Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 5412170, 9 pages
https://doi.org/10.1155/2020/5412170

Research Article

Static Output Feedback Predictive Control for Cyber-Physical System under Denial of Service Attacks

Zhiwen Wang,[1,2,3] Xiaoping Wang,[1] Hongtao Sun,[4] and Peng Xin[1]

[1] *College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou 730050, China*
[2] *Key Laboratory of Gansu Advanced Control for Industrial Processes, Lanzhou University of Technology, Lanzhou 730050, China*
[3] *National Demonstration Centre for Experimental Electrical and Control Engineering Education, Lanzhou University of Technology, Lanzhou 730050, China*
[4] *College of Engineering, Qufu Normal University, Qufu 273100, China*

Correspondence should be addressed to Zhiwen Wang; wwwangzhiwen@163.com

Received 21 March 2020; Revised 19 July 2020; Accepted 10 August 2020; Published 31 August 2020

Academic Editor: Laurent Dewasme

This paper addresses the static output feedback predictive (SOFP) control problem with cyber-physical system (CPS) subject to Denial-of-Service (DoS) attacks. The effects of DoS attacks are reasonably assumed to the bounded consecutive packet dropouts by considering the energy constraints of an attacker. Then, a novel predictive control sequence, in which only the latest successfully received output is employed, is designed to compensate such packet dropouts caused by DoS attacks. Furthermore, the stability criterion and predictive control design are carefully derived by using the switching Lyapunov functional approach and linear matrix inequality. Compared with the previous works, the proposed predictive control strategy can compensate arbitrary packet dropouts under DoS attacks while only the latest successfully received output is available. At last, a simulation example illustrates the effectiveness of the SOFP control strategy.

1. Introduction

The rapid development of CPS is attributed to the strong integration among computation, communication, and control technology, in which CPS has received considerable attention in the past decades. Taking advantage of low cost and flexible network architecture, it has been widely applied in some engineering fields such as smart grid, healthcare, and water/gas distribution and industrial process control [1–3].

Due to the capacity of connecting deeply integration physical plants and cyber elements in an unprecedented way, CPS offers ample opportunities for malicious threats to launch attacks. The applications of next-generation information technologies such as big data, cloud computing, and Internet of Things greatly provide performance improvements for physical systems but at the same time introduce more risks which make physical isolation more difficult to implement. Therefore, how to ensure the safe operation and preserve the control performance under malicious attacks are the basic security issues in CPS. In fact, CPS has realized more complex and high-risk industrial process control through the transmission of information in the heterogeneous network [4]. However, the vulnerability of open communication networks, as the key components of society safety-critical infrastructures in CPS, increases the severity of such malicious cyber-attacks in [5], which can menace the control systems. There have been an increasing number of cyber-attacks on power grids reported worldwide. For instance, a devastating cyber-attack on the power station brought down the information flow from the physical process to the remote management system, which plunges 225,000 people into blackout in Ukraine [6]. Besides, the "Stuxnet", an advanced computer worm virus, intruded the nuclear facility and caused severe damage in Iran [7]. These facts show the serious economic loss and severe social detriment attacked by malicious network in CPS, which has attracted extensive attention of many scholars [8–10].

The typical network attacks in CPS are categorized as deceptive attack, false data injection attack and DoS attack in [11]. The DoS attack, a more reachable attack pattern, prevents the exchange of information for the adversary, while the false data injection attack affects the data integrity of packets by modifying their payloads in [12]. The essence of DoS attack is that the measurement state or the control signal transmitted through the wireless communication network is blocked, which results in the fact that the information update is not timely and complete. Thus, the DoS attack focuses on deteriorating the system performance and even leads to system instability. One of the main issues under DoS attacks in CPS is the packet dropout phenomenon [13]. It should be pointed out that information data can be transmitted in a "packet", which implies sending a sequence of control prediction in one data packet and then selecting the appropriate one corresponding to the current network condition to compensate the packet dropout. In this case, the SOFP control strategy has been proposed in this paper.

In many existing works, various efforts have been devoted to the security control influenced by DoS attacks. Some of the literatures focused on the effects of network-induced delays. Many methods for the delay issue have been done in [14–16]. Some other literatures show that a large number of the approaches have been investigated to alleviate the severe impact influenced by packet dropouts. A defence strategy is proposed to deal with the information flow which congests the transmission signal between the sensor and the controller against DoS attacks on the multichannel CPS in [17]. In addition, some necessary scheduling algorithms are proposed to ensure transmission security when control plants can gain access to the network at each sampling instant because of the limitation of network bandwidth. If there is no optimal scheduling algorithm in CPS design, the packet dropout in smaller sampling frequency should be considered. That is, it not only ensures the system is schedulable and guarantees that the overall CPS is stable. Then, the relationship based applicable scheduling algorithm design between the packet dropout rate and the stability of the closed-loop system should be established, and the corresponding controllers design procedures to make the closed-loop system stability should be given. As stated in [18–20], such as the stochastic system and the switching system method, some effective strategies are employed to address the model and control issues with packet dropout. The networked system with arbitrary and finite packet loss is modelled as a switching system, and the design control method of state feedback is proposed in [21]. Furthermore, by using the measured output information, a token-dependent static output feedback SMC is designed in [22]. By only considering attacks in the backward channels in [23, 24], the security control is established to address attack-induced severe packet dropout. Notice that both-side communication with arbitrary packet dropout caused by attacks is more realistic in the practical attack pattern and the state feedback controller is given in [25].

Motivated by the fact that not all states are available and only the latest received output measurements can be obtained at the controller, the SOFP control strategy is proposed to deal with the security control problem. In contrast with the existing results, the main contributions of this paper can be summarised as follows:

(1) A novel switching system model is established to characterize the security properties of CPS under DoS attacks. Different from [26], only limited output measurements are used to design the security controller in this paper.

(2) Only the latest received measurements are used to design the proposed predictive control gains. Compared with traditional model predictive control methods, the proposed security control strategy will predict their future control gains rather than state prediction.

The remainder of this paper is organized as follows. Section 2 gives the problem formulations with the proposed SOFP control strategy by considering the energy-limited DoS attacks. Section 3 is presented in the security analysis, which infers the stability criterion to guarantee the security performance. The SOFP controller is designed in Section 4, and a simulation example is shown in Section 5 to illustrate the feasibility of the desired controller. And finally, Section 6 concludes this paper.

Notation: R^n and R^m denote the n-dimensional and m-dimensional Euclidean space, respectively. $R^{n\times m}$ is the set of $n\times m$ real matrices. The superscript "T" stands for matrix transposition. The notation $X>0$ means that the matrix X is real symmetric positive definite.

2. Problem Formulations

2.1. System Framework. The structure of SOFP control considered in this paper is shown in Figure 1, where the studied CPS is composed by the sensor, controller, buffer, and actuator. The SOFP control strategy against attack-induced severe packet dropout is that the controller receives all the measurement outputs from sensor and calculates the sequence of control inputs, which transmits to the buffer simultaneously. Then, the actuator selects the corresponding control value from $[u(t_h)^T, u(t_h+1)^T, \cdots, u(t_h+\tau)^T]^T$ and delivers appropriate control inputs to the plant, which can compensate the arbitrary packet dropouts caused by DoS attacks.

Consider a discrete-time linear system described by

$$\begin{cases} x(t+1) = Ax(t) + Bu(t), \\ y(t) = Cx(t), \end{cases} \tag{1}$$

where $t+1 \triangleq (t+1)T$, T represents the sampling period, $x(t) \in R^n$ and $u(t) \in R^m$ are the system state and control input, respectively, and A,B are real matrices of appropriate dimensions.

To make the proposed method more suitable for practical network attacks, the DoS attacks behaviours considered energy constraints are presented as

$$H_n := \{h_n\} \cup [h_n, h_n+\tau], \tag{2}$$

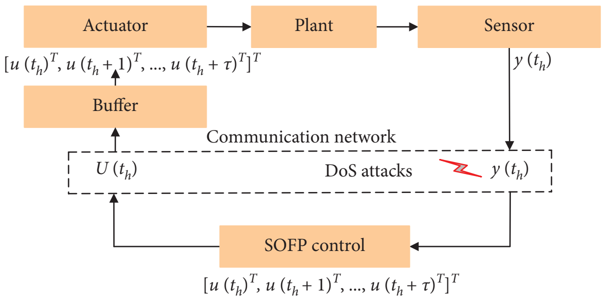

Figure 1: Structure of the SOFP control under DoS attacks.

where τ is the attack duration and h_n is the instant transition time of the attack state.

As shown in Figure 2, "↑" denotes that the DoS is converted to the attack state and "↓" indicates that the DoS is the end of the attack process. When $\tau \in R \geq 0$, the DoS launches a limited attack with the duration of τ ($\tau = 0$ is a pulse attack only).

To clearly describe the energy-limited characteristics of DoS attacks in this paper, the following assumption is given.

Assumption 1. The maximum packet dropouts of consecutive DoS attacks are bounded with N.

Remark 1. In practice, the attackers gradually run out of energy because of an inherent characteristic of energy constraints [27]. Based on this reliable fact, it is reasonable to consider that the packet dropouts of consecutive DoS attacks are bounded. Furthermore, to achieve predictive compensation for packet dropout, a data buffer is involved at the controller side to record recently successfully transmitted data packets.

2.2. Switching Model under DoS Attacks. Suppose that the controller latest received the value of process output $y(t_h)$ at time t_h, then the predictive control based on output feedback control law is given by

$$u(t_h+\tau) = G_\tau y(t_h), \tag{3}$$

where $t_h + \tau \triangleq (t_h+\tau)T$, t_h stands for the switching instant time, and $\tau = 0, 1, \cdots, \sigma(t_h)$ is a time-varying switching signal which takes the value in a finite set $\tau \in Z \triangleq \{0, 1, \cdots, N\}$.

The packet-based transmission mechanism in CPS determines that the corresponding control input at time $t_h, t_h+1, \cdots, t_h+\tau$ is $u(t_h), u(t_h+1), \cdots, u(t_h+\tau)$, respectively. It is known that the neighboring two switching points have the following relation:

$$\begin{aligned} t_{h+1} &= t_h + 1 + \sigma(t_h), \\ t_0 &= 0. \end{aligned} \tag{4}$$

Therefore, the evolution law of dynamics can be described by the following $N+1$ cases:

Case 0. DoS-free $(\sigma(t_h) = 0)$:

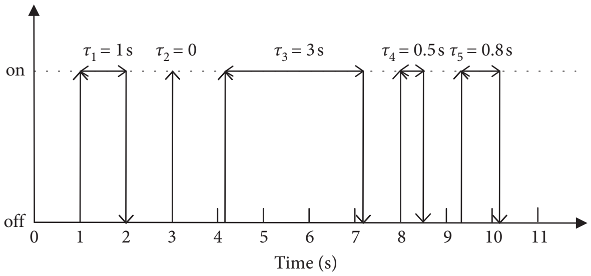

Figure 2: An illustration of the DoS attacks.

$$\begin{aligned} x(t_h+1) &= (A + BG_0C)x(t_h), \\ t_{h+1} &= t_h + 1, \\ x(t_{h+1}) &= x(t_h+1) = \Phi_0 x(t_h), \\ \Phi_0 &\triangleq A + BG_0C. \end{aligned} \tag{5}$$

Case 1. One-step packet dropout $(\sigma(t_h) = 1)$:

$$\begin{aligned} x(t_h+1) &= (A + BG_0C)x(t_h), \\ x(t_h+2) &= Ax(t_h+1) + BG_1Cx(t_h), \\ t_{h+1} &= t_h + 2, \\ x(t_h+1) &= x(t_h+2) = \Phi_1 x(t_h), \\ \Phi_1 &\triangleq A\Phi_0 + BG_1C, \\ &\vdots \end{aligned} \tag{6}$$

Case N: N-steps packets dropouts $(\sigma(t_h) = N)$:

$$\begin{aligned} x(t_h+1) &= (A + BG_0C)x(t_h), \\ x(t_h+2) &= Ax(t_h+1) + BG_1Cx(t_h), \\ &\vdots \\ x(t_{h+1}+N+1) &= x(t_h+N) + BG_NCx(t_h), \\ t_{h+1} &= t_h + N, \\ x(t_h+1) &= x(t_{h+1}+N+1) = \Phi_N x(t_h), \\ \Phi_N &\triangleq A\Phi_{N-1} + BG_NC. \end{aligned} \tag{7}$$

According to (5)–(7), model (1) with SOFP control strategy can be transformed into the following closed-loop system included N-steps packet dropouts:

$$x(t_{h+1}) = \Phi_i x(t_h), \tag{8}$$

where $\Phi_i = A^{i+1} + \sum_{l=0}^{i} A^l BG_{i-l}C$. It illustrates the essential characteristics of the proposed SOFP control strategy, that is, the state is unchanged and the controller gain is changed.

3. Stability Analysis

In this section, the security analysis based SOFP strategy is given with some mathematical derivations. The following necessary definition and lemmas are introduced.

Definition 1. If there are positive scalars c and $\lambda < 1$ such that the following inequality,

$$\|x(t)\| \le c\lambda^{t}\|x(0)\|, \tag{9}$$

holds, the CPS (1) is said to be exponentially stable, where $x(0) \in R^{n}$ is an arbitrary initial value.

Lemma 1 (see [27]). *For an arbitrary matrix $\Psi \in R^{n\times n}$ and an arbitrary vector $x \in R^{n}$, the following inequality,*

$$\lambda_{\min}\|x\| \le \|\Psi x\| \le \lambda_{\max}\|x\|, \tag{10}$$

holds, where $\lambda_{\min}$ and $\lambda_{\max}$ are the minimum singular value and the maximum singular value, respectively, of Ψ.

Based on the above, the following theorem gives criteria for system exponentially stable with arbitrary switching characteristics under DoS attacks.

Theorem 1. *For some given scalars $0 < \lambda_i < 1$, $\mu > 0$, if there exist matrices $P_i > 0$, such that the following inequalities,*

$$-\lambda_i P_i + \Phi_i^{T} P_i \Phi_i < 0, \tag{11}$$

$$P_{\alpha} < \mu P_{\beta}, \forall \alpha, \beta \in Z \triangleq \{0, 1, \cdots, N\}, \tag{12}$$

$$\rho \triangleq \max\{\lambda_i \mu \mid i \in Z\} < 1, \tag{13}$$

hold, then the system (8) will be exponentially stable with the decay rate $\sqrt[2(N+2)]{\rho}$.

Proof. Choose the following Lyapunov function:

$$V_{\sigma(t_h)}(t_h) = x^{T}(t_h)P_{\sigma(t_h)}x(t_h). \tag{14}$$

Therefore, it is derived from (14) at time t_{h+1} that

$$V_{\sigma(t_h)}(t_{h+1}) = x^{T}(t_{h+1})P_{\sigma(t_h)}x(t_{h+1}). \tag{15}$$

Then, pre- and post-multiplying inequality (11) by $x^{T}(t_h)$ and $x(t_h)$, one has

$$\left[\Phi_{\sigma(t_h)}x(t_h)\right]^{T} P_{\sigma(t_h)}\left[\Phi_{\sigma(t_h)}x(t_h)\right] - \lambda_{\sigma(t_h)}x^{T}(t_h)P_{\sigma(t_h)}x(t_h) < 0. \tag{16}$$

Substituting the function (14) and (15) into (16), we have,

$$V_{\sigma(t_h)}(t_{h+1}) < \lambda_{\sigma(t_h)}V_{\sigma(t_h)}(t_h). \tag{17}$$

Similarly,

$$V_{\sigma(t_{h+1})}(t_{h+2}) < \lambda_{\sigma(t_{h+1})}V_{\sigma(t_{h+1})}(t_{h+1}). \tag{18}$$

Suppose that one-step packet dropout at time t_{h+1} and t_{h+2} caused by DoS attacks, respectively. Thus, we obtain that

$$V_{\sigma(t_{h+1})}(t_{h+1}) = x^{T}(t_{h+1})P_{\sigma(t_{h+1})}x(t_{h+1}), \tag{19}$$

$$V_{\sigma(t_{h+1})}(t_{h+2}) = x^{T}(t_{h+2})P_{\sigma(t_{h+1})}x(t_{h+2}). \tag{20}$$

Utilizing (12) and (18) together leads to

$$\begin{aligned} V_{\sigma(t_{h+2})}(t_{h+2}) &< \mu V_{\sigma(t_{h+1})}(t_{h+2}) < \mu\lambda_{\sigma(t_{h+1})}V_{\sigma(t_{h+1})}(t_{h+1}) \\ &< \mu\lambda_{\sigma(t_{h+1})}\mu V_{\sigma(t_h)}(t_{h+1}) < \mu\lambda_{\sigma(t_{h+1})}\mu\lambda_{\sigma(t_h)}V_{\sigma(t_h)}(t_h). \end{aligned} \tag{21}$$

Define $\rho = \mu\lambda_{\sigma(t_{h+1})}$, then the above law (21) can be written as

$$\begin{aligned} V_{\sigma(t_{h+2})}(t_{h+2}) &< \rho V_{\sigma(t_{h+1})}(t_{h+1}) < \rho^{2}V_{\sigma(t_h)}(t_h) < \cdots \\ &< \rho^{t+1}V_{\sigma(t_1)}(t_1) < \rho^{t+2}V_{\sigma(t_0)}(t_0). \end{aligned} \tag{22}$$

Then, it is concluded from (13) and (14) that

$$\lim_{t\longrightarrow\infty} x(t_h) = 0. \tag{23}$$

which implies that the system will be stable in $\{x(t)\}$.

Notice that the system should not only be stable in the discrete regions $\{x(t)\}$ but also converge to the subset $\left\{x(t_{d,h})\right\}$ after dT sampling periods.

Therefore, by Lemma 1, we obtain by induction that the following inequality holds:

$$\left\|x\left(t_{d,h}\right)\right\| \le \xi\left\|x(t_h)\right\|, \tag{24}$$

where $\xi \triangleq \max\{\sigma_{\max}(\Phi_i) \mid i = 0, 1, \cdots, N-1\}$. It means that the upper bounded value of $\|x(t_{d,h})\|$ is $\xi\|x(t_h)\|$. Thus,

$$\lim_{t\longrightarrow\infty} x\left(t_{d,h}\right) = 0. \tag{25}$$

Based on the above analysis, the closed-loop switching system (8) tends to be exponentially stable and then the exponential decay rate is obtained.

It is deduced from (19) that

$$V_{\sigma(t_{h+2})}(t_{h+2}) = x^{T}(t_{h+2})P_{\sigma(t_{h+2})}x(t_{h+2}). \tag{26}$$

Further, it is easy to see that

$$V_{\sigma(t_{h+2})}(t_{h+2}) = x^{T}(t_{h+2})P_{\sigma(t_{h+2})}x(t_{h+2}) \ge \eta_1\left\|x((t_{h+2})\right\|^{2}. \tag{27}$$

It is derived from (22) that

$$\begin{aligned} \eta_1\|x(t_{h+2})\|^{2} &\le \rho V_{\sigma(t_{h+1})}(t_{h+1}) < \rho^{2}V_{\sigma(t_h)}(t_h) < \cdots \\ &< \rho^{t+2}V_{\sigma(t_0)}(t_0) \le \rho^{t+2}\eta_2\|x(0)\|^{2}, \end{aligned} \tag{28}$$

where η_1 and η_2 are the minimum singular value and the maximum singular value, respectively, of P.

Therefore, it is easy to know from (28) that

$$\left\|x(t_{h+2})\right\| < (\sqrt{\rho})^{t+2}\sqrt{\left(\frac{\eta_2}{\eta_1}\right)}\|x(0)\|^{2}. \tag{29}$$

Substituting (24) into (29), it can be found that

$$\left\|x\left(t_{d,h+2}\right)\right\| \le \left\|x(t_{h+2})\right\| < \xi(\sqrt{\rho})^{t+2}\sqrt{\left(\frac{\eta_2}{\eta_1}\right)}\|x(0)\|^{2}. \tag{30}$$

Meanwhile, $t_{d,h+2}$, t_{h+2}, and $t+2$ have the following relations:

$$t_{h+2} \leq (N+1)(t+2). \tag{31}$$

$$t_{d,h+2} \leq (N+1)(t+2) + N \leq (N+2)(t+2), \tag{32}$$

where $h + 2 \geq N$.

It is clearly deduced from (31) and (32) that

$$\frac{t_{h+2}}{(N+1)} \leq t + 2. \tag{33}$$

Because of $\rho < 1$, the following inequalities hold.

$$\left\| x\left(t_{h+2}\right) \right\| < \left(\sqrt[2(N+1)]{\rho}\right)^{t_{h+2}} \sqrt{\left(\frac{\eta_2}{\eta_1}\right)} \| x(0) \|^2, \tag{34}$$

$$\left\| x\left(t_{d,h+2}\right) \right\| < \xi \left(\sqrt[2(N+2)]{\rho}\right)^{t_{d,h+2}} \sqrt{\left(\frac{\eta_2}{\eta_1}\right)} \| x(0) \|^2, \tag{35}$$

where $h + 2 \geq N$.

Finally, we can further obtain from (34) and (35) that, for an arbitrary instant time t, the following inequality,

$$\| x(t) \| < \xi \left(\sqrt[2(N+2)]{\rho}\right)^{t} \sqrt{\left(\frac{\eta_2}{\eta_1}\right)} \| x(0) \|^2, \tag{36}$$

holds. The proof is thus completed. □

4. Control Design of SOFP

In this section, the SOFP control sequence based on Theorem 1 is derived below.

Theorem 2. *For given scalars $0 < \lambda_i < 1$, $\mu > 0$, if there exist matrices X, Ω_i, and $P_i > 0$, such that the following inequalities,*

$$\begin{bmatrix} -\lambda_i \Omega_i & * \\ \Xi & -X - X^T + \Omega_i \end{bmatrix} < 0, \tag{37}$$

$$\Omega_\alpha < \mu \Omega_\beta, \quad \forall \alpha, \beta \in Z \triangleq \{0, 1, \cdots, N\}, \tag{38}$$

$$\rho \triangleq \max\{\lambda_i \mu \mid i \in Z\} < 1, \tag{39}$$

where $\Xi = (A^{i+1} + \sum_{l=0}^{i} A^l B G_{i-l} C) X$, hold, then the system (8) will be exponentially stable with the decay rate $\sqrt[2(N+2)]{\rho}$.

Proof. According to the stability condition of the discrete-time linear system, for matrices A, $P > 0$, the following inequality,

$$A^T P A - P < 0, \tag{40}$$

holds, if and only if there exists a matrix Ψ such that

$$\begin{bmatrix} -P & * \\ \Psi A & -\Psi - \Psi^T + P \end{bmatrix} < 0. \tag{41}$$

Therefore, the inequality (11) will be held if there exists a matrix Ψ such that the following inequality,

$$\begin{bmatrix} -\lambda_i P_i & * \\ \Psi \Phi_i & -\Psi - \Psi^T + P_i \end{bmatrix} < 0, \tag{42}$$

holds. Based on this fact, the controller can be easily obtained below.

Define $X = \Psi^{-1}$and $\Omega_i = X^T P_i X$. Then pre- and post-multiplying inequality (42) by $\operatorname{diag}\{\Psi^{-T}, \Psi^{-T}\}$ and $\Omega_i = X^T P_i X$ (notice from (41) that the matrix Ψ is invertible), one has

$$\begin{bmatrix} -\lambda_i \Omega_i & * \\ \Phi_i X & -X - X^T + \Omega_i \end{bmatrix} < 0. \tag{43}$$

Substituting (5)–(7) into (43),

$$\begin{bmatrix} -\lambda_i \Omega_i & * \\ \left(A^{i+1} + \sum_{l=0}^{i} A^l B G_{i-l} C\right) X & -X - X^T + \Omega_i \end{bmatrix} < 0. \tag{44}$$

It can be found that the inequalities (44) and (37) in Theorem 2 are equivalent.

Meanwhile, the inequality (38) in Theorem 2 is derived by pre- and post-multiplying X^T, X for $P_\alpha < \mu P_\beta, \forall \alpha, \beta \in Z$. This completes the proof.

However, the above inequalities still cannot be solved due to the coupling nonlinear item ABGCX. In order to deal with such items, Theorem 3 transformed nonlinear item is presented. □

Theorem 3. *For given scalars $0 < \lambda_i < 1$, $\varepsilon > 0$, if there exist matrices X, Ω_i, and $P_i > 0$, full rank matrix M, and any matrix V of appropriate dimensions such that the following inequalities,*

$$\begin{bmatrix} -\lambda_i \Omega_i & * \\ \tilde{\Xi} & -X - X^T + \Omega_i \end{bmatrix} < 0, \tag{45}$$

$$\begin{cases} \begin{bmatrix} -\varepsilon I & * \\ MC - CX & -I \end{bmatrix} < 0, \\ \varepsilon \longrightarrow 0, \end{cases} \tag{46}$$

where $\tilde{\Xi} = A^{i+1} X + \sum_{l=0}^{i} A^l B V_\tau C, \tau = i - l$, hold, then the system (8) secured by $G_\tau = V_\tau M^{-1}$ will be exponentially stable with the decay rate $\sqrt[2(N+2)]{\rho}$.

Proof. It is deduced from (44) that $C = M^{-1} C X$. By replacing $G_\tau C X$ with $V_\tau C$, we can easily obtain the above result with $G_\tau = V_\tau M^{-1}$ which completes this proof. □

5. Simulation Example

In this section, an inverted pendulum control system is presented to illustrate the proposed security method with the SOFP control strategy. The plant model is described as

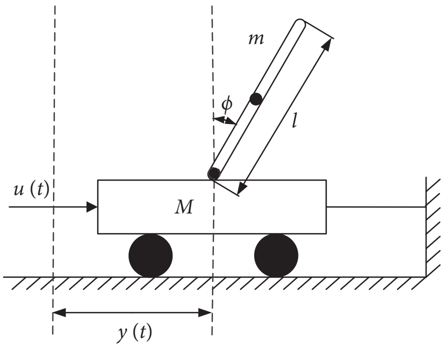

Figure 3: Single inverted pendulum system.

Table 1: Parameters of the inverted pendulum system.

Symbol	Meaning	Value
M	Mass of the cart	1.378 kg
m	Mass of the pendulum	0.051 kg
l	Length of the pendulum	0.25 m
g	Acceleration of gravity	9.8 m/s^2
Φ	Angle from the upright position	—

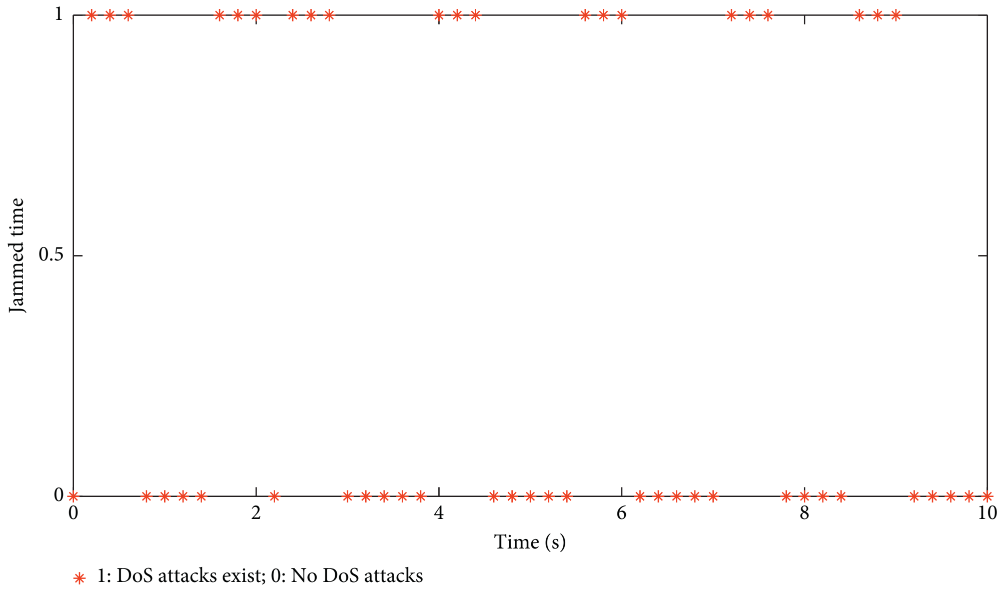

Figure 4: Distribution of DoS attacks.

$$\begin{cases} u = M\dfrac{d^2 y}{dt^2} + m\dfrac{d^2}{dt^2}(y + l\sin\phi), \\ \text{mg}l\ \sin\phi = m\dfrac{d^2}{dt^2}(y + l\sin\phi)l\cos\phi, \end{cases} \tag{47}$$

and the inverted pendulum system is shown in Figure 3.

Based on the above inequality, the initial state variables of the system can be defined as

$$\begin{aligned} x_1 &= y, \\ x_2 &= \phi, \\ x_3 &= \dot{y}, \\ x_4 &= \dot{\phi}. \end{aligned} \tag{48}$$

To make the description simpler, the inverted pendulum control system takes the following parameters, which are given in Table 1.

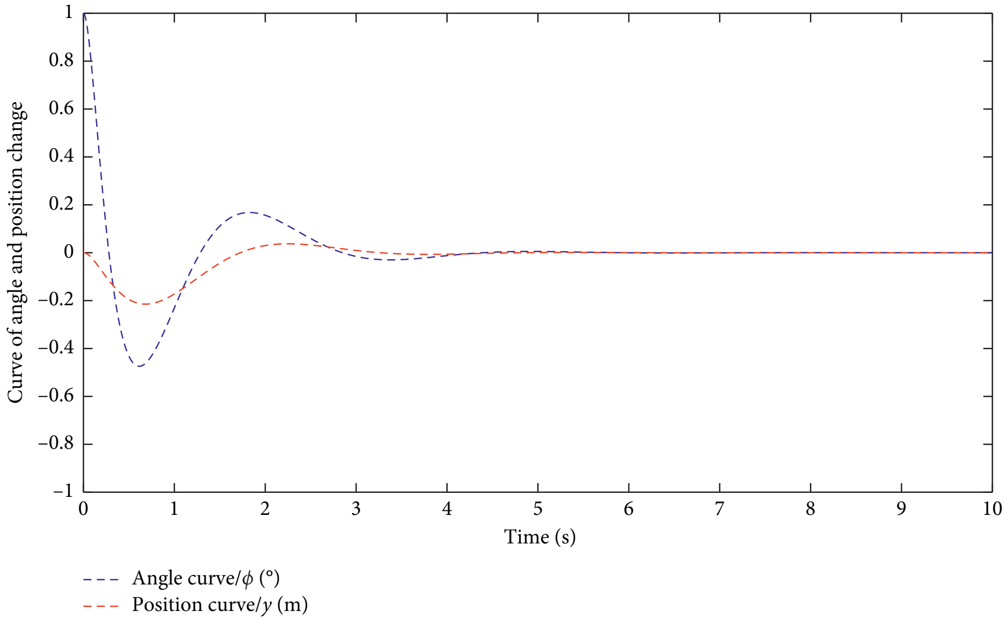

Figure 5: State responses of CPS with DoS-free case.

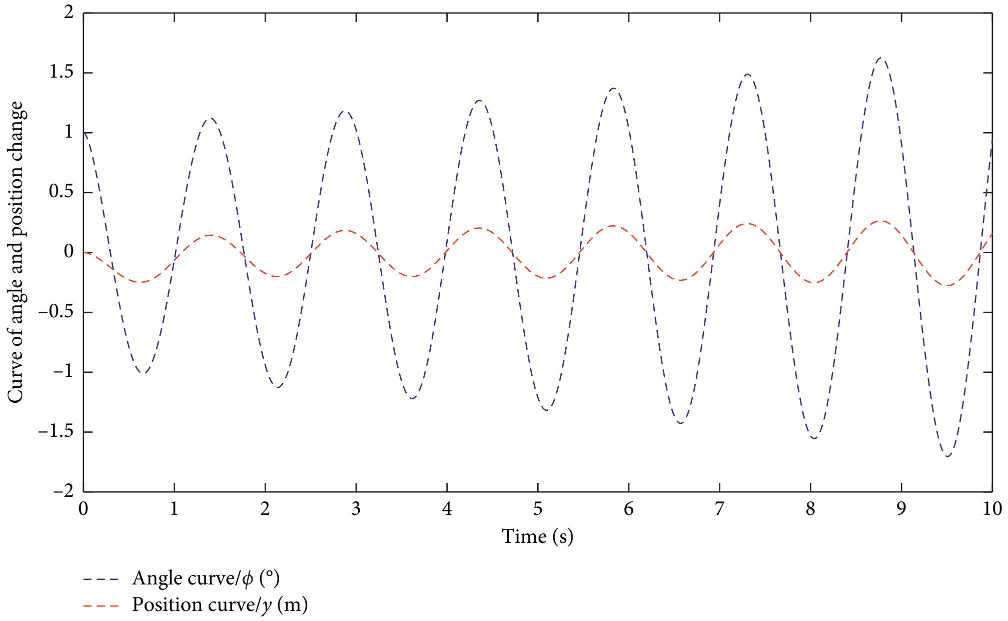

Figure 6: State responses of CPS under the worst DoS attacks.

Let the sampling period $T = 0.01s$, then the discrete-time model of the inverted pendulum is given as

$$\begin{cases} x(k+1) = Ax(k) + Bu(k), \\ y(k) = Cx(k), \end{cases} \tag{49}$$

where

$$\begin{gathered} A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 29.43 & 0 \end{bmatrix}, \\ B = \begin{bmatrix} 0 & 1 & 0 & 3 \end{bmatrix}^T, \\ C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \end{gathered} \tag{50}$$

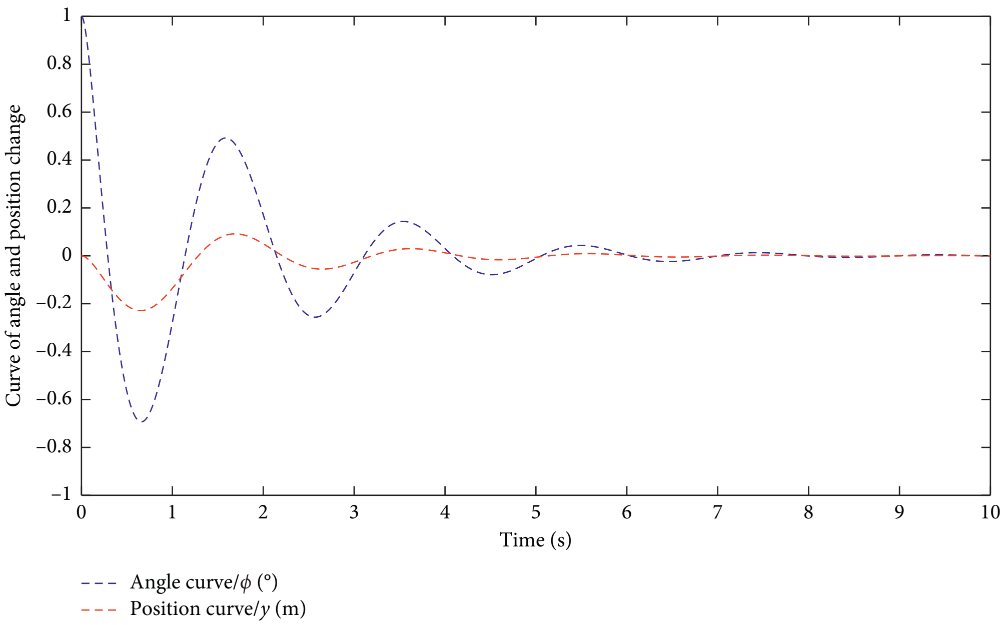

Figure 7: State responses of CPS with SOFP control under the worst DoS attacks.

In the simulation settings, by selecting $\delta = 0.85$, $\mu = 1$, $\lambda_0 = \lambda_1 = \lambda_2 = \lambda_3 = 0.9$. The initial condition is set to be $x_0 = \begin{bmatrix} 10 & 0 & 0 & 0 \end{bmatrix}^T$ and the simulation time is chosen as $t \in \begin{bmatrix} 0 & 10 \end{bmatrix}$. Then, the stabilization control law in Theorem 3 can be resorting to LMI toolbox in MATLAB. Suppose that the maximum number of packet dropouts is $N = 3$ under the worst attacks in this simulation example. Therefore, the corresponding gain $G = \begin{bmatrix} -3.7808 & 1.9434 \end{bmatrix}$ is obtained. Meanwhile, the distribution of DoS attacks is shown in Figure 4.

Case I. DoS-free case:

The state responses of the system (49) with the designed controller under DoS-free case are shown in Figure 5, in which the stability of the studied is verified. It is worth noting that the angle value in Figures 5–7 has been reduced by one tenth in order to make a more intuitive comparison between the angle and position curves.

Case II. DoS attacks case:

In the second scenario, the designed controller in Case I is still used. Under the DoS attacks in Figure 4, the state responses of the system (49) are depicted in Figure 6. It is evident that the angle and position states of the inverted pendulum system are not convergent, in which state responses are presented in a worse performance. Thus, one can see that the switching system is unstable when there are no SOFP control inputs to confront uncertain packet dropouts caused by DoS attacks.

Case III: DoS attacks migration with SOFP

The third scenario considered the SOFP control strategy. In such case, the corresponding output feedback gain G against the worst attacks is employed to ensure system stability and maintain the desired control performance. Similarly, we can obtain the following in Figure 7.

Based on the angle and position curves, the proposed method is effective, as the control strategy demonstrates that the closed-loop system is stable with bounded packet dropouts. One can see that the system performance is better than the one without predictive control. As a result, the proposed packet-based compensation control method has certain robustness and security.

According to the simulation examples shown above, it can be summarised that the designed controller is stable against DoS attacks and the feasibility of the proposed designing method is verified.

6. Conclusion

In this paper, a novel predictive control strategy is proposed to cope with packet dropouts caused by DoS jamming attacks. Firstly, the discrete-time switched linear control system is formulated to characterize the properties of CPS under DoS attacks. Then, the stability criterion is derived, and the predictive control sequences have been given by LMIs. Finally, the corresponding simulation example results have shown the validity of the SOFP control method.

Data Availability

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

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This work was supported by the Natural Science Foundation of China under grants nos. 61863026 and 61563031. Also, it is partially supported by the Industrial Support and Guidance Project for Higher Education of Gansu Province (2019C-05), the Open Fund Project of Key Laboratory of Gansu Advanced Control for Industrial Process (2019KFJJ03), and the Project of Shandong Province Higher Educational Science and Technology Program (J17KA084).

References

[1] T. Lu, J. Lin, L. Zhao, Y. Li, and Y. Peng, "A security architecture in cyber-physical systems: security theories, analysis, simulation and application fields," *International Journal of Security and its Applications*, vol. 9, no. 7, pp. 1–16, 2015.

[2] H. Sandberg, S. Amin, and K. Johansson, "Cyber physical security in networked control systems: an introduction to the issue," *Control Systems IEEE*, vol. 35, no. 1, pp. 20–23, 2015.

[3] A. Chattopadhyay, A. Prakash, and M. Shafique, "Secure cyber-physical systems: current trends, tools and open research problems," in *Proceedings of the Conference on Design, Automation & Test in Europe*, pp. 1104–1109, Lausanne, Switzerland, March 2017.

[4] H. Kim, J. Kang, and J. H. Park, "A light-weight secure information transmission and device control scheme in integration of CPS and cloud computing," *Microprocessors and Microsystems*, vol. 52, pp. 416–426, 2016.

[5] Z. Zhang, Y. Niu, and J. Song, "Input-to-State stabilization of interval type-2 fuzzy systems subject to cyberattacks: an observer-based adaptive sliding mode approach," *IEEE Transactions on Fuzzy Systems*, vol. 28, no. 1, pp. 190–203, 2020.

[6] M. Robert, J. Michael, and C. Tim, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Electricity In-Formation Sharing and Analysis Center, Washington, DC, USA, 2016.

[7] N. Arash and M. Stuart, "A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet," *IEEE Transactions on Dependable & Secure Computing*, vol. 15, no. 1, pp. 2–13, 2018.

[8] H. Foroush and S. Martínez, "On triggering control of single-input linear systems under pulse-width modulated DoS signals," *Siam Journal on Control & Optimization*, vol. 54, no. 6, pp. 3084–3105, 2016.

[9] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Event-Triggered output feedback control resilient against jam-ming attacks and random packet losses," *IFAC-Papers OnLine*, vol. 86, no. 6, pp. 270–275, 2015.

[10] H. T. Sun, C. Peng, W. Zhang et al., "Security-based resilient event-triggered control of networked control systems under denial of service attacks," *Journal of the Franklin Institute*, vol. 21, pp. 1–19, 2018.

[11] A. Teixeira, D. Perez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proceedings of the 1st International Conference on High Confidence Networked Systems*, pp. 55–64, Beijing, China, April 2012.

[12] Z. Cao, Y. Niu, and J. Song, "Finite-time sliding-mode control of markovian jump cyber-physical systems against randomly occurring injection attacks," *IEEE Transactions on Automatic Control*, vol. 65, no. 3, pp. 1264–1271, 2020.

[13] W. A. Zhang and L. Yu, "Output feedback stabilization of networked control systems with packet dropouts," *IEEE Transactions on Automatic Control*, vol. 52, no. 9, pp. 1705–1710, 2007.

[14] L. Q. Zhang, Y. Shi, T. W. Chen, and B. Huang, "A new method for stabilization of networked control systems with random delays," *IEEE Transactions on Automatic Control*, vol. 50, no. 8, pp. 1177–1181, 2005.

[15] F. W. Yang, Z. D. Wang, Y. S. Huang, and M. Gani, "Control for networked systems with random communication delays," *IEEE Transactions on Automatic Control*, vol. 51, no. 3, pp. 512–518, 2006.

[16] G. P. Liu, J. X. Mu, D. Rees, and S. C. Chai, "Design and stability analysis of networked control systems with random communication time delay using the modified MPC," *International Journal of Control*, vol. 79, no. 4, pp. 288–297, 2006.

[17] K. Ding, Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "A multi-channel transmission schedule for remote state estimation under Dos attacks," *Automatica*, vol. 78, pp. 194–201, 2017.

[18] H. Lin and P. J. Antsaklis, "Stability and persistent disturbance attenuation properties for a class of networked control systems: switched system approach," *International Journal of Control*, vol. 78, no. 18, pp. 1447–1458, 2005.

[19] M. Yu, L. Wang, and T. Chu, "Sampled-data stabilisation of networked control systems with nonlinearity," *IEE Proceedings-Control Theory and Applications*, vol. 152, no. 6, pp. 609–614, 2005.

[20] J. Xiong and J. Lam, "Stabilization of linear systems over networks with bounded packet loss," *Automatica*, vol. 43, no. 1, pp. 80–87, 2007.

[21] M. Yu, L. Wang, G. Xie, and T. Chu, "Stabilization of networked control systems with data packet dropout via switched system approach," in *Proceedings of the IEEE Conference on Decision and Control*, pp. 362–367, New Orleans, LA, USA, October 2004.

[22] J. Song, Z. Wang, and Y. Niu, "Static output-feedback sliding mode control under round-robin protocol," *International Journal of Robust and Nonlinear Control*, vol. 28, no. 18, pp. 5841–5857, 2018.

[23] H. T. Sun, C. Peng, W. He et al., "Attack frequency estimation of networked control systems under denial of service with energy constraints," in *Proceedings of the Conference of the IEEE Industria*, pp. 4301–4306, Beijing, China, October 2017.

[24] J. Hu, C. Liu, and Y. Song, "Switching control for networked control system with denial-of-service attacks," in *Proceddings of the 36th Chinese Control Conference*, pp. 7667–7672, Dalian, China, July 2017.

[25] W. Zhang, *Stability analysis of networked control systems*, Ph.D. dissertation, Case Western Reserve University, Cleveland, OH, USA, 2001.

[26] S. Lai, B. Chen, T. Li, and L. Yu, "Packet-based state feedback control under DoS attacks in cyber-physical systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 8, pp. 1421–1425, 2018.

[27] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 843–852, 2016.