actuators

MDPI

Article

H_∞ Control for ICPS with Hybrid-Triggered Mechanism Encountering Stealthy DoS Jamming Attacks

Mufeng Wang [1], Yangyang Geng [2], Jingpei Wang [3,*], Ke Liu [2], Xin Che [3] and Qiang Wei [2]

[1] China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China; wangmufeng@cics-cert.org.cn
[2] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China; young9471@163.com (Y.G.); bendawang@gmail.com (K.L.); funnywei@163.com (Q.W.)
[3] College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China; chexin@zju.edu.cn
* Correspondence: wjpbupt@163.com or 0618222@zju.edu.cn

Abstract: In recent years, with the upgrading of the attack technology, stealthy DoS jamming attacks have become the primary factor to threaten the security of Industrial Cyber-Physical Systems (ICPS). Considering the complex industrial scenarios of ICPS, which are influenced by a variety of external and internal interference, a H_∞ controller designing problem is studied in this paper for an ICPS which deploys a hybrid-triggered mechanism (HTM) in the wireless channel encountering stealthy DoS jamming attacks. By employing a compensation mechanism which is employed in the controller to mitigate the impacts of attacks, external disturbance, limited channel capacity, wireless channel noise, we establish a closed-loop system and prove the closed-loop system is mean square exponentially stable and can achieve the desired H_∞ disturbance rejection level theoretically. Finally, simulation examples are used to demonstrate effectiveness of the proposed H_∞ controller.

Keywords: Industrial Cyber-Physical System (ICPS); H_∞ control; stealthy DoS jammer; hybrid-triggered mechanism (HTM); system security

Citation: Wang, M.; Geng, Y.; Wang, J.; Liu, K.; Che, X.; Wei, Q. H_∞ Control for ICPS with Hybrid-Triggered Mechanism Encountering Stealthy DoS Jamming Attacks. *Actuators* **2022**, *11*, 193. https://doi.org/10.3390/act11070193

Academic Editor: Guanghong Yang

Received: 6 June 2022
Accepted: 14 July 2022
Published: 16 July 2022

1. Introduction

Recently, the traditional "air-gap" Industrial Control System (ICS) has been deeply integrated with advanced information technology (IT) and communication technology (CT) under the trend of Industry 4.0 [1], and then the Industrial Cyber-Physical System (ICPS) [2–5] was proposed and can be employed in many crucial infrastructures, such as smart grids [6], transportation systems [7], smart buildings [8], etc. However, almost all the ICPSs are facing serious security issues due to the lack of consideration of effective security guaranteeing mechanisms when engineers design and deploy an ICS [9]. In the past decade, many security events of ICPS occurred in nuclear facility, petroleum industry, and subway system, which resulted in huge economic loss and great social instability [10–12]. After analyzing the intrusion processes of these malicious security events, researchers found that these attackers not only have a comprehensive information of the system, but also have the ability to bypass intrusion detection systems and launch stealthy attacks [13,14]. Obviously, the ICPSs are at a distinct disadvantage from the defender's point of view.

As a research hotspot, recently, security issues in different control scenarios have been studied [15], and malicious attacks have been categorized into Denial-of-Service (DoS) jamming attacks, false data injection attacks, replay attacks, wormhole attacks, etc. [16–20]. Due to the integration of more shared and general CTs in ICPSs, DoS jamming attacks, which aim to interference communication quality, can be considered as the most reachable attacks [21–24]. Foroush et al. [25] established a periodic attack strategy for a DoS jammer in which partial information has been detected, and then studied a resilience controller design problem for a remote wireless control scenario. However, the assumption of partial information of the jammer has been detected, which is conservative from the view of

stealthy attacks in ICPS security analysis and research [26–28]. To maximize the effect of the attacks on the system performance, Zhang et al. studied the optimal attack strategy where a DoS jammer has constrained energy in a general wireless networked control scenario [29]. Ding et al. proposed a model by using the relationship among SER (Symbol Error Rate), SNR (Signal to Noise Ratio), and SINR (Signal to Interference plus Noise Ratio) in a communication channel based on the wireless communication technology, and studied the optimal attack scheduling of an energy constrained DoS jammer by establishing a two-player game in a multi-channel remote state estimation [30]. However, as a premeditated and supported attacker, the limitation of energy or other cost may not be the most important factors to be considered. Ding et al. studied an event-based security control for a discrete-time unified framework by defining a concept of working subcycle networked control system encountering randomly DoS jamming attacks [31]. However, as a purposeful and conscious individual compared with external disturbance, these kinds of attack strategies, which use random variables, cannot fully describe the jammer's intention [32]. In Ref. [33], a unified framework of the attack strategy for a DoS jammer is discussed, and a H_∞ controller design problem for a control system subject to DoS jamming attacks is studied without any known information of the DoS jammers' attack strategy.

Besides, as a system deployed in complex industrial scenarios, ICPS also faces interference factors from inside and outside [34–37]. These non-negligible factors, like external disturbance, limited channel capacity and channel noise, can result in random dropout of packet in the network and ultimately affect the stability of the whole system [38,39]. In the previous studies, a variable which follows the Bernoulli distribution was used to described random packet dropouts caused by external disturbance or channel fading, and some effective algorithms were deployed to increase the transmission efficiency. For example, in Ref. [40], a hybrid-driven communication scheme is proposed and a controller design method is investigated for networked control systems with time delay. In Ref. [41], an event-triggered scheme and a quantiser are deployed in an array of discrete time-varying systems, and a distributed state estimation problem is studied. However, these studies have not considered the security requirements of networked systems, which is an urgent problem to be solved. Therefore, as a fundamental problem in the industrial scenarios, the H_∞ controller design for an ICPS with traditional internal and external interference encountering stealthy DoS jamming attacks needs to be addressed. Then, in Ref. [42], we studied the H_∞ control for an ICPS with event-triggered mechanism (ETM) encountering reactive DoS jamming attacks. However, consider that the hybrid-triggered mechanism (HTM) has more advantages than the ETM in utilizing network resources, and a smart attacker can use the characteristics of HTM to achieve more stealthy attacks, the H_∞ control problem for an ICPS with HTM needs to be further investigated.

To sum up, due to the constraints of the current wireless communication technology and the increasingly complex industrial scenarios, ICPS not only faces a variety of external and internal interference, but also faces severe security issues caused by stealthy malicious attacks. In this paper, therefore, we consider that an ICPS, which deployed a HTM to improve the network bandwidth utilization, is intruded by a stealthy DoS jammer, where the DoS jammer keeps sensing the wireless channel and cleverly uses a reactive attack strategy to ensure its stealthiness based on the communication traffic. Then, based on the relationship among SER, SNR, and SINR, the impacts of stealthy DoS jamming attacks, external disturbance, limited channel capacity, and channel noise are described in a unified framework, and a compensation mechanism is employed in the controller to mitigate the impact of stealthy attacks due to the ICPS does not know the jammer's attack strategy. Finally, simulation examples are given to show the effectiveness of the proposed H_∞ control method. The main contributions of this paper can be summarized as follows.

- For a smart DoS jammer, it can use the trigger characteristics of HTM, which is an effective communication mechanism, to launch attacks on the premise of ensuring its stealth, and finally destroy the stable operation of the ICPS. Therefore, we studied the

H_∞ controller design problem for an ICPS with HTM to solve the stable operation of the ICPS encountering stealthy DoS jamming attacks.

- Unlike the existing studies that consider energy limitation of the attacker, we focus on attack purpose and stealthiness, and consider that the attacker keeps sensing the wireless channel traffic and cleverly uses a reactive attack strategy to achieve its purpose and ensure its stealthiness.
- We consider both of the stealthy DoS jamming attacks, external disturbance, limited channel capacity, wireless channel noise, and use the SER of wireless channel in a unified framework to describe the channel's communication quality.

Notation: $\mathbb{R}^n$ stands for the n-dimensional Euclidean space. The symbol $\|\cdot\|$ stands for Euclidean norm. $\mathbb{Z}^+$ stands for the set of positive integers. For a matrix A, $\lambda_{\max}(A)$ ($\lambda_{\min}(A)$) stands for the largest (smallest) eigenvalue of A, A^{T} stands for the transposition of A, and $A > 0$ ($A < 0$) stands for a positive (negative) definite matrix. Let I and 0 be identity matrix and zero matrix with appropriate dimensions, respectively. $Pr[\cdot]$ stands for the probability of a stochastic event. $\mathbb{E}\{\cdot\}$ denotes the expectation of a stochastic variable. The symbol $*$ within a matrix represents the symmetric entries.

2. Problem Formulation

In this section, the problem of H_∞ control for an ICPS with HTM encountering stealthy DoS jamming attacks is formulated.

2.1. Basic Structure

The basic structure of an ICPS with HTM encountering stealthy jamming attacks can be shown in Figure 1, which consists of a physical system, a time-triggered sensor, a controller, and an actuator. Specifically, states of the physical system are captured by the sensor and transmitted to the controller through a memoryless wireless channel with a HTM. Meanwhile, based on Ref. [33], a stealthy DoS jammer who keeps sensing the traffic of wireless channel and uses the reactive attack strategy to increase the probability of packet dropouts, and we assume that the ICPS does not have any intrusion detected systems and does not know any information of the DoS jammer's attack strategy. Considering the physical system has the following form

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + D_1\omega(k), \\ y(k) = C_1x(k), \\ z(k) = C_2x(k) + D_2\omega(k), \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^n$, $y(k) \in \mathbb{R}^m$, $z(k) \in \mathbb{R}^q$, and $\omega(k) \in \mathbb{R}^q$ stand for the system state, measured output, controlled output, and external disturbance input belonging to $l_2[0,\infty)$, respectively. A, B, C_1, C_2, D_1, and D_2 are known real matrices with appropriate dimensions. Consider the wireless channel has independent Additive White Gaussian Noise (AWGN), communication quality of the wireless channel can be modeled as [43,44]

$$SER = 2q\sqrt{\xi SNR}, SNR = \frac{p_s}{\sigma^2}, \tag{2}$$

where p_s, $\xi > 0$ and σ^2 stand for transmission power, network parameter and AWGN power, respectively. Meanwhile, $q = 1/\sqrt{2\pi}\int_x^\infty \exp(-\rho^2/2)\mathrm{d}\rho$.

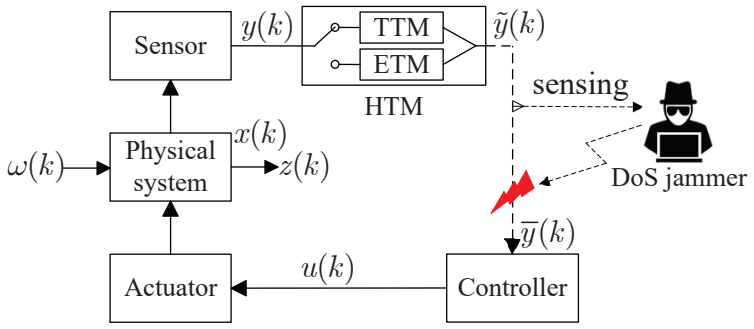

Figure 1. Basic structure of the ICPS with HTM encountering stealthy DoS jamming attacks.

2.2. Hybrid-Triggered Mechanism

A HTM is deployed in the wireless channel to alleviate the limitation of network resources. Specifically,

Time-triggered mechanism (TTM): Consider the measured output via only the TTM which received by the controller can be described as

$$\tilde{y}(k) = y(k), \tag{3}$$

Event-triggered mechanism (ETM): An ETM is deployed to improve the network bandwidth utilization, and consider the event-triggered condition as

$$k_{s+1} = \min_{k>k_s}\{k \mid (y(k) - y(k_s))^{\mathrm{T}}\Phi(y(k) - y(k_s)) \geq y(k_s)^{\mathrm{T}}\Psi y(k_s)\}, \tag{4}$$

where $\Phi > 0$ and $\Psi > 0$ stand for event-triggered matrices to be designed, $\{k_s\}_{s\geq 0} \subseteq \mathbb{Z}^+$ with $k_0 = 0$, $\{k_s\}_{s\geq 1}$ stand for the packet transmission instants sequence. We define

$$e_y(k) = y(k_s) - y(k), k \in [k_s, k_{s+1}), \tag{5}$$

then (4) can be rewritten as

$$e_y(k)^{\mathrm{T}}\Phi e_y(k) \leq y(k_s)^{\mathrm{T}}\Psi y(k_s), \forall k \in [k_s, k_{s+1}). \tag{6}$$

Then, the measured output via only the ETM which received by the controller can be described as

$$\tilde{y}(k) = e_y(k) + y(k), \tag{7}$$

Therefore, we can define a Bernoulli distribution stochastic variable $\theta(k)$ to stand for the probability of triggered mechanism being selected, and by combining (3) with (7), the measured output via the HTM, which is received by the controller, can be described as

$$\tilde{y}(k) = (1 - \theta(k))y(k) + \theta(k)(e_y(k) + y(k)), \tag{8}$$

where $Pr[\theta(k) = 1] = \bar{\theta}$, $Pr[\theta(k) = 0] = 1 - \bar{\theta}$, and the mathematical variance of $\theta(k)$ is δ^2. The sojourn probability $\bar{\theta}$ can be obtained by the following statistical method

$$\bar{\theta} = \lim_{n\to\infty} \frac{k_i}{n}, k_i \in \mathbb{Z}^+, n \in \mathbb{Z}^+ \tag{9}$$

where k_i is the times of $\theta(k) = 1$ in the interval $[1, n]$, and we assume that $\bar{\theta}$ in the wireless channel is known.

2.3. Stealthy DoS Jamming Attacks

A stealthy DoS jammer who uses reactive attack strategy keeps sensing the traffic of wireless channel and changes attack modes autonomously according to whether a packet is transmitting in the wireless channel [33]. Denoting $\alpha(k) \in \{0, 1\}$ stands for different

periods, the nth working subcycle of the DoS jammer, which consists of the start time $T(n)$, the duration of attack period $ta(n)$, and the duration of silent period $ts(n)$, can be described as

$$\alpha(k) = \begin{cases} 1, k \in [T(n), T(n) + ta(n) - 1], \\ 0, k \in [T(n) + ta(n), T(n) + ta(n) + ts(n) - 1], \end{cases} \tag{10}$$

where $\alpha(k) = 1$ and $\alpha(k) = 0$ stand for the attack period and the silent period, respectively. Combining (2), the inherent packet dropouts caused by limited capacity of wireless channel and channel noise are considered in the silent periods, and in the attack periods, the DoS jammer uses attack power p_a on the wireless channel to increase the probability of packet dropouts. Then, we have

$$SER = 2q\sqrt{\xi SINR}, SINR = \frac{p_s}{p_a + \sigma^2}. \tag{11}$$

Combining with (10) and (11), SER for the wireless channel can be described in a unified framework as

$$SER = 2q\sqrt{\xi \frac{p_s}{\alpha(k)p_a + \sigma^2}} = \begin{cases} 2q\sqrt{\xi SNR}, \alpha(k) = 0, \\ 2q\sqrt{\xi SINR}, \alpha(k) = 1. \end{cases} \tag{12}$$

2.4. Closed-Loop System

Let $\bar{y}(k)$ stand for received measurement of the controller, and let mutually independent Bernoulli stochastic variable $\beta(\alpha(k), k)$ indicate whether a packet is successfully received or not by the controller, we have

$$\beta(\alpha(k), k) = \begin{cases} 1, successfully, \\ 0, otherwise. \end{cases} \tag{13}$$

Then, combining with (11), (12), and (13), we have

$$\begin{cases} \Pr[\beta(\alpha(k), k) = 1] = 1 - SER = \bar{\beta}, \\ \Pr[\beta(\alpha(k), k) = 0] = SER = 1 - \bar{\beta}, \end{cases} \tag{14}$$

where $\bar{\beta} \in [0, 1)$ is a known constant.

Due to the deployment of HTM, it is difficult for the controller to know whether the packet is dropped or just not transmitted. Additionally, the ICPS dose not know the attack strategy of the DoS jammer due to it lack of intrusion detection systems. Thus, an compensation mechanism which employs the latest transmitted quantized measurement is established in the controller to decrease the impact of packet dropouts. Specifically, if the packet is received by the controller, we use $\bar{y}(k) = \tilde{y}(k)$. Otherwise, the previous packet $\bar{y}(k-1)$ will be used. Therefore, combining with (13), we have

$$\bar{y}(k) = \beta(\alpha(k), k)[(1 - \theta(k))y(k) + \theta(k)(e_y(k) + y(k))] + (1 - \beta(\alpha(k), k))\bar{y}(k-1). \tag{15}$$

To achieve the control objective, we consider an observer-based controller as

$$Observer: \begin{cases} \hat{x}(k+1) = A\hat{x}(k) + Bu(k) + L(\bar{y}(k) - \hat{\bar{y}}(k)), \\ \hat{\bar{y}}(k) = \beta(\alpha(k), k)\hat{y}(k) + (1 - \beta(\alpha(k), k))\bar{y}(k-1), \end{cases} \tag{16}$$

$$Controller: u(k) = K\hat{x}(k), \tag{17}$$

where $\hat{y}_k$ is the observer output, L is the observer gain matrix, and K is the controller gain matrix. We denote the estimation error as

$$e(k) = x(k) - \hat{x}(k). \tag{18}$$

Then, a closed-loop system for the ICPS with HTM encountering stealthy DoS jamming attacks can be described as

$$\begin{cases} x(k+1) = & (A+BK)x(k) - BKe(k) + D_1\omega(k), \\ e(k+1) = & (A-\bar{\beta}LC_1)e(k) - (\beta(\alpha(k),k)-\bar{\beta})LC_1)e(k) - \bar{\beta}(\theta(k)-\bar{\theta})Le_y(k) \\ & -\bar{\beta}\bar{\theta}Le_y(k) - (\beta(\alpha(k),k)-\bar{\beta})(\theta(k)-\bar{\theta})Le_y(k) - \bar{\theta}(\beta(\alpha(k),k)-\bar{\beta})L \\ & \times e_y(k) + D_1\omega(k). \end{cases} \tag{19}$$

Assumption 1. *The matrix B is of full column rank.*

As the closed-loop system (19) is a stochastic parameter system, the following Definition is needed.

Definition 1. *Consider the ICPS with HTM encountering stealthy DoS jamming attacks. Let $\eta(k) = \begin{bmatrix} x(k)^{\mathrm{T}} & e(k)^{\mathrm{T}} \end{bmatrix}^{\mathrm{T}}$. The closed-loop system (19) satisfies exponentially mean-square stable with $\omega(k) = 0$, if there exist constants $\epsilon > 0$ and $\tau \in (0,1)$ such that*

$$\mathbb{E}\{\|\eta(k)\|^2\} \leq \epsilon\tau^k \mathbb{E}\{\|\eta(0)\|^2\}, \tag{20}$$

where $\forall \eta(0) \in \mathbb{R}^n$, $k \in \mathbb{Z}^+$.

By the Definition 1, the objective of this paper is to design a controller to guarantee the closed-loop system (19) which satisfies the following requirements simultaneously.

(1) The closed-loop system (19) with $\omega(k) = 0$ is exponentially mean-square stable;
(2) Given a scalar $\gamma > 0$. For all nonzero $\omega(k)$, under the zero-initial condition, the controlled input $z(k)$ satisfies

$$\sum_{k=0}^{\infty} \mathbb{E}\{\|z(k)\|^2\} < \gamma^2 \sum_{k=0}^{\infty} \mathbb{E}\{\|\omega(k)\|^2\}, \tag{21}$$

3. Main Results

In this section, proof process of the H_∞ control is discussed. First, the required Lemmas are listed.

Lemma 1 ([45]). *Let $V(\eta(k))$ as a Lyapunov function. If there exist real scalars $\lambda \geq 0$, $\mu > 0$, $\nu > 0$, and $0 < \varphi < 1$ such that*

$$\begin{gathered} \mu\|\eta(k)\|^2 \leq V(\eta(k)) \leq \nu\|\eta(k)\|^2, \\ \mathbb{E}\{V(\eta(k+1))|\eta(k)\} - V(\eta(k)) \leq \lambda - \varphi V(\eta(k)), \end{gathered}$$

then

$$\mathbb{E}\{\|\eta(k)\|^2\} \leq \tfrac{\nu}{\mu}\|\eta(k)\|^2(1-\varphi)^k + \tfrac{\lambda}{\mu\varphi}.$$

Lemma 2 ([34]). *For the matrix B of full-column rank, there always exists a singular value decomposition (SVD), such that*

$$B = U^{\mathrm{T}}\begin{bmatrix}\Sigma \\ 0\end{bmatrix}V^{\mathrm{T}} = \begin{bmatrix}U_1 \\ U_2\end{bmatrix}\begin{bmatrix}\Sigma \\ 0\end{bmatrix}V^{\mathrm{T}}, \tag{22}$$

where $U \in \mathbb{R}^{n\times n}$ and $V \in \mathbb{R}^{m\times m}$ are orthogonal matrices, $\Sigma = diag\{\varpi_1, \varpi_2, \ldots, \varpi_m\}$, where $\varpi_i (i = 1, 2, \ldots, m)$ are nonzero singular values of B.

Lemma 3 ([38]). *For the matrix B of full-column rank, if there exist positive definite matrices $P_1 \in \mathbb{R}^{m\times m}$, $P_2 \in \mathbb{R}^{(n-m)\times(n-m)}$, and matrix P satisfies*

$$P = U^{\mathrm{T}}\begin{bmatrix} P_1 & 0 \\ 0 & P_2 \end{bmatrix}U = U_1^{\mathrm{T}}P_1U_1 + U_2^{\mathrm{T}}P_2U_2, \tag{23}$$

then there exist a nonsingular matrix $\bar{P}$, such that $PB = B\bar{P}$.

3.1. Stability Analysis

Theorem 1. *Consider the ICPS with HTM encountering stealthy DoS jamming attacks. Given the controller gain matrix K and the observer gain matrix L. The closed-loop system (19) is exponentially mean-square stable, if there exist positive definite matrices P and S satisfying (24).*

$$\begin{bmatrix} \Delta_1 & * & * & * & * & * & * & * \\ 0 & \Delta_4 & * & * & * & * & * & * \\ 0 & 0 & \Delta_8 & * & * & * & * & * \\ \Delta_2 & \Delta_5 & 0 & \Delta_{11} & * & * & * & * \\ 0 & \Delta_6 & 0 & 0 & \Delta_{12} & * & * & * \\ 0 & \Delta_7 & 0 & 0 & 0 & \Delta_{13} & * & * \\ \Delta_3 & 0 & \Delta_9 & 0 & 0 & 0 & \Delta_{14} & * \\ 0 & 0 & \Delta_{10} & 0 & 0 & 0 & 0 & \Delta_{15} \end{bmatrix} < 0, \tag{24}$$

where $\Delta_1 = -P$, $\Delta_2 = A + BK$, $\Delta_3 = C_1$, $\Delta_4 = -S$, $\Delta_5 = -BK$, $\Delta_6 = A - \bar{\beta}LC_1$, $\Delta_7 = LC_1$, $\Delta_8 = -\Phi$, $\Delta_9 = I$, $\Delta_{10} = L$, $\Delta_{11} = -P^{-1}$, $\Delta_{12} = -S^{-1}$, $\Delta_{13} = -\varepsilon_1^{-1}S^{-1}$, $\Delta_{14} = -\Psi^{-1}$, $\Delta_{15} = -\bar{\beta}^{-1}\bar{\theta}^{-1}S^{-1}$, $\varepsilon_1 = (1-\bar{\beta})\bar{\beta}$, $\varepsilon_2 = (1-\bar{\theta})\bar{\theta}$.

Proof. We define a Lyapunov function as

$$V(\eta(k)) = x(k)^{\mathrm{T}}Px(k) + e(k)^{\mathrm{T}}Se(k). \tag{25}$$

By (19), we have

$$\begin{aligned}
&\mathbb{E}\{V(\eta(k+1))\} - V(\eta(k)) \\
=&\mathbb{E}\{x(k+1)^{\mathrm{T}}Px(k+1) + e(k+1)^{\mathrm{T}}Se(k+1)\} - x(k)^{\mathrm{T}}Px(k) - e(k)^{\mathrm{T}}Se(k) \\
=&\mathbb{E}\{[(A+BK)x(k) - BKe(k)]^{\mathrm{T}}P[(A+BK)x(k) - BKe(k)] + [(A-\bar{\beta}LC_1) \\
&\times e(k) - (\beta(\alpha(k),k) - \bar{\beta})LC_1)e(k) - \bar{\beta}(\theta(k)-\bar{\theta})Le_y(k) - \bar{\beta}\bar{\theta}Le_y(k) \\
&- (\beta(\alpha(k),k) - \bar{\beta})(\theta(k)-\bar{\theta})Le_y(k) - \bar{\theta}(\beta(\alpha(k),k) - \bar{\beta})Le_y(k)]^{\mathrm{T}}P \\
&\times [(A-\bar{\beta}LC_1)e(k) - (\beta(\alpha(k),k) - \bar{\beta})LC_1)e(k) - \bar{\beta}(\theta(k)-\bar{\theta})Le_y(k) \\
&- \bar{\beta}\bar{\theta}Le_y(k) - (\beta(\alpha(k),k) - \bar{\beta})(\theta(k)-\bar{\theta})Le_y(k) - \bar{\theta}(\beta(\alpha(k),k) - \bar{\beta})Le_y(k)] \\
&- x(k)^{\mathrm{T}}Px(k) - e(k)^{\mathrm{T}}Se(k).
\end{aligned}$$

Combining with $\mathbb{E}\{(\beta(\alpha(k),k) - \bar{\beta})^2\} = (1-\bar{\beta})\bar{\beta}$, $\mathbb{E}\{(\theta(k)-\bar{\theta})^2\} = (1-\bar{\theta})\bar{\theta}$ and (6), we have

$$e_y(k)^{\mathrm{T}}\Phi e_y(k) \le [e_y(k) + y(k)]^{\mathrm{T}}\Psi[e_y(k) + y(k)], \tag{26}$$

where $\forall k \in [k_s, k_{s+1})$. Therefore,

$$\begin{aligned}
&\mathbb{E}\{V(\eta(k+1))\} - V(\eta(k)) \\
\leq &\mathbb{E}\{x(k+1)^{\mathrm{T}} P x(k+1) + e(k+1)^{\mathrm{T}} S e(k+1)\} \\
&- x(k)^{\mathrm{T}} P x(k) - e(k)^{\mathrm{T}} S e(k) + [e_y(k) + y(k)]^{\mathrm{T}} \Psi \\
&[e_y(k) + y(k)] - e_y(k)^{\mathrm{T}} \Phi e_y(k) \\
= &\hat{\eta}(k)^{\mathrm{T}} \begin{bmatrix} \Pi_1^{\mathrm{T}} \Pi_2 \Pi_1 + \Pi_3 & * \\ \Pi_4 & \Pi_5 \end{bmatrix} \hat{\eta}(k) \\
= &\hat{\eta}(k)^{\mathrm{T}} \Pi \hat{\eta}(k), \forall k \in [k_s, k_{s+1}),
\end{aligned}$$

where $\hat{\eta}(k) = \begin{bmatrix} \eta(k)^{\mathrm{T}} & e_y(k)^{\mathrm{T}} \end{bmatrix}^{\mathrm{T}}$, $\Pi_2 = diag\{P, S, \varepsilon_1 S, \Psi\}$, $\Pi_3 = diag\{-P, -S\}$, $\Pi_4 = \begin{bmatrix} \Pi_{41} & \Pi_{42} \end{bmatrix}$, $\Pi_{41} = \Psi C_1$, $\Pi_{42} = \varepsilon_1 \bar{\theta} L^{\mathrm{T}} S L C_1 - \bar{\beta} \bar{\theta} L^{\mathrm{T}} S (A - \bar{\beta} L C_1)$, $\Pi_5 = \bar{\beta} \bar{\theta} L^{\mathrm{T}} S L + \Psi - \Phi$, $\Pi_1 = \begin{bmatrix} A + BK & -BK \\ 0 & A - \bar{\beta} L C_1 \\ 0 & L C_1 \\ C_1 & 0 \end{bmatrix}$.

By Schur complement, (24) implies that $\Pi < 0$, and Π is a strick matrix inequality, then there exits a constant κ such that

$$\mathbb{E}\{V(\eta(k+1))\} - V(\eta(k)) \leq \hat{\eta}(k)^{\mathrm{T}} diag\{-\kappa I, 0\} \hat{\eta}(k) < -\kappa \eta(k)^{\mathrm{T}} \eta(k), \tag{27}$$

where $0 < \kappa < \min\{\lambda_{\min}(-\Pi), \vartheta\}$, $\vartheta = \max\{\lambda_{\max}(P), \lambda_{\max}(S)\}$. Then, we have

$$\mathbb{E}\{V(\eta(k+1))\} - V(\eta(k)) < -\kappa \eta(k)^{\mathrm{T}} \eta(k) \leq \frac{\kappa}{\vartheta} \eta(k)^{\mathrm{T}} \eta(k). \tag{28}$$

By Lemma 1, we have

$$\mathbb{E}\{\|\eta(k)\|^2\} - V(\eta(k)) \leq \frac{\kappa}{\vartheta} (1 - \frac{\kappa}{\vartheta})^k \|\eta(0)\|^2, \tag{29}$$

where $0 < \frac{\kappa}{\vartheta} < 1$. Therefore, the closed-loop system (19) is exponentially mean-square stable. This completes the proof. □

3.2. H_∞ Controller Design

Theorem 2. *Consider the ICPS with HTM encountering stealthy DoS jamming attacks. The closed-loop system (19) is exponentially mean-square stable and the H_∞ norm constraint (21) is achieved for all nonzero $\omega(k)$, if there exist positive definite matrices P and S, the controller gain matrix K and the observer gain matrix L satisfying (30).*

$$\begin{bmatrix}
\Xi_1 & * & * & * & * & * & * & * & * & * \\
0 & \Xi_5 & * & * & * & * & * & * & * & * \\
0 & 0 & \Xi_9 & * & * & * & * & * & * & * \\
0 & 0 & 0 & \Xi_{12} & * & * & * & * & * & * \\
\Xi_2 & \Xi_6 & 0 & \Xi_{13} & \Xi_{16} & * & * & * & * & * \\
0 & \Xi_7 & 0 & \Xi_{14} & 0 & \Xi_{17} & * & * & * & * \\
0 & \Xi_8 & 0 & 0 & 0 & 0 & \Xi_{18} & * & * & * \\
\Xi_3 & 0 & \Xi_{10} & 0 & 0 & 0 & 0 & \Xi_{19} & * & * \\
0 & 0 & \Xi_{11} & 0 & 0 & 0 & 0 & 0 & \Xi_{20} & * \\
\Xi_4 & 0 & 0 & \Xi_{15} & 0 & 0 & 0 & 0 & 0 & \Xi_{21}
\end{bmatrix} < 0, \tag{30}$$

where $\Xi_1 = -P$, $\Xi_2 = A + BK$, $\Xi_3 = C_1$, $\Xi_4 = C_3$, $\Xi_5 = -S$, $\Xi_6 = -BK$, $\Xi_7 = A - \bar{\beta} L C_1$, $\Xi_8 = L C_1$, $\Xi_9 = -\Phi$, $\Xi_{10} = I$, $\Xi_{11} = L$, $\Xi_{12} = -\gamma^2 I$, $\Xi_{13} = D_1$, $\Xi_{14} = D_1$, $\Xi_{15} = D_2$, $\Xi_{16} = -P^{-1}$, $\Xi_{17} = -S^{-1}$, $\Xi_{18} = -\varepsilon_1^{-1} S^{-1}$, $\Xi_{19} = -\Psi^{-1}$, $\Xi_{20} = -\bar{\beta}^{-1} \bar{\theta}^{-1} S^{-1}$, $\Xi_{21} = -I$, $C_3 = \begin{bmatrix} C_2 & 0 & 0 \end{bmatrix}$.

Proof. Let $\tilde{\eta}(k) = \begin{bmatrix}\hat{\eta}(k)^{\mathrm{T}} & \omega(k)^{\mathrm{T}}\end{bmatrix}^{\mathrm{T}}$, and combine with (26). For any nonzero $\omega(k)$, we have

$$\begin{aligned}
&\mathbb{E}\{V(\eta(k+1))\} - \mathbb{E}\{V(\eta(k))\} + \mathbb{E}\{z(k)^{\mathrm{T}}z(k)\} - \gamma^2\mathbb{E}\{\omega(k)^{\mathrm{T}}\omega(k)\}\\
\leq&\mathbb{E}\{V(\eta(k+1))\} - \mathbb{E}\{V(\eta(k))\} + \mathbb{E}\{z(k)^{\mathrm{T}}z(k)\} - \gamma^2\mathbb{E}\{\omega(k)^{\mathrm{T}}\omega(k)\}\\
&+ [e_y(k) + y(k)]^{\mathrm{T}}\Psi[e_y(k) + y(k)] - e_y(k)^{\mathrm{T}}\Phi e_y(k)\\
=&\mathbb{E}\{\tilde{\eta}(k)^{\mathrm{T}}\begin{bmatrix}\Pi + \Lambda_1 & *\\ \Lambda_2 & \Lambda_3\end{bmatrix}\tilde{\eta}(k)\}\\
=&\mathbb{E}\{\tilde{\eta}(k)^{\mathrm{T}}\Lambda\tilde{\eta}(k)\},
\end{aligned}$$

where $\Lambda_1 = C_3^{\mathrm{T}}C_3$, $\Lambda_2 = \begin{bmatrix}\Lambda_{21} & \Lambda_{22} & \Lambda_{23}\end{bmatrix}$, $\Lambda_{21} = D_1^{\mathrm{T}}P(A+BK) + D_2^{\mathrm{T}}C_2$, $\Lambda_{22} = -D_1^{\mathrm{T}}PBK + D_1^{\mathrm{T}}S(A - \bar{\beta}LC_1)$, $\Lambda_{23} = -\bar{\beta}\bar{\theta}D_1^{\mathrm{T}}SL$, $\Lambda_3 = D_1^{\mathrm{T}}PD_1 + D_1^{\mathrm{T}}SD_1 + D_2^{\mathrm{T}}D_2 - \gamma^2 I$.
By Schur complement, (30) implies that $\Lambda < 0$, we have

$$\mathbb{E}\{V(\eta(k+1))\} - \mathbb{E}\{V(\eta(k))\} + \mathbb{E}\{z(k)^{\mathrm{T}}z(k)\} - \gamma^2\mathbb{E}\{\omega(k)^{\mathrm{T}}\omega(k)\} < 0. \tag{31}$$

For $k = 0 \to \infty$, by summing up (31) we can obtain

$$\sum_{k=0}^{\infty}\mathbb{E}\{\|z(k)\|^2\} < \gamma^2\sum_{k=0}^{\infty}\mathbb{E}\{\|\omega(k)\|^2\} + \mathbb{E}\{V(\eta(0))\} - \mathbb{E}\{V(\eta(\infty))\}. \tag{32}$$

Due to $\eta(0) = 0$ and Theorem 1, we have

$$\sum_{k=0}^{\infty}\mathbb{E}\{\|z(k)\|^2\} < \gamma^2\sum_{k=0}^{\infty}\mathbb{E}\{\|\omega(k)\|^2\}, \tag{33}$$

which means the H_∞ norm constraint (21) is achieved. This completes the proof. □

Theorem 3. *Consider the ICPS with HTM encountering stealthy DoS jamming attacks. The closed-loop system (19) is exponentially mean-square stable and the H_∞ norm constraint (21) is achieved for all nonzero $\omega(k)$, if there exist positive definite matrices P_1, P_2 and S, real matrices X and Y satisfying (34) and (35). Furthermore, the controller gain matrix K and the observer gain matrix L can be given by (36).*

$$\begin{bmatrix}
\Omega_1 & * & * & * & * & * & * & * & * & *\\
0 & \Omega_5 & * & * & * & * & * & * & * & *\\
0 & 0 & \Omega_9 & * & * & * & * & * & * & *\\
0 & 0 & 0 & \Omega_{12} & * & * & * & * & * & *\\
\Omega_2 & \Omega_6 & 0 & \Omega_{13} & \Omega_{16} & * & * & * & * & *\\
0 & \Omega_7 & 0 & \Omega_{14} & 0 & \Omega_{17} & * & * & * & *\\
0 & \Omega_8 & 0 & 0 & 0 & 0 & \Omega_{18} & * & * & *\\
\Omega_3 & 0 & \Omega_{10} & 0 & 0 & 0 & 0 & \Omega_{19} & * & *\\
0 & 0 & \Omega_{11} & 0 & 0 & 0 & 0 & 0 & \Omega_{20} & *\\
\Omega_4 & 0 & 0 & \Omega_{15} & 0 & 0 & 0 & 0 & 0 & \Omega_{21}
\end{bmatrix} < 0, \tag{34}$$

where $\Omega_1 = -P$, $\Omega_2 = PA + BX$, $\Omega_3 = \Psi C_1$, $\Omega_4 = C_3$, $\Omega_5 = -S$, $\Omega_6 = -BX$, $\Omega_7 = SA - \bar{\beta}YC_1$, $\Omega_8 = YC_1$, $\Omega_9 = -\Phi$, $\Omega_{10} = \Psi$, $\Omega_{11} = Y$, $\Omega_{12} = -\gamma^2 I$, $\Omega_{13} = PD_1$, $\Omega_{14} = SD_1$, $\Omega_{15} = D_2$, $\Omega_{16} = -P$, $\Omega_{17} = -S$, $\Omega_{18} = -\varepsilon_1^{-1}S$, $\Omega_{19} = -\Psi$, $\Omega_{20} = -\bar{\beta}^{-1}\bar{\theta}^{-1}S$, $\Omega_{21} = -I$.

$$PB = B\bar{P}, \tag{35}$$

$$K = V\Sigma^{-1}P_1^{-1}\Sigma V^{\mathrm{T}}X, \quad L = S^{-1}Y. \tag{36}$$

Proof. Because (30) is not an LMI, we need to pre- and post-multiply both side of (30) with matrix $diag\{I, I, I, I, P, S, S, \Psi, S, I\}$ and obtain

$$\begin{bmatrix} \hat{\Omega}_1 & * & * & * & * & * & * & * & * & * \\ 0 & \hat{\Omega}_5 & * & * & * & * & * & * & * & * \\ 0 & 0 & \hat{\Omega}_9 & * & * & * & * & * & * & * \\ 0 & 0 & 0 & \hat{\Omega}_{12} & * & * & * & * & * & * \\ \hat{\Omega}_2 & \hat{\Omega}_6 & 0 & \hat{\Omega}_{13} & \hat{\Omega}_{16} & * & * & * & * & * \\ 0 & \hat{\Omega}_7 & 0 & \hat{\Omega}_{14} & 0 & \hat{\Omega}_{17} & * & * & * & * \\ 0 & \hat{\Omega}_8 & 0 & 0 & 0 & 0 & \hat{\Omega}_{18} & * & * & * \\ \hat{\Omega}_3 & 0 & \hat{\Omega}_{10} & 0 & 0 & 0 & 0 & \hat{\Omega}_{19} & * & * \\ 0 & 0 & \hat{\Omega}_{11} & 0 & 0 & 0 & 0 & 0 & \hat{\Omega}_{20} & * \\ \hat{\Omega}_4 & 0 & 0 & \hat{\Omega}_{15} & 0 & 0 & 0 & 0 & 0 & \hat{\Omega}_{21} \end{bmatrix} < 0, \tag{37}$$

where $\hat{\Omega}_1 = -P$, $\hat{\Omega}_2 = PA + PBK$, $\hat{\Omega}_3 = \Psi C_1$, $\hat{\Omega}_4 = C_3$, $\hat{\Omega}_5 = -S$, $\hat{\Omega}_6 = -PBK$, $\hat{\Omega}_7 = SA - \bar{\beta}SLC_1$, $\hat{\Omega}_8 = SLC_1$, $\hat{\Omega}_9 = -\Phi$, $\hat{\Omega}_{10} = \Psi$, $\hat{\Omega}_{11} = SL$, $\hat{\Omega}_{12} = -\gamma^2 I$, $\hat{\Omega}_{13} = PD_1$, $\hat{\Omega}_{14} = SD_1$, $\hat{\Omega}_{15} = D_2$, $\hat{\Omega}_{16} = -P$, $\hat{\Omega}_{17} = -S$, $\hat{\Omega}_{18} = -\varepsilon_1^{-1}S$, $\hat{\Omega}_{19} = -\Psi$, $\hat{\Omega}_{20} = -\bar{\beta}^{-1}\bar{\theta}^{-1}S$, $\hat{\Omega}_{21} = -I$.

Let $X = \bar{P}K$, $Y = SL$, and combining with (35), we have (34), which means the closed-loop system (19) is exponentially mean-square stable and the H_∞ norm constraint (21) is satisfied. However, it should be noted that (34) has matrix equation constraint.

By Assumption 1, therefore, the column of matrices B and PB are all linearly independent with $\bar{P} > 0$. Hence, if (34) is satisfied, then

$$rank(\bar{P}) \geq rank(B\bar{P}) = rank(PB) \geq rank(B) = m.$$

So, we have

$$K = \bar{P}^{-1}X, \quad L = P^{-1}Y. \tag{38}$$

By Lemma 2 and Lemma 3, we have matrices P_1, P_2, U_1, and U_2, satisfying (22) and (23). The $\bar{P}$ can be computed by (39) from $PB = B\bar{P}$, namely

$$PB = PU^{\mathrm{T}}\begin{bmatrix}\Sigma \\ 0\end{bmatrix}V^{\mathrm{T}} = U^{\mathrm{T}}\begin{bmatrix}\Sigma \\ 0\end{bmatrix}V^{\mathrm{T}}\bar{P} = \begin{bmatrix}U_1 \\ U_2\end{bmatrix}\begin{bmatrix}\Sigma \\ 0\end{bmatrix}V^{\mathrm{T}}\bar{P}. \tag{39}$$

Then, substituting (23) into (39), we have

$$U^{\mathrm{T}}\begin{bmatrix}P_1 & 0 \\ 0 & P_2\end{bmatrix}\begin{bmatrix}\Sigma \\ 0\end{bmatrix}V^{\mathrm{T}} = U^{\mathrm{T}}\begin{bmatrix}\Sigma \\ 0\end{bmatrix}V^{\mathrm{T}}\bar{P}, \tag{40}$$

which implies that

$$P_1\Sigma V^{\mathrm{T}} = \Sigma V^{\mathrm{T}}\bar{P}. \tag{41}$$

Therefore, the problem of matrix equation constraint is solved by using (23). Then, by (23) and (41), we can obtain (36). This completes the proof. □

Therefore, the optimal H_∞ control problem can be solved by

$$\min_{P_1>0, P_2>0, S>0, X, Y} \gamma \quad s.t.\ (23)\ and\ (34). \tag{42}$$

4. Numerical Simulation

In this section, numerical simulations are used to demonstrate the effectiveness of the proposed H_∞ control method. Consider the transmission power $P_s = 1.5$, the AWGN power $\sigma^2 = 1.0$, and the network parameter $\xi = 3$. Then, the probability of inherent randomly packet dropouts caused by external disturbance, limited channel capacity, and channel noise can be calculated as 0.0850. By choosing the attack power of DoS jammer $p_a = 1.7500$, the probability of packet dropouts caused by attacks increases to 0.5034.

(1) Consider an uninterruptible power system (UPS) with 1KVA. Its discrete-time model (1) can be described with 10 ms at half-load operating point in the following [46]

$$A = \begin{bmatrix} 0.9226 & -0.6330 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix},$$

$$C_1 = \begin{bmatrix} 23.7380 & 20.2870 & 0 \end{bmatrix}, C_2 = \begin{bmatrix} 0.1 & 0 & 0 \end{bmatrix}, D_1 = \begin{bmatrix} 0.5 & 0 & 2 \end{bmatrix}^{\mathrm{T}}, D_2 = 0.1.$$

We chose the initial conditions as $x(0) = \begin{bmatrix} 1 & -1 & 0 \end{bmatrix}^{\mathrm{T}}$, $\hat{x}(0) = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}}$. Let $\gamma = 1$, by using the H_∞ control method, we can obtain that

$$\Psi = 12.2804, \Phi = 3.9826,$$
$$K = \begin{bmatrix} -0.0037 & -0.0035 & -0.0054 \end{bmatrix}, L = \begin{bmatrix} 0.1512 & 0.5958 & -0.7268 \end{bmatrix}^{\mathrm{T}}.$$

Figure 2 shows the norm of states for the UPS encountering stealthy DoS jamming attacks, which indicates that the proposed H_∞ control method can achieve the control objective successfully and effectively. Figure 3 shows switch times of the HTM. Figure 4 shows times of the DoS jamming attacks on the wireless channel.

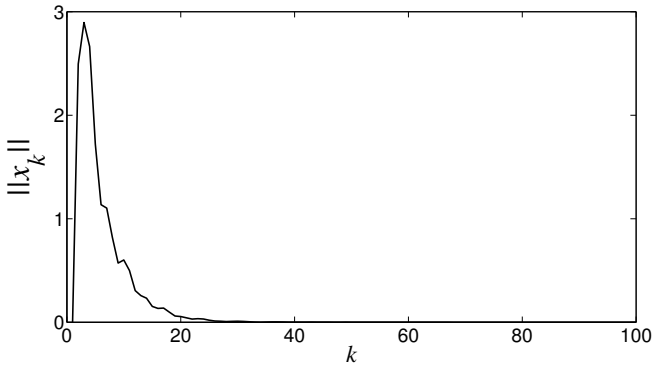

Figure 2. Norm of states for the UPS encountering stealthy DoS jamming attacks when $\gamma = 1$.

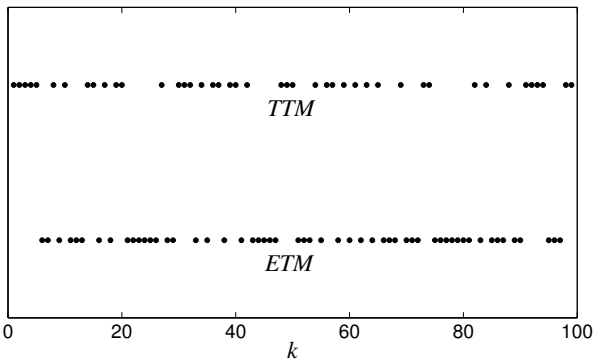

Figure 3. Switch times of the HTM.

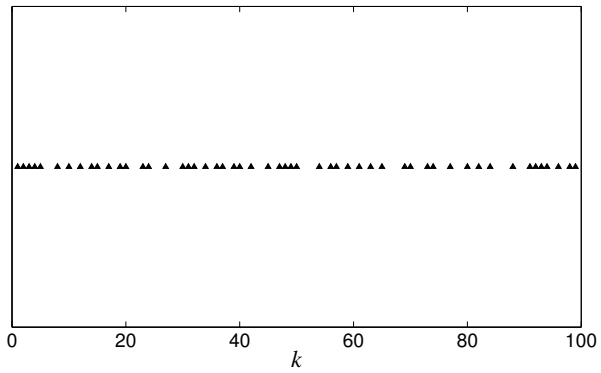

Figure 4. Times of DoS jamming attacks.

(2) Consider a tunnel diode circuit in the following [47]

$$A = \begin{bmatrix} 0.9887 & 0.9024 \\ -0.0180 & 0.8100 \end{bmatrix}, B = \begin{bmatrix} 0.0093 \\ -0.0181 \end{bmatrix},$$
$$C_1 = \begin{bmatrix} 1 & 0 \end{bmatrix}, C_2 = \begin{bmatrix} 1 & 0 \end{bmatrix}, D_1 = \begin{bmatrix} 1 & 1 \end{bmatrix}^{\mathrm{T}}, D_2 = 1.$$

We chose the initial conditions as $x(0) = \begin{bmatrix} 0.1 & -0.1 \end{bmatrix}^{\mathrm{T}}$, $\hat{x}(0) = \begin{bmatrix} 0 & 0 \end{bmatrix}^{\mathrm{T}}$. Let $\gamma = 1$, by using the H_∞ control method, we can obtain that

$$\Psi = 9.0342, \Phi = 3.3312,$$
$$K = 0.1 - 5 \times \begin{bmatrix} 0.2683 & -0.3196 \end{bmatrix}, L = \begin{bmatrix} -5.8106 & 4.6382 \end{bmatrix}^{\mathrm{T}}.$$

Figure 5 shows the norm of states for the tunnel diode circuit encountering stealthy DoS jamming attacks, which indicates that the proposed H_∞ control method can achieve the control objective successfully and effectively. Figure 6 shows switch times of the HTM. Figure 7 shows times of the DoS jamming attacks on the wireless channel.

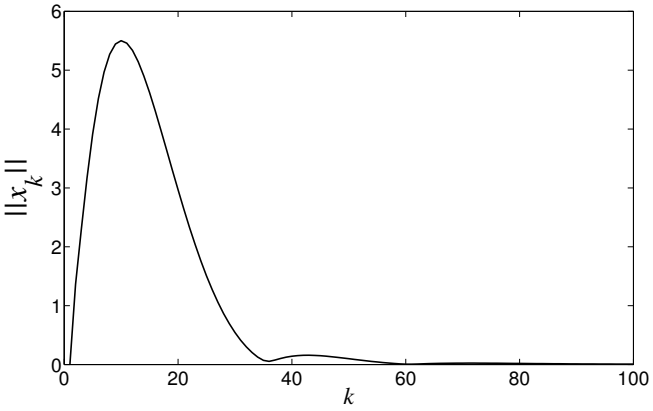

Figure 5. Norm of states for the tunnel diode circuit encountering stealthy DoS jamming attacks when $\gamma = 1$.

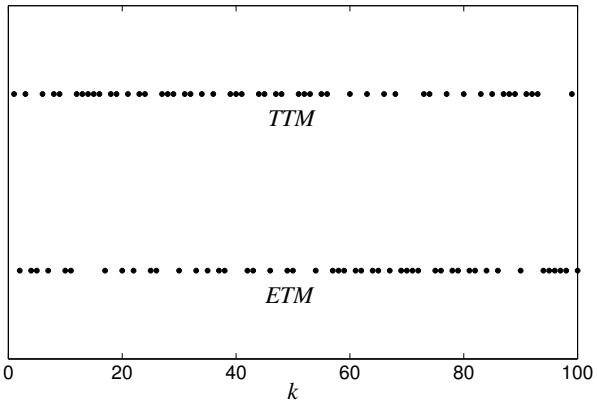

Figure 6. Switch times of the HTM.

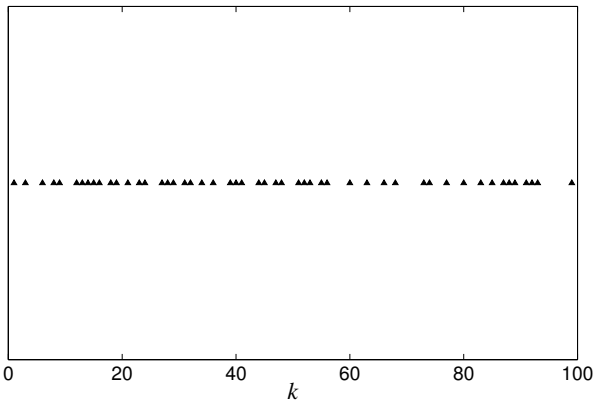

Figure 7. Times of DoS jamming attacks.

5. Conclusions

In this paper, considering the external disturbance, limited channel capacity, and channel noise, a H_∞ controller designing problem was studied for an ICPS with HTM encountering stealthy DoS jamming attacks. A closed-loop system was established based on a compensation mechanism, which compensates the impacts of stealthy DoS jamming attacks and inherent random packet dropouts. We proved that the closed-loop system is mean square exponentially stable and can achieve the desired H_∞ disturbance rejection level, and simulation results shown the effectiveness of the H_∞ control method. In the future, we will study the controller designing problem for industrial scenarios which deployed intrusion detection systems and industrial protocol enhancement methods, and the relationship between system security and operating efficiency will be further discussed.

Author Contributions: Conceptualization, M.W. and J.W.; methodology, M.W. and Y.G.; software, M.W. and K.L.; validation, M.W., Y.G. and X.C.; formal analysis, M.W., Y.G. and J.W.; investigation, K.L., X.C. and Q.W.; writing—original draft preparation, M.W., Y.G. and J.W.; writing—review and editing, M.W. and Q.W.; supervision, J.W. and Q.W.; project administration, M.W., J.W. and X.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Funds of the National Natural Science Foundation of China (No. 61972345), the Natural Science Foundation of Zhejiang (No. LZ22F030010), the National Natural Science Foundation of China-Guangdong big data Science Center Project (No. U1911401), the Fundamental Research Funds for the Central Universities (Zhejiang University NGICS Platform) (No. K20210001).

Institutional Review Board Statement: This study did not require ethical approval.

Informed Consent Statement: This study did not involve humans

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4. [CrossRef]
2. Derler, P.; Lee, E.A.; Vincentelli, A.S. Modeling Cyber-Physical Systems. *Proc. IEEE* **2012**, *100*, 13–28. [CrossRef]
3. Kim, K.; Kumar, P.R. Cyber-Physical Systems: A Perspective at the Centennial. *Proc. IEEE* **2012**, *100*, 1287–1308. [CrossRef]
4. Wolf, M.; Serpanos, D. Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. *Proc. IEEE* **2018**, *106*, 9–20. [CrossRef]
5. Mo, L.; You, P.C.; Cao, X.H.; Song, Y.Q.; Kritikakou, A. Event-driven joint mobile actuators scheduling and control in Cyber-Physical Systems. *IEEE Trans. Ind. Inform.* **2019**, *15*, 5877–5891. [CrossRef]
6. Mo, Y.L.; Kim, T.H.J.; Brancik, K.; Dickinson, D.; Lee, H.; Perrig, A.; Sinopoli, B. Cyber-Physical Security of a Smart Grid Infrastructure. *Proc. IEEE* **2012**, *100*, 195–209. [CrossRef]
7. Liu, Y.G.; Xu, B.G.; Ding, Y.H. Convergence Analysis of Cooperative Braking Control for Interconnected Vehicle Systems. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 1894–1906. [CrossRef]
8. Razmara, M.; Bharati, G.R.; Shahbakhti, M.; Paudyal, S.; Robinett, R.D. Bilevel Optimization Framework for Smart Building-to-Grid Systems. *IEEE Trans. Smart Grid* **2018**, *9*, 582–593. [CrossRef]
9. Khan, M.T.; Serpanos, D.; Shrobe, H. ARMET: Behavior-Based Secure and Resilient Industrial Control Systems. *Proc. IEEE* **2018**, *106*, 129–143. [CrossRef]
10. Farwell, J.P.; Rohozinski, R. Stuxnet and the Future of Cyber War. *Survival* **2011**, *53*, 23–40. [CrossRef]
11. Iasiello, E. Cyber attack: A dull tool to shape foreign policy. In Proceedings of the 5th International Conference on Cyber Conflict, Tallinn, Estonia, 4–7 June 2013; pp. 1–18. [CrossRef]
12. Petrenko, A.S.; Petrenko, S.A.; Makoveichuk, K.A.; Chetyrbok, P.V. Protection model of PCS of subway from attacks type wanna cry, petya and bad rabbit IoT. In Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, Moscow and St. Petersburg, Russia, 29 January–1 February 2018; pp. 945–949. [CrossRef]
13. Mo, Y.; Sinopoli, B. On the Performance Degradation of Cyber-Physical Systems Under Stealthy Integrity Attacks. *IEEE Trans. Autom. Control* **2016**, *61*, 2618–2624. [CrossRef]
14. Ma, R.K.; Cheng, P.; Zhang, Z.Y.; Liu, W.W.; Wang, Q.X.; Wei, Q. Stealthy Attack Against Redundant Controller Architecture of Industrial Cyber-Physical System. *IEEE Internet Things J.* **2019**, *6*, 9783–9793. [CrossRef]
15. Wang, D.; Wang, Z.; Shen, B.; Alsaadi, F.E.; Hayat, T. Recent advances on filtering and control for cyber-physical systems under security and resource constraints. *J. Frankl. Inst.* **2016**, *353*, 2451–2466. [CrossRef]
16. Cárdenas, A.A.; Amin, S.; Sastry, S. Secure Control: Towards Survivable Cyber-Physical Systems. In Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 495–500. [CrossRef]
17. Teixeira, A.; Pérez, D.; Sandberg, H.; Johansson, K.H. Attack Models and Scenarios for Networked Control Systems. In Proceedings of the 1st International Conference on High Confidence Networked Systems, Beijing, China, 17–18 April 2012; pp. 55–64. [CrossRef]
18. Lee, P.; Clark, A.; Bushnell, L.; Poovendran, R. A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems. *IEEE Trans. Autom. Control* **2014**, *59*, 3224–3237. [CrossRef]
19. Lu, A.Y.; Yang, G.H. Distributed consensus control for multi-agent systems under denial-of-service. *Inf. Sci.* **2018**, *439–440*, 95–107. [CrossRef]
20. Zhang, X.M.; Han, Q.L.; Ge, X.H. A novel approach to H_∞ performance analysis of discrete-time networked systems subject to network-induced delays and malicious packet dropouts. *Automatica* **2022**, *136*, 110010. [CrossRef]
21. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 245–257. [CrossRef]
22. Zhang, H.; Cheng, P.; Shi, L.; Chen, J.M. Optimal Denial-of-Service Attack Scheduling With Energy Constraint. *IEEE Trans. Autom. Control* **2015**, *60*, 3023–3028. [CrossRef]
23. 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]
24. Zhang, X.M.; Han, Q.L.; Ge, X.H.; Ding, L. Resilient Control Design Based on a Sampled-Data Model for a Class of Networked Control Systems Under Denial-of-Service Attacks. *IEEE Trans. Cybern.* **2020**, *50*, 3616–3626. [CrossRef]
25. Foroush, S.H.; Martínez, S. On event-triggered control of linear systems under periodic denial-of-service jamming attacks. In Proceedings of the 51st IEEE Conference on Decision and Control, Maui, HI, USA, 10–13 December 2012; pp. 2551–2556. [CrossRef]
26. Xu, W.Y.; Ma, K.; Trappe, W.; Zhang, Y.Y. Jamming sensor networks: Attack and defense strategies. *IEEE Netw.* **2006**, *20*, 41–47. [CrossRef]
27. Li, M.Y.; Koutsopoulos, I.; Poovendran, R. Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks. *IEEE Trans. Mobile Comput.* **2010**, *9*, 1119–1133. [CrossRef]
28. Wang, M.F.; Xu, B.G. Guaranteed cost control of cyber-physical systems with packet dropouts under DoS jamming attacks. *Asian J. Control* **2020**, *22*, 1659–1669. [CrossRef]

29. Zhang, H.; Cheng, P.; Shi, L.; Chen, J.M. Optimal DoS Attack Scheduling in Wireless Networked Control System. *IEEE Trans. Control Syst. Technol.* **2016**, *24*, 843–852. [CrossRef]
30. Ding, K.M.; Li, Y.Z.; Quevedo, D.E.; Dey, S.; Shi, L. A multi-channel transmission schedule for remote state estimation under DoS attacks. *Automatica* **2017**, *78*, 194–201. [CrossRef]
31. Ding, D.R.; Wang, Z.D.; Wei, G.L.; Alsaadi, F.E. Event-based security control for discrete-time stochastic systems. *IET Control Theory Appl.* **2016**, *10*, 1808–1815. [CrossRef]
32. Amin, S.; Cárdenas, A.A.; Sastry, S.S. Safe and Secure Networked Control Systems under Denial-of-Service Attacks. In *Proceedings of the International Workshop on Hybrid Systems: Computation and Control*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 31–45. [CrossRef]
33. Wang, M.F.; Liu, Y.G.; Xu, B.G. Observer-based H_∞ control for cyber-physical systems encountering DoS jamming attacks: An attack–tolerant approach. *ISA Trans.* **2020**, *14*, 1–14. [CrossRef]
34. Wang, Z.D.; Yang, F.W.; Ho, D.W.C.; Liu, X.H. Robust H_∞ Control for Networked Systems With Random Packet Losses. *IEEE Trans. Syst. Man Cybern.-Part B (Cybern.)* **2007**, *37*, 916–924. [CrossRef]
35. Mo, L.; Cao, X.H.; Song, Y.Q.; Kritikakou, A. Distributed Node Coordination for Real-Time Energy-Constrained Control in Wireless Sensor and Actuator Networks. *IEEE Internet Things J.* **2018**, *5*, 4151–4163. [CrossRef]
36. Cheng, J.; Park, J.H.; Cao, J.D.; Qi, W.H. Hidden Markov Model-Based Nonfragile State Estimation of Switched Neural Network With Probabilistic Quantized Outputs. *IEEE Trans. Cybern.* **2020**, *50*, 1900–1909. . [CrossRef]
37. Liu, X.L.; Lin, W.; Zhao, C.R.; Hu, Y.H. Digital control of a family of time-delay feedforward systems with sparse sampling. *Syst. Control Lett.* **2022**, *163*, 105200. [CrossRef]
38. Wu, J.; Chen, T.W. Design of Networked Control Systems With Packet Dropouts. *IEEE Trans. Autom. Control* **2007**, *52*, 1314–1319. [CrossRef]
39. Xiong, J.; Lam, J. Stabilization of linear systems over networks with bounded packet loss. *Automatica* **2007**, *43*, 80–87. [CrossRef]
40. Liu, J.L.; Zha, L.J.; Cao, J.; Fei, S.M. Hybrid-driven-based stabilisation for networked control systems. *IET Control Theory Appl.* **2016**, *10*, 2279–2285. [CrossRef]
41. Wang, S.Y.; Wang, Z.D.; Dong, H.L.; Chen, Y. Distributed State Estimation Under Random Parameters and Dynamic Quantizations Over Sensor Networks: A Dynamic Event-Based Approach. *IEEE Trans. Signal Inf. Process. Netw.* **2020**, *6*, 732–743. [CrossRef]
42. Wang, M.F.; Liu, K.; Wang, J.P.; Wang, M.Z.; Zhao, Z.J.; Xu, C. H_∞ Control for Industrial Cyber-Physical Systems Encountering Reactive DoS Jamming Attacks. In Proceedings of the 39th Chinese Control Conference, Shenyang, China, 27–29 July 2020; pp. 4328–4333. [CrossRef]
43. Proakis, J.; Salehi, M. *Digital Communications*, 5th ed.; McGraw-Hill: New York, NY, USA, 2007.
44. Li, Y.Z.; Quevedo, D.E.; Dey, S.; Shi, L. SINR-Based DoS Attack on Remote State Estimation: A Game-Theoretic Approach. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 632–642. [CrossRef]
45. Tarn, T.J.; Rasis, Y. Observers for nonlinear stochastic systems. *IEEE Trans. Autom. Control* **1976**, *21*, 441–448. [CrossRef]
46. Yang, F.W.; Wang, Z.D.; Hung, Y.S.; Gani, M. H_∞ control for networked systems with random communication delays. *IEEE Trans. Autom. Control* **2006**, *51*, 511–518. [CrossRef]
47. Wan, J.; Hu, Z.R.; Cai, J.P.; Luo, Y.X.; Mei, C.L.; Han, A.T. Non-fragile dissipative filtering of cyber–physical systems with random sensor delays. *ISA Trans.* **2020**, *104*, 115–121. [CrossRef]