sensors

MDPI

Article

Observer-Based Event-Triggered Predictive Control for Networked Control Systems under DoS Attacks

Weifan Lu [1], Xiuxia Yin [1,*], Yichuan Fu [2] and Zhiwei Gao [2]

[1] The Department of Mathematics, School of Science, Nanchang University, Nanchang 330031, China; luweifan1217@163.com

[2] The Faculty of Engineering and Environment, University of Northumbria at Newcastle, Newcastle upon Tyne NE1 8ST, UK; yichuan.fu@northumbria.ac.uk (Y.F.); zhiwei.gao@northumbria.ac.uk (Z.G.)

* Correspondence: yinxiuxiaa0635@163.com

Received: 2 November 2020; Accepted: 24 November 2020; Published: 30 November 2020

Abstract: This paper studies the problem of DoS attack defense based on static observer-based event-triggered predictive control in networked control systems (NCSs). First, under the conditions of limited network bandwidth resources and the incomplete observability of the state of the system, we introduce the event-triggered function to provide a discrete event-triggered transmission scheme for the observer. Then, we analyze denial-of-service (DoS) attacks that occur on the network transmission channel. Using the above-mentioned event-triggered scheme, a novel class of predictive control algorithms is designed on the control node to proactively save network bandwidth and compensate for DoS attacks, which ensures the stability of NCSs. Meanwhile, a closed-loop system with an observer-based event-triggered predictive control scheme for analysis is created. Through linear matrix inequality (LMI) and the Lyapunov function method, the design of the controller, observer and event-triggered matrices is established, and the stability of the scheme is analyzed. The results show that the proposed solution can effectively compensate DoS attacks and save network bandwidth resources by combining event-triggered mechanisms. Finally, a smart grid simulation example is employed to verify the feasibility and effectiveness of the scheme's defense against DoS attacks.

Keywords: event-triggered control; static observer; DoS attack; predictive control; compensation

1. Introduction

In recent years, with the development of computer networks and wireless communication technology, the rapid development of network control systems (NCSs) has led to a new round of industry change. With the emergence of 5G technology, more control systems can be combined with networks, and remote closed-loop NCSs can be formed through the network transmission of signals, which has been widely used in actual production [1–3]. Due to its wide range of applications, the stability and security of NCSs have attracted much attention in the academic community [4–8].

The combination of networks and control systems greatly improves the flexibility of all connected system devices. In other words, all system equipment can be connected through a wired or wireless network, replacing the original point-to-point control structure [9–11]. In [12–14] , the authors analyzed the modeling and design problems of NCSs. NCSs mainly exchange control information through the network. Because the network is introduced during the control loop, a series of network problems (limited bandwidth resources, data dropout, etc.) are introduced into the control system, which greatly

affect the performance of NCSs. In an open network environment, the security of control information is important. The most common network attack method of NCSs is a denial-of-service (DoS) attack. A DoS attack is a resource exhaustion-type attack. The primary purpose of a DoS attack is to render a computer or network incapable of providing normal services and to consume significant bandwidth resources. Ultimately, the lack of network bandwidth resources due to a DoS attack leads to serious consequences from such an attack, regardless of the processing speed of the computer, memory capacity or network bandwidth. For NCSs, DoS attacks prevent remote controllers and actuators from receiving feedback signals and control signals. Under DoS attacks, NCSs may be made unstable due to the lack of feedback measurement signals and control signals.

Based on the five issues of NCSs mentioned in [15] (sampled-data control, quantization control, networked control, event-triggered control and security control) and the analysis of NCSs exhibition trends and techniques, the security of NCSs can no longer be ignored. (i) For the current mainstream works on the safety of NCSs, NCSs mainly rely on digital sampling. The vast majority of DoS attacks can be modeled as packet loss of the control system. As a result, the security of NCSs primarily characterizes DoS attacks as packet loss. Currently, several design approaches for NCSs schemes have been reported in [16–18]. It is noteworthy that, except for a few works [19–28], most of the available results mentioned above do not consider the safety of NCSs but only discuss the design approach of NCSs schemes. For example, in [19], the stability of a network linear continuous-time system under power-constrained, known and unknown, pulse-width modulated DoS attack signals is investigated. In [20], a more general model for DoS attacks is proposed, where the characteristics of DoS attack are defined by the DoS attack frequency and the DoS attack duration. Based on similar ideas, extensions are made in [21] for dynamic output feedback controllers, in [22] for nonlinear networked control systems, and in [23] for distributed networked control systems. In [24], the stability and robustness of a network linear discrete-time system with random packet loss and random attacks is investigated. In [25], the zero-sum static game framework is applied to deal with the optimal control and scheduling problem of a linear network control system with communication constraints and DoS attacks. In [26], a state feedback resilient controller design method that relies on acyclically sampled data for the maximum and minimum durations of DoS attacks is presented by embedding a logic processor in the controller to capture DoS attack information and compute DoS parameters. Most of the results mentioned above are limited to performance analysis and do not explore controller synthesis [27]. Furthermore, these results assume the availability of system-wide state information, which limits their application in real control systems where only preliminary observations of the actual system state are measurable, usually due to limited communication and bandwidth resources or unavoidable noise [28]. (ii) In addition to the security issues caused by DoS attacks in NCSs, the network bandwidth resources are also very limited, reducing the frequent use of network bandwidth resources is also an urgent problem to be solved. The reduction of network bandwidth consumption by event-triggered control (ETC) has been extensively studied (see [16,29] for a single continuous-time system and [30,31] for multiagent systems), which makes ETC a promising solution for limited bandwidth resources of NCSs. Based on the above observations, is it possible to develop a unified observer-based output feedback scheme that can maintain system performance (stability) and compensate for the loss of control information caused by DoS attacks, while greatly saving limited network bandwidth resources and being more suitable for real-life scenarios (greater use of network convenience)? It is the focus of this paper to address this set of problems in a way that can be uniformly handled when the simultaneous effects of malicious DoS attacks, limited bandwidth resources, and unavailability of all state information are present.

This paper proposes a novel observer-based predictive control defense scheme, as shown in Figure 1, called observer-based event-triggered predictive control (OB-ETPC). Under this framework, we will study the observer-based predictive control system to actively compensate for data dropout due to a DoS attack and use the basic ideas of predictive control, linear matrix inequality (LMI) and Lyapunov function

methods to solve the corresponding problems of event-triggered matrices, observer gain matrices and controller matrices. This work represents a significant expansion of previous results involving predictive control (PC) and the event-trigger mechanism (ET) under a DoS attack. The advantages of the proposed control defense scheme are fourfold:

(1) Our method is very different to that in the works of networked PCs [32–34] which have used time-triggered communication schemes. This paper adopts event-triggered predictive communication schemes to design a controller. Whether the observer's state measurement information is sent depends on the error between the current observer state and the observer state of the most recently sent information. The event-triggered generator on the controller side greatly reduces the size of the sent predictive control sequences, greatly reduces the occupation of bandwidth resources and can also meet the needs of control performance [35].

(2) Compared with the existing predictive control compensation scheme for DoS attacks [7], another advantage of the OB-ETPC scheme adopted in this paper is the combination of the advantages of PC and ET [27,36–42]. With the combination of a model and static observer, it can cope with the problem that state information cannot be obtained directly and can also actively compensate for data packet dropout due to DoS attacks and greatly improve the stability of NCSs under DoS attacks.

(3) Compared with the latest DoS attack compensation scheme, the method in [27] only considers DoS attacks from the controller to the actuator side. In real-life scenarios, the attack from the sensor to controller side is often through a network link. In this paper, the novel OB-ETPC solves the problem of DoS attacks on both the sensor-to-controller and controller-to-actuator sides, which is more in line with real-life scenarios.

(4) The OB-ETPC is established to actively compensate for DoS attacks in NCSs. The observer gain matrix L and controller gain matrix K are co-designed based on the Lyapunov function method, and related criteria for event-triggered matrices are proposed based on linear matrix inequalities (LMIs).

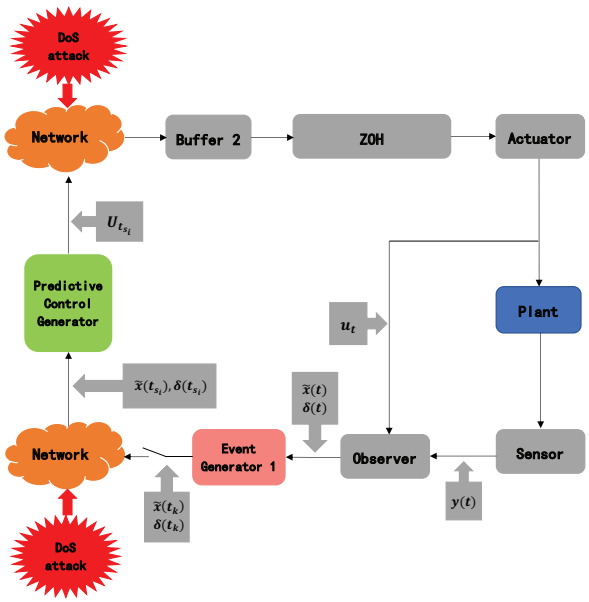

Figure 1. The diagram of the observer-based event-triggered predictive control (OB-ETPC) systems under denial-of-service (DoS) attacks.

The remainder of this paper is organized as follows. Section 2 deals with the problem descriptions and preliminaries. Section 3 considers OB-ETPC and the stability analysis of NCSs under DoS attacks. Section 4 verifies the feasibility of OB-ETPC under DoS attacks through a simulation example. We draw conclusions in Section 5.

All notations used in this paper are defined in the Table 1.

Table 1. All notations in this paper.

Notations	Definitions
$x(t) \in \mathbb{R}^n$	The state vector.
$u(t) \in \mathbb{R}^m$	The control vector.
$y(t) \in \mathbb{R}^q$	The device output vector.
$\widetilde{x}(t) \in \mathbb{R}^n$	The state vector of the observer.
$\widetilde{y}(t) \in \mathbb{R}^q$	The output vector of the observer.
$\widehat{x}(t) \in \mathbb{R}^n$	The state vector of the predictive control generator.
$\delta(t)$	The observer state error.
t_k $(k = 1, 2, ...,)$	The time to trigger the Event Generator 1.
t_{s_i}	The moment at which the predictive control generator that successfully receives the data.
A, B and C	The appropriate dimension matrices of the system.
L	The gain matrix of the observer.
K	The feedback gain matrix.
$\mu > 0$	A given scalar.
M	A given positive integer.
Φ	A positive definite weight matrix.
T	The period of DoS attacks.
$n \in R$	The number of the DoS attack cycle.
$T_{off}^{min} \in (0, +\infty)$	A real number which satisfies $T_{off}^{min} \leq T_{off} < T$.
p	A real number which satisfies $p \triangleq T - T_{off}^{min}$.
M	A given positive integer.
P and Q	The symmetrical positive definite matrices.

2. Problem Descriptions and Preliminaries

In this paper, we will study an observer-based state feedback networked control system under DoS attacks, as shown in Figure 1. The sensor component and the control component and the control component and the actuator component are connected through the network. Due to the openness and vulnerability of the network, NCSs are vulnerable to DoS attacks [43,44].

It is assumed that the dynamic evolution law of the controlled plant can be described by the following discrete system:

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

where $x(t) \in \mathbb{R}^n$ represents the state vector, $u(t) \in \mathbb{R}^m$ represents the control vector and $y(t) \in \mathbb{R}^q$ represents the device output vector. A, B and C are the appropriate dimension matrices of 1.00,0.00,0.00 system (1) and K is the feedback gain matrix (to be solved below). The initial state of 1.00,0.00,0.00 system (1) is $x(t_0) = x(0)$.

Description of Each Component

(1) Sensor: The high-sensitivity sensor sends the output signal from plant to the observer [45].

(2) Observer: In reality, most systems cannot directly obtain the system's state vector $x(t)$. Using $u(t) = Cx(t)$ to analyze the problem is restrictive and inaccurate. Therefore, in order to estimate plant state information, the observer is introduced into the NCSs. The full-dimension state observer is

$$\begin{aligned} \widetilde{x}(t+1) &= A\widetilde{x}(t) + Bu(t) + L(y(t) - \widetilde{y}(t)), \\ \widetilde{y}(t) &= C\widetilde{x}(t). \end{aligned} \tag{2}$$

where $\widetilde{x}(t) \in \mathbb{R}^n$ is the state vector of the observer, $\widetilde{y}(t) \in \mathbb{R}^q$ is the output vector of the observer and L is the gain matrix of the observer. We define $\delta(t)$ as the observer state error. Then,

$$\begin{aligned} \delta(t) &= x(t) - \widetilde{x}(t), \\ \delta(t_0) &= x(t_0) - \widetilde{x}(t_0), \end{aligned} \tag{3}$$

and the observer error system can be described by

$$\begin{aligned} \delta(t+1) &= x(t+1) - \widetilde{x}(t+1) \\ &= Ax(t) + Bu(t) - [A\widetilde{x}(t) + Bu(t) + L(y(t) - \widetilde{y}(t)] \\ &= (A - LC)\delta(t) \\ &= (A - LC)^{t+1}\delta(t_0). \end{aligned} \tag{4}$$

(3) Event Generator 1: Due to the limitation of network bandwidth resources, in order to reduce the transmission of data packets, prevent network congestion and improve the utilization of network bandwidth resources and the performance of NCSs, Event Generator 1 is designed on the sensor side to determine whether data packets need to be transmitted to the controller side [46].

In this paper, we first introduce the event-triggered scheme in Event Generator 1 and assume that the time to trigger the Event Generator 1 is t_k $(k = 1, 2, ...,)$; then, the observer state information which is transmitted at this time is $\widetilde{x}(t_k)$. The next trigger moment is

$$\begin{aligned} t_{k+1} &= t_k + \min\{r_k, M\}, \\ r_k &= \min_r \left\{ r | \left[\widetilde{x}(t_k + r) - \widetilde{x}(t_k)\right]^T \Phi \left[\widetilde{x}(t_k + r) - \widetilde{x}(t_k)\right] > \mu \widetilde{x}(t_k + r)^T \Phi \widetilde{x}(t_k + r) \right\}. \end{aligned} \tag{5}$$

where $\mu > 0$ is a given scalar, M is a given positive integer, and Φ is a positive definite weight matrix. According to the above 1.00,0.00,0.00 condition (5), the next trigger time is determined by the current observer state $\widetilde{x}(t_k + r)$ and the observer state $\widetilde{x}(t_k)$ at the latest trigger time, μ and Φ. Therefore, for $\mu > 0$ and $\Phi > 0$, if $f(t_k + r, t_k) \leq 0$, the state data packets at $t_k + r$ need not be transmitted.

$$f(t_k + r, t_k) \triangleq \left[\widetilde{x}(t_k + r) - \widetilde{x}(t_k)\right]^T \Phi \left[\widetilde{x}(t_k + r) - \widetilde{x}(t_k)\right] - \mu \widetilde{x}(t_k + r)^T \Phi \widetilde{x}(t_k + r). \tag{6}$$

In other words, the embedded trigger condition of the Event Generator 1 is

$$f(t_k + r, t_k) > 0. \tag{7}$$

When the trigger 1.00,0.00,0.00 condition (7) is satisfied, the observer's state information and state error are transmitted through the network and released to the controller.

Remark 1. *Reducing network bandwidth consumption through event-driven control (ETC) has been extensively studied in [16,29–31]. Thus, ETC provides a very promising option to solve the bandwidth resource problem of NCSs under DoS attacks.*

Remark 2. *The data packet which is transmitted from the observer to the controller includes* $\widetilde{x}(t_k)$ *and* $\delta(t_k)$.

Remark 3. *M is the upper limit of the trigger time interval given by us to prevent long-term non-triggering from affecting the stability of the system.*

(4) Predictive control generator: Combined with the model-based event-triggered predictive control (MB-ETPC) system, the plant's predictive model is introduced on the control side. The predictive model is used to actively compensate a DoS attack and generate corresponding predictive control sequences. Then, Event Generator 2 is introduced at the control side, which is used to reduce the sending size of the predictive control sequences and further reduce the occupation of bandwidth resources. The predictive control sequences that trigger Event Generator 2 are packaged into a single data packet and sent to the actuator side through the network.

(5) Buffer: The buffers are used to store the incoming data packets.

(6) Zero-order holder (ZOH): The ZOH is used to choose a suitable control signal with a hold event interval of $\Omega = [t_{s_i}, t_{s_{i+1}})$. t_{s_i} is the moment that the predictive control generator successfully receives the data.

(7) Actuator: The function of the actuator is to receive the control signal from the ZOH and control the plant.

In order to facilitate the analysis, we make the following assumptions regarding the above OB-ETPC system:

Assumption 1. *1.00,0.00,0.00 System (1) performs isochronous sampling. The sampling time is h, and all data packets are time-stamped.*

Assumption 2. *The sensor is time-driven, and the predictive controller and actuator are event-driven.*

Assumption 3. *This paper does not consider the time delay of the system and the delay of the transmission process.*

Assumption 4. *Assume that (A, B) is completely controllable and (A, C) is completely observable.*

Assumption 5. $\widetilde{x}(t_0)$ *and* $\delta(t_0)$ *are successfully sent at the initial moment* t_0 *from the observer to the controller.*

3. OB-ETPC of NCSs under DoS Attacks and Stability Analysis

3.1. DoS Attack Description

Denial-of-service (DoS) attacks are simple and effective attacks against a server. The purpose of DoS attacks is to allow the attacked host and server to deny normal users access and disrupt the normal operation of the system. Internet users cannot reach the attacked server and host, causing the server to fail [47]. DoS attacks occur on the sensor-to-controller and controller-to-actuator communication channels. Under DoS attacks, the network control systems will become unstable due to the lack of feedback

measurement signals and control signals. Several typical examples of defenses against DoS attacks on modern NCSs are as follows: the United States specifically established the "National Infrastructure Protection Plan" in 2006 and the "Control System Security Plan (CSSP)" in 2010 to incorporate the protection of related national infrastructure control systems into national strategic plans, the European Union released the "European Program for Critical Infrastructure Protection (EPCIP)" in 2013 and the Ministry of Industry and Information Technology (MIIT) in China issued the "Notice on Strengthening the Information Security Management of Industrial Control Systems" in September 2011 [48].

Due to DoS attacks affecting the communication channel, at this time, the observer state data packets released to the control end by Event Generator 1 and the system control sequence packets sent to the actuator side will suffer data dropout due to the DoS attacks. The information transmission under DoS attacks is shown in Figure 2.

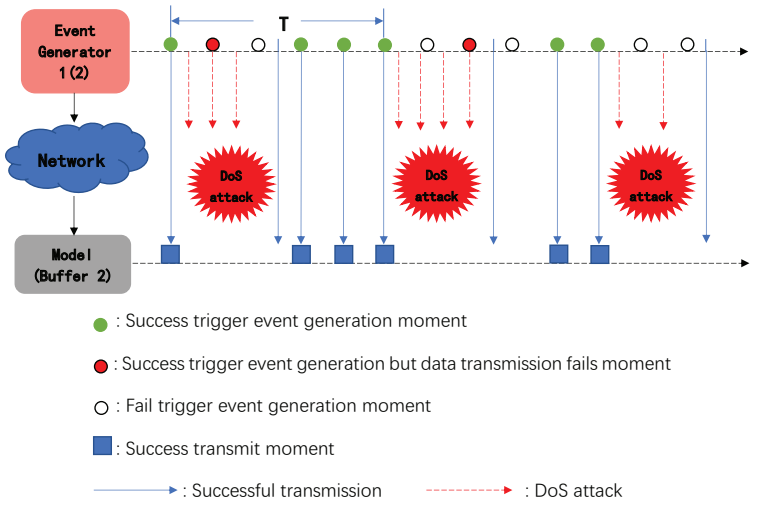

Figure 2. Diagram of information transmission under DoS attacks.

This paper considers periodic DoS attacks of a variable duration, which is a more general approach. According to [49], the model of DoS attacks is described as follows:

$$I_{DoS} = \begin{cases} 0, t \in [nT, nT + T_{off}), \\ 1, t \in [nT + T_{off}, nT + T). \end{cases} \tag{8}$$

where $n \in R$ represents the number of the DoS attack cycle, $\bigcup_{n\in R}[nT, nT + T_{off})$ represents the time interval without DoS attacks and $\bigcup_{n\in R}[nT + T_{off}, nT + T)$ represents the time interval of DoS attacks; see Figure 3.

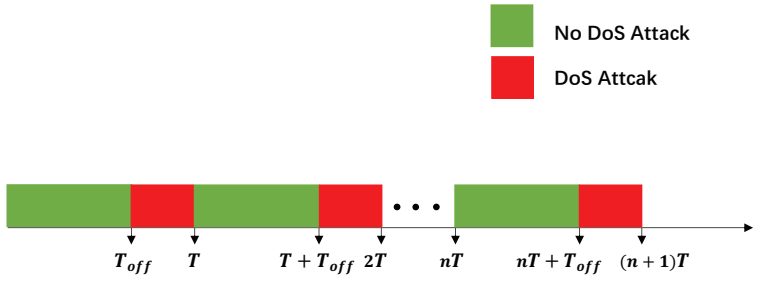

Figure 3. Diagram of the DoS attacks' periodicity.

The main aim of this paper is to use the idea of predictive control to actively compensate for the loss of triggered data packets due to DoS attacks. Based on the received observer state signal $\widetilde{x}(t_{s_i})$, the prediction controller not only needs to calculate the current control signal $u(t_{s_i})$ but also to perform continuous control serial prediction based on the current observer state signal. The generated data packets $U_{t_{s_i}}$ are stored in Buffer 2. The ZOH chooses the suitable control signal to control the plant, which plays an active role in compensating for data packet loss due to DoS attacks.

Remark 4. *In the process of DoS attack compensation, the ZOH adopts a time-driven mechanism. The ZOH continuously sends the $u(t_{s_i})$ of Buffer 2 to the executor until a split-second before $\widehat{t}_{s_{i+1}}$. If the packet in Buffer 2 is not updated before $\widehat{t}_{s_{i+1}}$, the ZOH will send the data $\widehat{u}(\widehat{t}_{s_{i+1}}|t_{s_i})$ of the latest packet in Buffer 2 to the actuator continuously, and so on, until the packet of Buffer 2 is updated. If the packet in Buffer 2 is updated, the new packet is used to perform the above compensation mechanism.*

Remark 5. *At present, several design methods for network NCSs schemes have been reported in [16–18] (except for a few works [19–22,24,25]). Most of the above design schemes do not consider the security of network NCSs but only discuss the design methods of NCSs schemes. Therefore, exploring NCS compensation under DoS attack is particularly important to solve the security problem of NCSs.*

Assumption 6. *DoS attacks lead to a data packet dropout rate of* 100% .

Assumption 7. *This paper considers periodic DoS attacks, and the period of DoS attacks is T. Because the duration of DoS attacks is variable, we define a real number $T_{off}^{min} \in (0, +\infty)$ which satisfies $T_{off}^{min} \leq T_{off} < T$ and $p \triangleq T - T_{off}^{min}$.*

Assumption 8. *The time interval between two adjacent DoS attacks is greater than M.*

3.2. OB-ETPC of NCSs under DoS Attacks

Most of the currently researched DoS attack compensation predictive controllers directly compensate for data packet loss by predicting the dynamic evolution of NCSs under a predictive event-driven mechanism. In order to prevent DoS attacks, this paper uses a new predictive controller which combines ET and PC. We assume that the predictive model of the plant is known. The OB-ETPC actively compensates for DoS attacks to ensure system stability and ultimately achieve defense against DoS attacks. Therefore, the structure of the OB-ETPC controller design is shown in Figure 4.

Due to the existence of DoS attacks, the observer's state information $\{\widetilde{x}(t_k)\}_{k=1}^{\infty}$ triggered by Event Generator 1 cannot be completely transmitted because of data dropout. Thus, we introduce $\{\widetilde{x}(t_{s_i})\}_{i=1}^{\infty}$ to present the observer's state information which is successfully received at times $\{t_{s_i}\}_{i=1}^{\infty}$; then, $\{\widetilde{x}(t_{s_i})\}_{i=1}^{\infty} \subseteq \{\widetilde{x}(t_k)\}_{k=1}^{\infty}$.

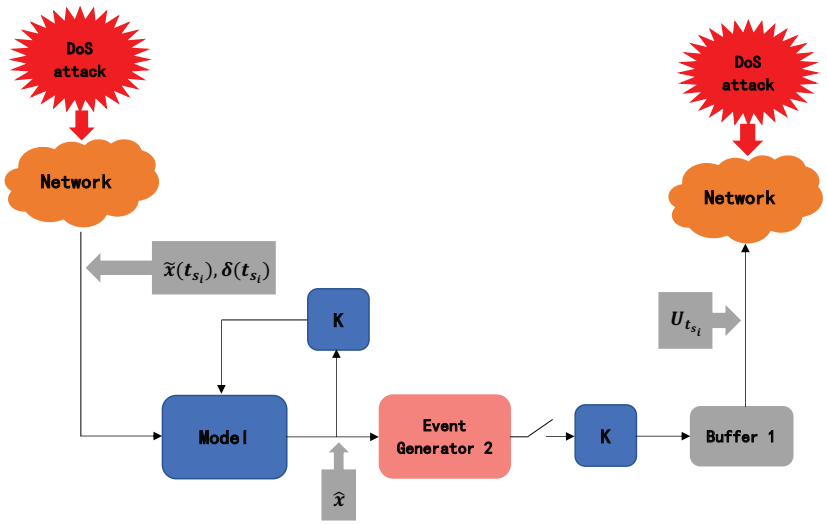

Figure 4. The block diagram of the predictive control generator.

Remark 6. *Compared with the latest DoS attack compensation scheme [27], when network communication is introduced from the sensor to controller, the proposed OB-ETPC solves the DoS attack problem from the sensor to controller and controller to actuator.*

Remark 7. *Based on Remark 2 and the existence of DoS attacks, we define* $\{\delta(t_{s_i})\}_{i=1}^{\infty}$ *to present the observer's state error which is successfully received at time* $\{t_{s_i}\}_{i=1}^{\infty}$*, then* $\{\delta(t_{s_i})\}_{i=1}^{\infty} \subseteq \{\delta(t_k)\}_{k=1}^{\infty}$.

Remark 8. *Based on Assumption 7, Assumption 8 and the event-triggering 1.00,0.00,0.00 condition (5), the times* $t_{s_{i+1}}$ *and* t_{s_i} *of two successful transmissions satisfy the following relationship:* $t_{s_{i+1}} - t_{s_i} \leq 2 \times M + p$.

The predictive model system is

$$\hat{x}(t+1) = A\hat{x}(t) + Bu(t) + LC\delta(t). \tag{9}$$

Next, we will explain in detail the use of OB-ETPC to prevent DoS attacks and actively compensate for state data packet loss due to DoS attacks. Due to the impact of DoS attacks, the moment of the successfully received from observer is t_{s_i}. As long as the observer's state $\tilde{x}(t_{s_i})$ is successfully received by the predictive controller, it will be predicted by the predictive model 1.00,0.00,0.00 system (9). The predictive model will perform prediction to obtain the corresponding predictive control sequences and actively compensate for the DoS attack. The closed-loop state prediction at the future trigger moment is as 1.00,0.00,0.00 follow:

$$
\begin{aligned}
\widehat{x}(t_{s_i}|t_{s_i}) &= \widetilde{x}(t_{s_i}), && (10)\\
\delta(t_{s_i}|t_{s_i}) &= \delta(t_{s_i}), && (11)\\
\widehat{x}(t_{s_i}+1|t_{s_i}) &= A\widehat{x}(t_{s_i}|t_{s_i}) + BK\widehat{x}(t_{s_i}|t_{s_i}) + LC\delta(t_{s_i}|t_{s_i}), && (12)\\
\widehat{x}(t_{s_i}+j+1|t_{s_i}) &= A\widehat{x}(t_{s_i}+j|t_{s_i}) + BKx(t_{s_i}+j|t_{s_i}) + LC\delta(t_{s_i}+j|t_{s_i}), && (13)\\
j &= 1,2,\ldots,\widehat{t}_{s_{i+1}} - t_{s_i} - 1, && (14)\\
&\vdots && (15)\\
\widehat{x}(\widehat{t}_{s_{i+m}}+j+1|t_{s_i}) &= A\widehat{x}(\widehat{t}_{s_{i+m}}+j|t_{s_i}) + BK\widehat{x}(\widehat{t}_{s_{i+m}}+j|t_{s_i}) + LC\delta(\widehat{t}_{s_{i+m}}+j|t_{s_i}), && (16)\\
j &\in \left\{0,1,2,\ldots,\widehat{t}_{s_{i+m+1}} - \widehat{t}_{s_{i+m}} - 1\right\}, && (17)\\
m &\in \{1,2,\ldots,l_i\}, && (18)
\end{aligned}
$$

where $\delta(t_{s_i}+j|t_{s_i}) = (A-LC)^j\delta(t_{s_i})$ and $\delta(\widehat{t}_{s_{i+m}}+j|t_{s_i}) = (A-LC)^j\delta(\widehat{t}_{s_{i+m}}|t_{s_i})$.

In order to reduce the size of the predictive control sequences that need to be sent, Event Generator 2 is introduced into the predictive control generator. $\widehat{t}_{s_{i+1}}$ is the first predictive event-triggered moment:

$$
\begin{aligned}
\widehat{t}_{s_{i+1}} &= t_{s_i} + \min\{r_{s_i}, M\},\\
r_{s_i} &= \min_r \Big\{ r|\ [\widehat{x}(t_{s_i}+r|t_{s_i}) - \widehat{x}(t_{s_i}|t_{s_i})]^T \Phi\, [\widehat{x}(t_{s_i}+r|t_{s_i}) - \widehat{x}(t_{s_i}|t_{s_i})]\\
&\quad > \mu\widehat{x}(t_{s_i}+r|t_{s_i})^T\Phi\widehat{x}(t_{s_i}+r|t_{s_i}) \Big\}, \qquad (19)
\end{aligned}
$$

and

$$
\begin{aligned}
\widehat{t}_{s_{i+m+1}} &= \widehat{t}_{s_{i+m}} + \min\{r_{s_{i+m}}, M\},\\
r_{s_{i+m}} &= \min_r \Big\{ r|\ \left[\widehat{x}(\widehat{t}_{s_{i+m}}+r|t_{s_i}) - \widehat{x}(\widehat{t}_{s_{i+m}}|t_{s_i})\right]^T \Phi\, \left[\widehat{x}(\widehat{t}_{s_{i+m}}+r|t_{s_i}) - \widehat{x}(\widehat{t}_{s_{i+m}}|t_{s_i})\right]\\
&\quad > \mu\widehat{x}(\widehat{t}_{s_{i+m}}+r|t_{s_i})^T\Phi\widehat{x}(\widehat{t}_{s_{i+m}}+r|t_{s_i}) \Big\}, \qquad (20)\\
m &\in \{1,2,\ldots,l_i\},
\end{aligned}
$$

where μ and Φ are given in 1.00,0.00,0.00 condition (5). Therefore, the predicted moment of transmission is $\mathcal{T}_{s_i} = \left\{\ \widehat{t}_{s_{i+1}},\ \ \widehat{t}_{s_{i+2}},\ \ \ldots,\ \ \widehat{t}_{s_{i+l_i}}\ \right\}$.

Remark 9. *Based on Remarks* 3, 8 *and Assumptions* $7-8$, l_i *satisfies* $\widehat{t}_{s_{i+l_i}} \le t_{s_i} + 2\times M + p < \widehat{t}_{s_{i+l_i+1}}$.

Then, l_i predictive event-triggered states are packed into $\widehat{X}(t_{s_i})$.

$$\widehat{X}(t_{s_i}) = \left[\ \widetilde{x}(t_{s_i}), \widehat{x}(\widehat{t}_{s_{i+1}}|t_{s_i}), \cdots, \widehat{x}(\widehat{t}_{s_{i+l_i}}|t_{s_i})\ \right].$$

In order to fully respond to DoS attacks, the controller generates l_i predictive control sequences based on the predictive event-triggered states $\widehat{X}(t_{s_i})$.

According to the corresponding predictive controller law $u(t) = Kx(t)$, the controller's predictive 1.00,0.00,0.00 control can be obtained:

$$
\begin{aligned}
u(t_{s_i}) &= K\widetilde{x}(t_{s_i}), && (21)\\
\widehat{u}(\widehat{t}_{s_{i+1}}|t_{s_i}) &= K\widehat{x}(\widehat{t}_{s_{i+1}}|t_{s_i}), && (22)\\
&\vdots && (23)\\
\widehat{u}(\widehat{t}_{s_{i+l_i}}|t_{s_i}) &= K\widehat{x}(\widehat{t}_{s_{i+l_i}}|t_{s_i}). && (24)
\end{aligned}
$$

1.00,0.00,0.00 Then control sequences are generated as:

$$U_{t_{s_i}} \triangleq \left[\; u(t_{s_i}), \quad \widehat{u}(\widehat{t}_{s_{i+1}}|t_{s_i}), \quad \widehat{u}(\widehat{t}_{s_{i+2}}|t_{s_i}), \quad \cdots, \quad \widehat{u}(\widehat{t}_{s_{i+l_i}}|t_{s_i}) \; \right].$$

The generated l_i predictive control signals are stored in Buffer 2 for the ZOH to select a suitable control input signal. Then, the ZOH sends the selected control input signal to the actuator to complete the defense against the DoS attack.

Compared with other PC approaches [32] without Event Generator 2, all predicted control sequences will be packed, and the predicted control sequences to be sent are $\widehat{U}_{t_{s_i}} = [u(t_{s_i}), \widehat{u}(t_{s_i}+1|t_{s_i}), \widehat{u}(t_{s_i}+2|t_{s_i}), \ldots, \widehat{u}(t_{s_i}+2\times M+p|t_{s_i})]$. Obviously, after Event Generator 2 is added, the size of the predictive control sequences to be transmitted is greatly reduced, and the occupation of bandwidth resources is reduced.

3.3. The Closed-Loop System

Lemma 1. *Comparing the observer 1.00,0.00,0.00 system (2) and predictive model 1.00,0.00,0.00 system (9), 1.00,0.00,0.00it is necessary to provide the proof for the following relationships.*

$$
\begin{aligned}
t_{s_{i+h}} &= \widehat{t}_{s_{i+h}}, && (25)\\
\widehat{x}(\widehat{t}_{s_{i+h}}) &= \widetilde{x}(t_{s_{i+h}}), && (26)\\
\widehat{x}(t) &= \widetilde{x}(t), && (27)\\
h &= 1,2,\ldots,s_{i+1}-s_i-1, && (28)\\
i &= 1,2,\ldots,\infty, && (29)\\
t &\in [t_0,\infty)\cap[t_{s_i},t_{s_{i+1}}). && (30)
\end{aligned}
$$

According to Remark 7 and Lemma 1, the closed-loop system with DoS attack compensation under event-triggering 1.00,0.00,0.00 condition (5) is expressed as

$$
\begin{aligned}
x(t+1) &= Ax(t)+BK\widehat{x}(\widehat{t}_{s_{i+m}}|t_{s_i}), && (31)\\
\widetilde{x}(t+1) &= A\widetilde{x}(t)+BK\widehat{x}(\widehat{t}_{s_{i+m}}|t_{s_i})+LC\delta(\widehat{t}_{s_{i+m}}|t_{s_i}), && (32)\\
\widehat{x}(t+1) &= A\widehat{x}(t)+BK\widehat{x}(\widehat{t}_{s_{i+m}}|t_{s_i})+LC\delta(\widehat{t}_{s_{i+m}}|t_{s_i}), && (33)\\
\delta(t+1) &= (A-LC)\delta(t), && (34)\\
\widehat{x}(t_{s_i}) &= \widetilde{x}(t_{s_i}), && (35)\\
t &\in [t_{s_i},t_{s_{i+1}})\cap[\widehat{t}_{s_{i+m}},\widehat{t}_{s_{i+m+1}}), && (36)\\
m &\in \{1,2,\ldots,l_i\}. && (37)
\end{aligned}
$$

Comparing the 1.00,0.00,0.00 observer system (32) and 1.00,0.00,0.00 predictive model system (33) in the closed-loop system, and to facilitate system analysis and controller design, for $t\in[t_{s_i},t_{s_{i+1}})\cap[\widehat{t}_{s_{i+m}},\widehat{t}_{s_{i+m+1}})$, we define $e_{s_i}(t)=\widetilde{x}(t)-\widetilde{x}(t_{s_{i+m}})$. According to e_{s_i} and $\delta(t)$, the above closed-loop 1.00,0.00,0.00 system (31)–(37) can be written as

$$\begin{aligned} x(t+1) &= Ax(t) + BKx(t) - BKe_{s_i}(t) - BK\delta(t), && (38)\\ \delta(t+1) &= (A - LC)\delta(t), && (39)\\ t &\in [t_{s_i}, t_{s_{i+1}}) \cap [\widehat{t}_{s_{i+m}}, \widehat{t}_{s_{i+m+1}}), && (40)\\ m &\in \{1, 2, \ldots, l_i\}. && (41) \end{aligned}$$

Remark 10. *Note that* $t_{s_{i+1}} = t_{s_i} + t_{s_{i+1}} - t_{s_i} \leq t_{s_i} + 2 \times M + p < \widehat{t}_{s_{i+l_i+1}}$, *and so the compensation selected from Buffer 2 by the ZOH is used to compensate for DoS attacks when* $t \in [t_{s_i}, t_{s_{i+1}})$.

Remark 11. *Comparing event-triggered 1.00,0.00,0.00 conditions (5) and (20), they are found to be consistent. Based on Remark 9, no event is triggered when* $t \in [t_{s_i}, t_{s_{i+1}}) \cap [\widehat{t}_{s_{i+m}}, \widehat{t}_{s_{i+m+1}})$ *[41]. Thus, based on event-triggering 1.00,0.00,0.00 condition (5) and* e_{s_i}, *the following inequality needs to be followed:*

$$\begin{aligned} &e_{s_i}^T(t)\Phi e_{s_i}(t) \leq \mu \widetilde{x}^T(t)\Phi \widetilde{x}(t),\\ &t \in [t_{s_i}, t_{s_{i+1}}) \cap [\widehat{t}_{s_{i+m}}, \widehat{t}_{s_{i+m+1}}). \end{aligned} \tag{42}$$

3.4. Stability Analysis

In this subsection, the design method of the state feedback controller gain matrix K, observer gain matrix L and triggering parameter Φ in 1.00,0.00,0.00 condition (5) will be given.

Theorem 1. *Based on Assumptions 1–7, for given parameters* $0 < \mu < 1$, *1.00,0.00,0.00 the system (38)–(41) will be asymptotically stable if there are matrices* $\widetilde{P} > 0$, $\widetilde{\Phi} > 0$, $Q > 0$ *and matrices* X, G *with appropriate dimensions such that the following LMI is satisfied:*

$$\begin{bmatrix} -\widetilde{P} & * & * & * & * & * \\ 0 & -\widetilde{\Phi} & * & * & * & * \\ 0 & 0 & -Q & * & * & * \\ A\widetilde{P} + BX & -BX & -BX & -\widetilde{P} & * & * \\ \mu\widetilde{\Phi} & -\mu\widetilde{\Phi} & -\mu\widetilde{\Phi} & 0 & -\mu\widetilde{\Phi} & * \\ 0 & 0 & QA - GC & 0 & 0 & -Q \end{bmatrix} < 0, \tag{43}$$

with

$$\Phi = \widetilde{P}^{-1}\widetilde{\Phi}\widetilde{P}^{-1}, K = X\widetilde{P}^{-1}, L = Q^{-1}G.$$

Proof. To connect $x(t)$ and $\delta(t)$, we choose an appropriate Lyapunov function as

$$V(x(t), \delta(t)) = x^T(t)Px(t) + \delta^T Q\delta(t),$$

where P and Q are symmetric positive definite matrices. When $t \in [t_{s_i}, t_{s_{i+1}}) \cap [\widehat{t}_{s_{i+m}}, \widehat{t}_{s_{i+m+1}})$, calculating the difference of $V(x(t), \delta(t))$ along the 1.00,0.00,0.00 system (38)–(41) and taking the inequalities in 1.00,0.00,0.00 condition (42) into account yields that

$$
\begin{aligned}
& \Delta V(x(t),\delta(t)) \\
= \;& V(x(t+1),\delta(t+1)) - V(x(t),\delta(t)) \\
\leq \;& [x^T(t+1)Px(t+1) + \delta^T(t+1)Q\delta(t+1)] - [x^T(t)Px(t) + \delta^T(t)Q\delta(t)] \\
& -e_{s_i}^T(t)\Phi e_{s_i}(t) + \mu\widetilde{x}^T(t_{s_{i+m}})\Phi\widetilde{x}(t_{s_{i+m}}) \\
= \;& [Ax(t) + BKx(t) - BKe_{s_i}(t) - BK\delta(t)]^T P\,[Ax(t) + BKx(t) - BKe_{s_i}(t) - BK\delta(t)] - x^T(t)Px(t) \\
& -\delta^T(t)Q\delta(t) - e_{s_i}^T(t)\Phi e_{s_i}(t) + [(A-LC)\delta(t)]^T Q[(A-LC)\delta(t)] \\
& +\mu[x(t) - e_{s_i} - \delta(t)]^T\Phi[x(t) - e_{s_i} - \delta(t)] \\
= \;& \begin{bmatrix} x^T(t) & e_{s_i}^T(t) & \delta^T(t) \end{bmatrix} [\begin{bmatrix} -P & * & * \\ 0 & -\Phi & * \\ 0 & 0 & -Q \end{bmatrix} + \begin{bmatrix} (A+BK)^T \\ (-BK)^T \\ (-BK)^T \end{bmatrix} P \begin{bmatrix} (A+BK) & (-BK) & (-BK) \end{bmatrix} \\
& + \begin{bmatrix} 0 \\ 0 \\ (A-LC)^T \end{bmatrix} Q \begin{bmatrix} 0 & 0 & (A-LC) \end{bmatrix} + \mu \begin{bmatrix} I \\ -I \\ -I \end{bmatrix} \Phi \begin{bmatrix} I & -I & -I \end{bmatrix}] \begin{bmatrix} x(t) \\ e_{s_i}(t) \\ \delta(t) \end{bmatrix}.
\end{aligned}
$$

By using Schur's complement, if the following inequality is satisfied, $\Delta V(x(t),\delta(t)) < 0$ can be concluded.

$$
\begin{bmatrix}
-P & * & * & * & * & * \\
0 & -\Phi & * & * & * & * \\
0 & 0 & -Q & * & * & * \\
P(A+BK) & P(-BK) & P(-BK) & -P & * & * \\
\mu\Phi & -\mu\Phi & -\mu\Phi & 0 & -\mu\Phi & * \\
0 & 0 & Q(A-LC) & 0 & 0 & -Q
\end{bmatrix} < 0. \tag{44}
$$

However, the above inequality is not in the form of LMI. To reduce it to a linear matrix inequality, we perform pre and 1.00,0.00,0.00 post-multiplying (44) with

$$
diag\{\; P^{-1}, \quad P^{-1}, \quad I, \quad P^{-1}, \quad P^{-1}, \quad I \;\}.
$$

The above matrix inequality is transformed into the following linear matrix inequality form:

$$
\begin{bmatrix}
-P^{-1} & * & * & * & * & * \\
0 & -P^{-1}\Phi P^{-1} & * & * & * & * \\
0 & 0 & -Q & * & * & * \\
(A+BK)P^{-1} & (-BK)P^{-1} & (-BK)P^{-1} & -P^{-1} & * & * \\
P^{-1}\mu\Phi P^{-1} & -P^{-1}\mu\Phi P^{-1} & -P^{-1}\mu\Phi P^{-1} & 0 & -P^{-1}\mu\Phi P^{-1} & * \\
0 & 0 & Q(A-LC) & 0 & 0 & -Q
\end{bmatrix} < 0. \tag{45}
$$

We define $\widetilde{P} \triangleq P^{-1}$, $\widetilde{\Phi} \triangleq P^{-1}\Phi P^{-1}$, $X \triangleq KP^{-1}$, $G \triangleq QL$. According to the Lyapunov stability theory, we find that if the 1.00,0.00,0.00 LMI in (43) holds, then 1.00,0.00,0.00the closed-loop system (38)–(41) is asymptotically stable. This completes the proof. □

Remark 12. *The main purpose of this paper is to apply the OB-ETPC to compensate for DoS attacks. Unlike the work in [50], this paper introduces two event-triggered generators that compensate for the DoS attack while saving a large amount of bandwidth resources.*

4. Simulation Example

In this section, we apply observer-based event-triggered predictive control to the smart grid example with a four-bus model of the distribution test feeders under DoS attacks [50]. The relevant parameters of the system can be found in [50,51]. The sampling time of the system is $h = 0.02s$, the DoS attack cycle is $T = 2s$ and the trigger parameter is $\mu = 0.08$.

$$A = \begin{bmatrix} 1.0156 & 0.0139 & 0.0457 & 0.0971 \\ -0.0353 & 0.9997 & -0.0008 & -0.0017 \\ -0.0526 & -0.0448 & 0.9625 & -0.0797 \\ -0.0080 & -0.0505 & 0.0903 & 0.9011 \end{bmatrix}, B = \begin{bmatrix} -0.0025 & 0.0315 & 0.0514 & -0.1118 \\ -0.0350 & 0.0006 & -0.0009 & 0.0019 \\ -0.0042 & -0.0057 & -0.0422 & -0.0742 \\ -0.0400 & -0.0392 & -0.0086 & -0.0980 \end{bmatrix}. \quad (46)$$

Other details of the system's parameters can be found in [50]. Then, the matrix C is chosen as

$$C = \begin{bmatrix} 1.0000 & 2.0000 & 0.0000 & 0.5000 \end{bmatrix}. \quad (47)$$

According to Theorem 1, using MATLAB to solve the corresponding linear matrix inequality (LMI), the corresponding controller gain matrix K, observer gain matrix L and event-triggering matrix Φ are obtained as follows:

$$K = \begin{bmatrix} 4.4570 & 9.2776 & -1.8638 & 1.0980 \\ -4.6407 & -6.9638 & -1.0600 & 2.4232 \\ 1.0259 & -0.2534 & 2.1682 & -1.2877 \\ 0.3916 & -0.9666 & 0.9551 & 0.3309 \end{bmatrix}, \quad (48)$$

$$L = \begin{bmatrix} -0.3809 \\ 0.6965 \\ 0.2680 \\ 0.0721 \end{bmatrix}, \quad (49)$$

$$\Phi = \begin{bmatrix} 0.2233 & 0.0067 & 0.1629 & 0.0964 \\ 0.0067 & 0.2842 & -0.1596 & -0.0537 \\ 0.1629 & -0.1596 & 0.2761 & 0.0572 \\ 0.0964 & -0.0537 & 0.0572 & 0.2232 \end{bmatrix}. \quad (50)$$

The effectiveness of OB-ETPC in the defense of DoS attacks is demonstrated by comparing the experimental results of three simulation cases under DoS attacks with different durations and two other mainstream DoS attack compensation schemes based on time-triggered predictive control (TTPC) [52–54] and event-triggered control (ETC) [27,48,49]. Assume that the plant initial state is $x_0 = \begin{bmatrix} 5.2 & 5.2 & 0.6 & 9.7 \end{bmatrix}^T$ and the observer initial state is $\widetilde{x}_0 = \begin{bmatrix} 5 & 4 & 0.4 & 6.4 \end{bmatrix}^T$, so the observer state initial error is $\delta_0 = \begin{bmatrix} 0.2 & 1.2 & 0.2 & 3.3 \end{bmatrix}^T$.

Case 1. *In this case, based on the controller gain matrix K and observer gain matrix L obtained by the above OB-ETPC and based on TTPC [52–54], the state responses and event intervals of the system with DoS attack are shown in Figure 5 and Figure 6, respectively.*

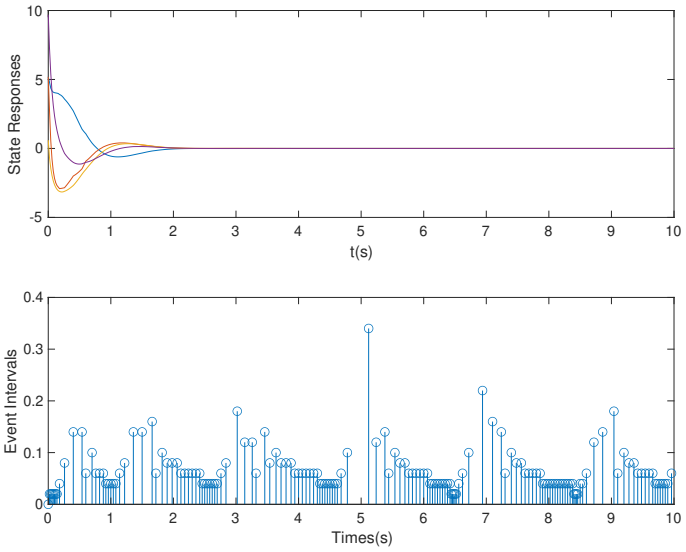

Figure 5. State responses and event intervals with DoS attack for OB-ETPC.

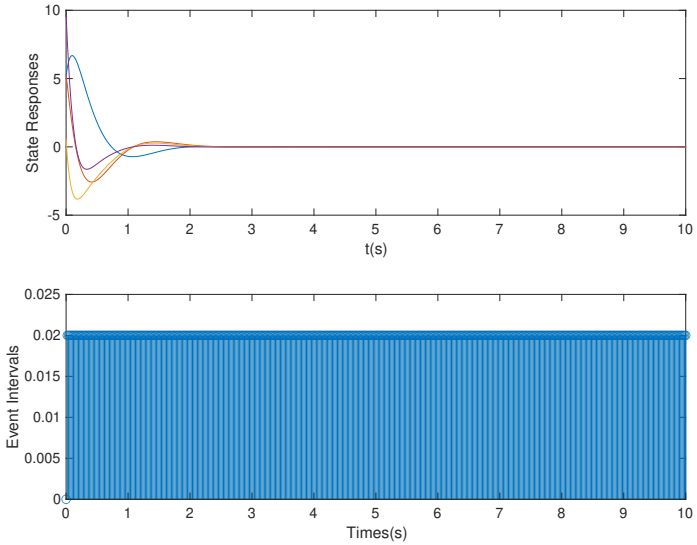

Figure 6. State responses and event intervals with DoS attacks for time-triggered predictive control (TTPC).

As shown in Figures 5 and 6, we can clearly see that both OB-ETPC-based or TTPC-based methods are able to make the system state stable when encountering DoS attacks. In this case, based on the OB-ETPC and the TTPC, all packet losses due to DoS attacks ($p = 1$ s or $p = 1.5$ s) are fully compensated. From Table 2 we can see that, based on OB-ETPC, there are 154 *triggered moments within* 500 *sampling times, and the average triggered time interval is* 0.0649 *s. Based on the TTPC, the system has* 500 *triggered moments when compensating for DoS attacks, and the average triggered time interval is* 0.02 s*. Moreover, it is also clear from the data in the Table 2 that the amount of data packets required to stabilize the OB-ETPC-based system is 114, while the amount of data packets required to stabilize the TTPC-based system is up to 380 when encountering weak DoS attacks. When encountering strong DoS attacks, the OB-ETPC-based system requires 54 data packets for stability, while the TTPC-based system requires 130 data packets for stability. Thus, the event-triggered mechanism not only does not degrade the performance of the system, but also greatly reduces the network bandwidth resource consumption.*

Table 2. Sampled numbers, released numbers, average trigger time and data numbers for three cases.

Different Methods	OB-ETPC$_{1s}$	OB-ETPC$_{1.5s}$	TTPC$_{1s}$	TTPC$_{1.5s}$	ETC$_{1s}$	ETC$_{1.5s}$
Cases	Case 1 and Case 2	Case 1 and Case 3	Case 1	Case 1	Case2	Case 3
Methods	This paper	This paper	[52–54]	[52–54]	[27,48,49]	[27,48,49]
Sampled numbers	500	500	500	500	500	500
Released numbers	154	154	500	500	143	117
Average trigger time	0.0649 s	0.0649 s	0.02 s	0.02 s	0.0699 s	0.0855 s
Data numbers	114	54	380	130	100	40

Case 2. *In this case, we assume that* $p = 1$ s *is used. Based on the controller gain matrix K and observer gain matrix L obtained by the above OB-ETPC and based on the ETC [27,48,49], the state responses and event intervals of the system are shown in Figure 7 and Figure 8, respectively.*

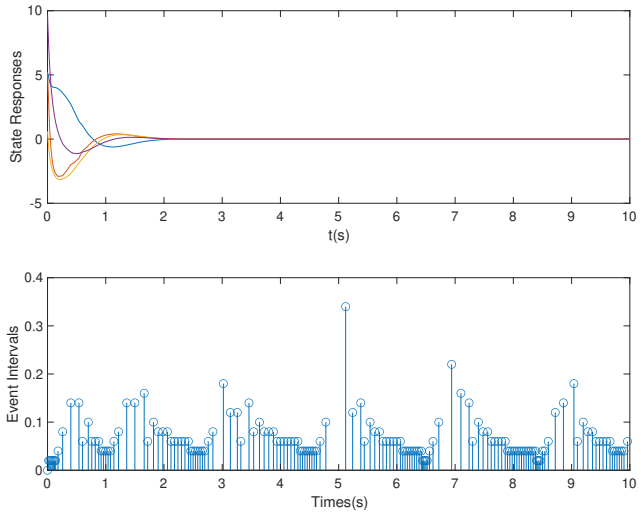

Figure 7. State responses and event intervals with DoS attacks ($p = 1$ s) for OB-ETPC.

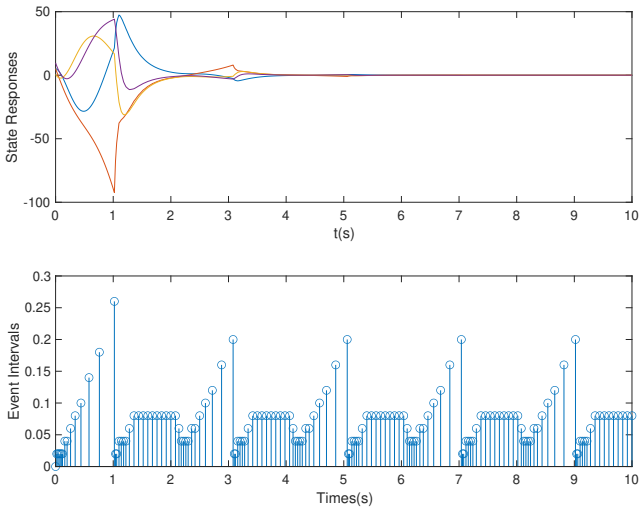

Figure 8. State responses and event intervals with DoS attacks ($p = 1$ s) for ETC.

As shown in Figures 7 and 8, the system can be seen to experience a weak DoS attack. From Table 2 we can see that, based on OB-ETPC, there are 154 *triggered moments and the average triggered time interval is* 0.0649 s. *In this*

case, based on ETC, there are 143 *triggered moments and the average triggered time interval is* 0.0699 s. *Because the simulation case is performed in the upper bound of the weak DoS attack, according to Assumption 7, the ETC-based method can defend against DoS attacks with an arbitrary duration in the weak attack duration range and remain stable after a period of time.*

Case 3. *In this case, we assume that* $p = 1.5$ s *is used. Based on the controller gain matrix K and observer gain matrix L obtained by the above OB-ETPC and based on the ETC [27,48,49], the state responses and event intervals of the system are shown in Figure 9 and Figure 10, respectively.*

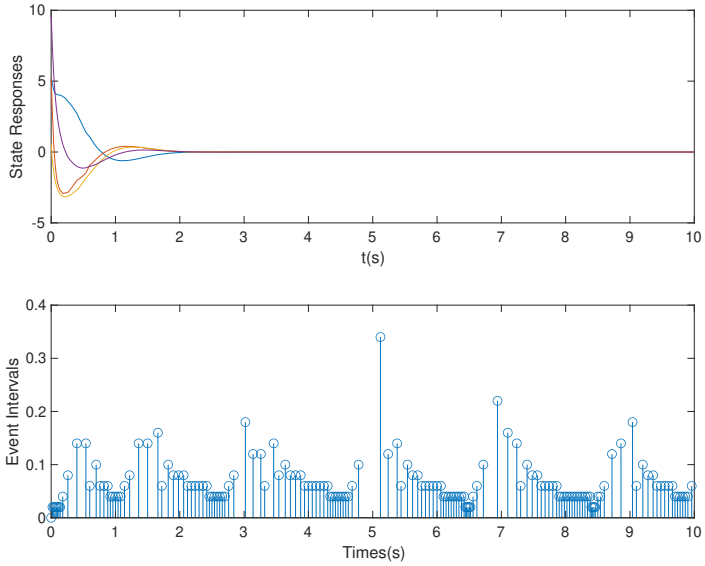

Figure 9. State responses and event intervals with DoS attacks ($p = 1.5$ s) for OB-ETPC.

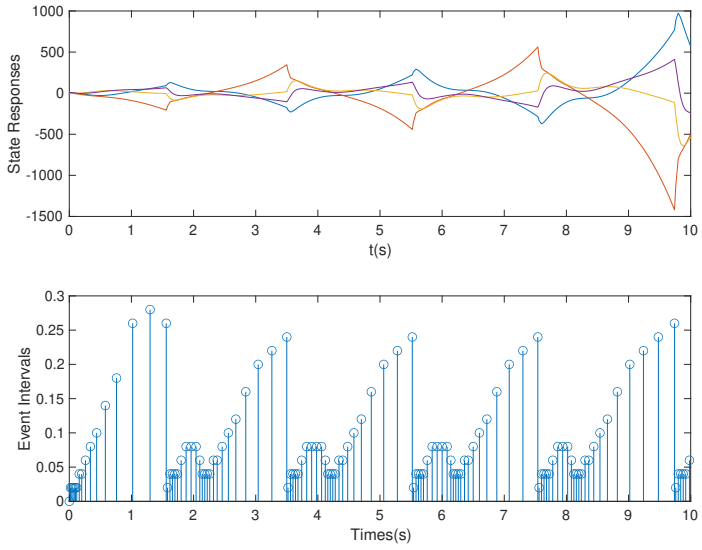

Figure 10. State responses and event intervals with DoS attacks ($p = 1.5$ s) for ETC.

As shown in Figures 9 and 10, the system can be seen to experience strong DoS attacks. From Table 2, we can see that, based on OB-ETPC, there are 154 *triggered moments and the average triggered time interval is*

0.0649 s. *In this case, based on ETC, there are* 117 *triggered moments and the average triggered time interval is* 0.0855 s. *In this case, the ETC-based method cannot defend against strong DoS attacks and the system loses stability. However, since OB-ETPC can fully compensate for DoS attacks, the system remains stable after encountering strong DoS attacks.*

Remark 13. *The data numbers represent the amount of data successfully transmitted to the actuator.*

Compared with TTPC [52–54], the above results verify the effectiveness of our proposed OB-ETPC in reducing bandwidth resource consumption. Furthermore, compared to ETC [27,48,49], the above results verify the feasibility of our proposed OB-ETPC approach to defend against DoS attacks. In summary, the OB-ETPC approach proposed in this paper can make up for the deficiency of different types of NCS compensation schemes under DoS attacks. In the case that the system state cannot be completely measured, OB-ETPC can ensure the stability of NCSs and reduce the occupancy of bandwidth resources, which cannot be achieved by other methods at present.

5. Conclusions

This paper studies the problem of event-triggered control based on a static observer in networked control systems (NCSs) under DoS attacks. The OB-ETPC is a new method to solve the problem of DoS attacks. The results show that the introduction of an observer and predictive model in the system has a significant effect on the defense against DoS attacks. The establishment of an event-triggered scheme greatly reduces the size of the predictive control sequence compensation packet. In addition, a ZOH is constructed in the actuator node to actively compensate for data packet loss due to DoS attacks. The OB-ETPC is an active compensation method for NCSs under DoS attacks that combines event-triggered conditions, robust controller-feedback gain and observer gain. The practical application example shows that this method can not only actively compensate for DoS attacks but can also reduce the bandwidth occupancy while maintaining the stability of the NCSs.

In future research, it would be beneficial to extend the OB-ETPC to the defense against DoS attack of distributed NCSs. In distributed NCSs, it is necessary to consider the impact of network-induced delay, data packet dropout and DoS attacks on the closed-loop system. In addition, the OB-ETPC approach would also be of great significance for solving noise problems [55].

Author Contributions: All authors contributed to writing and editing this manuscript. W.L.: Methodology, Writing—original draft. X.Y.: Supervision, Writing—Review and editing. Y.F.: Writing—review and editing. Z.G.: Writing—review and editing. All authors have read and agreed to the published version of the manuscript

Funding: Xiuxia Yin is supported by NSFC (No. 61603175 and No. 61963028) and Natural Science Foundation of Jiangxi Province (No. 20192BAB207023).

Acknowledgments: The authors would like to acknowledge the research support from the Department of Mathematics, School of Science, Nanchang University and the Faculty of Engineering and Environment, University of Northumbria at Newcastle.

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

References

1. Demestichas, P.; Georgakopoulos, A.; Karvounas, D.; Tsagkaris, K.; Stavroulaki, V.; Lu, J.; Xiong, C.; Yao, J. 5G on the horizon: Key challenges for the radio-access network. *IEEE Veh. Technol. Mag* **2013**, *8*, 47–53. [CrossRef]
2. Foukas, X.; Patounas, G.; Elmokashfi, A.; Marina, M.K. Network slicing in 5G: Survey and challenges. *IEEE Commun. Mag* **2017**, *55*, 94–100. [CrossRef]
3. Park, B.; Nah, J.; Choi, J.Y.; Yoon, I.J.; Park, P. Robust wireless sensor and actuator networks for networked control systems. *Sensors* **2019**, *19*, 1535. [CrossRef] [PubMed]

4. Galeano-Brajones, J.; Carmona-Murillo, J.; Valenzuela-Valdés, J.F.; Luna-Valero, F. Detection and mitigation of dos and ddos attacks in iot-based stateful sdn: An experimental approach. *Sensors* **2020**, *20*, 816. [CrossRef]
5. Singh, A.K.; Singh, R.; Pal, B.C. Stability analysis of networked control in smart grids. *IEEE Trans. Smart Grid* **2014**, *6*, 381–390. [CrossRef]
6. Aristidou, P.; Valverde, G.; Van Cutsem, T. Contribution of distribution network control to voltage stability: A case study. *IEEE Trans. Smart Grid* **2015**, *8*, 106–116. [CrossRef]
7. Liu, J.; Suo, W.; Zha, L.; Tian, E.; Xie, X. Security distributed state estimation for nonlinear networked systems against dos attacks. *Int. J. Robust Nonlinear Control* **2020**, *30*, 1156–1180. [CrossRef]
8. Yousef, K.M.A.; Almajali, A.; Ghalyon, S.A.; Dweik, W.; Mohd, B.J. Analyzing cyber-physical threats on robotic platforms. *Sensors* **2018**, *18*, 1643. [CrossRef]
9. Yang, T.C. Networked control system: A brief survey. *IEEE Proc. Control Theory Appl.* **2006**, *153*, 403–412. [CrossRef]
10. Gupta, R.A.; Chow, M.Y. Networked control system: Overview and research trends. *IEEE Trans. Ind. Electron.* **2009**, *57*, 2527–2535. [CrossRef]
11. Xia, F.; Ma, L.; Peng, C.; Sun, Y.; Dong, J. Cross-layer adaptive feedback scheduling of wireless control systems. *Sensors* **2008**, *8*, 4265–4281. [CrossRef] [PubMed]
12. Montestruque, L.A.; Antsaklis, P.J. On the model-based control of networked systems. *Automatica* **2003**, *39*, 1837–1843. [CrossRef]
13. Peng, C.; Sun, H.; Yang, M.; Wang, Y.L. A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1554–1569. [CrossRef]
14. Antunes, D.; Hespanha, J.P.; Silvestre, C. Stochastic hybrid systems with renewal transitions: Moment analysis with application to networked control systems with delays. *SIAM J. Control Optim.* **2013**, *51*, 1481–1499. [CrossRef]
15. Zhang, X.M.; Han, Q.L.; Ge, X.; Ding, D.; Ding, L.; Yue, D.; Peng, C. Networked control systems: A survey of trends and techniques. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 1–17. [CrossRef]
16. Garcia, E.; Cao, Y.; Casbeer, D.W. Periodic event-triggered synchronization of linear multi-agent systems with communication delays. *IEEE Trans. Autom. Control* **2017**, *62*, 366–371. [CrossRef]
17. Ge, X.; Yang, F.; Han, Q.L. Distributed networked control systems: A brief overview. *Inf. Sci.* **2017**, *380*, 117–131. [CrossRef]
18. Ding, L.; Han, Q.L.; Ge, X.; Zhang, X.M. An overview of recent advances in event-triggered consensus of multiagent systems. *IEEE Trans. Cybern.* **2018**, *48*, 1110–1123. [CrossRef]
19. Shisheh, H.F.; Mart, S. On triggering control of single-input linear systems under pulse-width modulated dos signals. *SIAM J. Control Optim.* **2016**, *54*, 3084–3105. [CrossRef]
20. De, C.; Persis, C.; Tesi, P. Input-to-state stabilizing control under denial-of-service. *IEEE Trans. Autom. Control* **2015**, *60*, 2930–2944.
21. Feng, S.; Tesi, P. Resilient control under denial-of-service: Robust design. *Automatica* **2017**, *79*, 42–51. [CrossRef]
22. De, C.; Persis, C.; Tesi, P. Networked control of nonlinear systems under denial-of-service. *Syst. Control Lett.* **2016**, *96*, 124–131.
23. Feng, S.; Tesi, P.; De Persis, C. Towards stabilization of distributed systems under denial-of-service. In Proceedings of the 2017 IEEE 56th Annual Conference on Decision and Control (CDC), Melbourne, VIC, Australia, 12–15 December 2017; pp. 5360–5365.
24. Cetinkaya, A.; Ishii, H.; Hayakawa, T. Networked control under random and malicious packet losses. *IEEE Trans. Autom. Control* **2017**, *62*, 2434–2449. [CrossRef]
25. Zhao, Y.; He, X.; Zhou, D. Optimal joint control and triggering strategies against denial of service attacks: A zero-sum game. *IET Control Theory Appl.* **2017**, *11*, 2352–2360. [CrossRef]
26. Zhang, X.M.; Han, Q.L.; Ge, X.; 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] [PubMed]
27. Hu, S.; Yue, D.; Han, Q.L.; Xie, X.; Chen, X.; Dou, C. Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. *IEEE Trans. Cybern.* **2020**, *50*, 1952–1964. [CrossRef]

28. Ge, X.; Han, Q.L. Consensus of multiagent systems subject to partially accessible and overlapping markovian network topologies. *IEEE Trans. Cybern.* **2017**, *47*, 1807–1819. [CrossRef]
29. Wang, X.; Lemmon, M.D. Event-triggering in distributed networked control systems. *IEEE Trans. Autom. Control* **2010**, *56*, 586–601. [CrossRef]
30. You, X.; Hua, C.; Guan, X. Event-triggered leader-following consensus for nonlinear multiagent systems subject to actuator saturation using dynamic output feedback method. *IEEE Trans. Autom. Control* **2018**, *63*, 4391–4396. [CrossRef]
31. You, X.; Hua, C.; Guan, X. Self-triggered leader-following consensus for high-order nonlinear multiagent systems via dynamic output feedback control. *IEEE Trans. Cybern.* **2018**, *49*, 2002–2010. [CrossRef]
32. Onat, A.; Naskali, T.; Parlakay, E.; Mutluer, O. Control over imperfect networks: Model-based predictive networked control systems. *IEEE Trans. Ind. Electron.* **2011**, *58*, 905–913. [CrossRef]
33. Li, H.; Shi, Y. Networked min–max model predictive control of constrained nonlinear systems with delays and packet dropouts. *Int. J. Control* **2013**, *86*, 610–624 . [CrossRef]
34. Pang, Z.H.; Liu, G.P.; Zhou, D. Design and performance analysis of incremental networked predictive control systems. *IEEE Trans. Cybern.* **2015**, *46*, 1400–1410. [CrossRef] [PubMed]
35. Hu, S.; Cheng, Z.; Yue, D.; Dou, C.; Xue, Y. Bandwidth allocation-based switched dynamic triggering control against dos attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**. [CrossRef]
36. Yin, X.X.; Yue, D.; Hu, S. Model-based event-triggered predictive control for networked systems with communication delays compensation. *Int. J. Robust Nonlinear Control* **2015**, *25*, 3572–3595 . [CrossRef]
37. Amullen, E.M.; Shetty, S.; Keel, L.H. Model-based resilient control for a multi-agent system against denial of service attacks. In Proceedings of the 2016 World Automation Congress (WAC), Rio Grande, Puerto Rico, 31 July–4 August 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
38. Zhang, J.; Chai, S.; Zhang, B. Model-based event-triggered dynamic output predictive control of networked uncertain systems with random delay. *Int. J. Syst. Sci.* **2020**, *51*, 20–34. [CrossRef]
39. Li, Y.X.; Yang, G.H. Model-based adaptive event-triggered control of strict-feedback nonlinear systems. *IEEE Trans. Neural Netw. Learn. Syst.* **2017**, *29*, 1033–1045. [CrossRef]
40. Sun, Y.C.; Yang, G.H. Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks. *Int. J. Robust Nonlinear Control* **2019**, *29*, 4797–4811. [CrossRef]
41. Yin, X.X.; Yue, D.; Hu, S. Observer-based control for networked systems with event-triggering predictive scheme. In Proceedings of the IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society, Dallas, TX, USA, 29 October–1 November 2014; pp. 4774–4780.
42. Peng, C.; Sun, H. Switching-like event-triggered control for networked control systems under malicious denial of service attacks. *IEEE Trans. Autom. Control* **2020**. [CrossRef]
43. Zhang, J.; Xia, Y.; Shi, P. Design and stability analysis of networked predictive control systems. *IEEE Trans. Control Syst. Technol.* **2012**, *21*, 1495–1501. [CrossRef]
44. Liu, J.; Yang, M.; Tian, E.; Cao, J.; Fei, S. Event-based security control for state-dependent uncertain systems under hybrid-attacks and its application to electronic circuits. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2019**, *66*, 4817–4828. [CrossRef]
45. Mohammed, A.A.S.; Moussa, W.A.; Lou, E. High sensitivity mems strain sensor: Design and simulation. *Sensors* **2008**, *8*, 642–2661. [CrossRef] [PubMed]
46. Tian, E.; Wang, Z.; Zou, L.; Yue, D. Probabilistic-constrained filtering for a class of nonlinear systems with improved static event-triggered communication. *Int. J. Robust Nonlinear Control* **2019**, *29*, 1484–1498. [CrossRef]
47. Cao, R.; Wu, J.; Long, C.; Li, S. Stability analysis for networked control systems under denial-of-service attacks. In Proceedings of the 2015 54th IEEE Conference on Decision and Control (CDC), Osaka, Japan, 15–18 December 2015; pp. 7476–7481.
48. Sun, H.; Peng, C.; Zhang, W.; Yang, T.; Wang, Z. Security-based resilient event-triggered control of networked control systems under denial of service attacks. *J. Frankl. Inst.* **2019**, *356*, 277–295. [CrossRef]
49. Hu, S.; Yue, D.; Xie, X.; Chen, X.; Yin, X. Resilient event-triggered controller synthesis of networked control systems under periodic dos jamming attacks. *IEEE Trans. Cybern.* **2018**, *49*, 4271–4281. [CrossRef] [PubMed]

50. Su, L.; Ye, D. Observer-based output feedback h_∞ control for cyber–physical systems under randomly occurring packet dropout and periodic dos attacks. *ISA Trans.* **2019**, *95*, 58–67. [CrossRef]
51. Kersting, W.H. Radial distribution test feeders. *IEEE Trans. Power Syst.* **1991**, *6*, 975–985. [CrossRef]
52. Sun, Q.; Zhang, K.; Shi, Y. Resilient model predictive control of cyber–physical systems under dos attacks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4920–4927. [CrossRef]
53. Liu, G.P.; Xia, Y.; Chen, J.; Rees, D.; Hu, W. Networked predictive control of systems with random network delays in both forward and feedback channels. *IEEE Trans. Ind. Electron.* **2007**, *54*, 1282–1297. [CrossRef]
54. Liu, G.P. Predictive controller design of networked systems with communication delays and data loss. *IEEE Trans. Circuits Syst. II Express Briefs* **2010**, *57*, 481–485. [CrossRef]
55. Zhang, D.; Lin, Z.; Gao, Z. A novel fault detection with minimizing the noise-signal ratio using reinforcement learning. *Sensors* **2018**, *18*, 3087. [CrossRef] [PubMed]