_4), \vartheta_1\tilde{\varsigma}_6\}$, $\tilde{\varsigma}_3 = (\sqrt{\sigma}\varrho_4)/\varrho_3$, $\tilde{\varsigma}_4 = \varpi/\varrho_3$, $\tilde{\varsigma}_5 = \hat{\omega}/\varrho_3$, $\tilde{\varsigma}_6 = \hat{\omega}/\varrho_3$, $\hat{\varsigma}_3 = 1 + \tilde{\varsigma}_3$, $\Gamma = \vartheta_1[1 + \sum_{n_f=1}^{N_{\text{dos}}+1} 2^{n_f-1}\hat{\varsigma}_3]$, $N_{\text{dos}} = \Delta_{\min}^{-1}(\mathcal{T}_{n+1} - \mathcal{T}_n^{\text{on}})$, $\varrho_3 = \lambda_{\min}(\hat{\Theta}_a)$, *and* $\varrho_4 = \lambda_{\max}(\hat{\Theta}_b)$.

Proof. See the Appendix A. □

Remark 3. *In view of the proposed resilient event-triggered rule (8), the purpose is to characterize two possible data update policies generated by intermittent DoS attacks through random variable $\alpha(t)$, where $\alpha(t) = 1$ and $\alpha(t) = 0$ represent dormant and active DoS attacks, respectively. Here, the existence of $\mathcal{J}_d$ makes the triggering threshold when $\alpha(t) = 0$ greater than that when $\alpha(t) = 1$. This implies that a higher triggering threshold may determine fewer packets to be transmitted. Note that it is quite possible to transmit a large number of packets in a short period of time because of an inappropriate event-triggered rule. Therefore, regardless of whether the triggering threshold is low or high, Zeno behavior needs to be strictly avoided. Moreover, the exogenous disturbance can direct the trajectory of $\|e_a(t)\|$ in the resilient event-triggered rule (8). In order to prevent the influence of the disturbance signal on the estimation of $\|e_a(t)\|$, it is necessary to develop an improved triggering inequality when discussing the feasibility of resilient event-triggered rule (8).*

Remark 4. *Note that the unreasonable event-triggered rules may also lead to singular triggering, which is another abnormal behavior that cannot transmit for a long time after a successful transmission attempt. By solving the maximum inter-execution interval between two consecutive transmissions, it is concluded that singular triggering can be avoided to guarantee the validity of the developed event-triggered rules. Due to intermittent DoS attacks, a large number of packets cannot be transmitted within the active DoS subintervals. Thus, it is necessary to characterize the maximum downtime between two adjacent successful updates to estimate the impact of intermittent DoS attacks on control performance. However, few results discuss this critical issue, and it is difficult to obtain an explicit representation for the maximum downtime caused by DoS attacks. Furthermore, similar to the procedures for avoiding Zeno behavior, we also study the potential impact of disturbance signal on calculating the maximum downtime.*

4. Design of Dual-Mode Security Controller under Resilient Event-Triggered Rule

In this section, inspired by the theoretical results of stability analysis under the resilient event-triggered rule (8), we present a design procedure of the proposed dual-mode security control protocol. The following results illustrate the stated objectives.

Theorem 3. *Given positive scalars σ, α, τ_p, τ_q, γ, $\xi_i \in \mathbb{R}_{>0}$, there is a dual-mode security controller (10) such that MJCPSs (1) are stochastically stable in the presence of intermittent DoS signal and have an H_∞ disturbance attenuation level γ, if there are positive definite matrices $X_i > 0$, $\tilde{Q}_i^a > 0$, $\tilde{Q}_i^b > 0$, $\tilde{S}_i^a > 0$, $\tilde{S}_i^b > 0$, $\tilde{R}_i^a > 0$, $\hat{R}_i^b > 0$, $\bar{\Theta}_a > 0$, $\bar{\Theta}_b > 0$, and real matrices $\bar{R}_i^b$, Y_i^a, and Y_i^b with appropriate dimensions such that the following conditions are satisfied:*

$$\Omega_\star = \begin{bmatrix} \bar{\Omega} & \Xi_i \\ * & \Lambda_i^1 \end{bmatrix} < 0,\ \mathcal{R}_\star = \begin{bmatrix} \hat{R}_i^b & \bar{R}_i^b \\ * & \hat{R}_i^b \end{bmatrix} > 0, \tag{30}$$

$$\begin{bmatrix} \mathcal{Q}_1 & \Xi_i \\ * & \Lambda_i^2 \end{bmatrix} < 0,\ \begin{bmatrix} \mathcal{Q}_2 & \Xi_i \\ * & \Lambda_i^3 \end{bmatrix} < 0, \tag{31}$$

where $\bar{\Omega} = [\tilde{\Omega}_c, \tilde{\Omega}_1, \tilde{\Omega}_2; \tilde{\Omega}_1^T, \tilde{\Omega}_3, 0; \tilde{\Omega}_2^T, 0, \tilde{\Omega}_4]$, $\check{\Omega} = [\tilde{\Omega}_1, \tilde{\Omega}_2]$,

$$\check{\Omega} = \begin{bmatrix} X_i^T A_i^T & X_i^T A_i^T & 0 & 0 & X_i^T C_i^T & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \bar{\varphi}_1 & \bar{\varphi}_1 & \bar{\varphi}_2 & \bar{\varphi}_2 & \bar{\varphi}_3 & \bar{\varphi}_4 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -\bar{\varphi}_1 & -\bar{\varphi}_1 & -\bar{\varphi}_2 & -\bar{\varphi}_2 & -\bar{\varphi}_3 & -\bar{\varphi}_4 \\ B_i^{\omega T} & B_i^{\omega T} & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\tilde{\Omega}_c = \begin{bmatrix} \hat{\varphi}_{11} & \bar{\tau}\tilde{R}_i^a & \hat{\varphi}_{13} & 0 & \hat{\varphi}_{15} & \hat{\varphi}_{16} \\ * & \hat{\varphi}_{22} & \hat{\varphi}_{23} & \tilde{\tau}\bar{R}_i^b & 0 & 0 \\ * & * & \hat{\varphi}_{33} & \hat{\varphi}_{34} & \hat{\varphi}_{35} & 0 \\ * & * & * & \hat{\varphi}_{44} & 0 & 0 \\ * & * & * & * & \hat{\varphi}_{55} & 0 \\ * & * & * & * & * & -\gamma^2 I \end{bmatrix},$$

$$\tilde{\Omega}_3 = -\mathrm{diag}[2\bar{\tau}X_i - \bar{\tau}\tilde{R}_i^a, 2\bar{\tau}X_i - \tilde{\tau}\hat{R}_i^b, 2\hat{\alpha}\bar{\tau}X_i - \hat{\alpha}\bar{\tau}\tilde{R}_i^a],$$

$$\tilde{\Omega}_4 = -\mathrm{diag}[2\hat{\alpha}\bar{\tau}X_i - \hat{\alpha}\tilde{\tau}\hat{R}_i^b, I, \hat{\alpha}I],\ \bar{\Theta}_a\bar{\Theta}_b = \Theta_a^{-1}\Theta_b^{-1},$$

$$\Lambda_i^1 = -\mathrm{diag}[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_S],\ \hat{\varphi}_{16} = B_i^{\omega}X_i,$$

$$\Lambda_i^2 = -\mathrm{diag}[2X_1 - \tilde{Q}_1^a, \ldots, 2X_{i-1} - \tilde{Q}_{i-1}^a, 2X_{i+1} - \tilde{Q}_{i+1}^a, \ldots, 2X_S - \tilde{Q}_S^a],\ \mathcal{Q}_1 = \pi_{ii}\tilde{Q}_i^a - \tilde{S}_i^a,$$

$$\Lambda_i^3 = -\mathrm{diag}[2X_1 - \tilde{Q}_1^b, \ldots, 2X_{i-1} - \tilde{Q}_{i-1}^b, 2X_{i+1} - \tilde{Q}_{i+1}^b, \ldots, 2X_S - \tilde{Q}_S^b],\ \mathcal{Q}_2 = \pi_{ii}\tilde{Q}_i^b - \tilde{S}_i^b,$$

$$\Xi_i = \left[\sqrt{\pi_{i1}}X_i^T, \ldots, \sqrt{\pi_{i(i-1)}}X_i^T, \sqrt{\pi_{i(i+1)}}X_i^T, \ldots, \sqrt{\pi_{iS}}X_i^T\right],\ \hat{\varphi}_{22} = \tilde{Q}_i^b - \tilde{Q}_i^a - \bar{\tau}\tilde{R}_i^a - \tilde{\tau}\hat{R}_i^b,$$

$$\bar{\varphi}_1^T = \alpha B_i^u Y_i^a + \bar{\alpha}\xi_i B_i^u Y_i^b,\ \bar{\varphi}_2^T = B_i^u Y_i^a - \xi_i B_i^u Y_i^b,$$

$$\bar{\varphi}_3^T = \alpha D_i^u Y_i^a + \bar{\alpha}\xi_i D_i^u Y_i^b,\ \bar{\varphi}_4^T = D_i^u Y_i^a - \xi_i D_i^u Y_i^b,$$

$$\hat{\varphi}_{11} = -\bar{\tau}\tilde{R}_i^a + \tilde{Q}_i^a + \tau_p\tilde{S}_i^a + \hat{\tau}\tilde{S}_i^b + \pi_{ii}X_i + X_i^T A_i^T + A_i X_i,\ \hat{\varphi}_{13} = -\hat{\varphi}_{15} = \alpha B_i^u Y_i^a + \bar{\alpha}\xi_i B_i^u Y_i^b,$$

$$\hat{\varphi}_{23} = \hat{\varphi}_{34} = \tilde{\tau}\hat{R}_i^b - \tilde{\tau}\bar{R}_i^b,\ \hat{\varphi}_{55} = 2\hat{\sigma}X_i - \sigma\bar{\Theta}_a + \bar{\Theta}_b,$$

$$\hat{\varphi}_{33} = -2\hat{\varphi}_{23} + \hat{\varphi}_{35} = 2\tilde{\tau}\bar{R}_i^b - 2\tilde{\tau}\hat{R}_i^b - 2\sigma X_i + \sigma\bar{\Theta}_b,$$

$$\hat{\varphi}_{35} = -2\sigma X_i + \sigma\bar{\Theta}_b,\ \hat{\varphi}_{44} = -\tilde{Q}_i^b - \tilde{\tau}\hat{R}_i^b,\ \hat{\sigma} = \sigma - 1,$$

and the remaining parameters are defined in Theorem 1. Then, the gains of the dual-mode security controller can be computed as

$$K_i^a = Y_i^a X_i^{-1},\ K_i^b = Y_i^b X_i^{-1},\ \forall i \in \mathbb{S} \tag{32}$$

Proof. Firstly, define the following new variables as $X_i = P_i^{-1}$, $\tilde{Q}_i^a = X_i^T Q_i^a X_i$, $\tilde{Q}_i^b = X_i^T Q_i^b X_i$, $\tilde{S}_i^a = X_i^T S_a X_i$, $\tilde{S}_i^b = X_i^T S_b X_i$, $\tilde{R}_i^a = X_i^T R_a X_i$, $\hat{R}_i^b = X_i^T R_b X_i$, $\bar{R}_i^b = X_i^T \tilde{R}_b X_i$, $\tilde{\Theta}_i^a = X_i^T \Theta_a X_i$, and $\tilde{\Theta}_i^b = X_i^T \Theta_b X_i$. Then, based on the proof of Theorem 1, it can be seen that only the parameters Ω_c, Ω_1, and Ω_2 in (13) can affect the solution of security control gains K_i^a and K_i^b. To characterize an explicit form of control gains, the left-hand inequality in (13) can be transformed into

$$\Omega = \begin{bmatrix} \Omega_c & \hat{\Omega}_1 & \hat{\Omega}_2 \\ * & \hat{\Omega}_3 & 0 \\ * & * & \hat{\Omega}_4 \end{bmatrix}, \tag{33}$$

where

$$\hat{\Omega}_1 = \begin{bmatrix} A_i^T & A_i^T & 0 \\ 0 & 0 & 0 \\ \bar{K}_i^T \bar{B}_i^{uT} & \bar{K}_i^T \bar{B}_i^{uT} & \bar{K}_i^T \bar{B}_i^{uT} \\ 0 & 0 & 0 \\ -\bar{K}_i^T \bar{B}_i^{uT} & -\bar{K}_i^T \bar{B}_i^{uT} & -\bar{K}_i^T \tilde{B}_i^{uT} \\ B_i^{\omega T} & B_i^{\omega T} & 0 \end{bmatrix},$$

$$\hat{\Omega}_2 = \begin{bmatrix} 0 & C_i^T & 0 \\ 0 & 0 & 0 \\ \bar{K}_i^T \tilde{B}_i^{uT} & \bar{K}_i^T \bar{D}_i^{uT} & \bar{K}_i^T \tilde{D}_i^{uT} \\ 0 & 0 & 0 \\ -\bar{K}_i^T \tilde{B}_i^{uT} & -\bar{K}_i^T \bar{D}_i^{uT} & -\bar{K}_i^T \tilde{D}_i^{uT} \\ 0 & 0 & 0 \end{bmatrix},$$

and $\mathrm{diag}\{\hat{\Omega}_3, \hat{\Omega}_4\} = -\mathrm{diag}\{\tau_p R_a, \hat{\tau} R_b, \tilde{\alpha}\tau_p R_a, \tilde{\alpha}\hat{\tau} R_b, I, \tilde{\alpha} I\}^{-1}$.

Then, by post- and pre-multiplying both sides of (33) with $\mathrm{diag}\{\underbrace{X_i, \ldots, X_i}_{5}, \underbrace{I, \ldots, I}_{7}\}$ and its transpose, we obtain

$$\tilde{\Omega} = \begin{bmatrix} \tilde{\Omega}_c & \tilde{\Omega}_1 & \tilde{\Omega}_2 & \Xi_i \\ * & \hat{\Omega}_3 & 0 & 0 \\ * & * & \hat{\Omega}_4 & 0 \\ * & * & * & \Lambda_i^1 \end{bmatrix} < 0, \tag{34}$$

where $\tilde{\Omega}_c$, $\tilde{\Omega}_1$, $\tilde{\Omega}_2$, Ξ_i, and Λ_i^1 are defined in Theorem 3. Next, the nonlinear terms R_a^{-1} and R_b^{-1} in condition (34) are further rewritten as $-R_a^{-1} = -X_i(X_i^T R_a X_i)^{-1} X_i^T \leq -2X_i + \tilde{R}_i^a$ as $-R_b^{-1} = -X_i(X_i^T R_b X_i)^{-1} X_i^T \leq -2X_i + \hat{R}_i^b$, respectively. Substituting the resulting inequalities into (34), it is concluded that the left-hand inequality in (30) is established.

In a similar way, by post-multiplying and pre-multiplying both sides of the right-hand inequality in condition (13) with $\mathrm{diag}\{X_i, X_i\}$ and its transpose, then we obtain the conclusion that the right-hand inequality in (30) is true. In addition, it follows from (14) that

$$X_i^T \sum_{j=1}^{S} \pi_{ij} Q_j^a X_i < \tilde{S}_i^a, \; X_i^T \sum_{j=1}^{S} \pi_{ij} Q_j^b X_i < \tilde{S}_i^b \tag{35}$$

which can be equivalent to

$$\mathcal{Q}_1 + X_i^T \sum_{j \neq i} \pi_{ij} Q_j^a X_i < 0 \tag{36}$$

and

$$\mathcal{Q}_2 + X_i^T \sum_{j \neq i} \pi_{ij} Q_j^b X_i < 0, \tag{37}$$

where $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are given in Theorem 3. According to the Schur complement lemma, it can be deduced that

$$\begin{bmatrix} \mathcal{Q}_1 & \Xi_i \\ * & \bar{\Lambda}_i^2 \end{bmatrix} < 0, \; \begin{bmatrix} \mathcal{Q}_2 & \Xi_i \\ * & \bar{\Lambda}_i^3 \end{bmatrix} < 0, \tag{38}$$

where

$$\bar{\Lambda}_i^2 = -\mathrm{diag}\left[Q_1^a, \ldots, Q_{i-1}^a, Q_{i+1}^a, \ldots, Q_S^a\right]^{-1},$$
$$\bar{\Lambda}_i^3 = -\mathrm{diag}\left[Q_1^b, \ldots, Q_{i-1}^b, Q_{i+1}^b, \ldots, Q_S^b\right]^{-1}.$$

As for the nonlinear terms $-(Q_i^a)^{-1}$ and $-(Q_i^b)^{-1}$, $\forall j \neq i$ in $\bar{\Lambda}_i^2$ and $\bar{\Lambda}_i^3$, it can be further rewritten as

$$-(Q_i^a)^{-1} \leq -2X_i + \tilde{Q}_i^a, \tag{39}$$

implying the same solution for $-(Q_i^b)^{-1}$. Therefore, it can be concluded that (38) can be guaranteed by condition (31). This completes the proof. □

5. Simulation Example

In this section, a simulation example is given to demonstrate the effectiveness of the event-based dual-mode security control strategy under DoS attacks.

As shown in Figure 4, we consider a Pulse-Width Modulation (PWM)-driven boost converter borrowed from [44], which can be captured by

$$\begin{cases} \dot{E}_c(t) = -\dfrac{1}{RC}E_c(t) + (1-s(t))\dfrac{1}{C}I_\ell(t) \\ \dot{I}_\ell(t) = -(1-s(t))\dfrac{1}{L}E_c(t) + s(t)\dfrac{1}{L}E_s(t) \end{cases} \tag{40}$$

where L, C and R denote the inductance, capacitance and load resistance, respectively. $E_c(t)$ and $E_s(t)$ represent the terminal voltage and source voltage of the capacitor, respectively. $I_\ell(t)$ is the current through the inductance. $s(t)$ is a switching signal controlled by a PWM-driven boost converter. Here, as a typical circuit system, the role of using a PWM-driven boost converter is to obtain higher voltage. Let $x(t) = \text{col}\{E_c(t), I_L(t), 1\}$ be the system state, then the differential Equation (40) is further rewritten as $\dot{x}(t) = A_{r(t)}x(t)$, $r(t) \in \{1, 2\}$, where the system parameters are $A_1 = [-1/RC, 1/C, 0; -1/L, 0, 0; 0, 0, 0]$ and $A_2 = [-1/RC, 0, 0; 0, 0, 1/L; 0, 0, 0]$. Selecting $L = 1H$, $C = 1F$, and $R = 1\Omega$, all parameters can be listed as follows: Mode 1:

$$A_1 = \begin{bmatrix} -1 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, B_1^\omega = \begin{bmatrix} 0.27 & -0.19 & -0.46 \\ -0.21 & -0.15 & 0.32 \\ 0.55 & -0.43 & 0.17 \end{bmatrix},$$
$$C_1 = \begin{bmatrix} -0.11 & 0.29 & 0.30 \\ 0.05 & 0.35 & 0.10 \\ -0.10 & 0.48 & 0.20 \end{bmatrix}, D_1^u = \begin{bmatrix} -0.19 \\ 0.15 \\ 0.23 \end{bmatrix}.$$

Mode 2:

$$A_2 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, B_2^\omega = \begin{bmatrix} 0.36 & -0.16 & -0.25 \\ -0.10 & 0.35 & -0.46 \\ 0.32 & 0.21 & -0.19 \end{bmatrix},$$
$$C_2 = \begin{bmatrix} -0.20 & -0.25 & 0.32 \\ -0.10 & 0.20 & 0.34 \\ -0.20 & 0.20 & 0.35 \end{bmatrix}, D_2^u = \begin{bmatrix} 0.17 \\ -0.21 \\ 0.39 \end{bmatrix},$$

and $B_1^u = B_2^u = \begin{bmatrix} -0.1 & 0.4 & 0.5 \end{bmatrix}^T$. Without loss of generality, the transition rate matrix is given as

$$\Pi = \begin{bmatrix} -1.2 & 1.2 \\ 0.5 & -0.5 \end{bmatrix},$$

and the exogenous disturbance signal is assumed to be $\omega(t) = 0.1\sin(x(t))$. According to Theorem 3, the given constants are selected as $\tau_p = 0.1$, $\tau_q = 0.2$, $\xi_1 = 0.2$, $\xi_2 = 0.5$, $\alpha = 0.46$, $\sigma = 0.012$, and $\gamma = 3$. Then, the security controller gains and weighting matrices can be calculated as

$$K_1^a = \begin{bmatrix} 0.3616 & -0.9208 & -0.7812 \end{bmatrix},$$
$$K_2^a = \begin{bmatrix} 0.1194 & -0.7287 & -1.3834 \end{bmatrix},$$
$$K_1^b = \begin{bmatrix} 1.8081 & -4.6038 & -3.9062 \end{bmatrix},$$
$$K_2^b = \begin{bmatrix} 0.2387 & -1.4573 & -2.7667 \end{bmatrix},$$
$$\Theta_a = \begin{bmatrix} 0.1133 & 0.0031 & 0.0025 \\ 0.0031 & 0.1059 & -0.0144 \\ 0.0025 & -0.0144 & 0.0904 \end{bmatrix},$$
$$\Theta_b = \begin{bmatrix} 1.2865 & -0.3221 & -0.3076 \\ -0.3221 & 2.2103 & 1.7366 \\ -0.3076 & 1.7366 & 4.2373 \end{bmatrix}.$$

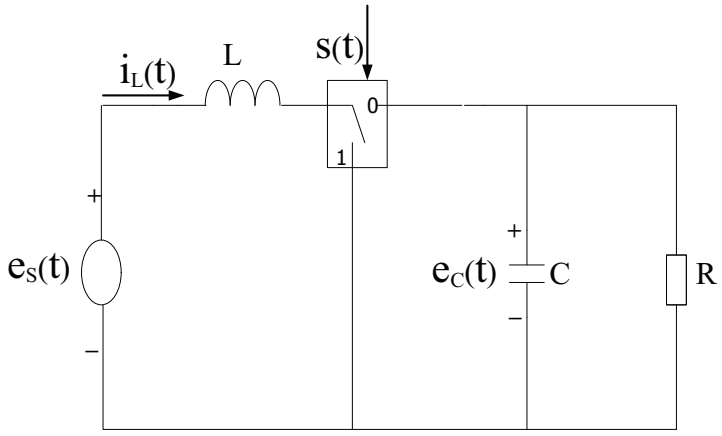

Figure 4. PWM-driven boost converter.

Under the initial state $x(0) = \begin{bmatrix} -0.25 & 0.15 & 0.24 \end{bmatrix}^T$, Figure 5 presents the state trajectories by using the proposed dual-mode security controller (10) when DoS attacks are not injected over the shared communication network. The time evolution of the regulated output $z(t)$ and actual state error $e_a(t)$ without DoS attacks are shown in Figure 6 and Figure 7, respectively. Obviously, by using the developed dual-mode security controller (10), the closed-loop MJCPSs (12) achieve stochastic stability and have good robustness. In Figure 8, we show the event-triggered instants determined by the resilient event-triggered condition (8) in the absence of DoS attacks, in which the number of successful transmissions is 67. From this, the average transmission period is calculated as 0.7463 s. Note that the proposed resilient event-triggered rule (8) is equivalent to the static event-triggered rule when DoS attacks do not occur. Once malicious attackers inject DoS attacks into the communication network, Figure 9 provides schematic diagrams of DoS attacks and system modes, where $\alpha(t) = 0$ and $\alpha(t) = 1$ represent the active and dormant DoS intervals, respectively. Then, based on the different values of $\mathcal{J}_d$, DoS attacks can be divided into two types, namely low-intensity and high-intensity DoS attacks. Assume that the upper bound of performance loss caused by low-intensity DoS attacks is $\mathcal{J}_d = 1.0 \times 10^{-4}$. In this case, Figure 10 shows the state response under the proposed dual-mode event-triggered security controller (10). Figure 11 presents the event-triggered instants determined by the resilient event-triggered condition (8) under low-intensity DoS attacks, where the number of the successful transmissions is 21. From this, the average transmission period is calculated as 2.3810 s. Compared with the situation without DoS attacks, the system state can only converge to a bounded range when the time approaches infinity, indicating that DoS attacks caused a serious negative impact on the system performance. Although the event triggering interval does not exceed the maximum inter-execution interval $\Delta_{\max}$ calculated in Theorem 2, the controller remains in an unreleased state for a long time. On the other hand, assume that the upper bound of performance loss caused by low-intensity DoS attacks is $\mathcal{J}_d = 0.1$. In this case, Figure 12 shows the state response under the proposed dual-mode event-triggered security controller (10). Compared with the above two situations, it can be seen that the system state cannot converge to zero when the time tends to infinity. This means that high-intensity DoS attacks can cause irreversible damage to the control performance of the system. Figure 13 shows the triggering instant and transmission sequence under high-intensity DoS attacks, where the number of the successful transmissions is 13 and the average transmission period is calculated as 3.8462 s. From this, it can be seen that once the event-triggering interval exceeds the maximum allowable inter-execution interval $\Delta_{\max}$, the system will completely lose control performance due to the controller not being updated for a long time. This means that the proposed event dual-mode event-triggered security controller (10) can ensure the safe and stable operation of the system under a specific DoS attack intensity.

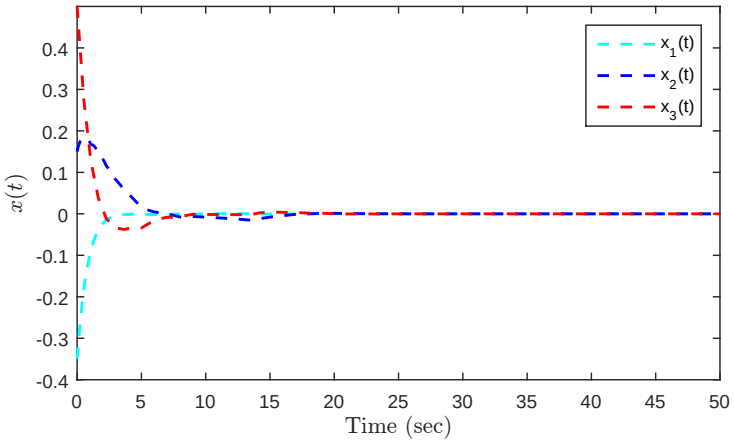

Figure 5. State responses without DoS attacks.

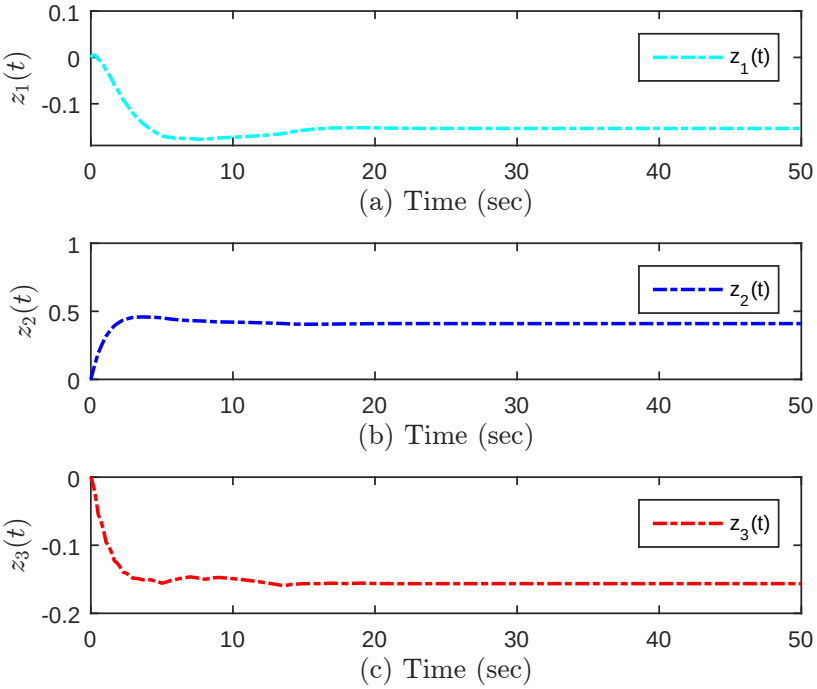

Figure 6. Evolution of the regulated output without DoS attacks.

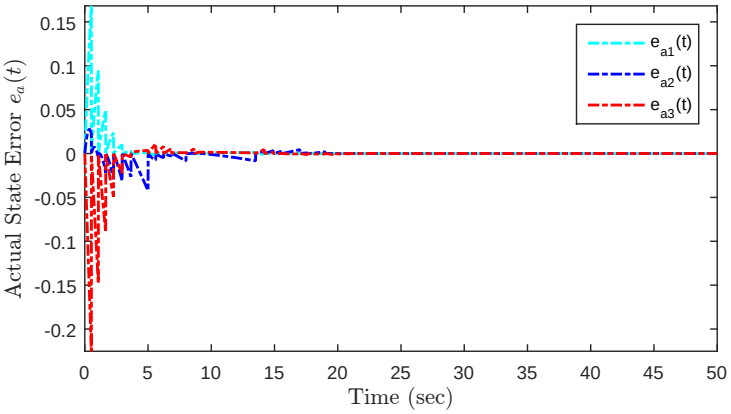

Figure 7. Evolution of the actual state error without DoS attacks.

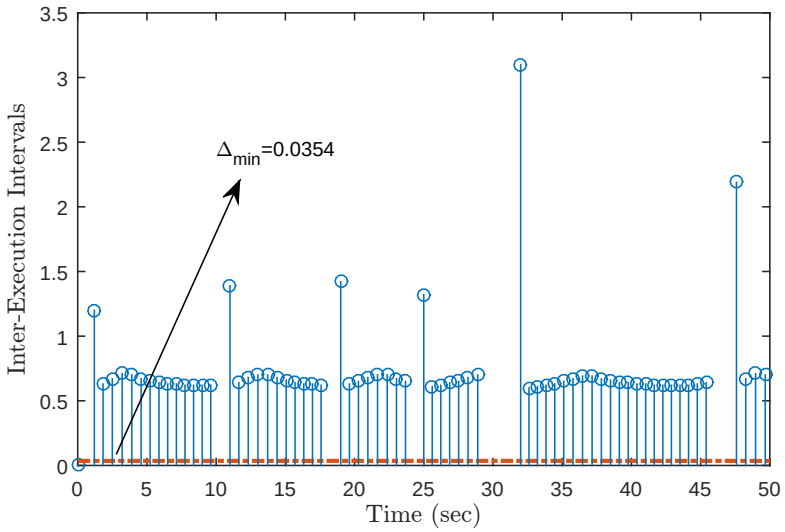

Figure 8. Update instants without DoS attacks.

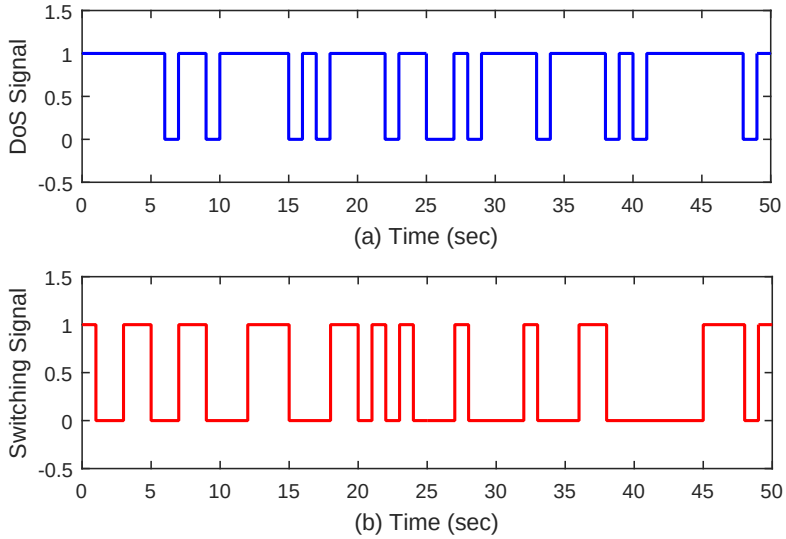

Figure 9. Top: (**a**) DoS signal. Bottom: (**b**) Switching signal.

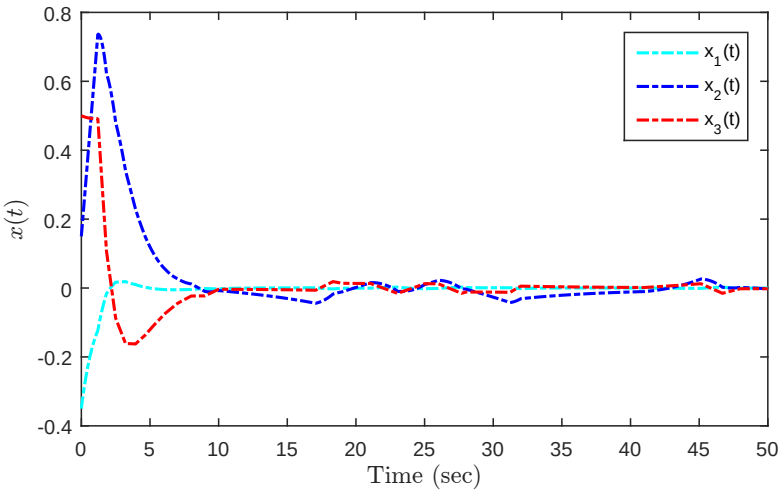

Figure 10. State responses under DoS attacks with $\mathcal{J}_d = 10^{-4}$.

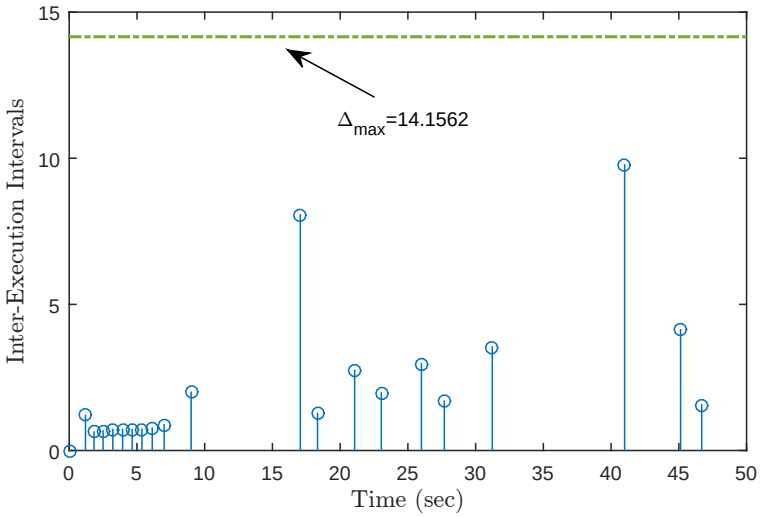

Figure 11. Update instants under DoS attacks with $\mathcal{J}_d = 10^{-4}$.

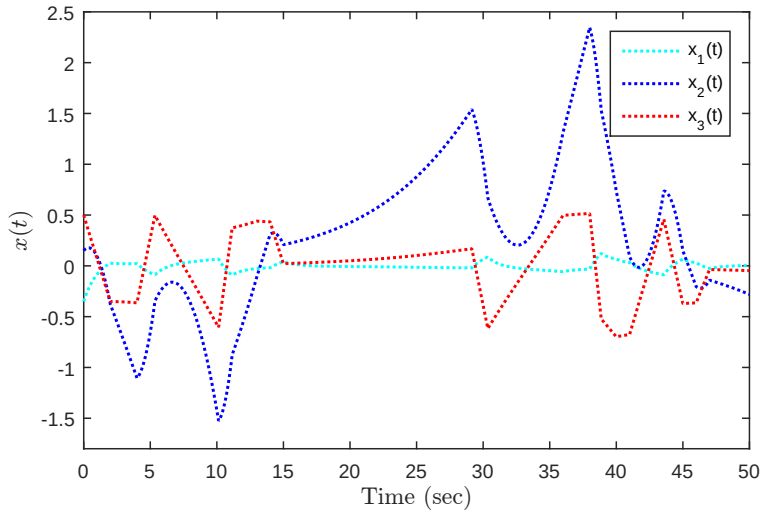

Figure 12. State responses under DoS attacks with $\mathcal{J}_d = 0.1$.

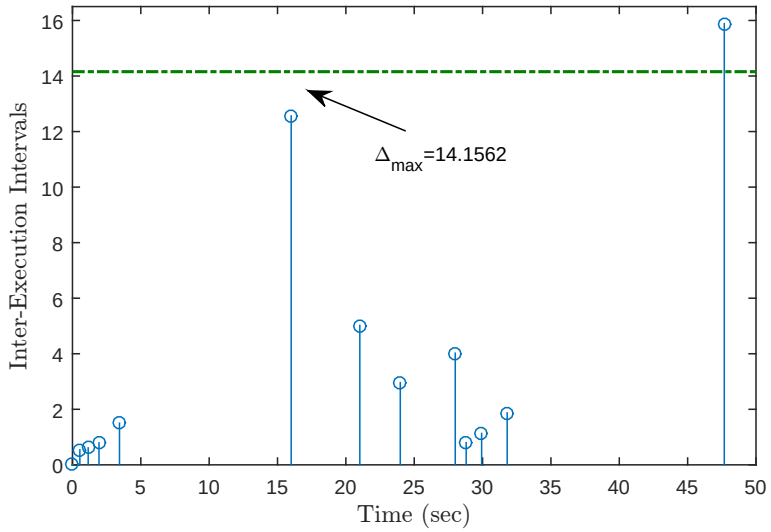

Figure 13. Update instants under DoS attacks with $\mathcal{J}_d = 0.1$.

On the other hand, in order to further demonstrate the effectiveness of the proposed control strategy, we consider a DC motor-driven inverted pendulum systems, which is modeled in [45]. The system parameters are as follows:

$$A_1 = \begin{bmatrix} -0.1397 & -0.0256 & 0 \\ 0.5121 & -0.0373 & 0 \\ -20 & -4 & -1 \end{bmatrix}, \; B_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$
$$A_2 = \begin{bmatrix} -0.0113 & -0.0037 & 0 \\ 0.1470 & -0.0181 & 0 \\ -20 & -4 & -5 \end{bmatrix}, \; B_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

and the other parameters remain unchanged. Then, the security controller gains and weighting matrices can be calculated as

$$K_1^a = \begin{bmatrix} 0.1465 & -0.9058 & -1.5451 \end{bmatrix},$$
$$K_2^a = \begin{bmatrix} 0.1605 & -0.7635 & -1.6873 \end{bmatrix},$$
$$K_1^b = \begin{bmatrix} 0.1321 & -0.6166 & -1.6526 \end{bmatrix},$$
$$K_2^b = \begin{bmatrix} 0.1646 & -0.4531 & -1.7936 \end{bmatrix},$$

$$\Theta_a = \begin{bmatrix} 0.7879 & -1.6667 & -2.8783 \\ -1.6667 & 7.7217 & 14.9392 \\ -2.8783 & 14.9392 & 31.7294 \end{bmatrix},$$
$$\Theta_b = \begin{bmatrix} 0.9435 & -1.4992 & -3.2100 \\ -1.4992 & 3.9094 & 9.2297 \\ -3.2100 & 9.2297 & 25.6459 \end{bmatrix}.$$

Under the initial state $x(0) = \begin{bmatrix} -0.25 & 0.15 & 0.24 \end{bmatrix}^T$, Figure 14 presents the state trajectories by using the proposed dual-mode security controller (10) when DoS attacks are not injected over the shared communication network. Similarly, assume that the upper bound of performance loss caused by low-intensity DoS attacks is $\mathcal{J}_d = 1.0 \times 10^{-4}$. In this case, Figure 15 shows the state response under the proposed dual-mode event-triggered security controller (10), while Figure 16 shows the state response by using a general one. Therefore, it can prove the effectiveness of the dual-mode security controller proposed in this paper.

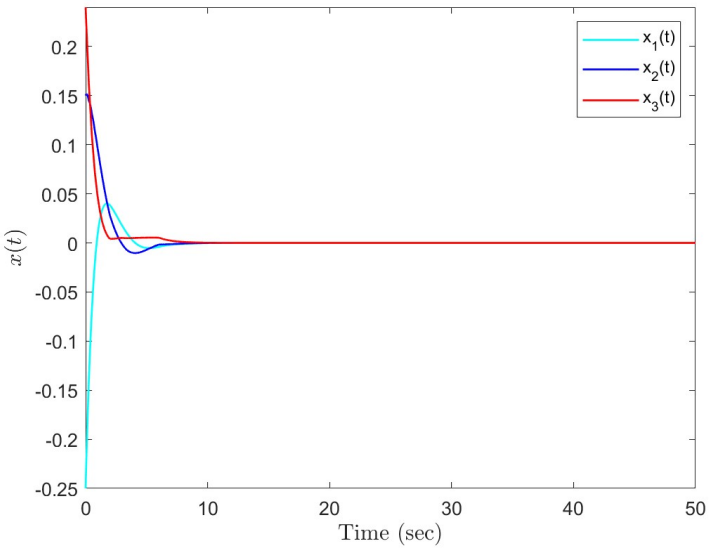

Figure 14. State responses without DoS attacks.

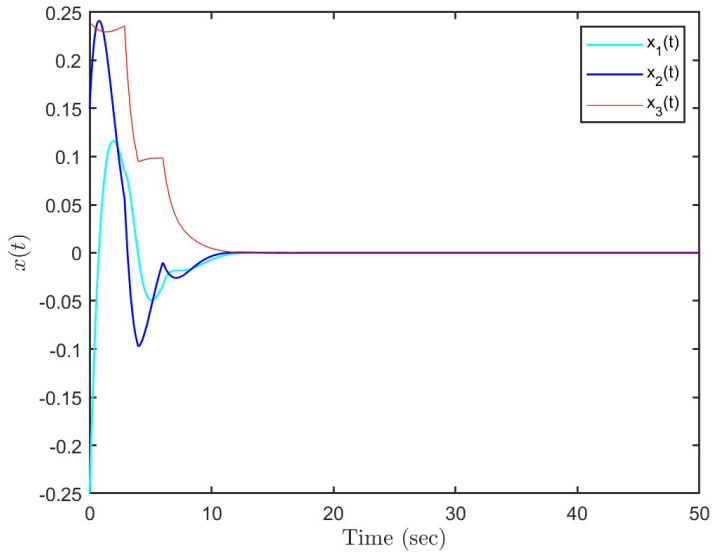

Figure 15. State responses under DoS attacks with $\mathcal{J}_d = 10^{-4}$ by using security controller.

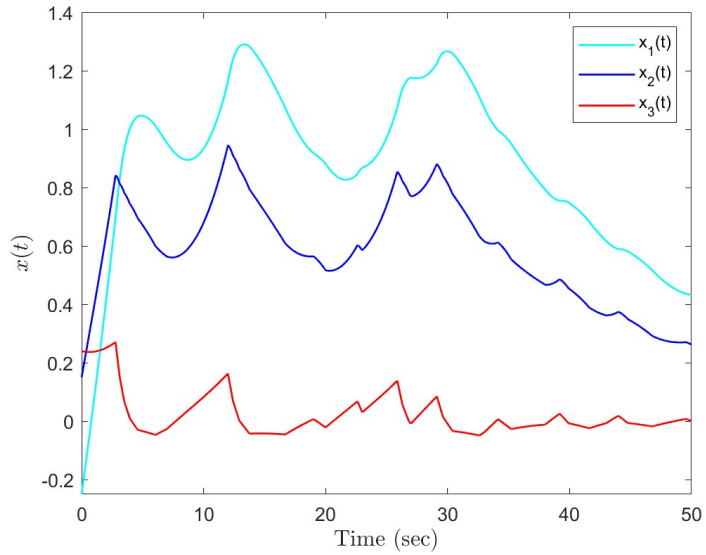

Figure 16. State responses under DoS attacks with $\mathcal{J}_d = 10^{-4}$ by using general controller.

6. Conclusions

This paper addressed the problem of dual-mode event-triggered control for MJCPSs under DoS attacks. A novel random event-triggering rule determined by DoS signal was developed to select appropriate control strategies as needed based on the current network service quality. Then, the relationship between triggering signals and system modes under DoS attacks was analyzed. By calculating the minimum and maximum inter-execution intervals, Zeno behavior and singular triggering can be avoided. On this basis, a mode-dependent event-triggered security was designed to ensure the stable operation of the system under DoS attacks. Finally, a new security control strategy was proposed to tolerate the packet loss caused by DoS attacks as much as possible. In our future work, we will focus on the problem of attack detection and resilient control of unmanned aerial vehicle systems under connectivity-preserved and connectivity-broken DoS attacks from a switching perspective.

Author Contributions: Conceptualization: M.G. Data curation: M.G. and H.X. Funding acquisition: M.G. and T.P. Investigation: H.X. and S.C. Software: M.G. and Z.L. Supervision: Z.L. Writing—original draft: M.G. Writing—review and editing: Z.L., M.G. and S.C. All authors have read and agreed to the published version of the manuscript.

Funding: The author(s) received funding from the Science and Technology Commission of Shanghai Municipality program (19510750200) for this research.

Conflicts of Interest: All authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Appendix A

Proof of the Theorem 2. For any transmission interval $[t_k, t_{k+1})$ determined by the general event-triggered rule (3), the following two cases are divided to explain the relationship between the jump signal $r(t)$ and the triggering sequence $\{t_k\}_{k\in\mathbb{N}_0}$, where $t \in \{t_{\tilde{k}}\}_{\tilde{k}\in\mathbb{N}_0}$ represents the jump instant sequence.

Case I: No jump occurs during the interval $[t_k, t_{k+1})$, that is, $t_{\tilde{k}} < t_k < t_{k+1} < t_{\tilde{k}+1}$ is assumed to be established. Then, it follows from (7) that

$$\begin{aligned}\frac{d\|e_a(t)\|}{\mathrm{dt}} &= \frac{1}{2}\left[e_a^T(t)e_a(t)\right]^{-\frac{1}{2}}\left[2\dot{e}_a^T(t)e_a(t)\right]\\ &\leq \left\|A_{r(t_{\tilde{k}})}x(t) + B^u_{r(t_{\tilde{k}})}u(t) + B^\omega_{r(t_{\tilde{k}})}\omega(t)\right\|.\end{aligned} \tag{A1}$$

As can be seen from the dual-mode security control protocol $u(t)$ in (A1), due to the intermittent DoS attacks, two additional crucial points need to be considered in the following analysis.

- DoS attacks are not activated by malicious attackers. This indicates that $\alpha(t) = 1$ and $x(t_k) = x(t_n^\ell)$.

  By virtue of (10), it can be derived from (A1) that

$$\begin{aligned}\frac{d\|e_a(t)\|}{\mathrm{dt}} &\leq \left\|A_{r(t_{\tilde{k}})}e_a(t) + \hat{A}_{r(t_{\tilde{k}})}x(t_k) + B^\omega_{r(t_{\tilde{k}})}\omega(t)\right\|\\ &\leq \vartheta_1\|e_a(t)\| + \vartheta_2\|x(t_k)\| + \vartheta_3\|\omega(t)\|,\end{aligned} \tag{A2}$$

where $\hat{A}_{r(t_{\tilde{k}})} = A_{r(t_{\tilde{k}})} + B^u_{r(t_{\tilde{k}})}K^a_{r(t_{\tilde{k}})}$, ϑ_1, ϑ_2, and ϑ_3 are given in Theorem 2. Then, a virtual auxiliary variable $f(t)$ satisfying $\dot{f}(t) = \vartheta_1 f(t) + \vartheta_2\|x(t_k)\| + \vartheta_3\|\omega(t)\|$ needs to be introduced, aiming to constrain the change of $\|e_a(t)\|$. Thus, the analytical solution of $f(t)$ can be governed by

$$f(t) = \frac{[\vartheta_2\|x(t_k)\| + \vartheta_3\|\omega(t)\|]}{\vartheta_1}\left(e^{\vartheta_1(t-t_k)} - 1\right). \tag{A3}$$

Combined with the actual state error $e_a(t)$ mentioned in (7), one can yield that

$$\begin{aligned}\|e_a(t)\| \leq \vartheta_1^{-1}[\vartheta_2(\|e_a(t)\| + \|x(t)\|) + \vartheta_3\|\omega(t)\|]\\ \times\left(e^{\vartheta_1(t-t_k)} - 1\right).\end{aligned} \tag{A4}$$

Based on the resilient event-triggered rule (8), it is concluded that $e_a^T(t)\Theta_a e_a(t) \leq \varrho_1^2\|e_a(t)\|^2$ and $x^T(t)\Theta_b x(t) \geq \varrho_2^2\|x(t)\|^2$ are established without DoS attacks, where ϱ_1 and ϱ_2 are given in Theorem 2. Then, we obtain $e_a^T(t)\Theta_a e_a(t) \leq \sigma x^T(t)\Theta_b x(t) + \varpi^2\|\omega(t)\|^2$, which is guaranteed by $\varrho_1^2\|e_a(t)\|^2 \leq \sigma\varrho_2^2\|x(t)\|^2 + \varpi^2\|\omega(t)\|^2$, where $\varpi \in \mathbb{R}_{>0}$ is a given constant. To calculate the minimum inter-execution interval $\Delta^1_{\min}$, we need to discuss the inherent relationship between $\|e_a(t)\|$, $\|x(t)\|$, and $\|\omega(t)\|$. With the help of Young's inequality, it can be further guaranteed by $\|e_a(t)\| \leq \varsigma_1\|x(t)\| + \varsigma_2\|\omega(t)\|$, where the forms of ς_1 and ς_2 consist of the parameters ϱ_1, ϱ_2, and ϖ. Combined with inequality (A4), one can yield

$$\frac{1}{\vartheta_1}\ln\left[\frac{\vartheta_1\varsigma_1\|x(t)\|+\vartheta_1\varsigma_2\|\omega(t)\|}{\vartheta_2(\varsigma_1+1)\|x(t)\|+(\vartheta_2\varsigma_2+\vartheta_3)\|\omega(t)\|}+1\right]\leq\Delta_k, \tag{A5}$$

which is greater than or equal to $\Delta^1_{\min}$ in condition (29).

- DoS attacks are injected remotely by malicious attackers. This means that $\alpha(t)=0$ and $x(t_k)\neq x(t_n^\ell)$.

  Due to DoS attacks, condition (A2) needs to be rewritten as

$$\begin{aligned}\frac{d\|e_a(t)\|}{\mathrm{dt}}\leq\Big\|&A_{r(t_{\tilde{k}})}e_a(t)+A_{r(t_{\tilde{k}})}x(t_k)\\&+B^{\omega}_{r(t_{\tilde{k}})}\omega(t)+\hat{B}^{u}_{r(t_{\tilde{k}})}x(t_n^\ell)\Big\|,\end{aligned} \tag{A6}$$

where $\hat{B}^u_{r(t_{\tilde{k}})}=\xi_{r(t_{\tilde{k}})}B^u_{r(t_{\tilde{k}})}K^b_{r(t_{\tilde{k}})}$. Then, it follows from (A6) that $\frac{d\|e_a(t)\|}{\mathrm{dt}}\leq\vartheta_1(\|e_a(t)\|+\|x(t_k)\|)+\vartheta_3\|\omega(t)\|+\vartheta_4\|x(t_n^\ell)\|$, where ϑ_4 is given in Theorem 2. Similarly, we define a virtual intermediate variable $g(t)$ satisfying $\dot{g}(t)=\vartheta_1(g(t)+\|x(t_k)\|)+\vartheta_3\|\omega(t)\|+\vartheta_4\|x(t_n^\ell)\|$, whose solution can be calculated as

$$\begin{aligned}g(t)=&\frac{\left[\vartheta_1\|x(t_k)\|+\vartheta_3\|\omega(t)\|+\vartheta_4\|x(t_n^\ell)\|\right]}{\vartheta_1}\\&\times\left(e^{\vartheta_1(t-t_k)}-1\right).\end{aligned} \tag{A7}$$

Substituting $\|x(t_k)\|\leq\|e_a(t)\|+\|x(t)\|$ into (A7), we obtain $\|e_a(t)\|\leq\vartheta_1^{-1}[\vartheta_1\|e_a(t)\|+\vartheta_1\|x(t)\|+\vartheta_3\|\omega(t)\|+\vartheta_4\|x(t_n^\ell)\|]\times(e^{\vartheta_1(t-t_k)}-1)$. Meanwhile, it can be known from the resilient event-triggered rule (8) that $\varrho_1^2\|e_a(t)\|^2\leq\sigma\varrho_2^2\|x(t)\|^2+\tilde{\omega}^2\mathcal{J}_d+\omega^2\|\omega(t)\|^2+\hat{\omega}^2\|x(t_n^\ell)\|^2$ is established when there are DoS attacks, where $\hat{\omega}$ and $\tilde{\omega}\in\mathbb{R}_{>0}$ are given scalars. Subsequently, we need to focus on the relationship between $\|e_a(t)\|$, $\|x(t_n^\ell)\|$, $\|x(t)\|$, $\|\omega(t)\|$, and $\mathcal{J}_d$. Based on Young's inequality, it can be concluded that $\|e_a(t)\|\leq\varsigma_3\|x(t)\|+\varsigma_4\|\omega(t)\|+\varsigma_5\|x(t_n^\ell)\|+\varsigma_6\tilde{\mathcal{J}}_d$, where $\tilde{\mathcal{J}}_d=\sqrt{\mathcal{J}_d}$, ς_3, ς_4, ς_5, and $\varsigma_6\in\mathbb{R}_{>0}$ are defined in Theorem 2. From this, one can yield

$$\frac{1}{\vartheta_1}\ln\left[\frac{\Upsilon_1(x(t),\omega(t),x(t_n^\ell),\tilde{\mathcal{J}}_d)}{\Upsilon_2(x(t),\omega(t),x(t_n^\ell),\tilde{\mathcal{J}}_d)}+1\right]\leq\Delta_k, \tag{A8}$$

where $\Upsilon_1(x(t),\omega(t),x(t_n^\ell),\tilde{\mathcal{J}}_d)=\vartheta_1\varsigma_3\|x(t)\|+\vartheta_1\varsigma_4\|\omega(t)\|+\vartheta_1\varsigma_5\|x(t_n^\ell)\|+\vartheta_1\varsigma_6\tilde{\mathcal{J}}_d$ and $\Upsilon_2(x(t),\omega(t),x(t_n^\ell),\tilde{\mathcal{J}}_d)=\vartheta_1(\varsigma_3+1)\|x(t)\|+(\vartheta_1\varsigma_4+\vartheta_3)\|\omega(t)\|+(\vartheta_1\varsigma_5+\vartheta_4)\|x(t_n^\ell)\|+\vartheta_1\varsigma_6\tilde{\mathcal{J}}_d$. This implies that the inter-execution interval Δ_k is greater than or equal to $\Delta^2_{\min}$ defined in condition (29).

Case II: Some jumps occur during the interval $[t_k,t_{k+1})$. This means that $t_{\tilde{k}}\leq t_k<t_{\tilde{k}+1}<\cdots<t_{\tilde{k}+l}\leq t_{k+1}$ with $l\in\mathbb{S}$.

Once there are some jumps during the interval $[t_k,t_{k+1})$, we need to divide it into a group of subintervals based on the jump instants. Furthermore, it can be seen from the above derivation that conditions (A2) and (A6) are satisfied regardless of whether DoS attacks are dormant or active. Since the jump signal $r(t_{\tilde{k}})$, $\tilde{k}\in\mathbb{N}_0$ obeys a right-continuous Markov process, this indicates that either $\|e_a(t^-_{\tilde{k}+1})\|\leq f(t^-_{\tilde{k}+1})$ or $\|e_a(t^-_{\tilde{k}+1})\|\leq g(t^-_{\tilde{k}+1})$ can be satisfied for the first subinterval $[t_{\tilde{k}},t_{\tilde{k}+1})$. Notice that $x(t_k)$ is maintained within the transmission interval $[t_k,t_{k+1})$ due to the effect of ZOH. In this case, no matter the subinterval, we can obtain $\|e_a(t^-_{\tilde{k}+h})\|=\|e_a(t_{\tilde{k}+h})\|\leq f(t_{\tilde{k}+h})=f(t^-_{\tilde{k}+h})$ and $\|e_a(t^-_{\tilde{k}+h})\|=\|e_a(t_{\tilde{k}+h})\|\leq g(t_{\tilde{k}+h})=g(t^-_{\tilde{k}+h})$. Thus, the same conclusion can be drawn as in Case I. That is, conditions (A2) and (A6) always hold, where there exist some jumps during the transmission interval $[t_k,t_{k+1})$. In summary, the parameter $\Delta_{\min}$ determined by (A2) and (A6) is regarded as the minimum execution interval, implying that Zeno behavior can be avoided.

On the other hand, DoS attacks can cause a severe mismatch of information between S-C and C-A sides. Therefore, we need to calculate the maximum downtime, which is reflected by the maximum update interval between two successful transmission attempts subject to the resilient event-triggered rule (8). Firstly, before embarking on this study, it can be concluded from Case I and Case II that the presence or absence of jumps during each transmission interval has no effect on estimating $\|e_a(t)\|$. Next, if $-e_a^T(t)\Theta_a e_a(t) + \sigma x^T(t)\Theta_b x(t) + \varpi^2\|\omega(t)\|^2 + \hat{\varpi}^2\|x(t_n^\ell)\|^2 + \tilde{\varpi}^2\mathcal{J}_d > 0$ is satisfied, then we can derive $\|e_a(t)\| \leq \tilde{\varsigma}_3\|x(t)\| + \tilde{\varsigma}_4\|\omega(t)\| + \tilde{\varsigma}_5\|x(t_n^\ell)\| + \tilde{\varsigma}_6\tilde{\mathcal{J}}_d$, where $\tilde{\mathcal{J}}_d$ is given in (A8) and the parameters $\tilde{\varsigma}_3$, $\tilde{\varsigma}_4$, $\tilde{\varsigma}_5$, $\tilde{\varsigma}_6$ are defined in Theorem 2. In view of the accumulation of sampling errors caused by DoS attacks, a large number of packets from S-C side cannot be transmitted normally. Therefore, it is necessary to re-estimate $\|e_a(t)\|$ over time period $[\mathcal{T}_n, \mathcal{T}_{n+1})$, $n \in \mathbb{N}_0$. Intuitively, we need to discuss the internal relationship between the latest transmission instant and DoS initiation instant. From this, the estimation of $\|e_a(t)\|$ during $[\mathcal{T}_n, \mathcal{T}_{n+1})$ can be divided into the following three steps.

Step I: The latest transmission attempt occurs at $\mathcal{T}_n^{\text{on}}$, that is, $t_k := \mathcal{T}_n^{\text{on}}$, where t_k and $\mathcal{T}_n^{\text{on}}$ denote the latest transmission and DoS initiation instants, respectively. Then, we obtain that

$$\begin{aligned}\|e_a(t)\| \leq{}& \tilde{\varsigma}_3\|x(t)\| + \tilde{\varsigma}_3(1+\tilde{\varsigma}_3)\|x(t)\| + \tilde{\varsigma}_4(2+\tilde{\varsigma}_3)\\ &\times\|\omega(t)\| + \tilde{\varsigma}_5(2+\tilde{\varsigma}_3)\|x(t_n^\ell)\| + \tilde{\varsigma}_6(2+\tilde{\varsigma}_3)\tilde{\mathcal{J}}_d,\end{aligned} \tag{A9}$$

where $t \in [t_n^\ell, t_n^{\ell+1})$. Since there may be some abnormal event-triggered packets during $[\mathcal{T}_n^{\text{on}}, \mathcal{T}_{n+1})$, it follows from (A9) that

$$\begin{aligned}\|e_a(t)\| \leq{}& \tilde{\varsigma}_3[1+\hat{\varsigma}_3+2\hat{\varsigma}_3+\cdots+2^{N_{\text{dos}}}\hat{\varsigma}_3]\|x(t)\|\\ &+\tilde{\varsigma}_4[1+\hat{\varsigma}_3+2\hat{\varsigma}_3+\cdots+2^{N_{\text{dos}}}\hat{\varsigma}_3]\|\omega(t)\|\\ &+\tilde{\varsigma}_5[1+\hat{\varsigma}_3+2\hat{\varsigma}_3+\cdots+2^{N_{\text{dos}}}\hat{\varsigma}_3]\|x(t_n^\ell)\|\\ &+\tilde{\varsigma}_6[1+\hat{\varsigma}_3+2\hat{\varsigma}_3+\cdots+2^{N_{\text{dos}}}\hat{\varsigma}_3]\tilde{\mathcal{J}}_d\\ ={}&\left[\tilde{\varsigma}_3\|x(t)\| + \tilde{\varsigma}_4\|\omega(t)\| + \tilde{\varsigma}_5\|x(t_n^\ell)\| + \tilde{\varsigma}_6\tilde{\mathcal{J}}_d\right]\\ &\times\left[1+\sum_{n_f=1}^{N_{\text{dos}}+1}2^{n_f-1}\hat{\varsigma}_3\right],\end{aligned} \tag{A10}$$

where $\hat{\varsigma}_3 = \tilde{\varsigma}_3 + 1$, and N_{dos} is the maximum number of packet losses caused by DoS attacks during $[\mathcal{T}_n^{\text{on}}, \mathcal{T}_{n+1})$.

Step II: The latest transmission attempt occurs before $\mathcal{T}_n^{\text{on}}$, that is, $t_k < \mathcal{T}_n^{\text{on}}$ is established. For $[\mathcal{T}_n^{\text{on}}, t_{k+1})$, we can obtain

$$\|e_a(t)\| \leq \tilde{\varsigma}_3\|x(t)\| + \tilde{\varsigma}_4\|\omega(t)\| + \tilde{\varsigma}_6\tilde{\mathcal{J}}_d. \tag{A11}$$

In a similar way, for the nth DoS active subinterval, $\|e_a(t)\|$ can be further calculated as

$$\begin{aligned}\|e_a(t)\| \leq{}&\left[\tilde{\varsigma}_3\|x(t)\| + \tilde{\varsigma}_4\|\omega(t)\| + \tilde{\varsigma}_5\|x(t_n^\ell)\| + \tilde{\varsigma}_6\tilde{\mathcal{J}}_d\right]\\ &\times\left[1+\sum_{n_f=1}^{N_{\text{dos}}}2^{n_f-1}\hat{\varsigma}_3\right].\end{aligned} \tag{A12}$$

Step III: Calculate the maximum update interval between two successful transmission attempts.

By comparing the magnitude of conditions (A10) and (A12), it can be found that the supermum of $\|e_a(t)\|$ is characterized by condition (A10). Substituting the fact $\|e_a(t)\| \leq$

$\vartheta_1^{-1}[\vartheta_1\|x(t_k)\| + \vartheta_3\|\omega(t)\| + \vartheta_4\|x(t_n^\ell)\|] \times (e^{\vartheta_1(t-t_k)} - 1)$ into condition (A10), it can be deduced that

$$\Delta_k \leq \frac{1}{\vartheta_1}\ln\left[\frac{\tilde{\Upsilon}_1(x(t),\omega(t),x(t_n^\ell),\tilde{\mathcal{J}}_d)}{\tilde{\Upsilon}_2(x(t),\omega(t),x(t_n^\ell),\tilde{\mathcal{J}}_d)} \times \Gamma + 1\right], \tag{A13}$$

where

$$\Gamma = \vartheta_1\left[1 + \sum_{n_f=1}^{N_{\text{dos}}+1} 2^{n_f-1}\hat{\varsigma}_3\right],$$

$\tilde{\Upsilon}_1(x(t),\omega(t),x(t_n^\ell),\tilde{\mathcal{J}}_d) = \tilde{\varsigma}_3\|x(t)\| + \tilde{\varsigma}_4\|\omega(t)\| + \tilde{\varsigma}_5\|x(t_n^\ell)\| + \tilde{\varsigma}_6\tilde{\mathcal{J}}_d$, $\tilde{\Upsilon}_2(x(t),\omega(t),x(t_n^\ell),\tilde{\mathcal{J}}_d) = \vartheta_1(\tilde{\varsigma}_3+1)\|x(t)\| + (\vartheta_1\tilde{\varsigma}_4+\vartheta_3)\|\omega(t)\| + (\vartheta_1\tilde{\varsigma}_5+\vartheta_4)\|x(t_n^\ell)\| + \vartheta_1\tilde{\varsigma}_6\tilde{\mathcal{J}}_d$, and $N_{\text{dos}} = (\mathcal{T}_{n+1} - \mathcal{T}_n^{\text{on}})/\Delta_{\min}$. Therefore, in order to ensure the safe operation under DoS attacks, the maximum downtime must be less than or equal to $\Delta_{\max}$ defined in Theorem 2. The proof is complete. □

References

1. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
2. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security—A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
3. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
4. Teixeira, A.; Shames, I.; Sandberg, H.; Johansson, K.H. A secure control framework for resource-limited adversaries. *Automatica* **2015**, *51*, 135–148. [CrossRef]
5. Molnar, T.G.; Kiss, A.K.; Ames, A.D.; Orosz, G. Safety-Critical Control With Input Delay in Dynamic Environment. *IEEE Trans. Control Syst. Technol.* **2023**, *31*, 1507–1520. [CrossRef]
6. Pasqualetti, F.; Dorfler, F.; Bullo, F. Attack Detection and Identification in Cyber-Physical Systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
7. Abdel-Basset, M.; Chang, V.; Hawash, H.; Chakrabortty, R.K.; Ryan, M. Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment. *IEEE Trans. Ind. Inform.* **2020**, *17*, 7704–7715. [CrossRef]
8. Qaddoura, R.; Al-Zoubi, A.M.; Almomani, I.; Faris, H. A Multi-Stage Classification Approach for IoT Intrusion Detection Based on Clustering with Oversampling. *Appl. Sci.* **2021**, *11*, 3022. [CrossRef]
9. Jovanov, I.; Pajic, M. Relaxing Integrity Requirements for Attack-Resilient Cyber-Physical Systems. *IEEE Trans. Autom. Control* **2019**, *64*, 4843–4858. [CrossRef]
10. Ding, D.; Han, Q.-L.; Ge, X.; Wang, J. Secure State Estimation and Control of Cyber-Physical Systems: A Survey. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 176–190. [CrossRef]
11. Incremona, G.P.; Rubagotti, M.; Tanelli, M.; Ferrara, A. A General Framework for Switched and Variable Gain Higher Order Sliding Mode Control. *IEEE Trans. Autom. Control* **2021**, *66*, 1718–1724. [CrossRef]
12. De Persis, C.; Tesi, P. Input-to-State Stabilizing Control Under Denial-of-Service. *IEEE Trans. Autom. Control* **2015**, *60*, 2930–2944. [CrossRef]
13. Lu, A.-Y.; Yang, G.-H. Input-to-State Stabilizing Control for Cyber-Physical Systems With Multiple Transmission Channels Under Denial of Service. *IEEE Trans. Autom. Control* **2018**, *63*, 1813–1820. [CrossRef]
14. Lu, A.-Y.; Yang, G.-H. Stability Analysis for Cyber-Physical Systems Under Denial-of-Service Attacks. *IEEE Trans. Cybern.* **2021**, *51*, 5304–5313 [CrossRef]
15. Umlauft, J.; Hirche, S. Feedback Linearization Based on Gaussian Processes With Event-Triggered Online Learning. *IEEE Trans. Autom. Control* **2020**, *65*, 4154–4169. [CrossRef]
16. Doostmohammadian, M.; Meskin, N. Finite-Time Stability Under Denial of Service. *IEEE Syst. J.* **2021**, *15*, 1048–1055. [CrossRef]
17. Tahoun, A.H.; Arafa, M. Secure control design for nonlinear cyber–physical systems under DoS, replay, and deception cyber-attacks with multiple transmission channels. *ISA Trans.* **2022**, *128*, 294–308. [CrossRef]
18. Lu, A.-Y.; Yang, G.-H. Resilient Observer-Based Control for Cyber-Physical Systems With Multiple Transmission Channels Under Denial-of-Service. *IEEE Trans. Cybern.* **2020**, *50*, 4796–4807. [CrossRef]
19. Li, Z.; Zhao, J. Resilient adaptive control of switched nonlinear cyber-physical systems under uncertain deception attacks. *Inf. Sci.* **2021**, *543*, 398–409 [CrossRef]
20. Kim, S.; Park, K.-J.; Lu, C. A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1534–1573. [CrossRef]
21. Cosentino, F.; Oberhauser, H.; Abate, A. Grid-free computation of probabilistic safety with malliavin calculus. *IEEE Trans. Autom. Control* **2023**, *68*, 6369–6376. [CrossRef]

22. Li, T.; Chen, B.; Yu, L.; Zhang, W.-A. Active Security Control Approach Against DoS Attacks in Cyber-Physical Systems. *IEEE Trans. Autom. Control* **2021**, *66*, 4303–4310. [CrossRef]
23. Feng, S.; Cetinkaya, A.; Ishii, H.; Tesi, P.; Persis, C.D. Networked control under DoS attacks: Tradeoffs between resilience and data rate. *IEEE Trans. Autom. Control* **2020**, *66*, 460–467. [CrossRef]
24. Feng, Z.; Wen, G.H.; Hu, G.Q. Distributed secure coordinated control for multiagent systems under strategic attacks. *IEEE Trans. Cybern.* **2017**, *47*, 1273–1284. [CrossRef]
25. Senejohnny, D.; Tesi, P.; De Persis, C. A Jamming-Resilient Algorithm for Self-Triggered Network Coordination. *IEEE Trans. Control Netw. Syst.* **2018**, *5*, 981–990. [CrossRef]
26. Yang, Y.; Xu, H.; Yue, D. Observer-Based Distributed Secure Consensus Control of a Class of Linear Multi-Agent Systems Subject to Random Attacks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2018**, *66*, 3089–3099. [CrossRef]
27. Deng, C.; Wen, C. MAS-Based Distributed Resilient Control for a Class of Cyber-Physical Systems With Communication Delays Under DoS Attacks. *IEEE Trans. Cybern.* **2021**, *51*, 2347–2358 [CrossRef]
28. Zhang, D.; Ye, Z.; Dong, X. Co-Design of Fault Detection and Consensus Control Protocol for Multi-Agent Systems Under Hidden DoS Attack. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 2158–2170. [CrossRef]
29. Persis, C.D.; Tesi, P. Formulas for data-driven control: Stabilization, optimality, and robustness. *IEEE Trans. Autom. Control* **2020**, *65*, 909–924. [CrossRef]
30. Gabriel, G.W.; Goncalves, T.R.; Geromel, J.C. Optimal and robust sampled-data control of Markov jump linear systems: A differential LMI approach. *IEEE Trans. Autom. Control* **2018**, *63*, 3054–3060. [CrossRef]
31. Gunasekaran, N.; Joo, Y.H. Robust Sampled-data Fuzzy Control for Nonlinear Systems and Its Applications: Free-Weight Matrix Method. *IEEE Trans. Fuzzy Syst.* **2019**, *27*, 2130–2139. [CrossRef]
32. De Persis, C.; Rotulo, M.; Tesi, P. Learning Controllers From Data via Approximate Nonlinearity Cancellation. *IEEE Trans. Autom. Control* **2023**, *68*, 6082–6097. [CrossRef]
33. Amini, A.; Asif, A.; Mohammadi, A. Formation-containment control using dynamic event-triggering mechanism for multi-agent systems. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 1235–1248. [CrossRef]
34. Peng, C.; Sun, H. Switching-Like Event-Triggered Control for Networked Control Systems Under Malicious Denial of Service Attacks. *IEEE Trans. Autom. Control* **2020**, *65*, 3943–3949. [CrossRef]
35. Xu, W.; Hu, G.; Ho, D.W.C.; Feng, Z. Distributed Secure Cooperative Control Under Denial-of-Service Attacks From Multiple Adversaries. *IEEE Trans. Cybern.* **2020**, *50*, 3458–3467. [CrossRef]
36. Peng, C.; Wu, J.; Tian, E. Stochastic Event-Triggered H∞ Control for Networked Systems Under Denial of Service Attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *52*, 4200–4210. [CrossRef]
37. Qi, W.; Hou, Y.; Zong, G.; Ahn, C.K. Finite-Time Event-Triggered Control for Semi-Markovian Switching Cyber-Physical Systems With FDI Attacks and Applications. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 2665–2674. [CrossRef]
38. Sun, H.; Peng, C.; Zhang, W.; Yang, T.; Wang, Z. Security-based resilient event-triggered control of networked control systems under denial of service attacks. *J. Frankl. Inst.* **2019**, *356*, 10277–10295. [CrossRef]
39. Xu, Y.; Fang, M.; Shi, P.; Wu, Z.-G. Event-based secure consensus of multiagent systems against DoS attacks. *IEEE Trans. Cybern.* **2020**, *50*, 3468–3476. [CrossRef]
40. Feng, Z.; Hu, G. Secure Cooperative Event-Triggered Control of Linear Multiagent Systems Under DoS Attacks. *IEEE Trans. Control Syst. Technol.* **2020**, *28*, 741–752. [CrossRef]
41. Deng, C.; Wen, C. Distributed resilient observer-based fault-tolerant control for heterogeneous multiagent systems under actuator faults and DoS attacks. *IEEE Trans. Control Netw. Syst.* **2020**, *7*, 1308–1318 [CrossRef]
42. Behera, A.K.; Bandyopadhyay, B. Robust sliding mode control: An event-triggering approach. *IEEE Trans. Circuits Syst. II Express Briefs* **2017**, *64*, 146–150. [CrossRef]
43. Xiong, J.; Lam, J.; Shu, Z.; Mao, X. Stability Analysis of Continuous-Time Switched Systems With a Random Switching Signal. *IEEE Trans. Autom. Control* **2014**, *59*, 180–186. [CrossRef]
44. Zhang, L.; Cui, N.; Liu, M.; Zhao, Y. Asynchronous filtering of discrete-time switched linear systems with average dwell time. *IEEE Trans. Circuits Syst. Regul. Pap.* **2011**, *58*, 1109–1118. [CrossRef]
45. Lian, J.; Li, C.; Liu, D. Input-to-state stability for discrete-time nonlinear switched singular systems. *IET Control Theory Appl.* **2017**, *11*, 2893–2899. [CrossRef]