energies

MDPI

Article

Demand-Driven Resilient Control for Generation Unit of Local Power Plant Under Unreliable Communication

Guizhou Cao [1], Dawei Xia [1], Bokang Liu [2], Kai Meng [3], Zhenlong Wu [4] and Yuan-Cheng Sun [4,*]

[1] State Grid Henan Electric Power Research Institute, Zhengzhou 450052, China; caoguizhou2006@163.com (G.C.); xiadaw1980@163.com (D.X.)
[2] Henan Electric Power Dispatching and Control Center, Zhengzhou 450001, China; cogizh@163.com
[3] Shangqiu Power Supply Company, State Grid Henan Electric Power Company, Shangqiu 476002, China; zzusub@163.com
[4] School of Electrical and Information Engineering, Zhengzhou University, Zhengzhou 450001, China; wuzhenlong2020@zzu.edu.cn
* Correspondence: dksyc294@126.com

Abstract: The resilient control issue for the generation unit (GU) in a local power plant with unreliable communication is addressed in this article, where the communication may be jammed by denial-of-service (DoS) attacks. Based on the GU model of voltage and current at the point of common coupling, a demand-driven network communication protocol is proposed to decrease the number of scheduling signal transmissions, and an observer-based prediction method is provided to replenish the lack of dispatching data during transmission intervals when the demand has not changed. The closed-loop performance is analyzed for the GU system in the input-to-state stable framework with or without attack. According to the DoS attack model, which is described by the assumptions of frequency and duration, the conservativeness of the tolerable DoS attack index is reduced by using the thought of robustness to the maximum disturbance-induced error. Simulation examples are provided to verify the effectiveness of the approach proposed in this article.

Keywords: generation unit system; resilient control; network communication; denial-of-service attack; stability analysis

Academic Editor: Ahmed Abu-Siada

Received: 8 December 2024
Revised: 8 January 2025
Accepted: 8 January 2025
Published: 11 January 2025

Citation: Cao, G.; Xia, D.; Liu, B.; Meng, K.; Wu, Z.; Sun, Y.-C. Demand-Driven Resilient Control for Generation Unit of Local Power Plant Under Unreliable Communication. *Energies* **2025**, *18*, 300. https://doi.org/10.3390/en18020300

1. Introduction

In recent decades, with the vigorous progress of renewable energy, the randomness of renewable generation such as wind power and photovoltaics has made the smooth scheduling of power systems a hot topic [1]. In order to enhance the flexible capacity and peaking capacity of the power system, voltage and frequency control of small generation units (GUs) in local power plants becomes necessary. Recently, the scheduling scheme based on network communication has been widely used in power systems [2]. However, the utilization of heterogeneous electrical and electronic components with networks has made the data transmission fairly open to various cyber attacks. This can lead to serious security consequences. Unlike the attacks on traditional systems that limit the influence to the cyber level, the physical world of power systems can be impacted by malicious cyber attacks [3], causing serious social and livelihood problems. Thus, these strong demands for power systems exist, despite malicious cyber attacks, designing analysis and synthesis approaches to ensure their reliability and security [4,5].

Typically, the various malicious attacks involve deception attacks and denial-of-service (DoS) attacks, where the latter attack leads to the information absence of the actuator and

sensor by blocking the data transmission to their respective destinations. The DoS attack is very common in networked control systems, and lots of studies have been presented on networked power systems under DoS attacks. In [6], an H_∞ load frequency control based on an event-triggered strategy is studied for multi-area power systems, and the resilient control approach is proposed to deal with the presence of DoS attacks. Security issues in remote state estimation with the existence of jamming attacks are investigated in [7] using a game-theoretic approach. In [8,9], the optimal DoS attack strategies for maximizing the deterioration on the system performance from the view of the adversary are investigated.

Stability analysis is a popular research topic on security problems of control systems under DoS attacks. In [10], the DoS attack model is characterized according to its frequency and duration, input-to-state stable (ISS) is demonstrated for the attacked closed-loop system, and transmission timing is scheduled based on this DoS attack model. Based on the analysis strategy proposed in [10], to maximize the attack intensity index according to the frequency and duration of the attack model with which the stability of the system is not destroyed, a resilient control framework is proposed in [11]. In [12], the controller design and analysis is investigated with this DoS attack model for nonlinear dynamics. In [13], based on the ISS control framework, the scenario of multiple transmission channels is considered for linear systems under DoS attacks. In [14], an output-based synthetical control design strategy for a class of hybrid nonlinear dynamics under DoS attacks is provided in a dynamic event-triggered framework. In [15], observer-based asynchronous control for switching power systems subject to DoS attacks is discussed. However, research on the resilient control of power systems under the condition of unreliable communication is still insufficient; particularly, the design of the output voltage and current control scheme of the GU via the network is still a challenging problem.

Traditionally, the control algorithms are executed in the time-scheduled strategy, in which the sampling and data communication are carried out periodically. Although the time-based periodic sampling might be preferable from the point of view of system analysis and design, it leads to the unnecessary waste of limited resources. Usually, network-based scheduling signals in power systems are not transmitted in real time but communicate when scheduling needs arise. In this way, the traditional time-triggered control method is no longer suitable. The event-triggered control scheme as a control strategy based on intermittent communication has been a wide concern for networked control systems [16–18], and it can be used to construct a demand-based control scheme for GUs. In [19], an event-triggered control (ETC) strategy with a periodic verification mechanism for linear systems is proposed, which is named periodic event-triggered control (PETC). By merging the time-scheduled strategy and ETC, the characteristic of PETC is to verify the triggering condition periodically—that is, whether to calculate and send new sampling data or new control data is determined at each periodic verification time. In [20], consider the scenario where both the sensor-to-controller channel and the controller-to-actuator channel are communicated via a network, a PETC algorithm is designed according to the retrievable system state space model. The above studies are all about networked control systems without attacks. Practically, power system scheduling also has a fixed sampling period; however, it is still a challenge to construct a resilient control scheme for the GU under unreliable communication using the idea of PETC.

For grid-connected power plants, the purpose of scheduling is to maintain the balance and stability of voltage and frequency, which are specified by the main grid when there are demands. However, for the local power plants tasked with flexibility and peaking, voltage and frequency outputs for GU are definitively controlled according to the networked scheduling signals, and it is necessary to save network resources. By introducing the concept of neutral interactions, the dynamic model of GU in this paper is established by

exploiting quasi-stationary line approximations of line dynamics [21]. To improve the security of networked scheduling, the unreliable network communication channel is modeled as the communication interruption of the sensor channel due to the presence of a DoS attack. To construct the control framework, a smart sensor system is adopted in order to design the demand-driven mechanism (DDM)—that is, network communication is performed only when scheduling is required. Unfortunately, in the design of the control system, the load current of the unit connection is difficult to estimate. The conventional idea is to treat it as an unknown disturbance, but how to deal with the error term introduced by disturbance and noise is still a difficult point in the DDM design. To improve resilience against DoS attacks, a predictor is proposed in the controller system to compensate for the lack of data during communication intervals. Based on the ISS analysis framework, the stability when there are DoS attacks is proved and the maximum tolerable attack intensity index is quantified.

The prime innovations of this article are generalized below: First, the dynamic model of the GU for local power plant is established by exploiting quasi-stationary line approximations, and the unknown loads are treated as unmodeled disturbances, which can be restricted by the designed H_∞ observer. At the same time, the effects of disturbance and noise during the DDM design can be addressed by the quantified H_∞ performance index. Second, the advanced demand-driven resilient control method with a periodic verification strategy is presented to deal with the unreliable communication caused by DoS attacks, and the intermittent communication scenario meets the requirements of network scheduling for the GU by applying the prediction-based method. Third, based on the thought of robustness to the maximum disturbance accumulation error, the conservatism of the tolerable attack intensity in this result is decreased compared with [10,14].

The rest of this article is organized as follows: The GU model is described in Section 2, and the observer and the predictor are designed. In Section 3, the ISS of the demand-driven control approach is proved. Section 4 gives the resilient control strategy under DoS attacks. Section 5 provides simulation results. The conclusions of this paper are given in Section 6.

2. System Formulation and Problem Description

First of all, the meanings of the symbols used in this paper are shown in the notation below. Then, the state space model of the GU is constructed, and the resilient control framework is designed based on it.

Notation: Let $\mathbb{R}$ and $\mathbb{R}^n$ be the sets of real and Euclidean spaces with dimension n, respectively. Let $\mathbb{N}$ be the natural number set and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. $\|x\|$ denotes the Euclidean norm for any vector $x \in \mathbb{R}^n$. A^T is the transpose of a given matrix A, $\|A\|$ is the spectral norm, and μ_A is the logarithmic norm [22] with $\mu_A = \max\left\{\lambda | \lambda \in \text{spectrum}\left\{\frac{A+A^T}{2}\right\}\right\}$. For sets S_1 and S_2, denote $S_2 \backslash S_1$ by the relative complement of S_1 in S_2. $|T(t_1, t_2)| = t_2 - t_1$ denotes by the length of an interval $T = [t_1, t_2)$. For a measurable function $h(t)$ defined in $[0, t)$, the $\mathcal{L}_\infty$ norm of $h(\cdot)$ is denoted by $\|h_t\|_\infty = ess\ \sup_{s\in[0,t)} \|h(s)\|$.

2.1. Generation Unit Model

In this section, the dynamical model of the GU for a local power plant is presented. To simplify the analysis process, the realistic model of GU is assumed to consist of transformers, associated filters, and voltage source converters (VSCs) [21]. As shown in Figure 1, through a non-zero impedance three-phase line with (R_{ij}, L_{ij}), the considered GU denoted by i is connected with other units j. The GU is made up of a VSC, a DC voltage source (representing a biomass or waste incineration unit), an inductance L_t, a series filter characterized by a resistance R_t, and a station step-up transformer $(Y - \Delta)$; further, at the point of common coupling (PCC) of the electrical network, the GUs are connected with each other

through the transformer, where the transformer coefficients are represented by R_t and L_t, and k is defined as the transformation ratio.

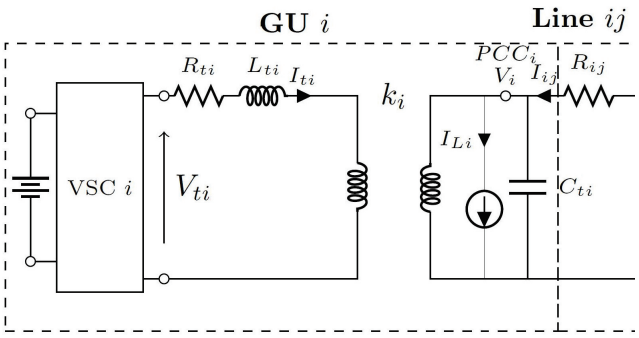

Figure 1. Electrical scheme of GU with unmodeled loads.

For the local loads that are connected to the PCC, consider the case where the GU proves the real and reactive powers. Suppose that the loads are time-varying and unknown, and the load current I_L is treated as the disturbance for the GU. At the PCC of each local area, the effect of high-frequency harmonics of the load voltage is attenuated by using the shunt capacitance C_t. In the abc-frame, based on the dynamical equations of this scheme and by applying Park's transformation, the model rotating with speed ω_0 in the dq-frame is obtained as follows:

$$GU\ i: \begin{cases} \frac{dV_{i,dq}}{dt} + j\omega_0 V_{i,dq} = \frac{k_i}{C_{ti}} I_{ti,dq} + \frac{1}{C_{ti}} I_{ti,dq} - \frac{1}{C_{ti}} I_{Li,dq} \\ \frac{dI_{ti,dq}}{dt} + j\omega_0 I_{ti,dq} = -\frac{R_{ti}}{L_{ti}} I_{ti,dq} - \frac{k_i}{L_{ti}} V_{i,dq} + \frac{1}{L_{ti}} V_{ti,dq} \end{cases} \tag{1}$$

$$Line\ ij: \left\{ \frac{dI_{ij,dq}}{dt} + j\omega_0 I_{ij,dq} = \frac{1}{L_{ij}} V_{j,dq} - \frac{R_{ij}}{L_{ij}} I_{ij,dq} - \frac{1}{L_{ij}} V_{i,dq} \right. \tag{2}$$

where $V_{i,dq}$ is the output voltage at the PCC, and $V_{ti,dq}$ and $I_{ti,dq}$ are the output voltage and current of the GU, respectively. The states in (1) and (2) can be divided into two segments—that is, the dq reference frame is divided as the real component d- and the imaginary component q-, respectively, and I_{ij} is the line current. Modeling the load current $I_{Li,dq}$ as the disturbance, (1) and (2) can be represented through the following continuous time linear dynamic form:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + E\omega(t) \\ y(t) &= Cx(t) + v(t) \end{aligned} \tag{3}$$

where $x = [V_{i,d}, V_{i,q}, I_{ti,d}, I_{ti,q}, I_{ij,d}, I_{ij,q}]^T$ is the state vector, $u = [V_{ti,d}, V_{ti,q}, V_{tj,d}, V_{tj,q}]^T$ is the control input, $\omega = [I_{Li,d}, I_{Li,q}, I_{Lj,d}, I_{Lj,q}]^T$ is the unknown disturbance, $y = [V_{i,d}, V_{i,q}, V_{j,d}, V_{j,q}]^T$ is the measurement output, and $v(t)$ is the measurement noise. Suppose that $\omega(t)$ and $v(t)$ are bounded, where $\|\omega(t)\| \leq \delta_\omega$, $\|v(t)\| \leq \delta_v$. A, B, C, and E are system matrices to be determined later. This model is regarded as the master model here, since the states of the line are controlled by the GU i only for the control purpose.

To isolate the effects of other connected GUs on the grid, an approximate model is given to avoid the requirement of applying the line current in the GU's dynamic equations. Let $\frac{dI_{ij,dq}}{dt} = 0$; the quasi-stationary line approximations model is given as

$$\bar{I}_{ij,dq} = \frac{V_{j,dq}}{(R_{ij} + j\omega_0 L_{ij})} - \frac{V_{i,dq}}{(R_{ij} + j\omega_0 L_{ij})}.$$

Then, replace variable $I_{ij,dq}$ in (2) and divide the complex dq quantities into the corresponding d and q components; the transformed model for GUi is formulated as follows:

$$GU\ i: \begin{cases} \frac{dV_{i,d}}{dt} = \omega_0 V_{i,q} + \frac{k_i}{C_{ti}} I_{ti,d} - \frac{1}{C_{ti}} I_{Li,d} + \frac{1}{C_{ti}} \bar{I}_{ij,d} \\ \frac{dV_{i,q}}{dt} = -\omega_0 V_{i,d} + \frac{k_i}{C_{ti}} I_{ti,q} - \frac{1}{C_{ti}} I_{Li,q} + \frac{1}{C_{ti}} \bar{I}_{ij,q} \\ \frac{dI_{ti,d}}{dt} = -\frac{k_i}{L_{ti}} V_{i,d} - \frac{R_{ti}}{L_{ti}} I_{ti,d} + \omega_0 I_{ti,q} + \frac{1}{L_{ti}} V_{ti,d} \\ \frac{dI_{ti,q}}{dt} = -\frac{k_i}{L_{ti}} V_{i,q} - \frac{R_{ti}}{L_{ti}} I_{ti,q} - \omega_0 I_{ti,d} + \frac{1}{L_{ti}} V_{ti,q} \end{cases} \tag{4}$$

then, the dynamic model (1) of the GU is constructed as the following state space model form:

$$A = \begin{bmatrix} -\frac{1}{C_{ti}}\left(\frac{R_{ij}}{Z_{ij}^2}\right) & \omega_0 - \frac{1}{C_{ti}}\left(\frac{X_{ij}}{Z_{ij}^2}\right) & \frac{k_i}{C_{ti}} & 0 \\ -\omega_0 + \frac{1}{C_{ti}}\left(\frac{X_{ij}}{Z_{ij}^2}\right) & -\frac{1}{C_{ti}}\left(\frac{R_{ij}}{Z_{ij}^2}\right) & 0 & \frac{k_i}{C_{ti}} \\ -\frac{k_i}{L_{ti}} & 0 & -\frac{R_{ti}}{L_{ti}} & \omega_0 \\ 0 & -\frac{k_i}{L_{ti}} & -\omega_0 & -\frac{R_{ti}}{L_{ti}} \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ \frac{1}{L_{ti}} & 0 \\ 0 & \frac{1}{L_{ti}} \end{bmatrix},$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, E = \begin{bmatrix} -\frac{1}{C_{ti}} & 0 \\ 0 & -\frac{1}{C_{ti}} \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

where $X_{ij} = \omega_0 L_{ij}$, $Z_{ij} = \left|R_{ij} + jX_{ij}\right|$, $x(t) = [V_{i,d}, V_{i,q}, I_{ti,d}, I_{ti,q}]^T$, $u(t) = [V_{ti,d}, V_{ti,q}]^T$, and $\omega(t) = [I_{Li,d}, I_{Li,q}]^T$.

2.2. Control Framework

In order to meet the scheduling and control practice based on the network communication while guaranteeing the desirable scheduling performance of the GU, the control construction is designed as in Figure 2. A sensor system is designed to transmit the measurement information to the remote controller system based on the communication network. At the same time, the network communication is unreliable, which is caused by DoS attacks.

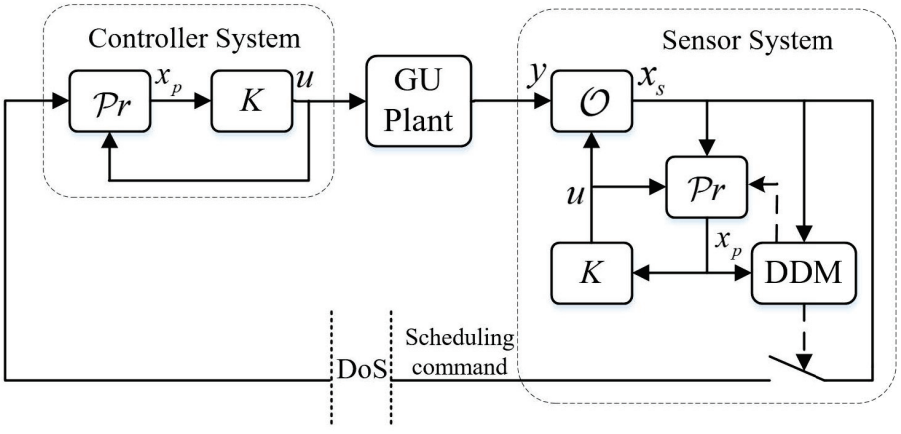

Figure 2. The framework of resilient control for GU under DoS.

The smart sensor system with a demand-driven method and periodic verification strategy is designed to schedule the scheduling commands. The sensor system consists of an observer $\mathcal{O}$ that deals with disturbance and noise, and the time when information is needed to be sent to the controller system is decided by a designed DDM. Furthermore, the controller system contains a predictor $\mathcal{P}r$ that can compensate the GU's state data loss

during the transmission interval using the latest received data. To suppress the impact of disturbance and noise, the H_∞ observer is designed as follows:

$$Observer\ \mathcal{O}\ :\ \ \dot{x}_s(t) = Ax_s(t) + Bu(t) + L(y(t) - Cx_s(t)) + Lv(t) \tag{5}$$

where $x_s(t)$ denotes by the state estimation of the sensor system and L is the designed gain matrix. Denote $e_s(t) = x(t) - x_s(t)$ by the observation error; then, the error dynamic can be formulated as

$$\dot{e}_s(t) = \Phi_L e_s(t) + \Gamma\xi(t) \tag{6}$$

where $\Phi_L = A - LC$, $\Gamma = [I \quad -L]$, $\xi(t) = \begin{bmatrix} E\omega(t) \\ v(t) \end{bmatrix}$. Based on continuous-time systems' bounded real lemma [23], the gain matrix L is able to be calculated based on the LMI in (7) and $\|e_s(t)\|_2 < \gamma\|\xi(t)\|_2$ is obtained.

$$\begin{bmatrix} \bar{P}\Phi_L + \Phi_L^T\bar{P} & \bar{P}\Gamma & I \\ * & -\gamma I & 0 \\ * & * & -\gamma I \end{bmatrix} < 0 \tag{7}$$

where $\bar{P}$ is a symmetric positive definite matrix and γ is a small positive scalar, which represents the H_∞ performance index. The predictor is given as

$$Predictor\ \mathcal{P}r\ :\ \begin{cases} \dot{x}_p(t) = Ax_p(t) + Bu(t), & x_s(t)\ is\ not\ received \\ x_p(t) = x_s(t), & x_s(t)\ is\ received. \end{cases} \tag{8}$$

Whether the observer data $x_s(t)$ are sent is determined by the demand of scheduling control, which is represented by the difference between the observed states of the GU and the predicted value of the remote controller. Then, the DDM is designed as follows:

$$x_s(t)\ is\ sent \Leftrightarrow \left\|x_s(t) - x_p(t)\right\| > \sigma_s\|x_s(t)\| + \sigma_c\rho \tag{9}$$

where $\rho = \gamma\|C\|\delta + \delta_v$, $\delta = \|E\|\delta_\omega + \delta_v$, σ_s and σ_c are suitable positive demand parameters to be selected later, and γ is obtained by solving LMI (7). Besides, when the DDM (9) is met, an acknowledgment (ACK) signal is required to affirm that the transmission attempt was successful, and this assumption is consistent with the TCP-type communication protocol.

Define $\{t_k\}_{k\in\mathbb{N}_0}$ as the sequence performing data transmission of control update, and denote $\Delta_k = t_{k+1} - t_k$ by the data transmission interval between two consecutive attempts, which

$$0 < \underline{\Delta} \le \Delta_k \le \bar{\Delta} \tag{10}$$

where $\bar{\Delta}$ and $\underline{\Delta}$ are upper and lower bounds of the intervals between two consecutive attempts, respectively.

Remark 1. *The length of interval Δ_k is decided by the DDM (9), but it is necessary to set the lower and upper bound. Due to the characteristic of periodic verification strategy, the lower bound $\underline{\Delta}$ can be selected as the DDM verification period. Inspired by the pre-specified upper bound of inter-event times in* [17]*, the upper bound $\bar{\Delta}$ is needed to force the sensor to send data to the remote controller if the transmission is not executed for long periods of time.*

The sensor system transmits the latest estimation value $x_s(t)$ to the controller system by network communication to renew the state prediction $x_p(t)$ at $\{t_k\}_{k\in\mathbb{N}_0}$—that is, $x_p(t_k) =$

$x_s(t_k)$, and it is the initial value for the state prediction when $t \in [t_k, t_{k+1})$. Then, $x_p(t)$ is calculated by (8) and the control value is able to be designed by the switching controller formulated as

$$u(t) = \begin{cases} Kx_p(t), & x_s(t) \text{ is not received} \\ Kx_s(t), & x_s(t) \text{ is received.} \end{cases} \tag{11}$$

where K is the state feedback gain matrix. In order to improve the rate of convergence, region poles assignment lemma [23] is used to solve K with α stability margin. Let $\Phi_2 = A + BK$; then, K can be obtained by solving the following LMI:

$$P_2\Phi_2 + \Phi_2^T P_2 + 2\alpha P_2 < 0 \tag{12}$$

where $\alpha > 0$ is a given coefficient and P_2 is a symmetric positive definite matrix.

As in Figure 2, a replica of the predictor $\mathcal{P}r$ is run in the sensor system so that it can synchronize $x_p(t)$ that the controller system has and can judge whether (9) is satisfied. When the DDM (9) is not satisfied, $x_s(t)$ is not sent and the error between $x_p(t)$ and $x_s(t)$ is accumulated until (9) is satisfied; then, $x_s(t)$ is transmitted to the predictor $\mathcal{P}r$, and an ACK signal is sent and returned to the sensor from the controller system by the network to ascertain that the transmission attempt was triumphant.

3. Demand-Driven Control Strategy

This section gives the design process of the demand-driven control strategy—that is, the selection method of driven parameters under the premise of ensuring the control objective. First of all, the control objective is described as the definition provided below:

Definition 1 ([24]). *Given the GU system (3) with control input (11), for each* $\omega_t \in \mathcal{L}_\infty(\mathbb{R}, \omega \geq 0)$ *and* $x(0) \in \mathbb{R}^n$, *if there is a* $\mathcal{KL}$*-function* $h_1(\cdot)$ *and a* $\mathcal{K}_\infty$*-function* $h_2(\cdot)$ *such that*

$$\|x(t)\| \leq h_1(\|x(0)\|, t) + h_2(\|\omega_t\|_\infty) \tag{13}$$

holds for all $t \in \mathbb{R}$ *with* $t \geq 0$, *the system is considered to be ISS. Besides, the system (3) is globally asymptotically stable if (13) is satisfied for* $\omega_t \equiv 0$.

Then, the design process of the demand-driven parameters is given. For $t \in \mathbb{R}$, $t \geq 0$, to measure the difference between the truth state $x(t)$ and the state prediction $x_p(t)$, which represents the demand of network communication, denote the prediction error by

$$e(t) = x_p(t) - x(t) \tag{14}$$

Then, the formula for the closed-loop GU system is given as

$$\dot{x}(t) = \Phi_2 x(t) + BKe(t) + E\omega(t) \tag{15}$$

Design the Lyapunov function as $V(t) = x^T(t)Px(t)$, where P is the unique solution of the following Lyapunov equation:

$$P\Phi_2 + \Phi_2^T P + Q = 0 \tag{16}$$

where Q is any given positive definite symmetric matrix. Then, we have

$$\alpha_1\|x(t)\| \leq V(t) \leq \alpha_2\|x(t)\| \tag{17}$$

$$\dot{V}(t) \leq -\gamma_1 \|x(t)\|^2 + \gamma_2 \|x(t)\| \|e(t)\| + \gamma_3 \|x(t)\| \|\omega(t)\| \tag{18}$$

for any $t \in \mathbb{R},\ t \geq 0$, where α_1 and α_2 are equal to the smallest and largest eigenvalues of P, respectively. γ_1 is the smallest eigenvalue of Q; $\gamma_2 = \|2PBK\|$ and $\gamma_3 = \|2PE\|$. Notice that $\|x_s(t) - x_p(t)\| \leq \sigma_s \|x_s(t)\| + \sigma_c \rho$ is always true when $t \in [t_k, t_{k+1})$; then, it yields

$$\|x(t) - x_p(t)\| \leq \sigma_s \|x(t)\| + \sigma_c \rho + \lambda \|\xi(t)\|_\infty \tag{19}$$

where the inequality comes from the triangle inequality and the fact that $\|e_s(t)\| = \|x(t) - x_s(t)\| < \gamma \|\xi(t)\|_\infty$. Then, $\|\xi(t)\|_\infty \leq \|E\|\delta_\omega + \delta_v = \delta$ yields

$$\|e(t)\| = \|x(t) - x_p(t)\| \leq \sigma_s \|x(t)\| + \sigma_\delta \delta \tag{20}$$

where $\sigma_\delta = \gamma \sigma_c \|C\| + \gamma + \sigma_c$. Then, $\dot{V}(t) \leq -(\gamma_1 - \sigma_s \gamma_2)\|x(t)\|^2 + (\gamma_3 + \sigma_\delta \gamma_2)\|x(t)\|\delta$ can be obtained by substituting (20) into (18) and indicates that when $\gamma_1 - \sigma_s \gamma_2 > 0$ holds,

$$V(x(t)) \leq e^{-\theta_1 t} V(x(0)) + \gamma_4 \delta^2 \tag{21}$$

where $\theta_1 = \frac{\gamma_5}{2\alpha_1}$, $\gamma_4 = \frac{(\gamma_3 + \sigma_\delta \gamma_2)^2}{2\gamma_5 \theta_1}$, and $\gamma_5 = \gamma_1 - \sigma_s \gamma_2$.

The use of the prediction method makes the controller system able to simulate the true state value; then, the discrepancy accumulated in the transmission interval is degraded by the information compensation. From (14), it yields for any $t \in [t_k, t_{k+1})$ that the dynamic of the prediction error can be formulated as

$$\begin{aligned} \dot{e}(t) &= \dot{x}_p(t) - \dot{x}(t) \\ &= Ae(t) - E\omega(t) \end{aligned} \tag{22}$$

then, we have the upper bound of the error as

$$\begin{aligned} \|e(t)\| &\leq \int_{t_k}^{t} e^{\mu_A (t-\tau)} (\|A\| \|e_s(t_k)\| + \|E\| \|\omega(\tau)\|) d\tau \\ &< f(t - t_k)(\gamma \|A\| \delta + \|E\| \delta_\omega) \\ &= \varepsilon (\gamma \|A\| \delta + \|E\| \delta_\omega) \end{aligned} \tag{23}$$

where $f(t - t_k) = \int_{t_k}^{t} e^{\mu_A (t-\tau)} d\tau$ and $\varepsilon = \begin{cases} \Delta_k, & \mu_A \leq 0 \\ \frac{1}{\mu_A}(e^{\mu_A \Delta_k} - 1), & \mu_A > 0 \end{cases}$.

Because the DDM (9) is periodically validated in the case of a continuous system process, it is necessary to investigate the transmission attempt sequence $\{t_k\}_{k \in \mathbb{N}_0}$ to eliminate continuous transmissions within each validation period. Denote the estimation–prediction error by $e_p(t) = x_s(t) - x_p(t)$; then, the dynamic of this error is

$$\dot{e}_p(t) = Ae_p(t) + L\bar{y}(t) \tag{24}$$

where $\bar{y}(t) = Ce_s(t) + v(t)$. Since $e_p(t_k) = 0$ for any $t \in [t_k, t_{k+1})$, it yields

$$\begin{aligned} \|e_p(t)\| &\leq \|L\| \int_{t_k}^{t} e^{\mu_A (t-\tau)} \|\bar{y}(\tau)\| d\tau \\ &\leq \|L\| \int_{t_k}^{t} e^{\mu_A (t-\tau)} d\tau (\|C\| \|e_s(t)\| + \|v(t)\|_\infty) \\ &\leq \begin{cases} \rho \|L\| (t - t_k), & \mu_A \leq 0 \\ \rho \frac{\|L\|}{\mu_A} (e^{\mu_A (t-t_k)} - 1), & \mu_A > 0 \end{cases} \end{aligned}$$

where $\rho = \gamma\delta\|C\| + \delta_v$ as in (9); further, it yields that if $t - t_k \geq \underline{\Delta}$ with

$$\underline{\Delta} = \begin{cases} \frac{\sigma_c}{\|L\|}, & \mu_A \leq 0 \\ \frac{1}{\mu_A}\log(\frac{\mu_A\sigma_c}{\|L\|} + 1), & \mu_A > 0 \end{cases} \tag{25}$$

then for any $\sigma_c > 0$, the DDM (9) cannot be satisfied if $t \in [t_k, t_k + \underline{\Delta})$.

Remark 2. *Notice that the threshold part of the mechanism is divided into two items. One influences the stability of the system and is determined by the parameter σ_s. If the selected parameter σ_s is large, the demand error will be too large compared to the updated data $x_s(t)$, and the updated data may not stabilize the system. The other parameter is σ_c, which determines the influence of the disturbance and noise to the DDM. The selection of σ_c directly determines the minimum transmission interval $\underline{\Delta}$, and σ_c can be chosen based on the quantitative relationship (25).*

4. Resilient Control with Unreliable Communication

Notice that when the demand-driven control strategy is designed, the status of the communication is unknown. In other words, the prediction-based control algorithm is a passive resilient scheme. When a DoS attack occurs, the active communication scheduling protocol is another resilient scheme, which is presented in this section. Besides, the stability analysis under DoS attacks is given.

4.1. DoS Attack Model

To extend the application range of resilient control as far as possible, the unreliable communication caused by DoS attacks is considered here, and a general attack model is adopted that restricts the attack behavior by only posing constraints in time on their duration and frequency. Denote $\{d_n\}_{n\in\mathbb{N}_0}$ by the DoS off/on transitions sequence with $d_0 \geq 0$—that is, the time instant set in which attack behavior turns from zero (communication channel is reliable) to one (transmissions are jammed). The nth DoS time-interval is $D_n = \{d_n\} \cup [d_n, d_n + \tau_n)$, and $\tau_n \in \mathbb{R},\ \tau_n \geq 0$ is the length. Then, D_n is a single pulse if $\tau_n = 0$. Suppose that $\{D_n\}_{n\in\mathbb{N}}$ has no overlap; then, consider an interval $[t, \zeta)$ with $0 \leq t < \zeta$ and let

$$\mathcal{D}(t,\zeta) = \bigcup_{n\in\mathbb{N}_0} D_n \cap [t,\zeta) \tag{26}$$

$$\mathcal{H}(t,\zeta) = [t,\zeta)\backslash\mathcal{D}(t,\zeta) \tag{27}$$

be the subset of time intervals in $[t, \zeta)$ where the network is in attack status and healthy, respectively. Denote $n(t, \zeta)$ by the number of DoS off/on transitions over $[t, \zeta)$. Referring to [10], the following assumptions are proposed to restrict the frequency and duration of DoS attacks.

Assumption 1. *For any $0 \leq t < \zeta$, there exist scalars $\kappa \in \mathbb{R},\ \eta \geq 0$ and $\tau_D \in \mathbb{R},\ \tau_D \geq \underline{\Delta}$ such that*

$$n(t,\zeta) \leq \kappa + \frac{\zeta - t}{\tau_D} \tag{28}$$

Assumption 2. *For any $0 \leq t < \zeta$, there exist scalars $\varsigma \in \mathbb{R},\ \varsigma \geq 0$ and $T \in \mathbb{R},\ T > 1$ such that*

$$|\mathcal{D}(t,\zeta)| \leq \varsigma + \frac{\zeta - t}{T} \tag{29}$$

Remark 3. *The frequency and duration assumptions for DoS attacks are necessary. Take into account the worst scenario without the limitations: firstly, if $n(t,\zeta)$ is sufficient large, each transmission attempt may be overridden by attack pulses; secondly, when $|\mathcal{D}(t,\zeta)|$ is sufficient large, an attack interval may never stop in any given $[t,\zeta)$. In both cases, all the transmissions can be jammed and the scheduling control performance cannot be guaranteed. Besides, the two assumptions can be understood in terms of attack energy. Assume that an attacker having confined energy to carry out attack behaviors is reasonable and the usable energy is proportional to the length of time interval $[t,\zeta)$ with a scale factor. The energy expended by each attack off/on transition is τ_D, and for each unit of time, the required energy to sustain an attack execution is T. Furthermore, κ and ς can be considered as regularized scalars.*

4.2. Control Update Protocol Under DoS Attacks

Define the first time instant where the DDM is verified to be true after a data communication success at t_k as

$$\lambda_k = \inf\{t \in \mathbb{R},\ t > t_k \big| \big\|x_s(t) - x_p(t)\big\| \geq \sigma_s \|x_s(t)\| + \sigma_c \rho\} \tag{30}$$

If a data transmission appears in an attack interval D_n, the attempt cannot be successful. Define $\mathcal{F} = \{k \in \mathbb{N}_0 | t_k \in \underset{n\in\mathbb{N}_0}{\cup} D_n\}$ as the set of integers associated with communication attempts that occur under attack. During the attack intervals, the control strategy of the GU system is converted to a periodic communication protocol—that is, the selected communication attempt period is smaller than or equal to the demand-driven control scheduling interval for the purpose of decreasing the communication delay introduced by the jamming attack. For any $k \in \mathbb{N}_0$, the time when that communication attempt occurs is described below:

$$t_{k+1} = \begin{cases} t_k + \Delta^*, & if\ k \in \mathcal{F} \\ t_k + \bar{\Delta}\ , & if\ k \notin \mathcal{F} \vee\ \bar{\Delta} < \lambda_k - t_k \\ \lambda_k, & \text{otherwise} \end{cases} \tag{31}$$

where the control update period during the jamming attack intervals is denoted by Δ^*, which satisfies $0 < \Delta^* \leq \underline{\Delta}$.

Remark 4. *Equation (31) provides the resilient update protocol against the jamming attack behaviors described in Assumptions 1 and 2. If the sensor can receive the ACK signal at t_k, then the data transmission at t_k succeeds. Then, the next data transmission will be attempted at λ_k when $\bar{\Delta} \geq \lambda_k - t_k$. If $\bar{\Delta} < \lambda_k - t_k$, then the next data transmission will be attempted at $t_k + \bar{\Delta}$. If the ACK signal cannot be received at t_k for the sensor, it indicates that an attack off/on transition appeared before t_k, and from t_k, the data communication is performed at the periodic update rate appointed by Δ^* tentatively until the sensor is able to receive the ACK signal again.*

Remark 5. *The resilience is achieved based on an active and passive combined control scheme. First, the predictor provides predicted values as close as possible to the state of the system when there is no data transmission. In this way, when malicious communication interferences occur and data cannot be transmitted, the predictor can compensate for the missing data, thereby improving resilience to unreliable communications actively. Meanwhile, the resilient update protocol designed in this paper is able to minimize the additional transmission periods caused by communication interruptions, so that the system can resume data transmission as early as possible at the end of the attack. This is a passive resilience improvement method.*

Define $\hat{\mathcal{H}}(t_1, t_2)$ as the union of time subintervals in which the DDM (9) is not held in $[t_1, t_2)$ with $0 \leq t_1 < t_2$—i.e., the union of healthy subintervals in $[t_1, t_2)$—and define the union of valid attack subintervals in which DDM (9) is true as $\hat{\mathcal{D}}(t_1, t_2)$; then, the disjoint union of $\hat{\mathcal{H}}(t_1, t_2)$ and $\hat{\mathcal{D}}(t_1, t_2)$ is the whole interval $[t_1, t_2)$ for any $0 \leq t_1 < t_2$, and $\hat{\mathcal{D}}(t_1, t_2) = [t_1, t_2) \backslash \hat{\mathcal{H}}(t_1, t_2)$. Denote

$$\rho_n = \begin{cases} 0, & if\ \mathcal{F} = \emptyset \\ t_{\sup\{k \in \mathcal{F}\}} - d_n, & otherwise \end{cases} \tag{32}$$

$$\Lambda_n = \begin{cases} 0, & if\ \mathcal{F} = \emptyset \\ \Delta_{\sup\{k \in \mathcal{F}\}} = \Delta^*, & otherwise \end{cases} \tag{33}$$

then, $\hat{H}_n = \{d_n\} \cup [d_n, d_n + \rho_n + \Lambda_n)$ is the n-th effective attack subinterval. It is worth noting that $\hat{H}_n$ and $\hat{H}_n + 1$ may overlap since d_{n+1} may be located in $\hat{H}_n$. For convenience, the two overlapped subintervals can be considered as an incorporative, effective attack interval. Define $\{\phi_m\}_{m \in \mathbb{N}_0}$ as the sequence of off/on transitions of the m-th effective attack interval—that is,

$$\phi_0 = d_0,\ \phi_{m+1} = \inf\{d_n > \phi_m | d_n > d_{n-1} + \rho_{n-1} + \Lambda_{n-1}\} \tag{34}$$

and the length of the m-th effective attack interval is $\nu_m = \sum_{\substack{n \in \mathbb{N}_0 \\ \phi_m \leq d_n < \phi_{m+1}}} \left| \hat{H}_n \backslash \hat{H}_{n+1} \right|$; then, $\hat{\mathcal{D}}(t_1, t_2) = \bigcup_{m \in \mathbb{N}_0} [\phi_m, \phi_m + \nu_m) \cap [t_1, t_2)$ and $\hat{\mathcal{H}}(t_1, t_2) = \bigcup_{m \in \mathbb{N}_0} [\phi_m + \nu_m, \phi_{m+1}) \cap [t_1, t_2)$. From Assumptions 1 and 2, it can be obtained that the upper bound of the time interval for the impact of an attack is

$$\begin{aligned} \left| \hat{\mathcal{D}}(t_1, t_2) \right| &\leq |\mathcal{D}(t_1, t_2)| + (n(t_1, t_2) + 1)\Delta^* \\ &\leq \varsigma^* + \tfrac{t_2 - t_1}{T^*} \end{aligned} \tag{35}$$

where $\varsigma^* = \varsigma + (\eta + 1)\Delta^*$ and $\frac{1}{T^*} = \frac{\Delta^*}{\tau_D} + \frac{1}{T}$. The following lemma gives a quantitative characterization of the interval between two successive successful transmissions.

Lemma 1. *Define $\{z_m\}_{m \in \mathbb{N}_0}$ as the time sequence at which the data transmissions succeed. For the communication update protocol as in (31), and considering the DoS attacks satisfying Assumptions 1 and 2, $z_{m+1} - z_m \leq \Omega + \bar{\Delta}$ holds for $z_0 \leq \Omega$, where $\Omega = (\varsigma + \kappa\Delta^*)(1 - \frac{\Delta^*}{\tau_D} - \frac{1}{T})^{-1}$.*

Remark 6. *Inspired by a similar result in [11], the above lemma gives an upper bound on the interval between two successful transmissions with a demand-driven strategy. Since the inner-demand interval is unknown, the time interval between transmission attempts during D_n is also unknown. Fortunately, based on the known upper bound of the communication interval $\bar{\Delta}$, the worst case of the data updates can be bounded. Evidently, $\frac{1}{T^*} < 1$ is necessary, and it is the loosest restriction to achieve closed-loop stability under any DoS attacks satisfying Assumptions 1 and 2, as discussed in [11].*

According to Lemma 1, (22) and (23) yield the upper bound of the prediction error $e(t)$ as

$$\|e(t)\|_\infty < \bar{\varepsilon}(\gamma \|A\| \delta + \|E\| \delta_\omega) \tag{36}$$

for any $t \in [z_m, z_{m+1})$, where $\bar{\varepsilon} = \begin{cases} \Omega + \bar{\Delta}, & \mu_A \leq 0 \\ \frac{1}{\mu_A}(e^{\mu_A(\Omega+\bar{\Delta})} - 1), & \mu_A > 0 \end{cases}$. It indicates that the prediction error between $x_p(t)$ and $x(t)$ is bound even under DoS attacks. By applying (36), we have the main results as the following theorem.

Theorem 1. *Consider the GU system (3) with a control structure that consists of the observer $\mathcal{O}$ and the predictor $\mathcal{P}r$, the scheduling control input (11), and the DDM (9), and select the parameters such that $\gamma_1 - \sigma_s\gamma_2 > 0$ holds. Under Assumptions 1 and 2, if for any DoS attacks with arbitrary scalars ς, κ, τ_D, and T such that*

$$\frac{\Delta^*}{\tau_D} + \frac{1}{T} < 1 \tag{37}$$

holds, where Δ^* is a positive constant and satisfies $\Delta^* \leq \bar{\Delta}$, then the GU control system is ISS with the periodic update protocol (31).

Proof. The proof is provided in Appendix A. □

Remark 7. *The conservatism of the results in* [10,20] *results from decomposing the timeline into attack intervals and non-attack intervals. In fact, the attack intervals can also be decomposed into valid attack intervals and invalid attack intervals; the latter are the subintervals where the DDM has not been met—that is, $\|x_s(t) - x_p(t)\| < \sigma_s\|x_s(t)\| + \sigma_c\rho$. The actual effective attack intervals are the subintervals where the DDM is verified to be true and the data transmissions fail. Due to the unknown time at which the attack behavior's off/on transition occurs, the conservatism of the resilience cannot be decreased by splitting the timeline. Based on the maximum disturbance–accumulation error, which is calculated from (36), the procedure can be understood in turn as the difference converging from the maximum error to $\sigma_s\|x_s(t_k)\| + \sigma_c\rho$ with $k = \inf\{k \in \mathcal{F} | t_k \in \bigcup_{n\in\mathbb{N}_0} D_n\}$; in this way, the optimal bound of the tolerable intensity of a DoS attack can be achieved.*

5. Simulation Examples

In this section, the GU model constructed in Section 2.1 is applied to validate the resilient control performance of the designed methods. The parameters of the GU system are shown as follows: $f_0 = 1$ Hz, $\omega_0 = 6.283$ rad/s, $R_{ij} = 1.3 \times 10^{-3}$ Ω, $C_{ti} = 62.86$ F, $k_i = 0.0435$, $L_{ij} = 0.6$ H, $L_{ti} = 9.26 \times 10^{-3}$ H, $R_{tj} = 1.3 \times 10^{-3}$ Ω. The system matrices of the GU model can be calculated as follows:

$$A = \begin{bmatrix} -1.3 & 2.516 & 0.691 & 0 \\ -2.516 & -1.3 & 0 & 0.691 \\ -4.69 & 0 & -0.14 & 6.283 \\ 0 & -4.69 & -6.283 & -0.14 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1.07 & 0 \\ 0 & 1.07 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

In the simulation, the unknown disturbance $\omega(t)$ is assumed as stochastic signals with a uniform distribution in $[-0.4,\ 0.4]$ and noise $v(t)$ is $v(t) = a\sin(\Omega_y)$, $\Omega_y \in [0, 2\pi]$, where a is a stochastic number with a uniform distribution bounded in $[0,\ 0.2]$. The initial conditions are $x(0) = x_p(0) = [0.8, -1, 0, 0.3]^T$. The control objective is to track the reference signal $[0.08\ \ -0.09\ \ -0.12\ \ -0.63]^T$. Selecting $\lambda = 5.97$, the gain matrices of observer and controller can be calculated by solving the LMIs (7) and (12) as follows:

$$L = \begin{bmatrix} 0.5755 & 0.5755 \\ -0.1981 & 3.8506 \\ 1.1000 & -3.8657 \\ -5.5976 & -6.8427 \end{bmatrix}, K = \begin{bmatrix} 0.0630 & -0.2771 & -0.3848 & -0.0003 \\ 0.2788 & 0.1109 & -0.0003 & -0.3278 \end{bmatrix}.$$

The relative parameters can be obtained such that $\|\Phi_2\| = 8.1528$, $\alpha_1 = 1.4768$, $\alpha_2 = 0.3375$, $\gamma_1 = 1$, $\gamma_2 = 1.4976$, and $\gamma_3 = 2.9536$. Thus σ_s has to be chosen such that $\sigma_s < 0.6677$. Setting $\sigma_s = 0.66$, and $\bar{\Delta} = 0.5s$ and $\underline{\Delta} = 0.01$ s, the demand-driven parameter σ_c is chosen as $\sigma_c = 0.004$. When there are no DoS attacks, the state responses of the controlled system, the evolution of the transmission times, and the demand-driven conditions $\|x_s(t) - x_c(t)\|$ and $\sigma_s\|x_s(t)\| + \sigma_c\rho$ are exhibited in Figures 3 and 4, respectively. From the above figures, it is obvious that the demand-driven control algorithm is able to ensure that the state responses of the GU system track the reference values while the number of network transmissions is decreased significantly. From Figure 4, when the demand (black) exceeds the transmission condition (red), the data are transmitted over the network (such as at 9.8 s). The black line quantifies the information difference between the controller side and the sensor side, which represent the control requirements in real application scenarios. The red line quantifies the acceptable demand threshold. If the information difference does not exceed the threshold, it indicates that the impact of the difference on system performance during actual application is tolerable, and no data transmission is required.

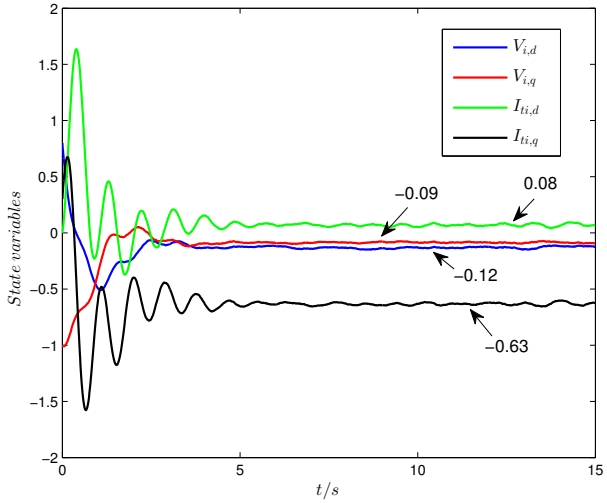

Figure 3. State responses without DoS attacks.

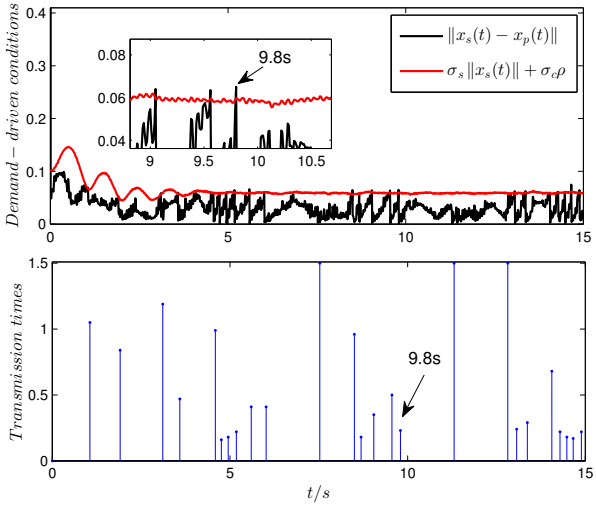

Figure 4. (**Top**): the evolution of demand-driven condition. (**Bottom**): the values of the transmission times.

When DoS attacks occur, the transmission protocol is provided in (31), and the transmission attempt period is $\Delta_* = 0.01$ s. In the simulation time domain of 15 s, the DoS

attack is executed randomly and satisfies $n(0,15) = 12$ and $|\mathcal{D}(0,15)| = 10.93$ s. According to the duration and frequency of the attack, we have $\tau_D \approx 1.25$ and $T \approx 1.372$; then, $\frac{\Delta^*}{\tau_D} + \frac{1}{T} \approx 0.737$. Then, the state responses of the closed-loop GU system, the evolution of the transmission times, and the demand-driven condition $\|x_s(t) - x_p(t)\|$ and $\sigma_s\|x_s(t)\| + \sigma_c\rho$ are exhibited in Figures 5–7, respectively. Finally, the control input of the GU model is given in Figure 8.

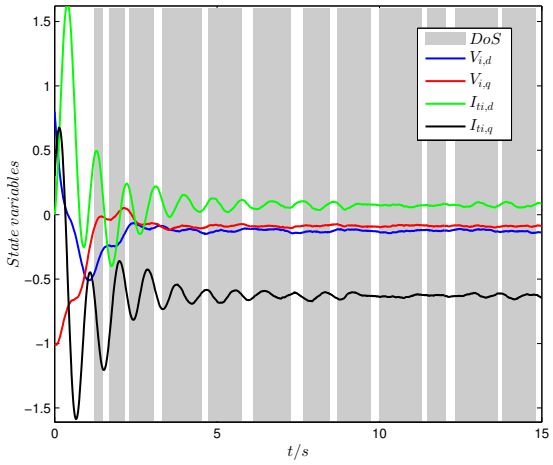

Figure 5. State responses under DoS attacks.

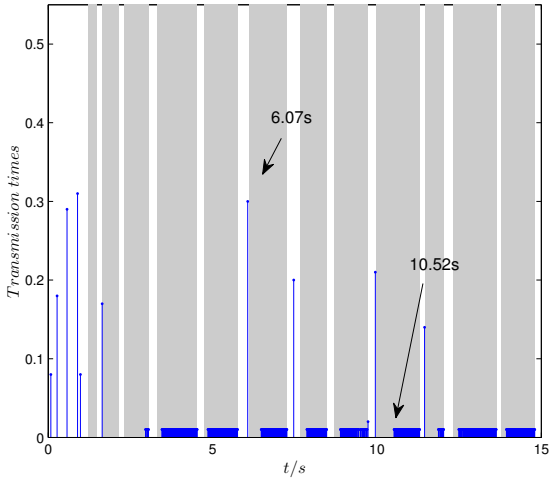

Figure 6. The transmission times under DoS attacks.

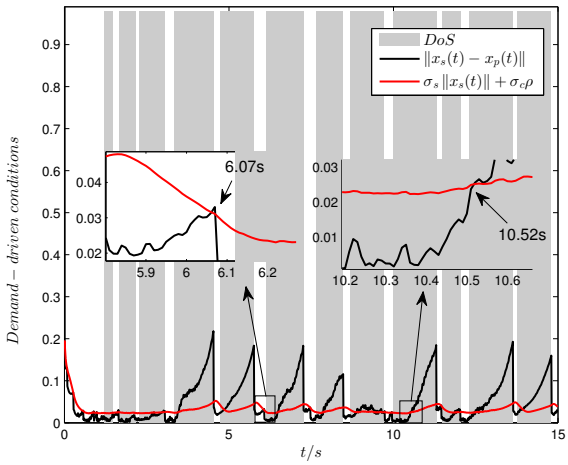

Figure 7. The evolution of $\|x_s(t) - x_c(t)\|$ and $\sigma_s\|x_s(t)\| + \sigma_c\rho$ under DoS attacks.

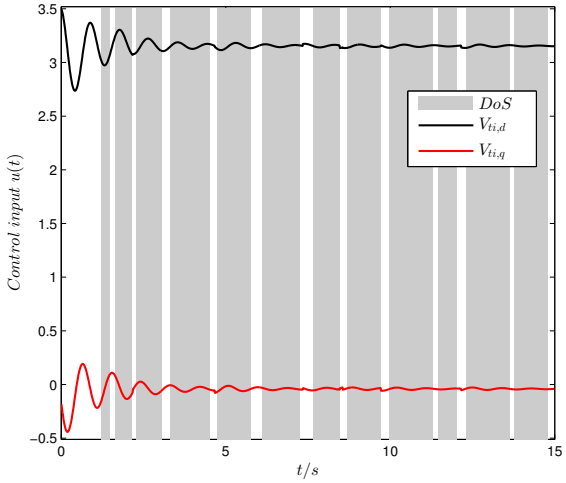

Figure 8. The control input of GU under DoS attacks.

From Figure 5, it can be observed that the states of the GU model can also track the reference values under DoS attacks. However, compared with Figures 3 and 5, it is shown that the time it takes for the wave of states under DoS attacks to end is significantly longer than that without DoS attacks, which indicates the influence of the DoS attacks to the networked control strategy. As can be observed from Figures 6 and 7, the demand-driven algorithm still works, and the transmission attempts succeed during the no-attack intervals when the demand exceeds the transmission condition (such as at 6.07 s) while the transmission mode switches to periodic attempts during the attack intervals (such as 10.52 s). As can be seen from the above figures, the demand-driven control scheme also has a certain potential resilience in practical applications. For instance, from Figure 7, it can be seen that the DoS attacks before the demand (black) exceeds the threshold (red) are invalid. In these intervals, there is no transmission attempt, which can be observed in Figure 6 before 10.52 s.

6. Conclusions

This paper focuses on the secure control problem for the GU of a local power plant under unreliable communication, and the demand-driven control strategy has been investigated. The unreliable communication in consideration is caused by DoS attacks, and the resilient control algorithm is designed to handle the problem of performance degradation in this scenario. An H_∞ observer-based prediction method is provided, and the DDM is designed based on the error between the state estimation and prediction. In this way, the communication resources are saved while the ideal scheduling control performance is obtained. Based on the ISS analysis, the sufficient conditions on the DoS attack model are provided to ensure the stability of the GU system. Finally, simulation results were presented to demonstrate the effectiveness of the designed methods.

The technical novelties are summed up as follows: First, the H_∞ observer-based prediction method is able to remove the influence of unknown load currents to the system and compensate the loss of state data in the interval between any two continuous transmissions of scheduling signals. Second, the advanced demand-driven strategy with periodic verification is presented to schedule the intermittent communication. Third, by using the thought of robustness to the maximum disturbance-induced error, the conservatism of the tolerable attack intensity is decreased.

Author Contributions: Conceptualization, G.C. and D.X.; methodology, Y.-C.S.; software, Z.W.; validation, D.X. and B.L.; formal analysis, G.C. and D.X.; investigation, Y.-C.S.; resources, K.M.; data curation, B.L. and K. M.; writing—original draft preparation, Y.-C.S.; writing—review and editing,

G.C. and Y.-C.S.; visualization, Y.-C.S.; supervision, G.C. and D.X.; project administration, G.C. and Z.W.; funding acquisition, G.C. and D.X. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the State Grid Henan Electric Power Company Technology Project (Grant No. 521702240003).

Data Availability Statement: Dataset available on request from the authors.

Conflicts of Interest: Author Guizhou Cao, Dawei Xia and Kai Meng was employed by the company State Grid Henan Electric Power Company. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Appendix A

Proof of Theorem 1. Firstly, a stability analysis of the effective attack subinterval $[\phi_m, \phi_m + \nu_m)$ and the healthy subinterval $[\phi_m + \nu_m, \phi_{m+1})$ is provided.

Select the Lyapunov function as $V(t) = x^T(t)Px(t)$, where P and Q are calculated as in (16). It is worth noting that $\|x(t) - x_p(t)\| \leq \sigma_s\|x(t)\| + \sigma_c\rho$ holds for all $t \in [\phi_m + \nu_m, \phi_{m+1})$, $m \in \mathbb{N}_0$; then, from (21), we have

$$V(x(t)) \leq e^{-\theta_1(t-\phi_m-\nu_m)}V(x(\phi_m + \nu_m)) + \gamma_4\delta^2 \tag{A1}$$

where $\theta_1 = \frac{\gamma_5}{2\alpha_1}$, $\gamma_4 = \frac{\gamma_3^2}{2\gamma_5\theta_1}$, and $\gamma_5 = \gamma_1 - \sigma_s\gamma_2$.

Then, the effective attack interval $t \in [\phi_m, \phi_m + \nu_m)$, $m \in \mathbb{N}_0$ is concerned. Beginning at some point in the above interval, $\|x(t) - x_p(t)\| \leq \sigma_s\|x(t)\| + \sigma_c\rho$ will become false. From (36), it yields that $\|e(t)\|_\infty < \bar{\varepsilon}(\gamma\|A\|\delta + \|E\|\delta_\omega)$ holds; then, from (18), we have

$$\begin{aligned}\dot{V}(x(t)) &\leq -\gamma_1\|x(t)\|^2 + \gamma_2\bar{\varepsilon}\|x(t)\|(\gamma\|A\|\delta + \|E\|\delta_\omega) + \gamma_3\|x(t)\|\|E\omega(t)\| \\ &\leq -\gamma_1\|x(t)\|^2 + (\gamma_2\bar{\varepsilon} + \gamma_3)\|x(t)\|\delta_e\end{aligned} \tag{A2}$$

where $\delta_e = \gamma\|A\|\delta + \|E\|\delta_\omega$. Then, based on Yang's inequality, it yields

$$\begin{aligned}\dot{V}(x(t)) &\leq -\tfrac{\gamma_1}{2}\|x(t)\|^2 + \tfrac{(\gamma_2\bar{\varepsilon}+\gamma_3)^2}{2\gamma_1}\delta_e^2 \\ &\leq -\theta_2 V(x(t)) + \gamma_6\delta_e^2\end{aligned} \tag{A3}$$

where $\theta_2 = \frac{\gamma_1}{2\alpha_1}$, $\gamma_6 = \frac{(\gamma_2\bar{\varepsilon}+\gamma_3)^2}{2\gamma_1}$; thus, it can be calculated that

$$V(x(t)) \leq e^{-\theta_2(t-\phi_m)}V(x(\phi_m)) + \gamma_7\delta_e^2 \tag{A4}$$

holds for all $t \in [\phi_m, \phi_m + \nu_m)$, $m \in \mathbb{N}_0$, and $\gamma_7 = \frac{\gamma_6}{\theta_2}$.

Secondly, stability analysis on the entire timeline is given. For any $t \in \mathbb{R}, t > 0$, it yields

$$V(x(t)) \leq e^{-\theta_1|\hat{\mathcal{H}}(0,t)|}e^{-\theta_2|\hat{\mathcal{D}}(0,t)|}V(x(0)) + \gamma_* \sum_{\substack{m\in\mathbb{N}_0; \\ \phi_m\leq t}} e^{-\theta_1|\hat{\mathcal{H}}(\phi_m+\nu_m,t)|}e^{-\theta_2|\hat{\mathcal{D}}(\phi_m,t)|}\delta_*^2 \tag{A5}$$

where $\gamma_* = \max\{\gamma_4, \gamma_7\}$ and $\delta_* = \max\{\delta, \delta_e\}$. Based on (35), one can obtain that for any $t \in \mathbb{R}, t > \phi_m$, $\left|\hat{\mathcal{D}}(\phi_m, t)\right| \leq \varsigma^* + \frac{t-\phi_m}{T^*}$ holds. When $t < \phi_m + \nu_m$, we have that $\hat{\mathcal{D}}(\tau, t) = [t_1, t_2]\backslash\hat{\mathcal{H}}(t_1, t_2)$ and $\hat{\mathcal{H}}(\phi_m + \nu_m, t) = 0$ hold, which yields

$$\hat{\mathcal{H}}(\phi_m + \nu_m, t) = t - \phi_m - \left|\hat{\mathcal{D}}(\phi_m, t)\right| \tag{A6}$$

It is worth noting that $\left|\hat{\mathcal{D}}(\phi_m, t)\right| = \nu_m$ and $\left|\hat{\mathcal{D}}(\phi_m + \nu_m, t)\right| = 0$ hold for any $t \in \mathbb{R}, t > \phi_m + \nu_m$; then, it is indicated that $\hat{\mathcal{H}}(\phi_m + \nu_m, t) = t - \phi_m - \nu_m = t - \phi_m - \left|\hat{\mathcal{D}}(\phi_m, t)\right|$ holds. Then, it yields

$$\sum_{\substack{m\in\mathbb{N}_0;\\ \phi_m\le t}} e^{-\theta_1\left|\hat{\mathcal{H}}(\phi_m+\nu_m,t)\right|} e^{-\theta_2\left|\hat{\mathcal{D}}(\phi_m,t)\right|} \le e^{-(\theta_2-\theta_1)\varsigma^*} \sum_{\substack{m\in N_0;\\ \phi_m\le t}} e^{-a(t-\phi_m)} \tag{A7}$$

where $a = \theta_1 + \frac{\theta_2-\theta_1}{T^*}$. It is obvious that $a > 0$ can be guaranteed by $\frac{1}{T^*} < 1$. Similar to the transformation of (A7), the term $e^{-\theta_1\left|\hat{\mathcal{H}}(0,t)\right|} e^{-\theta_2\left|\hat{\mathcal{D}}(0,t)\right|}$ in the right hand of (A5) can have an upper bound as $e^{-(\theta_2-\theta_1)\varsigma^*} e^{-at}$, which yields

$$V(x(t)) \le e^{-(\theta_2-\theta_1)\varsigma^*} e^{-at} V(x(0)) + \gamma_*(1 + e^{-(\theta_2-\theta_1)\varsigma^*} \sum_{\substack{m\in\mathbb{N}_0;\\ \phi_m\le t}} e^{-a(t-\phi_m)})\delta_*^2 \tag{A8}$$

Inspired by the result from [10], it yields $\sum_{\substack{m\in\mathbb{N}_0;\\ \phi_m\le t}} e^{-a(t-\phi_m)} \le \frac{e^{a\eta\tau_D}}{1-e^{-a\tau_D}}$; then, we have

$$\|x(t)\| \le \sqrt{\frac{\alpha_1}{\alpha_2}} e^{\frac{-(\theta_2-\theta_1)\varsigma^*}{2}} e^{-\frac{at}{2}} \|x(0)\| + \sqrt{\frac{\gamma_*}{\alpha_2}(1 + \frac{e^{a\kappa\tau_D}}{1-e^{-a\tau_D}} e^{-(\theta_2-\theta_1)\varsigma^*})}\delta_* \tag{A9}$$

It is obvious that the scalars of (A9) have no connection with the initial conditions of the dynamic process and the unknown disturbance; then, based on Definition 1, it can be ascertained that the GU control system (3) is ISS. This ends the proof. □

References

1. Qu, B.G.; Wang, Z.D.; Shen, B.; Dong, H.L. Distributed state estimation for renewable energy microgrids with sensor saturations. *Automatica* **2021**, *131*, 109730. [CrossRef]
2. Jonathan, D.; Wang, J.H. AGC signal modeling for energy storage operations. *IEEE Trans. Power Syst.* **2014**, *29*, 2567–2568.
3. Tian, J.W.; Wang, B.H.; Li, T.Y.; Shang, F.T.; Cao, K.R. Coordinated cyber-physical attacks considering DoS attacks in power systems. *Int. J. Robust Nonlinear Control* **2020**, *31*, 4345–4358. [CrossRef]
4. Deng, R.L.; Gao, G.X.; Lu, R.X.; Liang, H.; Athanasios, V. False data injection on state estimation in power systems–attacks, impacts, and defense: A survey. *IEEE Trans. Ind. Inform.* **2017**, *13*, 411–423. [CrossRef]
5. Qi, W.H.; Sha, M.X.; Park, J.H.; Yan, H.C.; Xie, X.P. Asynchronous stabilization for discrete hidden semi-markov jumping power models with cyber attacks. *IEEE Trans. Circuits Syst. II Express Briefs* **2023**, *70*, 2565–2569. [CrossRef]
6. Peng, C.; Li, J.C.; Fei, M.R. Resilient event-triggering H-infinity load frequency control for multi-area power systems with energy-limited DoS attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 4110–4118. [CrossRef]
7. Li, Y.Z.; Shi, L.; Cheng, P.; Chen, J.M.; Quevedo, D.E. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Trans. Autom. Control* **2015**, *60*, 2831–2836. [CrossRef]
8. Zhang, H.; Cheng, P.; Shi, L.; Chen, J.M. Optimal denial-of-service attack scheduling with energy constraint. *IEEE Trans. Autom. Control* **2015**, *60*, 3023–3028. [CrossRef]
9. Zhang, H.; Cheng, P.; Shi, L.; Chen, J.M. Optimal DoS attack scheduling in wireless networked control system. *IEEE Trans. Control. Syst. Technol.* **2016**, *24*, 843–852. [CrossRef]
10. Persis, C.D.; Tesi, P. Input-to-state stabilizing control under denial-of-service. *IEEE Trans. Autom. Control* **2015**, *60*, 2930–2944. [CrossRef]
11. Feng, S.; Tesi, P. Resilient control under denial-of-service: Robust design. *Automatica* **2017**, *79*, 42–51. [CrossRef]
12. Persis, C.D.; Tesi, P. Networked control of nonlinear systems under denial-of-service. *Syst. Control Lett.* **2016**, *96*, 124–131. [CrossRef]
13. Lu, A.Y.; Yang, G.H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial-of-service. *IEEE Trans. Autom. Control* **2018**, *63*, 1813–1820. [CrossRef]
14. Dolk, V.S.; Tesi, P.; Persis, C.D.; Heemels, W.P.M.H. Event-triggered control systems under denial-of-service attacks. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 93–105. [CrossRef]
15. Qi, W.H.; Sha, M.X.; Park, J.H.; Wu, Z.G.; Yan, H.C. Observer-based asynchronous control of discrete-time semi-Markov switching power systems under DoS attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2024**, *54*, 6424–6434. [CrossRef]
16. Lunze, J.; Lehmann, D. A state-feedback approach to event-based control. *Automatica* **2010**, *46*, 211–215. [CrossRef]

17. Zhang, J.H.; Feng, G. Event-driven observer-based output feedback control for linear systems. *Automatica* **2014**, *50*, 1852–1859. [CrossRef]
18. Yu, H.; Hao, F. Input-to-state stability of integral-based event-triggered control for linear plants. *Automatica* **2017**, *85*, 248–255. [CrossRef]
19. Heemels, W.P.M.H.; Donkers, M.C.F.; Teel, A.R. Periodic Event-triggered control for linear systems. *IEEE Trans. Autom. Control* **2013**, *58*, 847–861. [CrossRef]
20. Donkers, M.C.F.; Heemels, W.P.M.H. Model-based periodic event-triggered control for linear systems. *Automatica* **2013**, *49*, 698–711.
21. Riverso, S.; Sarzo, F.; Frerrari-Trecate, G. Plug-and-play voltage and frequency control of islanded microgrids with meshed topology. *IEEE Trans. Smart Grid* **2015**, *6*, 1176–1184. [CrossRef]
22. Strom, T. On logarithmic norm. *SIAM J. Numer. Anal.* **1975**, *12*, 741–753. [CrossRef]
23. Sun, Y.C.; Yao, L.N. Robust fault diagnosis and fault-tolerant control for non-Gaussian uncertain stochastic distribution control systems. *Int. J. Robust Nonlinear Control* **2017**, *27*, 1709–1725. [CrossRef]
24. Khalil, H.K. *Nonlinear Systems*; Prentice Hall: Saddle River, NJ, USA, 2002.