

Article

Preview Control for Cyber–Physical Systems under Periodic Denial-of-Service Attacks

Jiang Wu ^{1,*}, Hao Xie ², Jinming Liang ¹ and Zhiqiang Li ³¹ School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China² School of Mathematics and Statistics, Chongqing Technology and Business University, Chongqing 400067, China³ East-China Research Institute of Computer Technology, Shanghai 201800, China

* Correspondence: jiangwu@ustb.edu.cn

Abstract: In this paper, the preview control problem for cyber–physical systems (CPSs) under denial-of-service (DOS) attacks is studied. First, we employ an attack-tolerant strategy to design an augmented error system (AES) for scenarios where both state and reference signal channels are subject to periodic attacks. We then discuss the stochastic stability conditions for the AES and derive the corresponding controller. Subsequently, the preview controller for the original system is developed. Finally, the effectiveness of the obtained results is demonstrated through a numerical simulation using an unmanned ground vehicle (UGV) model, indicating the practical applicability of the proposed control strategy.

Keywords: cyber–physical systems; preview control; denial-of-service attacks; attack-tolerant strategy; augmented error system

MSC: 93C05



Citation: Wu, J.; Xie, H.; Liang, J.; Li, Z. Preview Control for Cyber–Physical Systems under Periodic Denial-of-Service Attacks.

Mathematics **2024**, *12*, 2653. <https://doi.org/10.3390/math12172653>

Academic Editor: Marek Lampart

Received: 22 July 2024

Revised: 20 August 2024

Accepted: 22 August 2024

Published: 27 August 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Preview control is a concept that enhances tracking effectiveness and suppresses disturbance by utilizing information about reference signals or disturbances ahead of time [1–3]. In a preview control model, measuring these signals in advance and incorporating this “future” information into the controller can save total energy consumption during tracking, thereby improving overall efficiency. Additionally, by applying “future” disturbance information to design a reverse buffer in advance, the impact caused by disturbances can be mitigated. Research on preview control has garnered significant attention, with the augmented error system (AES) being a key technology in the optimal preview control theory [1–3]. When designing a preview controller, the AES is first established, which includes the state equation, the error equation, and some equalities regarding previewable signals. Using the maximum principle and solving an equation with previewable signals backwards, an optimal preview controller can be derived. Building upon a fractionation tower model, a series of preview control problems for multi-rate setting systems have been solved [4–6]. The core method to address this involves introducing the discrete lifting technique to convert the multi-rate setting system into a single-setting one.

In [7,8], the authors address the preview repetitive control problem. They develop optimal and robust preview repetitive controllers, which are applied in research on permanent magnet synchronous motor drive systems. Similarly, in [9–11], preview control technology is applied to carrier-based unmanned aerial vehicles. For the problem of safe auto-landing, deck motion and air-wake disturbances are treated as preview signals. The authors derive optimal and robust control algorithms for both linear and nonlinear models.

Cyber–physical systems (CPSs) are complex dynamic systems that require the transmission and reception of various signals. They are sorts of intelligence systems that can

realize the combination and cooperation of multi-dimensional resources [12,13]. By utilizing environmental perception, CPSs can monitor and control physical entities through the integration of embedded computing, network communication, and control engineering. CPSs have been applied to various fields, including autonomous driving [14,15], power systems [16], healthcare [17], etc. Compared to traditional network control systems (NCSs), CPSs offer more efficient and versatile communication modes [18]. CPSs are vital in an interconnected world, bridging the gap between the physical and digital realms. They enable advanced real-time monitoring, automation, and control across a wide range of critical applications to enhance efficiency, safety, and innovation, making them indispensable for the advancement of technology and the functioning of modern society.

However, as CPSs become increasingly essential, they also face significant security threats, such as eavesdropping, denial-of-service (DoS) attacks, man-in-the-middle attacks, spoofing, and falsified messages [19]. These attacks can disrupt communication channels, delay critical signals, and compromise system functionality, leading to potential failures or even catastrophic consequences in vital applications. Among these, DoS attacks are particularly common and easy to implement. By overwhelming network resources or disrupting communication channels, DoS attacks can render essential services unavailable, leading to severe disruptions in operations, financial losses, and even endangering lives in sectors like healthcare, transportation, and energy. Therefore, ensuring the security and resilience of CPSs against such threats is of paramount importance.

Some studies investigate effective defense control strategies from the perspective of attacked systems [20–23]. In [20], the issue of attack-resilient distributed formation control through online adaptation is explored. A novel distributed control algorithm is proposed, enabling operators to adjust their strategies in real time by utilizing the most recent information gathered on adversaries. The authors of ref. [21] study the problem of designing elastic control strategies for NCSs under DoS attacks. The study proposes analog and digital predictor-based controllers with state resetting, which successfully achieved the targeted control objective across a broad range of DoS signals. In ref. [22], utilizing a simplified model of CPSs and accounting for DoS attacks on the wireless channel of the system's state signal, a set of attack-tolerance strategies is employed to derive sufficient conditions for ensuring system stochastic stability. Based on these conditions, a controller is subsequently designed. In [23], the problem of output feedback stabilization is examined for a class of discrete-time NCSs with an uncertain transition probability matrix and random packet dropouts. The study establishes sufficient conditions for the existence of an output feedback controller that ensures the stochastic stability of the NCS, utilizing a stochastic Lyapunov function and a linear matrix inequality approach.

When addressing the tracking problems of CPSs, both state and reference sensors can be targeted by attackers. The loss of the reference signals can degrade tracking performance or even cause serious accidents, similar to the blinding effect experienced when driving at night due to oncoming high beams. Motivated by [22,23], this paper examines the preview tracking problem for CPSs under periodic DoS attacks and extends the attack-tolerant strategy to the reference signal channel. Based on this strategy, we discuss the stochastic stability conditions for the constructed AES and design the corresponding preview controller.

Our primary goals are to address the challenges of tracking with DoS attacks in both state and reference signal channels by proposing an attack-tolerant strategy and preview controller. The key contributions of our work include the following:

- (a) We propose an attack-tolerant strategy for reference signal channels when the reference signal can be previewed;
- (b) Based on the proposed attack-tolerant strategy, we design a corresponding AES and preview controller;
- (c) We discuss the stochastic stability of the closed-loop system of the AES under the designed controller.

The paper is organized as follows. In Section 2, we explain the fundamentals, including the system model, DoS attack model, attack-tolerant strategy, and construction of the AES.

In Section 3, we present the necessary conditions for the stochastic stability of the AES and propose a preview controller under DoS attacks. In Section 4, the effectiveness of the preview controller from Section 3 is demonstrated through an example involving an unmanned ground vehicle (UGV).

Notations: The notations in this paper are standard. $A \in \mathbb{R}^n$ and $A \in \mathbb{R}^{m \times n}$ denote an n -dimensional matrix and an $m \times n$ matrix, respectively. $\mathbb{R}^+$ denotes the set of positive real numbers. $\mathcal{E}(\cdot)$ stands for the expected value of a random variable. For any matrix A , $A > 0$ (≥ 0) indicates that A is positive definite (semi-definite), and A^T denotes the transpositions of A . I is the identity matrix, and the symbol $*$ in a matrix indicates symmetric entries.

2. Problem Statement

Let us consider a class of CPSs with two communication channels subject to DoS attacks, as shown in Figure 1.

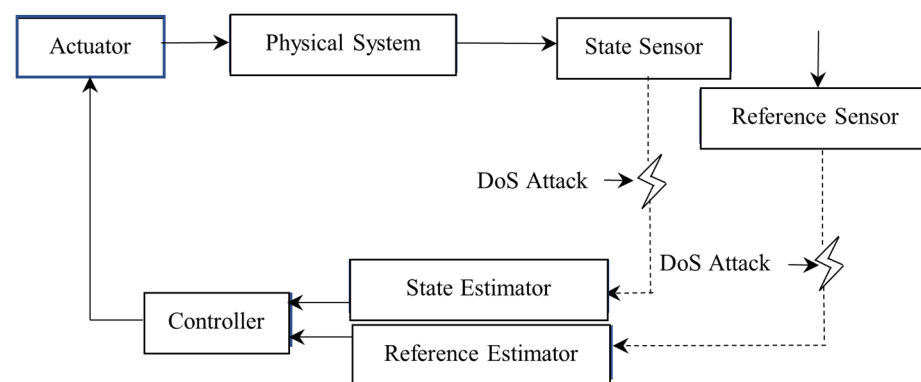


Figure 1. Structure of CPSs under DoS attacks.

Figure 1 illustrates the structure of CPSs when both the state and reference signal channels are under DoS attacks. Data in Figure 1 are transmitted wirelessly from the state and reference sensors to the controller and through wired channels among other system components. The estimators contain buffers that store the last successfully updated data packets.

Remark 1. The reference channel described in Figure 1 is justifiable. In [24,25], data on car-following performance, such as the acceleration, speed, and position of tracked vehicles, are collected in a database. All this information can be considered as reference signals and can assist in achieving automatic driving through detectors. However, since the transmission process is wireless, it is susceptible to attacks.

2.1. System Model

First, consider the system defined by

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + Dd(k) \\ y(k) = Cx(k) \end{cases}, x(0) = x_0. \quad (1)$$

where $x(k) \in \mathbb{R}^m$ is the state vector; $u(k) \in \mathbb{R}^n$, $y(k) \in \mathbb{R}^p$, and $d(k) \in \mathbb{R}^q$ ($\|d(k)\| \leq d^*$) are the control input, the output vector of the plant, and the disturbance, respectively. $A \in \mathbb{R}^{m \times m}$, $B \in \mathbb{R}^{m \times n}$, $C \in \mathbb{R}^{p \times m}$, and $D \in \mathbb{R}^{q \times m}$ are constant matrices.

We denote the reference signal as $r(k) \in \mathbb{R}^p$. Since future reference signals over a period are available in the preview control problem model, the following assumption is introduced.

Assumption 1 ([26]). At time instant k_0 , the future reference signals $r(k_0 + i)$ ($i = 1, 2, \dots, M_r$) are acquirable, where M_r represents the preview length. For $r(k)$ after time instant $k_0 + M_r$, we have

$$r(k_0 + M_r + i) = 0, \quad (i = 1, 2, 3, \dots). \quad (2)$$

Remark 2. Assumption 1 is a common assumption in the preview control problem. In (2), it is reasonable to set $r(k_0 + M_r + i) = 0$, ($i = 1, 2, 3, \dots$) beyond the previewable range. From a practical application perspective, when designing a preview controller, more focus should be given to preview information that will imminently impact the system, while the importance of information that is further away should gradually decrease. Information outside the previewable range should be considered invalid. To effectively utilize relevant previewable information and exclude invalid data from the controller design, (2) is established.

The measurement of the reference signals, as described above, is shown in Figure 2.

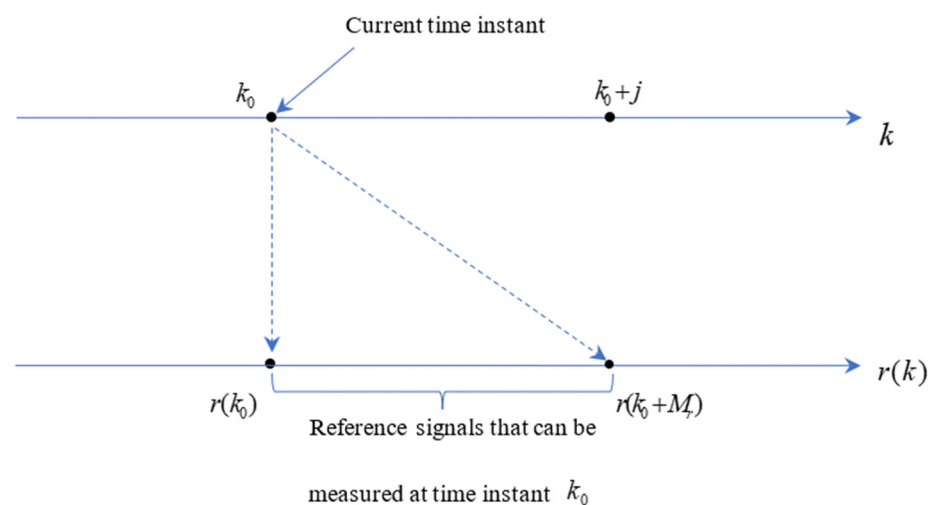


Figure 2. Reference signals known at time instant k_0 in the preview control model.

The tracking error is defined as

$$\begin{aligned} e(k) &= y(k) - r(k) \\ &= Cx(k) - r(k). \end{aligned} \quad (3)$$

Letting

$$q(k) = \sum_{i=0}^k e(i) \quad (4)$$

be the sum of $e(k)$, we have

$$\begin{aligned} q(k+1) &= q(k) + e(k+1) \\ &= q(k) + C[Ax(k) + Bu(k) + Dd(k)] - r(k+1). \end{aligned} \quad (5)$$

The objective of this paper is to design a preview controller that enables the system output $y(k)$ to track the reference signal $r(k)$ under periodic DoS attacks. This means that under the designed controller, if $\lim_{k \rightarrow \infty} q(k) = c$, where c is a constant, then the system error $e(k)$ satisfies $\lim_{k \rightarrow \infty} e(k) = 0$.

2.2. DoS Attack Model

In this paper, we consider a type of energy-constrained periodic DoS attack model as described in [22]. Each attack cycle consists of a dormancy stage and an attack stage. During the dormancy stage, $(n-1)T \leq k \leq (n-1)T + T_{off}$, the attackers conserve energy

for the upcoming attack. In the attack stage, $(n-1)T + T_{off} < k < nT$, they continuously target the estimators, where $T_{off} \in \mathbb{R}^+$ is the duration of dormancy.

Let $\theta(k)$ and $\varphi(k)$ denote the data reception status of the state and reference signals under periodic DoS attacks at time instant k , respectively, as follows:

$$\theta(k) = \begin{cases} 1, & \text{if the state signal received;} \\ 0, & \text{if the state signal not received.} \end{cases} \quad (6)$$

$$\varphi(k) = \begin{cases} 1, & \text{if the reference signal received;} \\ 0, & \text{if the reference signal not received.} \end{cases} \quad (7)$$

We define p_{attack} and q_{attack} as the probabilities that $\theta(k) = 1$ and $\varphi(k) = 1$ during the attack stage and p_{dorm} and q_{dorm} as the probabilities that $\theta(k) = 1$ and $\varphi(k) = 1$ during the dormancy stage, respectively.

Remark 3. Even during the dormancy stage, packet loss can occur in wireless channels. This is because wireless transmission is subject to multi-path fading and signal degradation, which can intermittently cause packet loss. These factors are crucial and should be considered when de-signing controllers. As a result, in practice, the values of p_{dorm} and q_{dorm} are typically less than 1.

2.3. Attack-Tolerant Strategy

To simplify the complexity, this paper adopts a common attack-tolerant strategy from [22] for state signals, extending it to reference signals.

Given the unknown attack strategy of the DoS attackers targeting state signal channel, let $\bar{x}(k)$ represent the state vector used for calculation. If the controller successfully receives the data packets from the sensor, then $\bar{x}(k) = x(k)$. Otherwise, $\bar{x}(k) = \bar{x}(k-1)$. That means that in the state estimator, if the new state information is lost, the previously recorded $\bar{x}(k-1)$ in the buffer will be used instead. Thus, we have

$$\bar{x}(k) = \theta(k)x(k) + (1 - \theta(k))\bar{x}(k-1). \quad (8)$$

For the reference signals, the attack-tolerant strategy differs. Let $\bar{r}(k)$ be the reference signal used to calculate $u(k)$. According to Assumption 1, if $\varphi(k) = 0$, then $\bar{r}(k+j)$ ($j = 0, 1, 2, \dots, M_r - 1$) are known, having been used for calculating $u(k-1)$, and only $\bar{r}(k+M_r)$ is unknown. In this case, we set $\bar{r}(k+M_r) = \bar{r}(k+M_r-1)$. If $\varphi(k) = 1$, then $\bar{r}(k+j)$ ($j = 0, 1, 2, \dots, M_r$) are updated by $r(k+j)$ ($j = 0, 1, 2, \dots, M_r$). Consequently, $\bar{r}(k+j)$ ($j = 0, 1, 2, \dots, M_r$) can be expressed as

$$\bar{r}(k+j) = \begin{cases} \varphi(k)r(k+j) + (1 - \varphi(k))\bar{r}(k+j) & (0 \leq j < M_r) \\ \varphi(k)r(k+j) + (1 - \varphi(k))\bar{r}(k+j-1) & (j = M_r) \end{cases}. \quad (9)$$

Further, we define

$$\begin{aligned} \bar{q}(k) &= \bar{q}(k-1) + C\bar{x}(k) - \bar{r}(k) \\ &= \bar{q}(k-1) + C[\theta(k)x(k) + (1 - \theta(k))\bar{x}(k-1)] \\ &\quad - [\varphi(k)r(k) + (1 - \varphi(k))\bar{r}(k)] \end{aligned} \quad (10)$$

as the sum of $e(k)$ used in $u(k)$ after introducing the attack-tolerant strategy.

In the following, an AES based on attack-tolerant strategies (8)–(10) is constructed.

2.4. The Construction of the AES

Firstly, we establish some equalities on $r(k+j)$ ($j = 0, 1, \dots, M_r$) and $\bar{r}(k+j)$ ($j = 0, 1, \dots, M_r$).

Denote

$$X_r(k) = \begin{bmatrix} r(k) \\ r(k+1) \\ \vdots \\ r(k+M_r) \end{bmatrix} \text{ and } A_r = \begin{bmatrix} 0 & I & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & I \\ 0 & \cdots & \cdots & \cdots & 0 \end{bmatrix},$$

Then, we can obtain the following identity

$$X_r(k+1) = A_r X_r(k). \quad (11)$$

Let

$$\bar{X}_r(k) = \begin{bmatrix} \bar{r}(k) \\ \bar{r}(k+1) \\ \vdots \\ \bar{r}(k+M_r) \end{bmatrix}, \bar{A}_{r0}(k) = \begin{bmatrix} \varphi(k)I & & & & \\ & \varphi(k)I & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \varphi(k)I \end{bmatrix},$$

$$\bar{A}_r(k) = \begin{bmatrix} 0 & (1-\varphi(k))I & 0 & \cdots & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & \cdots & 0 & (1-\varphi(k))I \\ 0 & 0 & \cdots & \cdots & 0 & (1-\varphi(k))I \end{bmatrix},$$

Then, we have

$$\bar{X}_r(k) = \bar{A}_{r0}(k)X_r(k) + \bar{A}_r(k)\bar{X}_r(k-1). \quad (12)$$

Define

$$X_0(k) = \begin{bmatrix} q(k) \\ x(k) \end{bmatrix}, \bar{X}_0(k) = \begin{bmatrix} \bar{q}(k) \\ \bar{x}(k) \end{bmatrix},$$

$$\tilde{A}_x = \begin{bmatrix} I & CA \\ 0 & A \end{bmatrix}, \tilde{B}_x = \begin{bmatrix} CB \\ B \end{bmatrix}, \tilde{D}_x = \begin{bmatrix} CD \\ D \end{bmatrix}, G_r = \begin{bmatrix} 0 & -I & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix},$$

$$\bar{A}_{x0}(k) = \begin{bmatrix} 0 & \theta(k)C \\ 0 & \theta(k)I \end{bmatrix}, \bar{A}_x(k) = \begin{bmatrix} I & (1-\theta(k))C \\ 0 & (1-\theta(k))I \end{bmatrix},$$

$$\bar{G}_{r0}(k) = \begin{bmatrix} -\varphi(k)I & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}, \bar{G}_r(k) = \begin{bmatrix} 0 & -(1-\varphi(k))I & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Combining Equations (1), (5), (8), and (10)–(12), we obtain

$$X(k+1) = \tilde{A}(k)X(k) + \tilde{B}u(k) + \tilde{D}d(k), \quad (13)$$

where

$$X(k) = \begin{bmatrix} X_0(k) \\ X_r(k) \\ \bar{X}_0(k-1) \\ \bar{X}_r(k-1) \end{bmatrix}, \tilde{A}(k) = \begin{bmatrix} \tilde{A}_x & G_r & 0 & 0 \\ 0 & A_r & 0 & 0 \\ \bar{A}_{x0}(k) & \bar{G}_{r0}(k) & \bar{A}_x(k) & \bar{G}_r(k) \\ 0 & \bar{A}_{r0}(k) & 0 & \bar{A}_r(k) \end{bmatrix}, \quad (14)$$

$$\tilde{B} = \begin{bmatrix} \tilde{B}_x \\ 0 \\ 0 \\ 0 \end{bmatrix}, \tilde{D} = \begin{bmatrix} \tilde{D}_x \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

As a result, the output $y(k)$ in (1) can be expressed as

$$y(k) = Cx(k) = \tilde{C}X(k), \quad (15)$$

where $\tilde{C} = [0 \quad C \quad 0 \quad 0]$. Combining (13) and (15) yields

$$\begin{cases} X(k+1) = \tilde{A}(k)X(k) + \tilde{B}u(k) + \tilde{D}d(k) \\ y(k) = \tilde{C}X(k) \end{cases}. \quad (16)$$

Thus, (16) represents the AES for calculating the preview controller.

Remark 4. Unlike the AES construction method in [26], the difference method for the state equation is not used here in (13). The reason for this is that, under the aforementioned attack-tolerant strategies, the AES constructed using the method in [26] must account for the signal reception status at both time instants k and $k-1$. This makes the AES a non-Markov jump system, complicating stability analysis.

3. Preview Controller Design and Stability Analysis

First, consider the preview controller with the following form

$$u(k) = K\bar{X}_0(k) + F\bar{X}_r(k), \quad (17)$$

where the feedback gain matrices $K = [K_1 \quad K_2]$ and $F = [F_0 \quad F_1 \quad \cdots \quad F_{M_r}]$ are block matrices of appropriate dimensions.

Substituting the control input (17) into (16), the closed-loop system becomes

$$\begin{aligned} X(k+1) &= \tilde{A}(k)X(k) + \tilde{B}(K\bar{X}_0(k) + F\bar{X}_r(k)) + \tilde{D}d(k) \\ &= \tilde{A}(k)X(k) + \tilde{B}\left[K_1\bar{q}(k) + K_2\bar{x}(k) + \sum_{i=0}^{M_r} F_i\bar{r}(k+i)\right] + \tilde{D}d(k) \end{aligned} \quad (18)$$

Substituting (8)–(10) into (18) and defining

$$\begin{aligned} H_1(k) &= \begin{bmatrix} 0 & \theta(k)C \\ 0 & \theta(k)I \end{bmatrix}, \quad H_2(k) = \begin{bmatrix} I & (1-\theta(k))C \\ 0 & (1-\theta(k))I \end{bmatrix}, \\ G_1(k) &= \begin{bmatrix} -\varphi(k)I & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \quad G_2(k) = \begin{bmatrix} 0 & -(1-\varphi(k))I & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \\ G_3(k) &= \begin{bmatrix} \varphi(k)I & & & \\ & \varphi(k)I & & \\ & & \ddots & \\ & & & \varphi(k)I \end{bmatrix}, \quad G_4(k) = \begin{bmatrix} 0 & (1-\varphi(k))I & & \\ & \ddots & \ddots & \\ & & 0 & (1-\varphi(k))I \\ & & & (1-\varphi(k))I \end{bmatrix}. \end{aligned}$$

(18) can be briefly rewritten as

$$X(k+1) = \Phi_{\gamma(k+1)}X(k) + \tilde{D}d(k), \quad (19)$$

where

$$\Phi_{\gamma(k+1)} = \tilde{A}(k) + \tilde{B}\left(K\tilde{H}(k) + F\tilde{G}(k)\right). \quad (20)$$

and

$$\tilde{H}(k) = [H_1(k) \quad G_1(k) \quad H_2(k) \quad G_2(k)], \quad \tilde{G}(k) = [0 \quad G_3(k) \quad 0 \quad G_4(k)].$$

Since $\theta(k)$ and $\varphi(k)$ can only take values of 0 or 1, (19) represents four different systems. We use $\gamma(k) = 1, 2, 3, 4$ to distinguish between these systems, and they can be summarized in Table 1.

Table 1. Values of $\gamma(k)$ corresponding to different combinations of $\theta(k)$ and $\varphi(k)$.

$\gamma(k)$	$\theta(k)$	$\varphi(k)$
1	1	1
2	0	1
3	1	0
4	0	0

Let the state transition probability of $\gamma(k)$ from time instant k to $k + 1$ be denoted by

$$\Pr\{\gamma(k+1) = j\} = \pi_j \geq 0. \quad (21)$$

According to (20) and Table 1, the transition probability π_j depends only on the probabilities of $\theta(k)$ and $\varphi(k)$. Therefore, System (19) is a Markovian jump system.

Next, the stochastic stability of (19) is analyzed.

To ensure that the closed-loop system (19) is stochastically stable, the following definition and lemma are needed.

Definition 1 ([22]). For the Markov jump system (19) without disturbance, if there exists $\Omega > 0$ such that

$$\sum_{k=0}^{\infty} \mathcal{E}\left\{\|X(k)\|^2 \middle| X(0)\right\} \leq X^T(0)\Omega X(0) \quad (22)$$

holds, then (19) is stochastically stable, where $X(0)$ is the initial state of (19).

Lemma 1 (Schur's complement [27]). The following three inequalities are equivalent.

- (1) $\begin{bmatrix} S_{11} & S_{12} \\ S_{12}^T & S_{22} \end{bmatrix} < 0$;
- (2) $S_{11} < 0, S_{22} - S_{12}^T S_{11}^{-1} S_{12} < 0$;
- (3) $S_{22} < 0, S_{11} - S_{12} S_{22}^{-1} S_{12}^T < 0$.

Then, we can derive the following theorem.

Theorem 1. For $i = 1, 2, 3, 4$ and a given positive scalar β , if there exist matrices $P_i > 0$, such that the following inequalities

$$\begin{bmatrix} -P_1^{-1} & 0 & 0 & 0 & \sqrt{\pi_1}\Xi_1 \\ * & -P_2^{-1} & 0 & 0 & \sqrt{\pi_2}\Xi_2 \\ * & * & -P_3^{-1} & 0 & \sqrt{\pi_3}\Xi_3 \\ * & * & * & -P_4^{-1} & \sqrt{\pi_4}\Xi_4 \\ * & * & * & * & -Q_i \end{bmatrix} < 0 \quad (23)$$

hold, where $\Xi_i = [\Phi_j \ D]$ and $Q_i = \begin{bmatrix} P_i \\ \beta I \end{bmatrix}$, then the closed-loop system (19) is stochastically stable.

Proof of Theorem 1. Consider the Lyapunov function of the form

$$V(k) = X^T(k)P_{\gamma(k)}X(k).$$

By analyzing the forward difference in $V(k)$ along with System (19), we have

$$\begin{aligned}\mathcal{E}(\Delta V(k)) - \beta d^T(k)d(k) &= \mathcal{E}(V(k+1)) - V(k) - \beta d^T(k)d(k) \\ &= \mathcal{E}(X^T(k+1)P_{\gamma(k+1)}X(k+1)) - X^T(k)P_{\gamma(k)}X(k) - \beta d^T(k)d(k) \\ &= \mathcal{E}((X^T(k)\Phi_{\gamma(k+1)}^T + d^T(k)D^T)P_{\gamma(k+1)}(\Phi_{\gamma(k+1)}X(k) + Dd(k)) \\ &\quad - X^T(k)P_{\gamma(k)}X(k) - \beta d^T(k)d(k)) \\ &= \tilde{X}^T(k) \left[\sum_{j=1}^4 \pi_j \Xi_j^T P_j \Xi_j - Q_i \right] \tilde{X}(k),\end{aligned}\quad (24)$$

where $\tilde{X}(k) = [X^T(k) \quad d^T(k)]^T$, $\Xi_j = [\Phi_j^T \quad D^T]^T$, and $Q_i = \begin{bmatrix} P_i & \\ & \beta I \end{bmatrix}$.

If $\Psi_i = \sum_{j=1}^4 \pi_j \Xi_j^T P_j \Xi_j - Q_i < 0$, then we can obtain

$$\mathcal{E}(\Delta V(k)) \leq \lambda_{\max}(\Psi_i) \|\tilde{X}(k)\|^2 + \beta \|d(k)\|^2. \quad (25)$$

where $\lambda_{\max}(\Psi_i) < 0$ is the maximal eigenvalue of matrix Ψ_i . Summing both sides of inequality (25) from 0 to T , then we have

$$\mathcal{E}(V(X(T+1))) - \mathcal{E}(V(X(0))) \leq \lambda_{\max}(\Psi_i) \mathcal{E} \left(\sum_{k=0}^T \|\tilde{X}(k)\|^2 \right) + \beta \sum_{k=0}^T \|d(k)\|^2. \quad (26)$$

Letting $T \rightarrow \infty$, (26) is equal to

$$\mathcal{E} \left(\sum_{k=0}^T \|X(k)\|^2 \right) \leq \mathcal{E} \left(\sum_{k=0}^T \|\tilde{X}(k)\|^2 \right) \leq -\frac{1}{\lambda_{\max}(\Psi_i)} (\mathcal{E}(V(X(0))) + \beta \sum_{k=0}^T \|d(k)\|^2) < \infty. \quad (27)$$

We set $d(k) = 0$, and according to Definition 1, (27) implies stochastic stability.

By Lemma 1, the inequalities $\sum_{j=1}^4 \pi_j \Xi_j^T P_j \Xi_j - Q_i < 0$ ($i = 1, 2, 3, 4$) are equivalent to (23), which completes the proof. $\square$

Due to the simultaneous inclusion of P_i^{-1} and P_i in (23), (23) does not represent linear matrix inequalities (LMIs). To solve for K , F in Φ , and P_i , we follow the approach in [22] by introducing X_i to replace P_i^{-1} in (23). Then, using the Cone Complementarity Linearization (CCL) method from [28], the problem of solving (23) is transformed into the following minimization problem constrained by LMIs

$$\min_{X_i, P_i} \text{Trace} \left(\sum_{i=1}^4 P_i X_i \right); \quad (28)$$

$$\text{s.t. } \begin{bmatrix} \Omega_1 & \Omega_2 \\ * & \Omega_3 \end{bmatrix} < 0, \quad \begin{bmatrix} P_i & I \\ I & X_i \end{bmatrix} > 0, \quad (29)$$

where

$$\begin{aligned}\Omega_1 &= -\text{diag}\{X_1, X_2, X_3, X_4\}, \\ \Omega_2 &= [\sqrt{\pi_1} \Xi_1^T \quad \sqrt{\pi_2} \Xi_2^T \quad \sqrt{\pi_3} \Xi_3^T \quad \sqrt{\pi_4} \Xi_4^T]^T, \\ \Omega_3 &= \begin{bmatrix} -P_i & \\ & \beta I \end{bmatrix}.\end{aligned}$$

This minimization problem still cannot be solved directly by the 'mincx' solver in the LMI toolbox of Matlab because it contains the quadratic terms $P_i X_i$. However, we can obtain P_i and the feedback gain matrices K and F using the following algorithm.

- Step 1: Initialize $k = 0$. Find a feasible solution group P_i^k, X_i^k, K^k , and F^k for LMIs in (29).
- Step 2: Minimize the following problem

$$\min_{X_i, P_i} \text{Trace} \left(\sum_{i=1}^4 (P_i^k X_i + P_i X_i^k) \right); \quad (30)$$

subject to the LMIs in (29). Denote the feasible solutions for this problem as $P_i^{k+1}, X_i^{k+1}, K^{k+1}$, and F^{k+1} .

- Step 3: If

$$\|P_i^{k+1} X_i^{k+1} - I\|_{Fro} < l,$$

where $\|\cdot\|_{Fro}$ represents the Frobenius norm of a matrix and l is a given stopping criterion, then exit. Otherwise, set $k = k + 1$ and return to step 2.

Additionally, we derive the following corollary for the preview controller of System (1) when both the state and the reference signal channels are subject to DoS attacks.

Corollary 1. According to Assumption 1, for $i = 1, 2, 3, 4$, and a given positive scalar β , if there exist matrices $P_i > 0$ ($i = 1, 2, 3, 4$) such that the LMIs (23) hold, then the controller (17) functions as the preview controller for System (1) under periodic DoS attacks.

4. Numerical Simulation

Consider an example of an unmanned ground vehicle (UGV) taken from [29]. It is assumed that the UGV travels in a straight line and comes to a complete stop before rotating. The dynamic model is described as follows:

$$\begin{cases} \begin{bmatrix} \dot{s}(t) \\ \dot{v}(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & \frac{-b}{M} \end{bmatrix} \begin{bmatrix} s(t) \\ v(t) \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{M} \end{bmatrix} F(t) \\ \begin{bmatrix} \dot{\rho}(t) \\ \dot{\omega}(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & \frac{-b_r}{J} \end{bmatrix} \begin{bmatrix} \rho(t) \\ \omega(t) \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{J} \end{bmatrix} (L(t) + d_0(t)) \\ y_i(t) = C_i \begin{bmatrix} s(t) \\ v(t) \\ \rho(t) \\ \omega(t) \end{bmatrix} \end{cases}, \quad (31)$$

where the variables s, v, ρ , and ω represent the position, linear velocity, angular position, and angular velocity, respectively. M and J denote the mass and moment of inertia. b and b_r are the translational and rotational friction coefficients. The inputs F and L are the force and torque applied of the UGV, and d_0 is the output disturbance. We set $M = 1$, $J = 2$, $b = 1$, and $b_r = 1$. Additionally, $C_1 = [1 \ 0 \ 0 \ 0]$ and $C_2 = [0 \ 0 \ 1 \ 0]$ represent the transmission channels.

By applying the forward Euler method to discretize the system with a step size of $T = 0.1$, we obtain the following discrete-time system:

$$\begin{cases} \begin{bmatrix} s(k+1) \\ v(k+1) \end{bmatrix} = \begin{bmatrix} 1 & 0.1 \\ 0 & 0.9 \end{bmatrix} \begin{bmatrix} s(k) \\ v(k) \end{bmatrix} + \begin{bmatrix} 0 \\ 0.1 \end{bmatrix} F(k) \\ y_1(k) = s(k) \end{cases}, \quad (32)$$

$$\begin{cases} \begin{bmatrix} \rho(k+1) \\ \omega(k+1) \end{bmatrix} = \begin{bmatrix} 1 & 0.1 \\ 0 & 0.95 \end{bmatrix} \begin{bmatrix} \rho(k) \\ \omega(k) \end{bmatrix} + \begin{bmatrix} 0 \\ 0.05 \end{bmatrix} (L(k) + d_0(k)) \\ y_2(k) = \rho(k) \end{cases}. \quad (33)$$

We set the initial state to $[s(0) \ v(0)]^T = [0.1 \ 0.1]^T$ and define the reference signal

$$r_s(k) = \begin{cases} 0 & 0 \leq k < 80 \\ \sin(0.02\pi(k - 80)) & 80 \leq k < 280 \\ 0 & 280 \leq k \leq 400 \end{cases}.$$

for straight path movement. For the rotating part, we choose the initial angular position $[\rho(0) \ w(0)]^T = [0.15 \ 0.05]^T$ and define the reference signal

$$r_\rho(k) = \begin{cases} 0 & 0 \leq k < 100 \\ 0.01(k - 100) & 100 \leq k < 200 \\ 1 & 200 \leq k \leq 400 \end{cases},$$

and the disturbance

$$d_0(k) = \begin{cases} 0 & 0 \leq k < 300 \\ 1 & 300 \leq k \leq 400 \end{cases}.$$

Under the condition of data packet reception, we have Figure 3.

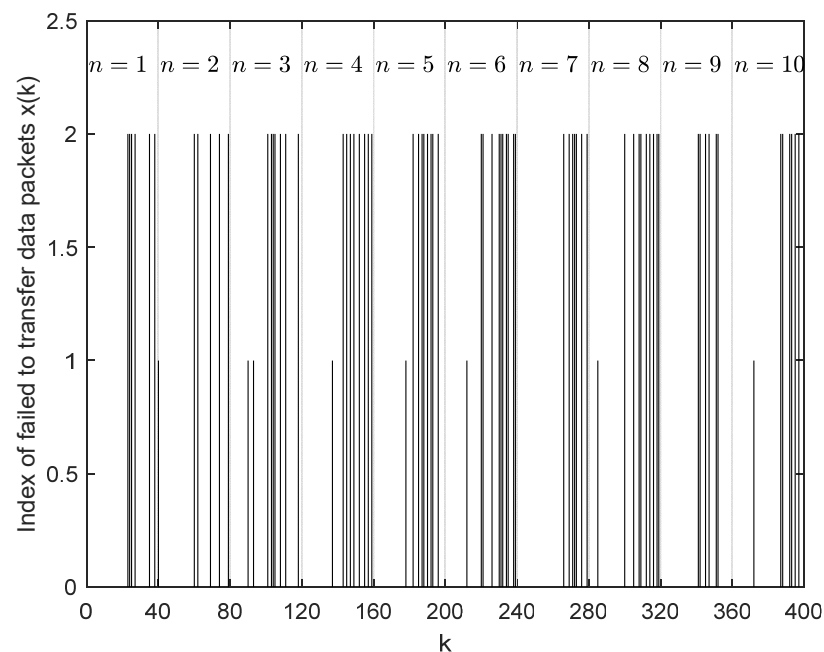


Figure 3. Packet reception affected by periodic DoS attacks, with $T = 20$ and $T_{off} = 10$.

Figure 3 illustrates an example of packet reception. In this figure, the long segments represent the packet loss during the attack stages, while the short segments represent the packet loss during the dormancy stages. This is consistent with the packet reception conditions described in Section 2.2, where $p_{attack} = 0.7$, and $p_{dorm} = 0.95$.

The tracking results for System (32) are presented below.

Figure 4 illustrates the output responses using the method from [22] in scenarios with packet loss in both the state signal and reference signal channels. The minimum p_{attack} and q_{attack} values that ensure system stochastic stability are 0.26 and 0.27, respectively. In Figure 4a, the parameters are set to $q_{attack} = q_{dorm} = 1$, $p_{dorm} = 0.95$, and $p_{attack} = 0.9, 0.7, 0.5$. This subfigure reveals that tracking effectiveness diminishes as p_{attack} decreases, indicating that packet loss in the state signal channel results in degraded tracking performance. In Figure 4b, the parameters are set to $p_{attack} = p_{dorm} = 1$, $q_{dorm} = 0.95$, and $q_{attack} = 0.9, 0.7, 0.5$. Similarly, this subfigure shows that the tracking effectiveness declines with decreasing q_{attack} , demonstrating that packet loss in the reference signal channel also

causes poorer tracking quality. However, the impact on tracking effectiveness is less severe than the loss in the state signal channel.

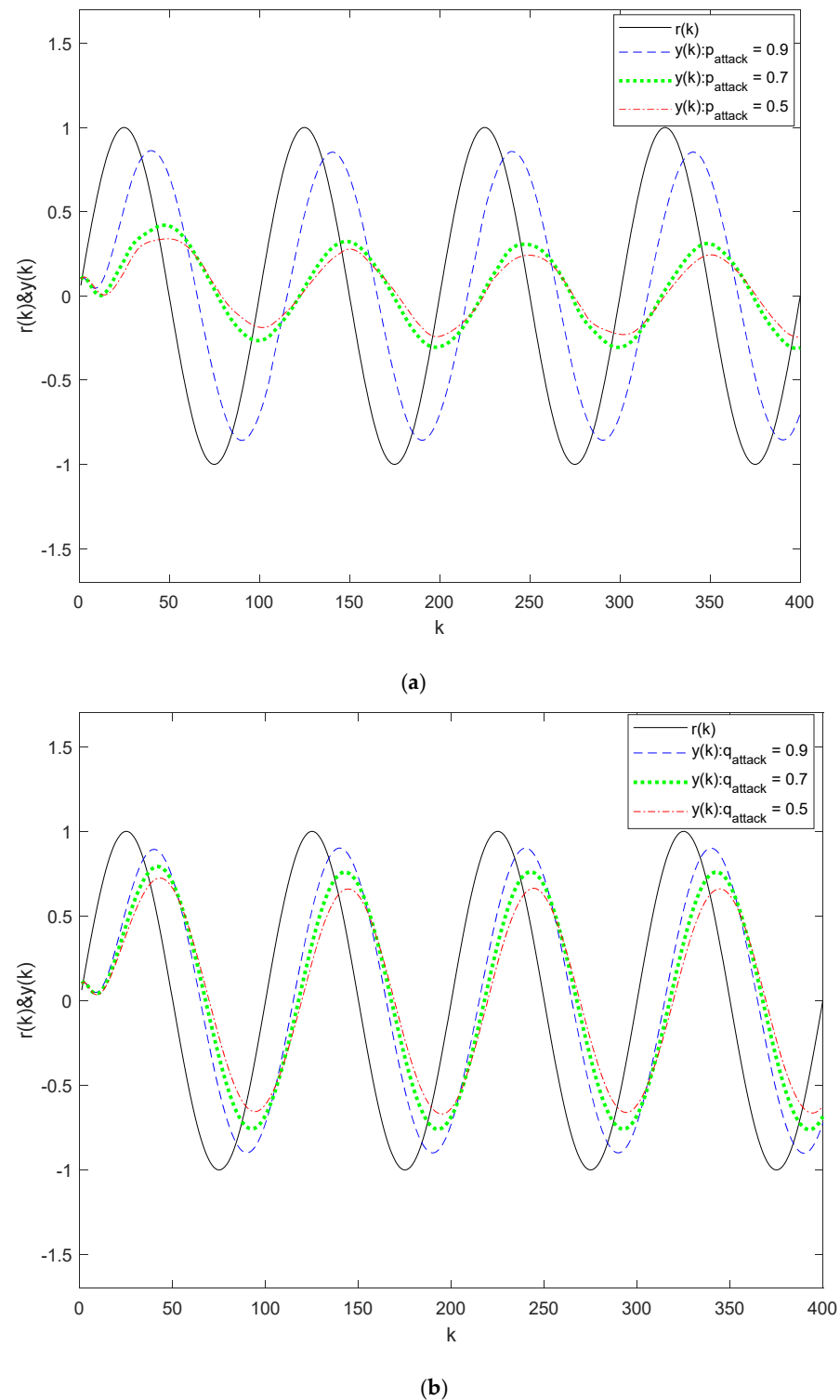
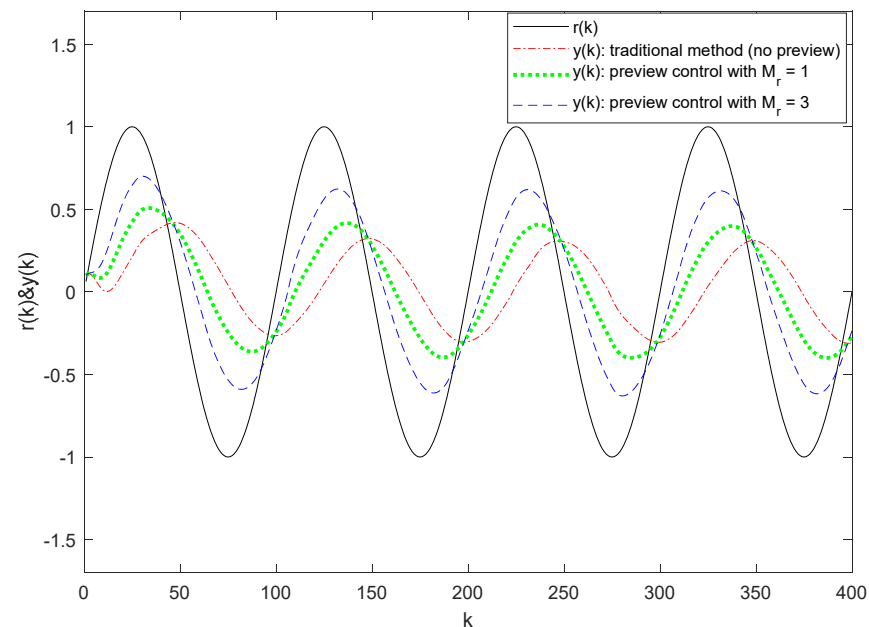


Figure 4. Output responses for System (32) using the method from [22]: (a) Output responses with different p_{attack} ; (b) Output responses with different q_{attack} .

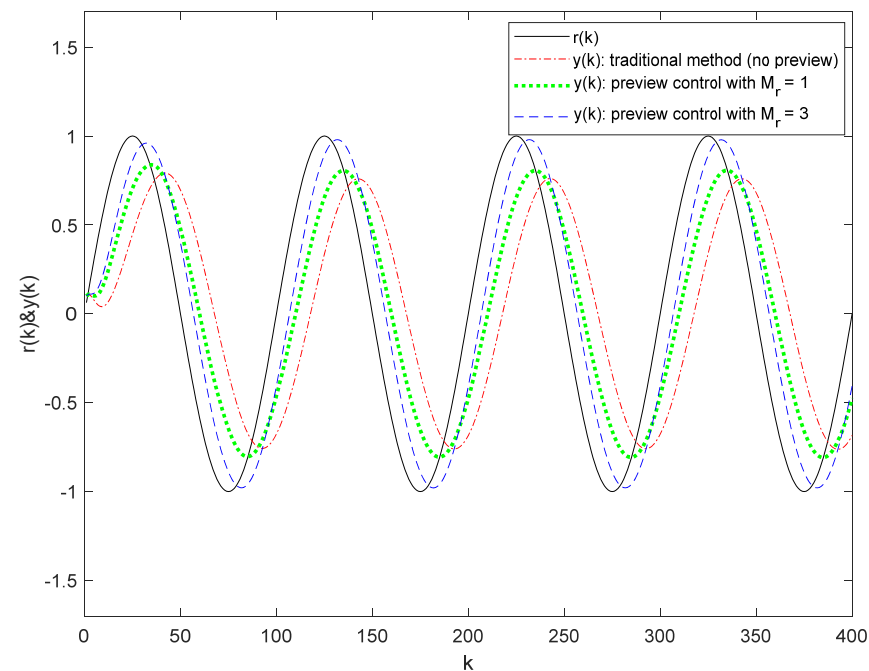
When using the preview controller, the tracking results are as follows.

Figure 5 compares the output responses under different preview conditions and the method from [22], when there is packet loss in both the state signal and reference signal channels. When $M_r = 1$, the minimum p_{attack} value that ensures system stochastic stability

is 0.26, and the system is stable for any q_{attack} . In Figure 5a, we set $q_{attack} = q_{dorm} = 1$, $p_{attack} = 0.7$, $p_{dorm} = 0.95$, and apply varying preview conditions: the method described in [22] (without preview), $M_r = 1$ and $M_r = 3$. Similarly, in Figure 5b, we use $p_{attack} = p_{dorm} = 1$, $q_{attack} = 0.7$, $q_{dorm} = 0.95$, and the same preview conditions. From these subfigures, it is evident that as the preview length M_r increases, the system output can track the reference signal better.



(a)



(b)

Figure 5. Output responses for System (32) using the preview controller proposed in this paper and method from [22]: (a) Output responses with packet loss in state signal channel; (b) Output responses with packet loss in reference signal channel.

Next, we consider the case with disturbance, i.e., System (33), and provide an evaluation of the system's performance. We set $\beta = 1$ in Theorem 1; then, we have the following figures.

Figure 6 illustrates the output responses and error under different preview conditions when there is packet loss in both the state signal and reference signal channels. Figure 6a,c show the system output, and Figure 6b,d show the error. In Figure 6a,b, we set $q_{\text{attack}} = q_{\text{dorm}} = 1$, $p_{\text{attack}} = 0.7$, $p_{\text{dorm}} = 0.95$, and apply varying preview conditions: the method described in [22] (without preview), $M_r = 1$ and $M_r = 3$. In Figure 6c,d, we use $p_{\text{attack}} = p_{\text{dorm}} = 1$, $q_{\text{attack}} = 0.7$, $q_{\text{dorm}} = 0.95$, and the same preview conditions. From these subfigures, it is evident that the system remains stable under the disturbance $d_0(k)$, and as the preview length M_r increases, the system output can track the reference signal more effectively.

We use the following index to evaluate the system's performance

$$J = \sum_{i=1}^{\infty} e^2(i). \quad (34)$$

We set $M_r = 3$, $q_{\text{attack}} = q_{\text{dorm}} = 1$, and $p_{\text{dorm}} = 0.95$. Based on different p_{attack} , we obtain the following table of system performance.

We set $M_r = 3$, $p_{\text{attack}} = p_{\text{dorm}} = 1$, and $q_{\text{dorm}} = 0.95$. Based on different q_{attack} , we obtain the following table of system performance.

It can be seen from Tables 2 and 3 that as the level of DoS attacks intensifies, indicated by the decrease in p_{attack} and q_{attack} , the tracking performance of the system gradually deteriorates. Under the same level of DoS attacks, the degradation in tracking performance is more pronounced when packet loss occurs in the state signal channel compared to the reference signal channel. The presence of preview control leads to improvement in the system's tracking performance.

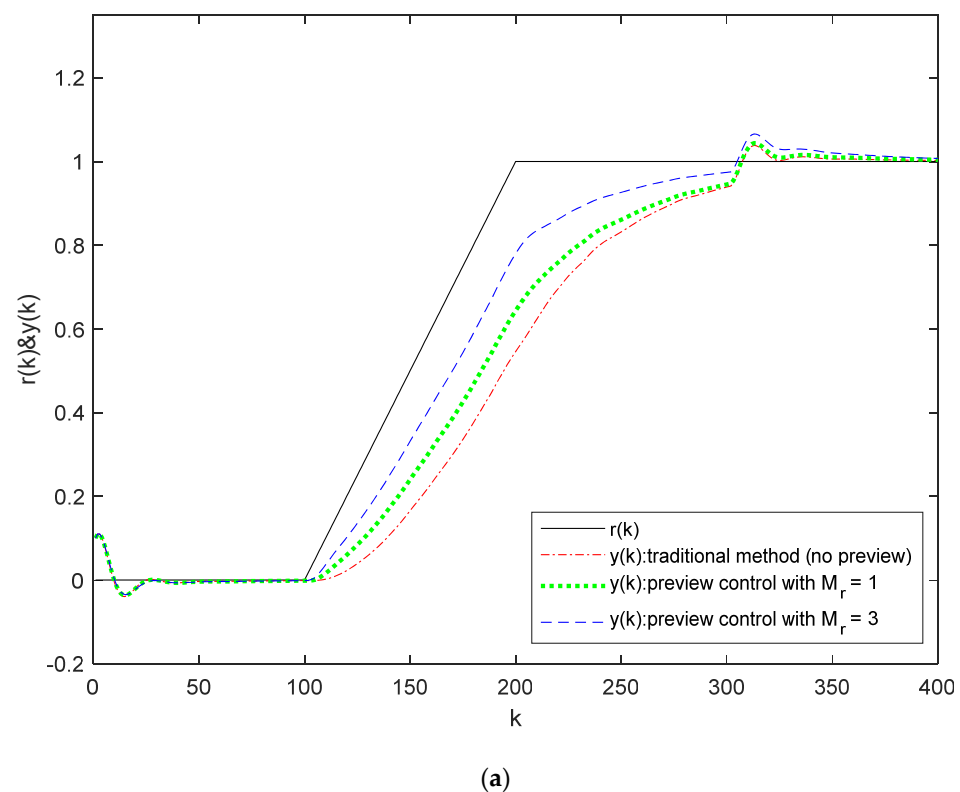
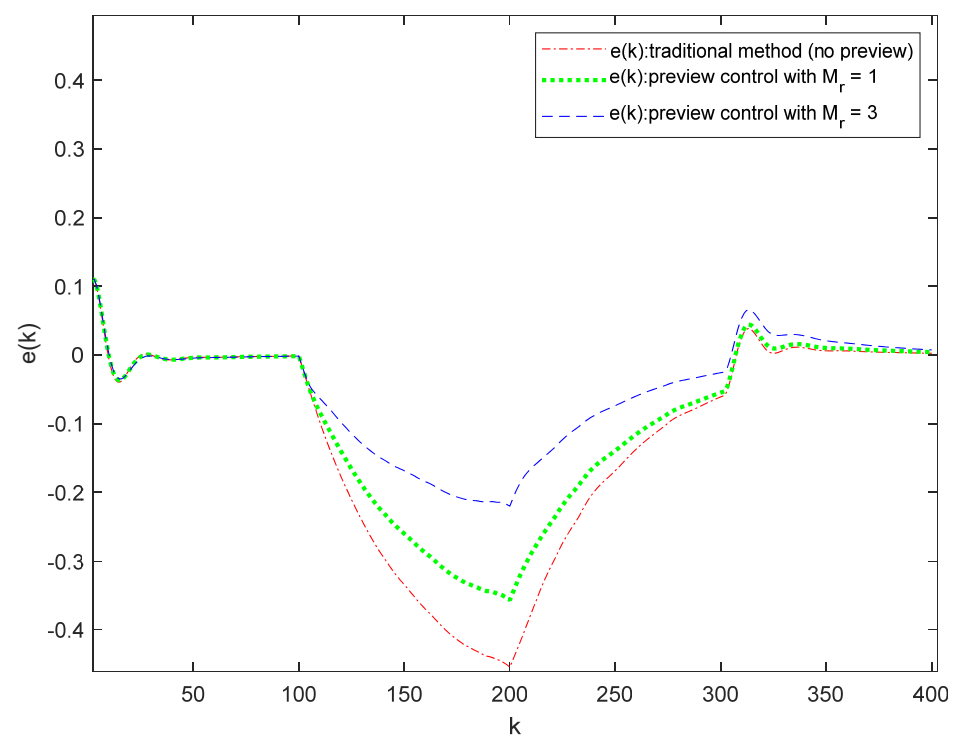
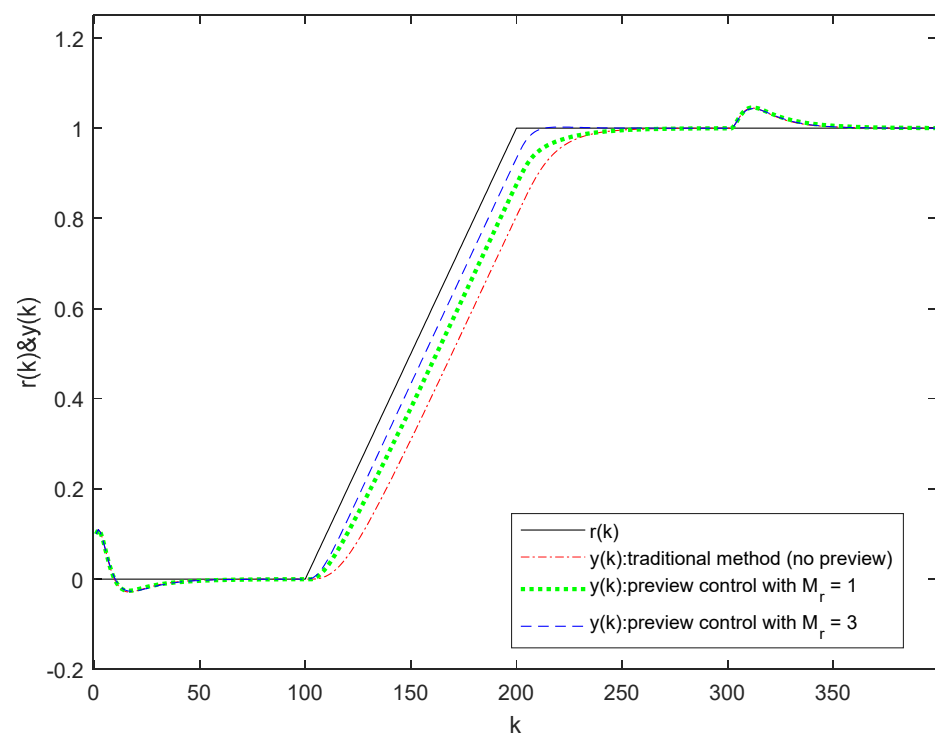


Figure 6. Cont.



(b)



(c)

Figure 6. Cont.

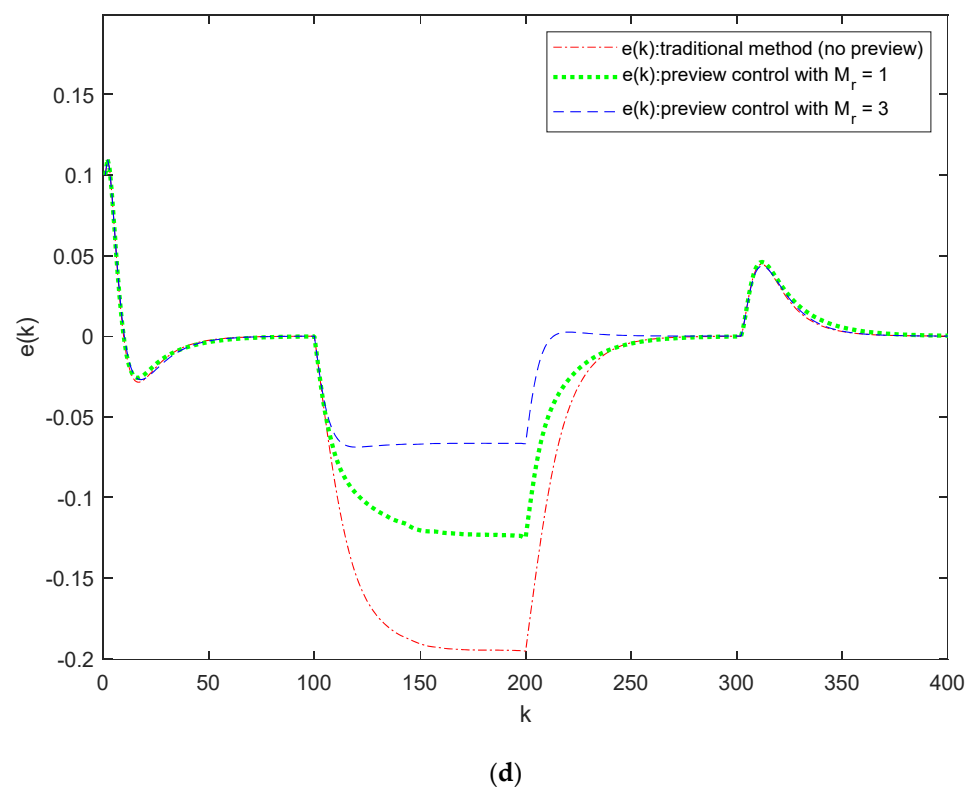


Figure 6. Output responses and error for System (33) using the preview controller proposed in this paper and the method from [22] (without preview): (a) Output responses with packet loss in state signal channel; (b) Error with packet loss in state signal channel; (c) Output responses with packet loss in reference signal channel; (d) Error with packet loss in reference signal channel.

Table 2. System performance under different p_{attack} .

p_{attack}	System Performance ($M_r=3$)	System Performance (without Preview) Method from [22]
0.9	0.6448	2.1533
0.7	2.2887	5.1785
0.5	51.3451	52.3229

Table 3. System performance under different q_{attack} .

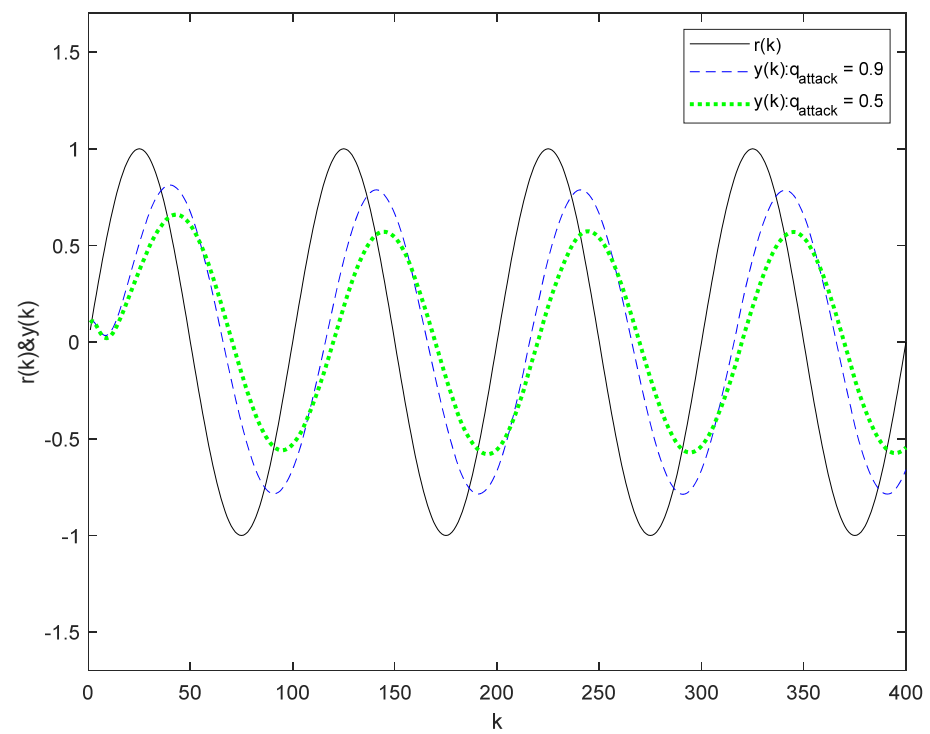
q_{attack}	System Performance ($M_r=3$)	System Performance (without Preview) Method from [22]
0.9	0.2604	1.0309
0.7	0.5131	1.3200
0.5	0.8119	1.5142

Finally, we analyze the advantages of the reference signal attack-tolerant strategy designed in this paper.

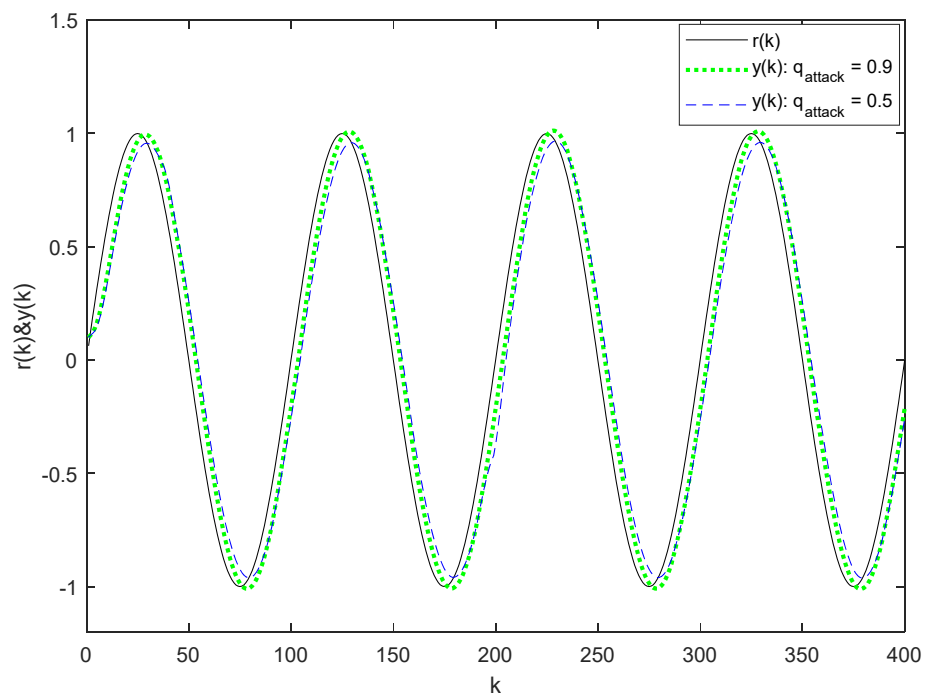
We set $d_0(k) = 0$; for different reference signal packet loss scenarios and varying preview conditions, we obtain the following system outputs.

Figures 7 and 8 display the output responses under different packet loss conditions in the reference signal channels, with varying preview conditions. Figures 7a and 8a represent the case without preview, while Figures 7b and 8b correspond to the case with a preview length of $M_r = 7$. The other parameters used are $p_{attack} = p_{dorm} = 0.95$, $q_{dorm} = 0.95$, and $q_{attack} = 0.9, 0.5$. By comparing Figure 7a,b, as well as Figure 8a,b, we observe that the tracking error significantly decreases between $q_{attack} = 0.9$ and $q_{attack} = 0.5$, indicating that

the preview controller based on the reference signal channel attack-tolerant strategy can mitigate the tracking error between different packet losses in the reference signal channel.

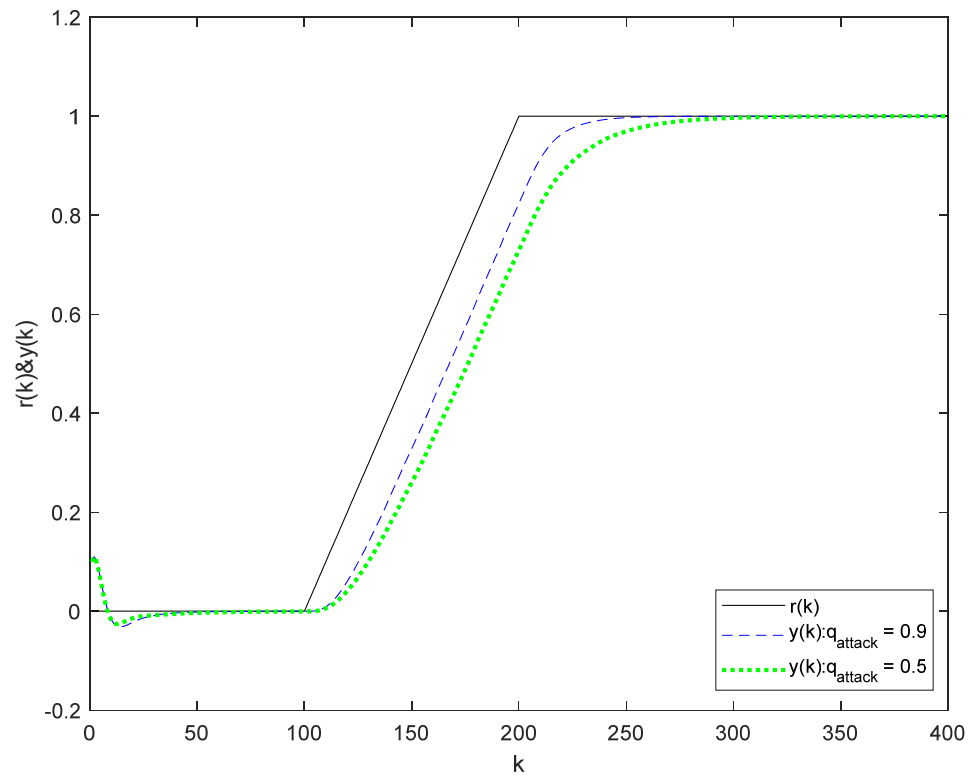


(a)

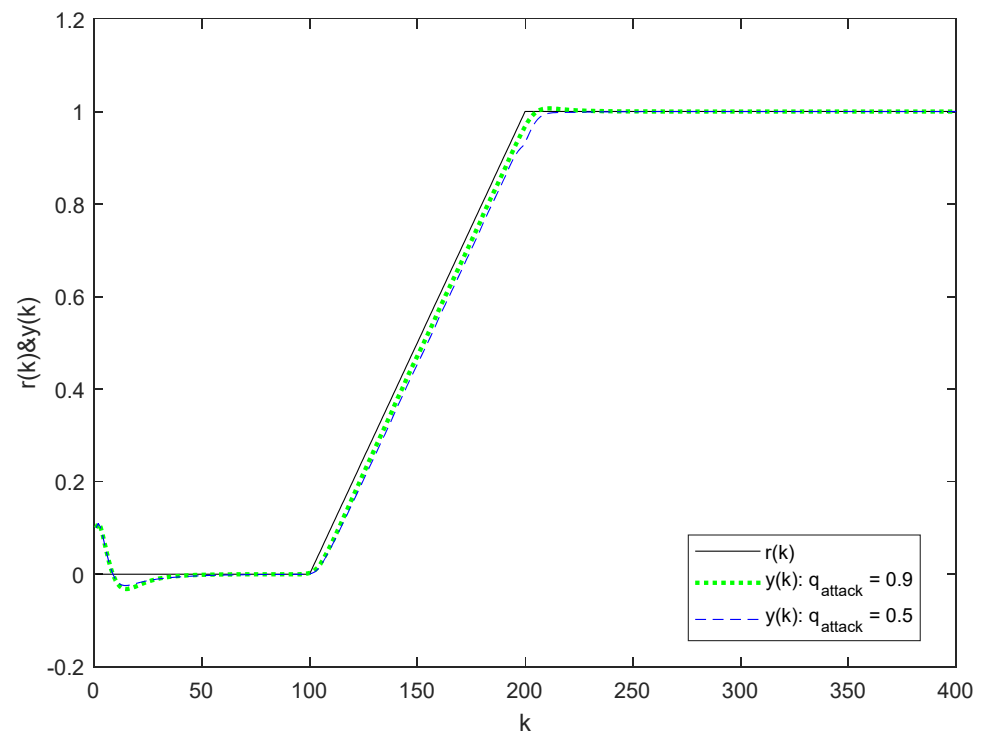


(b)

Figure 7. Output responses for System (32) under different packet loss conditions in the reference signal channel and varying preview conditions: (a) Output responses without preview; (b) Output responses with preview length $M_r = 7$.



(a)



(b)

Figure 8. Output responses for System (33) under different packet loss conditions in the reference signal channel and varying preview conditions: (a) Output responses without preview; (b) Output responses with preview length $M_r = 7$.

5. Conclusions

This paper presents the design of a preview controller for CPSs subject to periodic DoS attacks. Using an attack-tolerant strategy, a Markovian jump AES is constructed to address these challenges. This study investigates the stochastic stability of the AES and successfully develops a corresponding preview controller. This controller effectively tracks reference signals ahead of time, even under periodic DoS attacks affecting both the state and reference signal channels, and mitigates the tracking error between different packet loss in the reference signal channel. The validity of the proposed approach is demonstrated through a numerical simulation with a UGV model, confirming its practical applicability.

Future research could consider the design of preview controllers for CPSs under actuator saturation and state-constrained conditions and explore the extension of this approach to other types of attacks and evaluate their performance in real-world scenarios.

Author Contributions: Methodology, Writing—original draft, J.W.; Methodology, Software, Writing—review and editing, H.X.; Formal analysis, J.L. and Z.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by Interdisciplinary Research Project for Young Teachers of University of Science and Technology Beijing (Fundamental Research Funds for the Central Universities) under Grant FRF-IDRY-20-027.

Data Availability Statement: Data is contained within the article.

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

References

1. Sheridan, T.B. Three Models of Preview Control. *IEEE Trans. Hum. Factors Electron.* **1966**, *HFE-7*, 91–102. [\[CrossRef\]](#)
2. Tomizuka, M. Optimal Continuous Finite Preview Problem. *IEEE Trans. Automat. Control.* **1975**, *20*, 362–365. [\[CrossRef\]](#)
3. Katayama, T.; Ohki, T.; Inoue, T.; Kato, T. Design of an Optimal Controller for a Discrete-Time System Subject to Previewable Demand. *Int. J. Control.* **1985**, *41*, 677–699. [\[CrossRef\]](#)
4. Liao, F.; Takaba, K.; Katayama, T.; Katsuura, J. Design of an Optimal Preview Servomechanism for Discrete-Time Systems in a Multirate Setting. *Dyn. Contin. Discret. Impuls. Syst. Ser. B* **2003**, *10*, 727–744.
5. Liao, F.; Tomizuka, M.; Cao, M.; Wang, D. Optimal Preview Control for Discrete-Time Descriptor Causal Systems in a Multirate Setting. *Int. J. Control.* **2013**, *86*, 844–854. [\[CrossRef\]](#)
6. Liao, F.; Guo, Y.; Tang, Y.-Y. Design of an Optimal Preview Controller for Linear Time-Varying Discrete Systems in a Multirate Setting. *Int. J. Wavelets Multires. Inf. Process* **2015**, *13*, 1550050. [\[CrossRef\]](#)
7. Lan, Y.-H.; Xia, J.-J.; Shi, Y.-X. Robust Guaranteed-Cost Preview Repetitive Control for Polytopic Uncertain Discrete-Time Systems. *Algorithms* **2019**, *12*, 20. [\[CrossRef\]](#)
8. Lan, Y.-H.; He, J.-L.; Li, P.; She, J.-H. Optimal Preview Repetitive Control with Application to Permanent Magnet Synchronous Motor Drive System. *J. Franklin Inst. B.* **2020**, *357*, 10194–10210. [\[CrossRef\]](#)
9. Zhen, Z.; Peng, M.; Xue, Y.; Jiang, S. Robust Preview Control and Autoregressive Prediction for Aircraft Automatic Carrier Landing. *IEEE Access* **2019**, *7*, 181273–181283. [\[CrossRef\]](#)
10. Zhen, Z.; Jiang, S.; Ma, K. Automatic Carrier Landing Control for Unmanned Aerial Vehicles based on Preview Control and Particle Filtering. *Aerosp. Sci. Technol.* **2018**, *81*, 99–107. [\[CrossRef\]](#)
11. Zhen, Z.; Jiang, S.; Jiang, J. Preview Control and Particle Filtering for Automatic Carrier Landing. *IEEE Trans. Aerosp. Electron. Syst.* **2018**, *54*, 2662–2674. [\[CrossRef\]](#)
12. Kim, K.-D.; Kumar, P.R. Cyber-Physical Systems: A Perspective at the Centennial. In Proceedings of the International Congress on Ultra Modern Telecommunications and Control systems and Workshops (CUMTW), St. Petersburg, Russia, 3–5 October 2012; pp. 1287–1308.
13. Derler, P.; Lee, E.A.; Vincentelli, A.S. Modeling Cyber-Physical Systems. In Proceedings of the Data Stream Mining and Processing (DSMP), Lviv, Ukraine, 21–25 August 2020; pp. 13–28.
14. Tutsoy, O.; Asadi, D.; Ahmadi, K.; Nabavi-Chasmi, S.Y. Robust Reduced Order Thau Observer with the Adaptive Fault Estimator for the Unmanned Air Vehicles. *IEEE Trans. Veh. Technol.* **2023**, *72*, 1601–1610. [\[CrossRef\]](#)
15. Asadi, D.; Bagherzadeh, S.A. Nonlinear Adaptive Sliding Mode Tracking Control of an Airplane with Wing Damage. *J. Aerosp. Eng.* **2018**, *232*, 1405–1420. [\[CrossRef\]](#)
16. Kazemi, Z.; Safavi, A.A.; Naseri, F.; Urbas, L.; Setoodeh, P. A Secure Hybrid Dynamic-State Estimation Approach for Power Systems under False Data Injection Attacks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7275–7286. [\[CrossRef\]](#)
17. Gatouillat, A.; Badr, Y.; Massot, B.; Sejdić, E. Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine. *IEEE Internet Things* **2018**, *5*, 3810–3822. [\[CrossRef\]](#)

18. 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. Franklin Inst. B.* **2016**, *353*, 2451–2466. [[CrossRef](#)]
19. Sinha, P.; Jha, V.K.; Rai, A.K.; Bhushan, B. Security Vulnerabilities, Attacks and Countermeasures in Wireless Sensor Networks at Various Layers of OSI Reference Model: A Survey. In Proceedings of the International Conference on Signal Processing and Communication System. (ICSPC), Gold Coast, Australia, 16–18 December 2017; pp. 288–293.
20. Zhu, M.; Martinez, S. Attack-Resilient Distributed Formation Control via Online Adaptation. In Proceedings of the Conference on Decision and Control and European Control Conference (CDC-ECC), Orlando, FL, USA, 12–15 December 2011; pp. 6624–6629.
21. Feng, S.; Tesi, P. Resilient Control under Denial-of-Service: Robust Design. *Automatica* **2017**, *79*, 42–51. [[CrossRef](#)]
22. Wang, M.-F.; Xu, B.-G. State Feedback Stabilization of Cyber-Physical System under DoS Jamming Attacks. *J. Control Decis.* **2019**, *34*, 1681–1687.
23. Qiu, L.; Zhong, X.; Li, S.; Xu, B. Output Feedback Stabilization of Networked Control Systems with Uncertain Transition Probability Matrix. In Proceedings of the Conference on Intelligent Control and Automation Science (ICONS), Chengdu, China, 2–4 September 2013; pp. 292–297. [[CrossRef](#)]
24. Zhao, D.; Lam, H.; Peng, H.; Bao, S.; LeBlanc, D.J.; Nobukawa, K.; Pan, C.S. Accelerated Evaluation of Automated Vehicles Safety in Lane-Change Scenarios based on Importance Sampling Techniques. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 595–607. [[CrossRef](#)]
25. Zhao, D.; Huang, X.; Peng, H.; Lam, H.; LeBlanc, D.J. Accelerated Evaluation of Automated Vehicles in Car-Following Maneuvers. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 733–744. [[CrossRef](#)]
26. Liao, F.; Li, L. Robust Preview Control for Uncertain Discrete-Time Systems based on LMI. *Optim. Control. Appl. Methods* **2017**, *38*, 1022–1031. [[CrossRef](#)]
27. Boyd, S.; Feron, E.; Ghaoui, L.E.; Balakrishnan, V. *Linear Matrix Inequalities in System and Control Theory*, 1st ed.; Society for Industrial and Applied Mathematics (SIAM): Pennsylvania, PA, USA, 1994; pp. 7–27.
28. Chaomel, L.E.; Oustry, F.; Aitrami, M. A Cone Complementarity Linearization Algorithm for Static Output Feedback and Related Problems. *IEEE Trans. Autom. Control.* **1997**, *42*, 1171–1176.
29. Lu, A.-Y.; Yang, G.-H. Secure State Estimation for Cyber-Physical Systems under Sparse Sensor Attacks via a Switched Luenberger Observer. *Inf. Sci.* **2017**, *417*, 454–464. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.