energies

MDPI

Article

Observer-Based H_∞ Load Frequency Control for Networked Power Systems with Limited Communications and Probabilistic Cyber Attacks

Yixuan Ge, Guobao Liu *, Guishu Zhao *, Huai Liu and Ji Sun

School of Electrical and Automation, Nanjing Normal University, Nanjing 210046, China;
gyx2521270528@163.com (Y.G.); liuhuai@njnu.edu.cn (H.L.); sunji@njnu.edu.cn (J.S.)
* Correspondence: lgb5566778@163.com (G.L.); gzhao@njnu.edu.cn (G.Z.)

Abstract: This paper studies load frequency control (LFC) for networked power systems with limited communications and probabilistic cyber attacks. Some restrictions exist during the information transmission, which can impair behavior and lead to instability of power systems. Throughout this paper, we consider such power systems that involve multi-path missing measurements and input–output time-varying delays as well as cyber attacks in the communication channels. A feedback controller is presented, which is based on the observer to implement H_∞ LFC for power systems with disturbance rejection level γ. By Lyapunov stability theory, adequate criteria are given to ensure the stable operation of power systems. Finally, the validity of theoretical analysis is demonstrated and illustrated by numerical simulations.

Keywords: LFC; networked power systems; observer; time-varying delays; multi-path missing measurements; cyber attacks

check for updates

Citation: Ge, Y.; Liu, G.; Zhao, G.; Liu, H.; Sun, J. Observer-Based H_∞ Load Frequency Control for Networked Power Systems with Limited Communications and Probabilistic Cyber Attacks. *Energies* **2022**, *15*, 4234. https://doi.org/10.3390/en15124234

Academic Editor: Djaffar Ould-Abdeslam

Received: 19 April 2022
Accepted: 7 June 2022
Published: 8 June 2022

1. Introduction

Load frequency control (LFC) is a scheme that can control the output power of generators set so that instantaneous frequency deviation in each region and the power exchange between regions are kept within the specified range, and their steady-state error is equal to zero [1,2]. Traditional LFC schemes transmit measurement signals and control signals with the help of a purpose-built communication infrastructure [3,4]. LFC in modern power systems mainly applies open communication facilities to transmit the above-mentioned signals. On account of the inherent properties of open communication, time-varying delays and packet dropout, as well as cyber attacks, are inevitable, seriously affecting the efficiency of load frequency control schemes [5,6]. The issue of the LFC of power systems with delays as well as packet dropout and cyber attacks have received extensive attention in recent years [7–11].

In the last few years, a good deal of results have been reported with regard to LFC problems of power systems containing packet dropout as well as time delays [6,12–15]. A novel decentralized LFC control strategy based on switching control theory was researched by Yang et al. By means of transmission delays as a switching decision parameter, the LFC system as a range of subsystems was modeled, which provides a more accurate description of the impact of delays as well as packet dropout on the system [6]. Zhang et al. proposed a delay-dependent robust method for the analysis of PID-based LFC schemes that take into account time delays [12]; however, for the problem of LFC in power systems, many researchers have only studied packet dropout or time delays in the output communication channels, ignoring the controller-to-actuator link [16]. Furthermore, to our knowledge, few researchers have investigated the LFC problem in power systems with delays as well as packet loss both in the controller-to-actuator link and output communication channels.

Along with the large-scale application of open communication networks in power systems, the matter of power system security has also attracted widespread attention from scholars. Cyber attacks can cause serious power incidents, especially if there are cyber attacks during data transmission [17]. Cyber attacks can be divided into denial of service attacks as well as deception attacks, of which, deception attacks pose the greatest threat to power systems. Deception attacks are attacks in which an attacker modifies the integrity of packets transmitted between different parts of the network in order to obtain critical information. A great deal of work is being undertaken in relation to deception attacks. Finite-time constrained and adaptive event-triggered control problems for networked systems involved in deception attacks were studied by Sathishkumar et al. [18]. Tian et al. submitted a memory-based event-triggered H_∞ LFC for power systems that involve deception attacks [19]. Adaptive event-triggered control of neural networks affected by double deception attacks and time-varying delays were researched by Shen et al. [20].

In addition, in order to control the system more efficiently, scholars adopt state feedback control; however, state variables cannot be measured directly from the system, which makes the implementation of state feedback techniques more complex than output feedback. Most previous work made the assumption that all system states are accessible. Tapin et al. presented a full-state feedback controller design for LFC loops based on the pole positioning method [21]. A state estimation was presented by Vrdoljak et al., which is based on rapid measurement output sampling with full state feedback [22]. Instead, only a fraction of the system state can be obtained in practice. Motivated by this point, many scholars are paying attention to state feedback control that is based on an observer. A means of quasi-decentralized LFC scheme of power systems that is based on a function observer was proposed by Tyrone et al. [23]. To realize a global state feedback controller, a new distributed function observer was designed by Thanh et al. [24]. It is notable that the problem of observer-based LFC in power systems that involve limited communications and probabilistic deception attacks have not yet been researched—this is the motivation behind our article.

The aim of this paper is to design an observer-based H_∞ LFC scheme for power systems with limited communications and probabilistic cyber attacks. Networked power systems with input and output delays and packet dropout as well as cyber attacks are considered in this article. The main contributions of this paper are given as follows:

(1) An observer-based LFC model is established for networked power systems, which not only takes into account multi-path missing measurements and input–output time-varying delays in the communication channel but also considers the influences of random cyber attacks on data transmission.

(2) To implement the H_∞ load frequency controller, delay-dependent H_∞ stability criterion including time delays and packet dropout as well as cyber attacks phenomena are derived with the help of Lyapunov–Krasovskii function approach in LMI framework.

(3) On the basis of the resulting stability criteria, the stability gains of the observer and controller are calculated with the assistance of the LMI toolbox.

Notations: The transpose of the matrix L is represented by L^T. X^{-1} represents its inverse matrix. The symmetric terms in the matrix are denoted by $*$. $\mathbb{R}^n$ denotes the n-dimensional Euclidean space. $\mathbb{R}^{n\times n}$ is $n \times n$ real matrices. The diagonal matrix is denoted by $diag\{\cdots\}$. Identity matrix is denoted by I. $\|\cdot\|_2$ denotes the usual $\ell_2[0,\infty)$ norm. $\mathbb{E}$ is the expectation operator. The probability when the stochastic variable x is equal to a is denoted by $Prob\{x = a\}$. The dimension of these vectors and matrices will be cleared in the context.

2. Model Description and Preliminaries

In this paper, the structure of the power system's LFC model is shown in Figure 1. The system model is represented as follows [25]:

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu(t) + Cw(t),\\ \tilde{y}(t) &= Dx(t),\end{aligned} \tag{1}$$

where

$$x(t) = \begin{bmatrix} \Delta f & \Delta P_m & \Delta P_v & \Delta P_e \end{bmatrix}^T, \quad \omega(t) = P_d, \quad y(t) = ACE(t),$$
$$D = \begin{bmatrix} \beta & 0 & 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 0 & \frac{\alpha_g}{T_g} & \frac{\alpha_e k_e}{T_e} \end{bmatrix}^T,$$
$$C = \begin{bmatrix} -\frac{1}{M} \\ 0 \\ 0 \\ 0 \end{bmatrix}, \qquad A = \begin{bmatrix} -\frac{D}{M} & \frac{1}{M} & 0 & \frac{1}{M} \\ 0 & -\frac{1}{T_{ch}} & \frac{1}{T_{ch}} & 0 \\ -\frac{1}{T_g R} & 0 & -\frac{1}{T_g} & 0 \\ 0 & 0 & 0 & -\frac{1}{T_e} \end{bmatrix}.$$

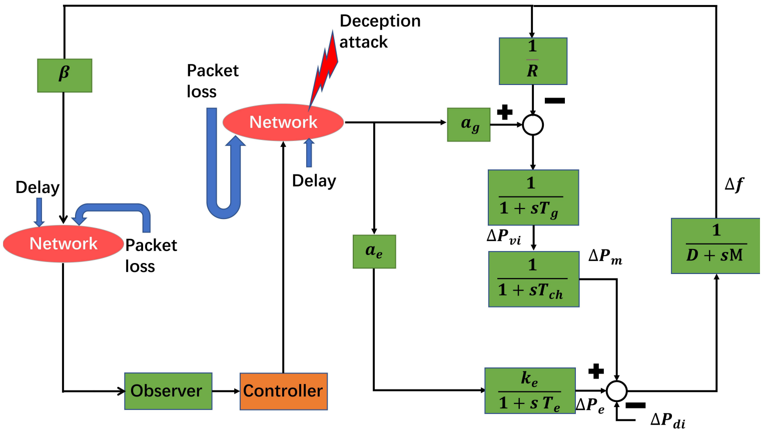

Figure 1. System LFC model including electric vehicles.

The parameters of the networked power systems, which are depicted in Figure 1, are listed in Table 1 [4,25].

Table 1. Networked power systems parameters and their names.

Symbol	Name
Δf	the deviations of frequency
ΔP_m	the deviations of generation mechanical output
ΔP_v	the deviations of valve position
ΔP_d	the deviations of load
ΔP_e	the deviations of electric vehicles output power
$ACE(t)$	area control error
M	the moment of inertia of the generator
D	the generator damping coefficient
T_g	the time constant of the governor
T_{ch}	the time constant of the turbine
T_e	the time constant of the electric vehicles
R	the speed drop
α_g	turbine proportionality factor
α_e	electric vehicles proportionality factor
β	the frequency bias factor
k_e	electric vehicles gain factor

As shown in Figure 2, considering the sudden changes in the operating environment as well as the jamming of the communication channels, the output communication channels are considered to be limited, that is, the output signal $\tilde{y}(t)$ suffer from data missing $\alpha(t)$ and time-varying delays $\vartheta(t)$; therefore, the output signal will be described as

$$y(t) = \alpha(t)\tilde{y}(t - \vartheta(t)), \tag{2}$$

time-varying delays that exist in the communication channels $\vartheta(t)$ satisfy

$$0 \leq \vartheta(t) \leq \vartheta_M, \quad \dot{\vartheta}(t) \leq \mu < \infty, \tag{3}$$

where ϑ_M and μ are some given constants.

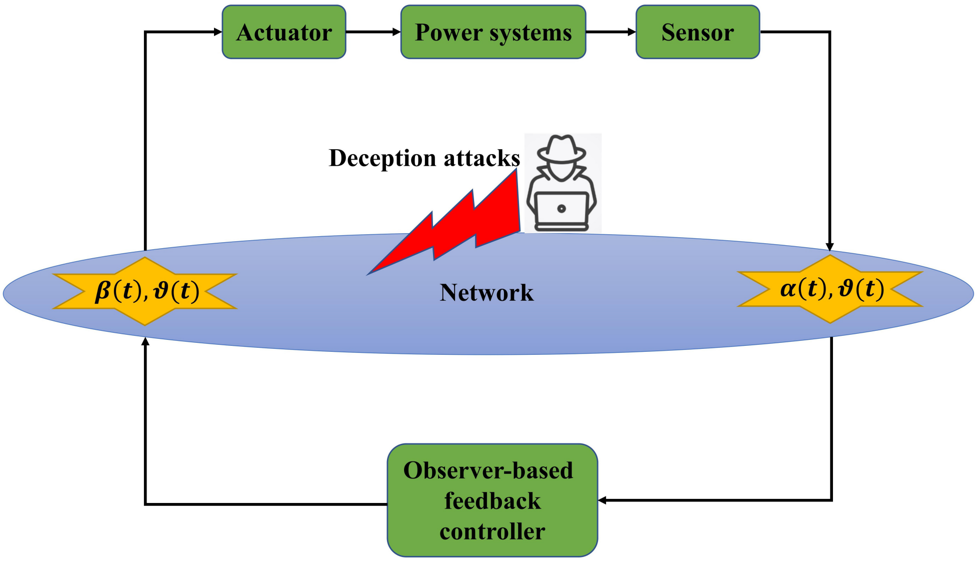

Figure 2. Structure of networked power systems with limited communications and cyber attacks.

Remark 1. *That packet loss from the sensor to the controller in a networked control system (1) is expressed as $\alpha(t)$, which is a Bernoulli stochastic variable. In particular, if the link fails, we have $\alpha(t) = 0$, otherwise $\alpha(t) = 1$ if the data are successfully transmitted.*

Moreover, we assume that

$$Prof\{\alpha(t) = \hbar\} = \begin{cases} \alpha, & \hbar = 1, \\ 1 - \alpha, & \hbar = 0. \end{cases}$$

From the above analysis, we have the following networked power systems involving time-varying delays as well as missing output data measurements

$$\begin{aligned} \dot{x}(t) =& Ax(t) + Bu(t) + Cw(t), \\ y(t) =& \alpha(t)(Dx(t - \vartheta(t))). \end{aligned} \tag{4}$$

We study the robustness of the networked power systems (4) by designing a feedback controller, which is based on an observer. Consider a controller with input missing measurements $\beta(t)$ and time-varying delays $\vartheta(t)$. Suppose that the deception attack restricted in Hypothesis 1 is performed as a nonlinear function $f(x(t - \vartheta(t)))$.

$$\begin{aligned} \dot{\hat{x}}(t) =& A\hat{x}(t) + Bu(t) + L[y(t) - \alpha(t)D\hat{x}(t - \vartheta(t))], \\ u(t) =& (1 - \theta(t))\beta(t)K\hat{x}(t - \vartheta(t)) + \theta(t)Kf(x(t - \vartheta(t))), \end{aligned} \tag{5}$$

where $\hat{x}(t) \in \mathbb{R}^n$ is the state vector, L and K are the estimated gain and the control gain to be designed, respectively. Furthermore, we assume that

$$Prof\{\beta(t) = \tau\} = \begin{cases} \beta, & \tau = 1, \\ 1 - \beta, & \tau = 0. \end{cases}$$

$$Prof\{\theta(t)=\iota\} = \begin{cases} \theta, & \iota = 1, \\ 1-\theta, & \iota = 0. \end{cases}$$

Remark 2. *Similar to the variable $\alpha(t)$, $\beta(t)$ is another Bernoulli stochastic variable representing the packet loss from the controller (5) to the actuator. In addition, we have $\beta(t)=1$ if controller (5) is enabled and on the other hand, $\beta(t)=0$ if controller is not enabled.*

Remark 3. *The Bernoulli random variable $\theta(t)$ is made to characterize the random deception attack. $\theta(t)=1$ means the attack occurred, otherwise, the data are carried as normal.*

Denote $\tilde{\alpha}(t)=\alpha(t)-\alpha$, $\tilde{\beta}(t)=\beta(t)-\beta$, $\tilde{\theta}(t)=\theta(t)-\theta$, $\alpha(1-\alpha)\triangleq\alpha_0^2$, $\beta(1-\beta)\triangleq\beta_0^2$, $\theta(1-\theta)\triangleq\theta_0^2$. Above all, we obtain the following networked power systems with considering the input and output limited communications

$$\begin{aligned}\dot{x}(t)=&Ax(t)+B((1-\theta(t))\beta(t)K\hat{x}(t-\vartheta(t))+\theta(t)Kf(x(t-\vartheta(t))))+Cw(t)\\ =&Ax(t)+(1-\theta)\beta BK(x(t-\vartheta(t))-e(t-\vartheta(t)))+\theta(t)BKf(x(t-\vartheta(t)))\\ &+(\beta(t)-\beta)(1-\theta)BK(x(t-\vartheta(t))-e(t-\vartheta(t)))\\ &-(\theta(t)-\theta)(\beta BK(x(t-\vartheta(t))-e(t-\vartheta(t)))-BKf(x(t-\vartheta(t))))\\ &-(\theta(t)-\theta)(\beta(t)-\beta)(BK(x(t-\vartheta(t))-e(t-\vartheta(t)))+C\omega(t).\end{aligned} \tag{6}$$

$$\begin{aligned}\dot{\hat{x}}(t)&=A\hat{x}(t)+Bu(t)+L[y(t)-\alpha(t)D\hat{x}(t-\vartheta(t))]\\ &=A\hat{x}(t)+Bu(t)+\alpha(t)LDe(t-\vartheta(t)).\end{aligned} \tag{7}$$

Letting the error vector be $e(t)=x(t)-\hat{x}(t)$, combining the system (6) and the observer-based feedback controller (7), the error system can be represented as

$$\begin{aligned}\dot{e}(t)=&\dot{x}(t)-\dot{\hat{x}}(t)\\ =&Ax(t)+Bu(t)+Cw(t)\\ &-[A\hat{x}(t)+Bu(t)+\alpha(t)LDe(t-\vartheta(t))]\\ =&Ae(t)-\alpha LDe(t-\vartheta(t))+Cw(t)\\ &-(\alpha(t)-\alpha)LDe(k-\vartheta(t)).\end{aligned} \tag{8}$$

According to the above definition for the stochastic variables, we have

$$\begin{aligned}&\mathbb{E}\{\tilde{\alpha}(t)\}=0, \quad \mathbb{E}\{\tilde{\beta}(t)\}=0, \quad \mathbb{E}\{\tilde{\theta}(t)\}=0, \quad \mathbb{E}\{\tilde{\alpha}^2(t)\}=\alpha_0^2, \quad \mathbb{E}\{\tilde{\beta}^2(t)\}=\beta_0^2,\\ &\mathbb{E}\{\tilde{\theta}^2(t)\}=\beta_0^2, \qquad \mathbb{E}\{\tilde{\alpha}(t)\tilde{\beta}(t)\}=0, \quad \mathbb{E}\{\tilde{\alpha}(t)\tilde{\theta}(t)\}=0, \qquad \mathbb{E}\{\tilde{\beta}(t)\tilde{\theta}(t)\}=0.\end{aligned}$$

Furthermore, defining $\zeta(t)=[x^T(t),e^T(t)]^T$, according to (6) and (8) the networked control system is described as

$$\begin{aligned}\zeta(t)=&\varphi_1(t)+(\beta(t)-\beta)\varphi_2(t)-(\theta(t)-\theta)\varphi_3(t)\\ &-(\theta(t)-\theta)(\beta(t)-\beta)\varphi_4(t)-(\alpha(t)-\alpha)\varphi_5(t),\\ y(t)=&\alpha(t)Dx(t-\vartheta(t)),\end{aligned} \tag{9}$$

where

$$\begin{aligned}&\varphi_1(t)=A_0\zeta(t)+A_1\zeta(t-\vartheta(t))+A_2w(t)+A_3,\\ &\varphi_2(t)=A_4\zeta(t-\vartheta(t)), \quad \varphi_3(t)=A_5\zeta(t-\vartheta(t))-A_6,\\ &\varphi_4(t)=A_7\zeta(t-\vartheta(t)), \qquad \varphi_5(t)=A_8\zeta(t-\vartheta(t)),\end{aligned} \tag{10}$$

and

$$A_0 = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}, \quad A_1 = \begin{bmatrix} (1-\theta)\beta BK & -(1-\theta)\beta BK \\ 0 & 0 \end{bmatrix},$$
$$A_2 = \begin{bmatrix} C \\ C \end{bmatrix}, \qquad A_3 = \begin{bmatrix} \theta BKf(x(t-\vartheta(t))) \\ 0 \end{bmatrix},$$
$$A_4 = \begin{bmatrix} (1-\theta)BK & -(1-\theta)BK \\ 0 & 0 \end{bmatrix}, \quad A_5 = \begin{bmatrix} \beta BK & -\beta BK \\ 0 & 0 \end{bmatrix},$$
$$A_6 = \begin{bmatrix} BKf(x(t-\vartheta(t))) \\ 0 \end{bmatrix}, A_7 = \begin{bmatrix} BK & -BK \\ 0 & 0 \end{bmatrix}, A_8 = \begin{bmatrix} 0 & 0 \\ 0 & LD \end{bmatrix}.$$

Next, we present some definitions that are necessary to derive the final results.

Definition 1 ([26])**.** *System (9) is mean square asymptotically stable, for* $\forall\varsigma > 0$*, if* $\exists\chi(\varsigma) > 0$ *such that when the initial value* $\psi(t)$ *satisfies* $sup_{-\vartheta_M<t\le 0}\mathbb{E}\{\|\psi(t)\|^2\} < \chi(t)$*, the solution* $\zeta(t)$ *of the system (9) satisfies* $\mathbb{E}\{\|\zeta(t)\|^2\} < \varsigma$*,* $t > 0$ *and* $lim_{t\to\infty}\mathbb{E}\{\|\zeta(t)\|^2\} = 0$*.*

Definition 2 ([27])**.** *If, for any initial conditions, there satisfies the limitation for a given scalar* $\gamma > 0$*, system (9) is said to be stabilization with H*$_\infty$*performance if two conditions below are met.*

(1) The closed-loop system is mean square asymptotically stable with $\omega(t) = 0$*.*

(2) For any nonzero $w(t) \in \ell_2[0,\infty)$ *as well as a prescribed indicators* γ*, the below inequality holds*

$$\| y(t) \|_2 \le \gamma \| w(t) \|_2 . \tag{11}$$

Hypothesis 1 ([28])**.** *Stochastically occurring deception attacks* $f(x(t-\vartheta(t)))$ *meets*

$$f^T(x(t-\vartheta(t)))f(x(t-\vartheta(t))) < x^T(t-\vartheta(t))H^T Hx(t-\vartheta(t)), \tag{12}$$

where H is a matrix of known constants that represents the upper boundary of non-linearity.

Lemma 1 ([29])**.** *For a given full rank matrix D, if some matrices P, K, Y of suitable dimensions exist, satisfying PBK = BY. Then, the matrix K can be derived from the following equation*

$$K = (B^T PB)^{-1} B^T BY. \tag{13}$$

3. Results

From the definition of mean square asymptotic stability, in this section, we discuss the stability and H_∞ performance of the system (9). Then, with some reasonable matrix processing, an observer-based feedback controller is designed with the presence of deception attacks as well as packet loss.

3.1. Stability and H$_\infty$ Performance Analysis

Theorem 1. *For the networked control systems (6) and the error systems (8), if there exist positive definite matrices* P_i*,* Q_i*,* R_i*,* S_i *(i = 1, 2), and W such that*

$$\Pi = \begin{bmatrix} \Xi & * \\ \Phi & \Lambda \end{bmatrix} < 0, \tag{14}$$

$$\begin{bmatrix} R & * \\ W & R \end{bmatrix} > 0, \tag{15}$$

where

$$\Xi = \begin{bmatrix} \Xi_{11} & * & * & * & * & * & * & * \\ 0 & \Xi_{22} & * & * & * & * & * & * \\ \Xi_{31} & -W_2 & \Xi_{33} & * & * & * & * & * \\ \Xi_{41} & \Xi_{42} & 2W_2^T & \Xi_{44} & * & * & * & * \\ W_1 & W_2^T & R_1 - W_1 & -W_2 & -Q_1 - R_1 & * & * & * \\ W_2 & W_3 & -W_2^T & R_2 - W_3 & 0 & -Q_2 - R_2 & * & * \\ \theta(P_1BK)^T & 0 & 0 & 0 & 0 & 0 & -\theta I & * \\ C^TP_1 & C^TP_2 & 0 & 0 & 0 & 0 & 0 & -\gamma I \end{bmatrix},$$

$$\Phi = \begin{bmatrix} \tau_M P_1 A & 0 & \phi_{13} & \phi_{14} & 0 & 0 & \phi_{17} & \tau_M P_1 C \\ 0 & \tau_M P_2 A & 0 & \phi_{24} & 0 & 0 & 0 & \tau_M P_2 C \\ 0 & 0 & \phi_{33} & \phi_{34} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \phi_{53} & \phi_{54} & 0 & 0 & \phi_{57} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \phi_{73} & \phi_{74} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \phi_{93} & \phi_{94} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \phi_{10,4} & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{aligned} &\Xi_{11} = A^TP_1 + P_1A + Q_1 + S_1 - R_1, \quad \Xi_{22} = A^TP_2 + P_2A + Q_2 + S_2 - R_2, \\ &\Xi_{33} = (\mu - 1)S_1 - 2R_1 + W_1 + W_1^T + \alpha D^TD + \theta H^TH, \\ &\Xi_{31} = (1-\theta)\beta(P_1BK)^T + R_1 - W_1, \quad \Xi_{41} = -(1-\theta)\beta(P_1BK)^T - W_2^T, \\ &\Xi_{42} = -\alpha(P_2LD)^T + W_2 - R_3, \quad \Xi_{44} = (\mu - 1)S_2 - 2R_2 + W_3 + W_3^T, \\ &\phi_{13} = \tau_M(1-\theta)\beta P_1BK, \qquad \phi_{14} = -\tau_M(1-\theta)\beta P_1BK, \quad \phi 17 = \tau_M\theta P_1BK, \\ &\phi_{24} = -\tau_M\alpha P_2LD, \quad \phi_{33} = \tau_M\beta_0(1-\theta)P_1BK, \quad \phi_{34} = -\tau_M\beta_0(1-\theta)P_1BK, \\ &\phi_{53} = \tau_M\theta_0\beta P_1BK, \quad \phi_{54} = -\tau_M\theta_0\beta P_1BK, \quad \phi_{57} = -\tau_M\theta_0P_1BK, \\ &\phi_{73} = \tau_M\theta_0\beta_0P_1BK, \quad \phi_{74} = -\tau_M\theta_0\beta_0P_1BK, \quad \phi_{10,4} = \tau_M\alpha_0P_2LD, \\ &P = diag\{P_1, P_2\}, \quad Q = diag\{Q_1, Q_2\}, \quad R = diag\{R_1, R_2\}, \quad S = diag\{S_1, S_2\}, \\ &W = \begin{bmatrix} W_1 & W_2 \\ * & W_3 \end{bmatrix}, \Lambda = diag\{-PR^{-1}P, -PR^{-1}P, -PR^{-1}P, -PR^{-1}P, -PR^{-1}P\}, \end{aligned}$$

then, the system (9) is mean square asymptotically stable. That is, the networked power systems (4) with limited communications could be mean square asymptotic stable by applying the controller (5), which also has limited communications.

Proof. Select the Lyapunov function as $V(t) = V_1(t) + V_2(t) + V_3(t)$, where

$$\begin{aligned} V_1(t) &= \zeta^T(t)P\zeta(t), \\ V_2(t) &= \int_{t-\vartheta_M}^{t} \zeta^T(s)Q\zeta(s)ds + \int_{t-\vartheta(t)}^{t} \zeta^T(s)S\zeta(s)ds, \\ V_3(t) &= \vartheta_M \int_{t-\vartheta_M}^{t}\int_{s}^{t} \dot{\zeta}(v)R\dot{\zeta}(v)dvds. \end{aligned} \tag{16}$$

Taking the derivative with respect to $V(t)$, we can acquire

$$\mathbb{E}\{\dot{V}_1(t)\} = 2(A_0\zeta(t) + A_1\zeta(t-\vartheta(t)) + A_2\omega(t) + A_3)^TP\zeta(t), \tag{17}$$

$$\begin{aligned}\mathbb{E}\{\dot{V}_2(t)\} =&\zeta^T(t)Q\zeta(t)-\zeta^T(t-\vartheta_M)Q\zeta(t-\vartheta_M)\\ &+\zeta^T(t)Q\zeta(t)-(1-\mu)\zeta^T(t-\vartheta(t))Q\zeta(t-\vartheta(t)),\end{aligned} \tag{18}$$

$$\mathbb{E}\{\dot{V}_3(t)\} =\mathbb{E}\{\tau_M^2\dot{\zeta}^T(t)R\dot{\zeta}(t)\}-\tau_M\int_{t-\tau_M}^{t}\dot{\zeta}^T(v)R\dot{\zeta}(v)dv, \tag{19}$$

$$\begin{aligned}\mathbb{E}\{\dot{\zeta}(t)R\dot{\zeta}(t)\} =&\varphi_1^T(t)R\varphi_1(t)+\beta_0^2\varphi_2^T(t)R\varphi_2(t)+\theta_0^2\varphi_3^T(t)R\varphi_3(t)\\ &+\theta_0^2\beta_0^2\varphi_4^T(t)R\varphi_4(t)+\alpha_0^2\varphi_5^T(t)R\varphi_5(t)\\ =&(A_0\zeta(t)+A_1\zeta(t-\vartheta(t))+A_2\omega(t)+A_3)^TR(A_0\zeta(t)\\ &+A_1\zeta(t-\vartheta(t))+A_2\omega(t)+A_3)\\ &+\beta_0^2(A_4\zeta(t-\vartheta(t)))^TR(A_4\zeta(t-\vartheta(t)))\\ &+\theta_0^2(A_5\zeta(t-\vartheta(t))-A_6)^TR(A_5\zeta(t-\vartheta(t))-A_6)\\ &+\theta_0^2\beta_0^2(A_7\zeta(t-\vartheta(t)))^TR(A_7\zeta(t-\vartheta(t)))\\ &+\alpha_0^2(A_8\zeta(t-\vartheta(t)))^TR(A_8\zeta(t-\vartheta(t))).\end{aligned} \tag{20}$$

With the help of the reciprocally convex approach [30], if (15) is satisfied, we acquire

$$\begin{aligned}&-\vartheta_M\int_{t-\vartheta_M}^{t}\dot{\zeta}^T(\vartheta)R\dot{\zeta}(\vartheta)d\vartheta\\ \leq&\begin{bmatrix}\zeta(t)\\ \zeta(t-\vartheta(t))\\ \zeta(t-\vartheta_M)\end{bmatrix}\begin{bmatrix}-R & R-W^T & W^T\\ R-W & -2R+W+W^T & R-W^T\\ W & R-W & -R\end{bmatrix}\begin{bmatrix}\zeta(t)\\ \zeta(t-\vartheta(t))\\ \zeta(t-\vartheta_M)\end{bmatrix}.\end{aligned} \tag{21}$$

According to Hypothesis 1, we have

$$\theta x^T(t-\vartheta(t))H^THx(t-\vartheta(t))-\theta f^T(x(t-\vartheta(t)))f(x(t-\vartheta(t)))>0. \tag{22}$$

From (17)–(22) we are able to attain that

$$\mathbb{E}\{\dot{V}(t)\}+y^T(t)y(t)-\gamma^2w^T(t)w(t)\leq\varpi^T(t)[\Xi-\Phi^T\Lambda^1\Phi]\varpi(t), \tag{23}$$

where $\varpi(t)$=

$$col\begin{bmatrix} x(t) & e(t) & x(t-\vartheta(t)) & e(t-\vartheta(t)) & x(t-\vartheta_M) & e(t-\vartheta_M) & fx(t-\vartheta(t)) & \omega(t)\end{bmatrix}.$$

With the aid of the Schur complement, one can acquire from (14) that $\Xi-\Phi^T\Lambda^1\Phi<0$, then we obtain

$$y^T(t)y(t)-\gamma^2w^T(t)w(t)\leq-\mathbb{E}\{\dot{V}(t)\}. \tag{24}$$

From the inequality (14) and (24), for $\omega(t)=0$, there exists a scalar $\lambda>0$ such that the following inequality holds

$$\mathbb{E}\{\dot{V}(t)\}\leq-\lambda\mathbb{E}\{\|\zeta(t)\|^2\}<0.$$

Further, because $V(t)>0$, from which we obtain

$$lim_{t\rightarrow\infty}\mathbb{E}\{\|\zeta(t)\|^2\}=0.$$

From Definition 1, we obtain that the system (9) is mean square asymptotically stable. When $\omega(t)\neq0$, integrating both side of (24) from 0 to $+\infty$, it follows that

$$\int_0^{+\infty}(y^T(t)y(t)-\gamma^2w^T(t)w(t))dt\leq V(0)-V(+\infty).$$

Under zero initial condition, we obtain

$$\|y(t)\|_2 \leq \gamma \|w(t)\|_2.$$

From which we obtain that the system (9) is mean square asymptotically stable with H_∞ performance. This completes the proof. □

Remark 4. *Actually, observed-based feedback control is an efficient way to maintain system stability. In previous related works [31–34], control methods that are based on observers are used to maintain the security of cyber power systems. Even though authors considered the communication delays or missing measurements, only input or output situations in communication channel were discussed. We know that communication channel limitations, including packet dropout as well as delays, exist not only in the output communication channels, but also in the communication channels from the controller to the actuator.*

3.2. The Observer-Based Feedback Controller Design

In this section, the load frequency controller (5) for the power systems (4) is presented. It could be found in the condition that the matrix inequality (14) is not feasible because of the existence of the nonlinear matrices P_1BK and P_2LD. To address this issue, by using Lemma 1, gain matrices L and K in the controller (5) are obtained.

Theorem 2. *Consider the networked power systems (9). For the H_∞ performance level γ, if there exist matrices $P_i > 0$, $Q_i > 0$, $R_i > 0$, $S_i > 0$ (i = 1, 2) and W, Y, G such that the following conditions hold*

$$\hat{\Pi} = \begin{bmatrix} \hat{\Xi} & * \\ \hat{\Phi} & \hat{\Lambda} \end{bmatrix} < 0, \tag{25}$$

$$\begin{bmatrix} R & * \\ W & R \end{bmatrix} > 0, \tag{26}$$

where

$$\hat{\Xi} = \begin{bmatrix} \hat{\Xi}_{11} & * & * & * & * & * & * & * \\ 0 & \hat{\Xi}_{22} & * & * & * & * & * & * \\ \hat{\Xi}_{31} & -W_2 & \hat{\Xi}_{33} & * & * & * & * & * \\ \hat{\Xi}_{41} & \hat{\Xi}_{42} & 2W_2^T & \hat{\Xi}_{44} & * & * & * & * \\ W_1 & W_2^T & R_1 - W_1 & -W_2 & -Q_1 - R_1 & * & * & * \\ W_2 & W_3 & -W_2^T & R_2 - W_3 & 0 & -Q_2 - R_2 & * & * \\ \theta(BY)^T & 0 & 0 & 0 & 0 & 0 & -\theta I & * \\ C^T P_1 & C^T P_2 & 0 & 0 & 0 & 0 & 0 & -\gamma I \end{bmatrix},$$

$$\hat{\Phi} = \begin{bmatrix} \tau_M P_1 A & 0 & \hat{\phi}_{13} & \hat{\phi}_{14} & 0 & 0 & \hat{\phi}_{17} & \tau_M P_1 C \\ 0 & \tau_M P_2 A & 0 & \hat{\phi}_{24} & 0 & 0 & 0 & \tau_M P_2 C \\ 0 & 0 & \hat{\phi}_{33} & \hat{\phi}_{34} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \hat{\phi}_{53} & \hat{\phi}_{54} & 0 & 0 & \hat{\phi}_{57} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \hat{\phi}_{73} & \hat{\phi}_{74} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \hat{\phi}_{93} & \hat{\phi}_{94} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \hat{\phi}_{10,4} & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$
\begin{aligned}
&\hat{\Xi}_{11} = A^T P_1 + P_1 A + Q_1 + S_1 - R_1, \qquad \hat{\Xi}_{22} = A^T P_2 + P_2 A + Q_2 + S_2 - R_2,\\
&\hat{\Xi}_{31} = (1-\theta)\beta(BY)^T + R_1 - W_1, \quad \hat{\Xi}_{33} = (\mu-1)S_1 - 2R_1 + W_1 + W_1^T + \alpha D^T D + \theta H^T H,\\
&\hat{\Xi}_{41} = -(1-\theta)\beta(BY)^T - W_2^T, \qquad \hat{\Xi}_{42} = -\alpha(GD)^T + W_2 - R_3,\\
&\hat{\Xi}_{44} = (\mu-1)S_2 - 2R_2 + W_3 + W_3^T, \quad \hat{\phi}_{13} = \tau_M(1-\theta)\beta BY, \quad \hat{\phi}_{14} = -\tau_M(1-\theta)\beta BY,\\
&\hat{\phi}_{17} = \tau_M \theta BY, \quad \hat{\phi}_{24} = -\tau_M \alpha GD, \quad \hat{\phi}_{33} = \tau_M \beta_0 (1-\theta) BY, \quad \hat{\phi}_{34} = -\tau_M \beta_0 (1-\theta) BY,\\
&\hat{\phi}_{53} = \tau_M \theta_0 \beta BY, \quad \hat{\phi}_{54} = -\tau_M \theta_0 \beta BY, \quad \hat{\phi}_{57} = -\tau_M \theta_0 BY, \quad \hat{\phi}_{73} = \tau_M \theta_0 \beta_0 BY,\\
&\hat{\phi}_{74} = -\tau_M \theta_0 \beta_0 BY, \quad \hat{\phi}_{10,4} = \tau_M \hat{\alpha}_0 GD, \quad P = diag\{P_1, P_2\}, \quad Q = diag\{Q_1, Q_2\},\\
&R = diag\{R_1, R_2\}, \qquad S = diag\{S_1, S_2\}, \qquad W = \begin{bmatrix} W_1 & W_2 \\ * & W_3 \end{bmatrix},\\
&\hat{\Lambda} = diag\{-2\kappa P + \kappa^2 R, -2\kappa P + \kappa^2 R, -2\kappa P + \kappa^2 R, -2\kappa P + \kappa^2 R, -2\kappa P + \kappa^2 R\}.
\end{aligned}
$$

In addition, K and L can be draw by

$$K = (B^T P_1 B)^{-1} B^T BY, \quad L = P_2^{-1} G. \tag{27}$$

Proof ([29])**.** For any matrix $R > 0$, $P > 0$ and scalar κ, from

$$(R - \kappa^{-1} P) R^{-1} (R - \kappa^{-1} P) \geq 0,$$

it can be seen that

$$-PR^{-1}P \leq -2\kappa P + \kappa^2 R.$$

Using $-2\kappa P + \kappa^2 R$ to replace $-PR^{-1}P$ of Λ in Theorem 1, we obtain

$$\hat{\Lambda} = diag\{-2\kappa P + \kappa^2 R, -2\kappa P + \kappa^2 R, -2\kappa P + \kappa^2 R, -2\kappa P + \kappa^2 R, -2\kappa P + \kappa^2 R\}.$$

Next, we linearize the nonlinear terms $P_1 BK$ as well as $P_2 LD$ in (14):

(1) By Lemma 1, To address nonlinear term $P_1 BK$, Let $P_1 BK = BY$.

(2) To address the nonlinear term $P_2 LD$, let $P_2 LD = GD$.
From the above transformation, matrix inequality (14) can be translated into the typical LMI. This completes the proof.

□

Remark 5. *Compared to past associated studies, the main challenge in controller design is to handle the nonlinear terms $P_1 BK$ and $P_2 LD$. We make $P_1 BK = BY$ and $P_2 LD = GD$ by introducing matrices Y and G of suitable dimensions. To ensure the H_∞ performance of cyber power systems, we give normal LMI conditions to design the observer-based feedback controller (9), which can be addressed by the LMI control toolbox.*

4. A Case Study

In the part, we show that the theoretical results achieved can be used to solve the LFC problem for power systems with multi-path missing measurements and input–output time-varying delays as well as cyber attacks in the communication channels with the help of an example. Table 2 shows the parameter values for system (9).

Table 2. Power Systems Parameters for LFC [25].

T_{ch}	T_g	R	D	M	β	T_e	k_e	α_g	α_e
0.3	0.1	0.05	1	10	0.4	1	1	0.9	0.1

Let the probability of the three Bernoulli stochastic variables as $\alpha = 0.9$, $\beta = 0.9$, and $\theta = 0.1$. Time delays are set as $\vartheta(t) = 0.1 + 0.1\sin(t)$, H_∞ performance index is set as $\gamma = 7$, and the noise signal is selected as $w(t) = \frac{0.1\sin(4\pi t)}{1+t^2}(\varepsilon(t) - \varepsilon(t-5))$. Next, using Algorithm 1, the controller gains matrix K and observer gains matrix L, and can be solved as follows:

$$K = \begin{bmatrix} 0.0391 & 0.0038 & -0.0032 & 0.0224 \end{bmatrix},$$

$$L = \begin{bmatrix} 2.1054 & -0.2981 & -0.4177 & 0.0568 \end{bmatrix}^T.$$

Algorithm 1: Load frequency controller and observer design for networked power systems

```
Require: $T_{ch}$ , $T_g$, R, D, M, $\beta$, $T_e$, $k_e$, $\mathbb{E}\{\alpha(t)\}$, $\mathbb{E}\{\beta(t)\}$, $\mathbb{E}\{\theta(t)\}$, $\alpha_g$ , $\alpha_e$, $\vartheta_M$, $\kappa$ and $\mu$
Ensure: The given parameters are reasonable in describing multi-area power systems
1: Computing the matrices A, B,C and D in system Figure 1 using the input parameters.
2: Solving linear matrix inequalities (25) and (26) in theorem 2 using LMI toolbox.
3: Obtaining matrices $P_1, P_2, G$ and $Y$.
4: Calculating $K = (B^T P_1 B)^{-1} B^T BY$; return K;
5: Calculating $L = P_2^{-1} G$; return L;
```

Suppose that cyber attacks signal $f(x(t-\vartheta(t))) = tanh(0.05x(t-\vartheta(t)))$, then it is easy to see that H = 0.05 satisfies Hypothesis 1. For the sake of simulation, the initial conditions for the state is selected as $x(0) = \begin{bmatrix} -0.4 & 0.1 & -0.2 & 0.5 \end{bmatrix}^T$ and the sampling period is set by 0.01 s and the simulation time is set to 15 s. Figure 3 depicts the Bernoulli distribution for the case of random variables $\alpha(t)$, $\beta(t)$, and $\theta(t)$ with expectation α = 0.9, β = 0.9, and θ = 0.1. The $\alpha = 0.9, \beta = 0.9$, and $\theta = 0.1$ in Figure 3 indicate that 10 percent of the packets from the sensor to the controller are lost, 10 percent of control input packets are lost in the communication network from the controller to the actuator, and the probability of a deception attack in the communication network is 10 percent. Frequency deviation curves of the system and the observer are shown in Figure 4 when the system is subject to packet loss and spoofing attacks. From Figure 4, it can be concluded that the frequency deviation in the power system tends to zero at around 11 s, proving the effectiveness of the designed controller. Figure 5 shows the error between the system frequency deviation and the frequency deviation observed by the observer. Combining Figures 4 and 5, we can see not only that the observer can observe the frequency deviation of the system very well but also that the error between the system frequency deviation and the observed frequency deviation of the observer tends to zero at around 8 s, demonstrating the good observational performance of the designed observer.

Figures 6–9 show all state trajectory, all state observation trajectory, systems error trajectory, and the control trajectory of the one-area power system. It is clear from Figures 6 and 7 that system (9) reaches mean square asymptotic stability within 12 s by designing controller (5). We can see that the error between the system state and the observed state of the observer converges to zero around 8 s from Figure 8, which proves that the designed observer (7) is capable of observing the actual value effectively. The control signal u(t) is shown in Figure 9. The disturbance signal is depicted in Figure 10. Figure 11 depicts the response curve of the network attack signal $f(x(t-\vartheta(t)))$. The results show that the presented LFC strategy is able to keep the stability of power systems in the presence of multipath missing measurements and input–output time-varying delays as well as cyber attacks on the communication channels.

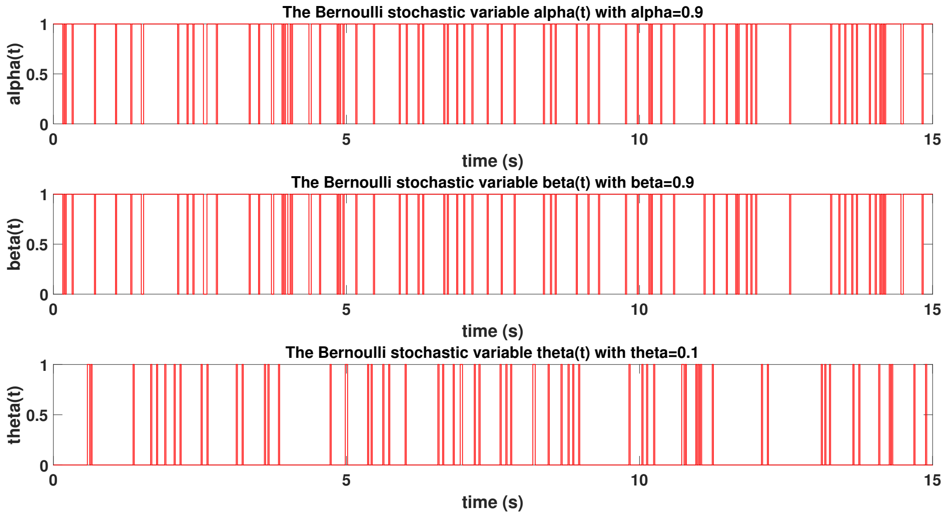

Figure 3. The evolution of the Bernoulli stochastic variables with $\alpha = 0.9$, $\beta = 0.9$, and $\theta = 0.1$.

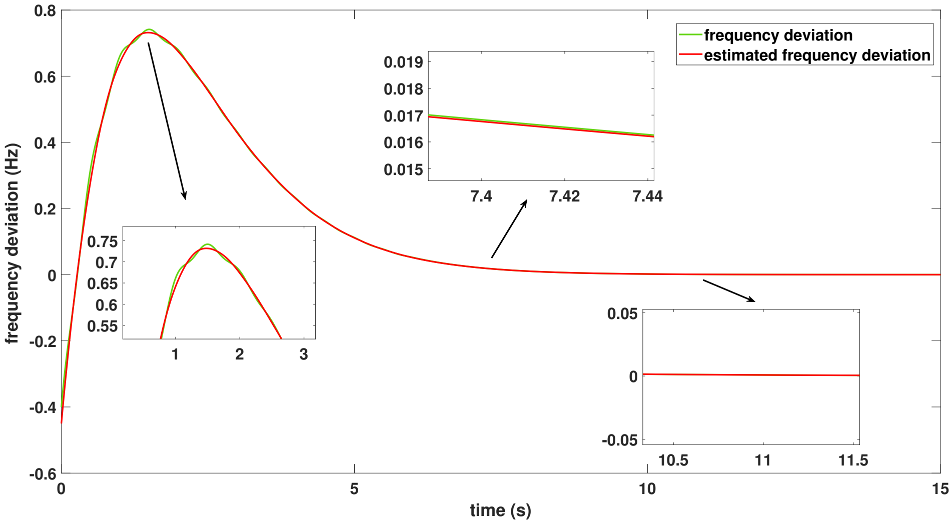

Figure 4. Frequency deviation Δf and estimated frequency deviation $\hat{\Delta} f$.

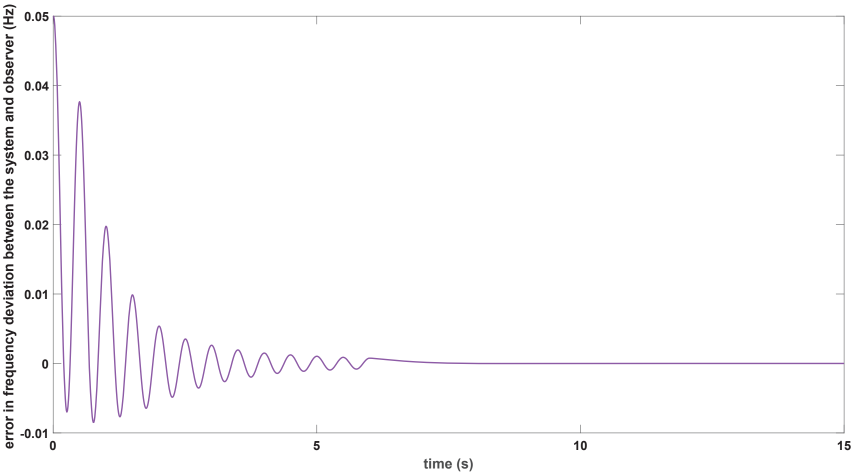

Figure 5. Error in frequency deviation between the system and observer.

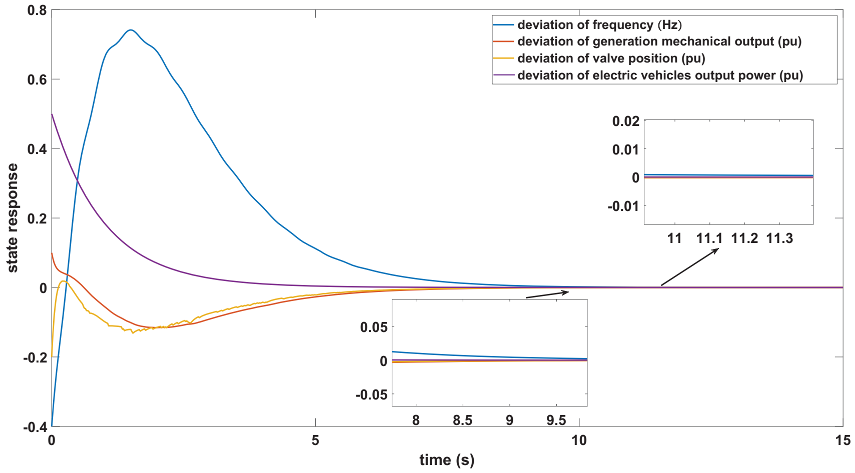

Figure 6. State trajectory of one-area power system.

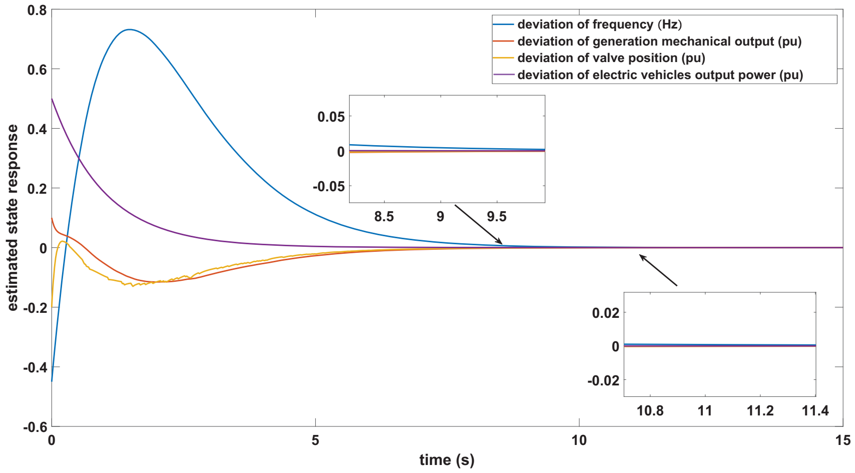

Figure 7. Observation trajectory of one-area power system.

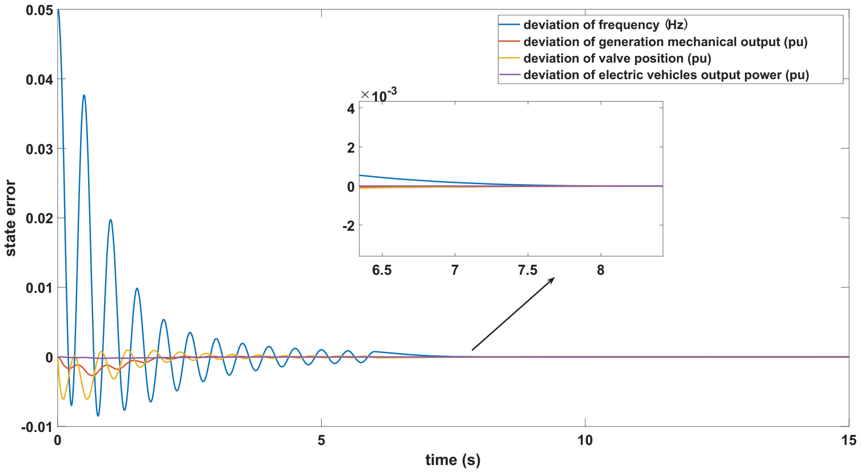

Figure 8. Error trajectory of one-area power system.

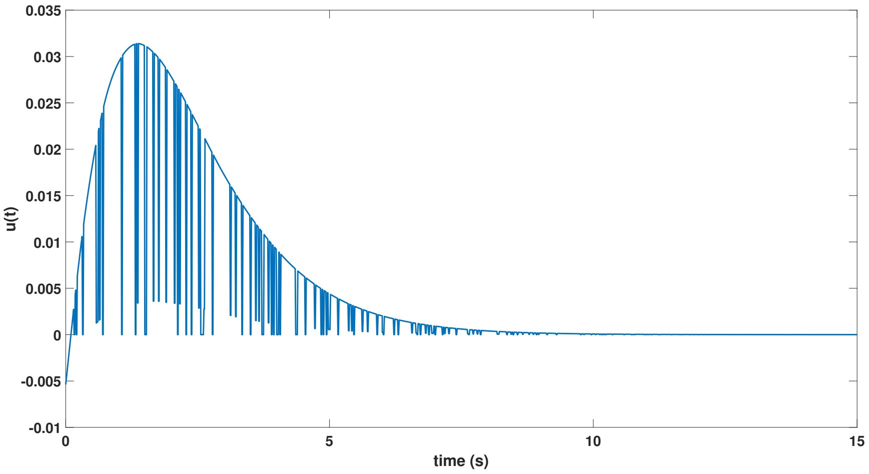

Figure 9. Control input trajectory of one-area power system.

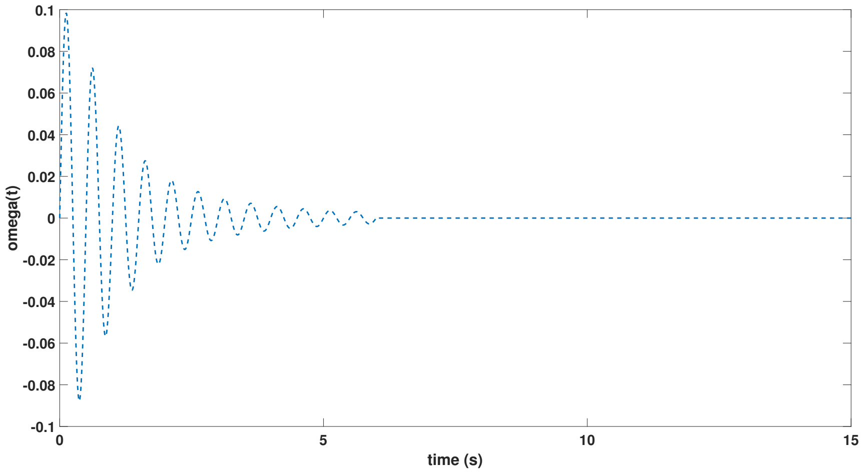

Figure 10. The response of disturbance signal.

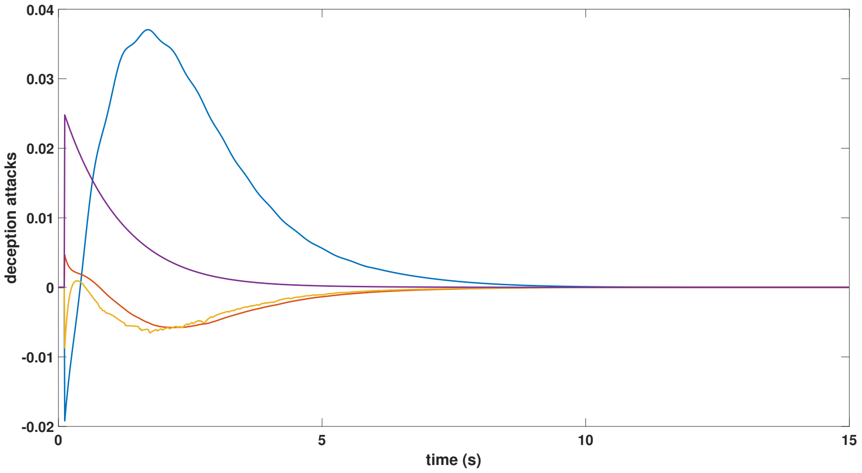

Figure 11. The response of deception attacks signals.

5. Conclusions

This paper is dedicated to studying the mean square asymptotic stability as well as H_∞ performance of networked power systems with multi-path missing measurements and input–output time-varying delays as well as cyber attacks on the communication channels.

An observer-based LFC model for networked power systems is established, which not only takes into account multi-path missing measurements and input–output time-varying delays in the communication channel but also considers the influences of random cyber attacks on data transmission. Based on this model, with the help of Lyapunov stability theory and LMI techniques, we derived sufficient conditions for the stability and H_∞ performance of the system. The validity of the proposed solution is verified by means of simulation examples. It should be noted that we extended the model to a practical situation comparing with previous works due to the frequently occurrence of packet dropouts and cyber attacks phenomenon since it may diminish system performance; however, the approach proposed in this paper also has the following limitations:

Firstly, we model the loss of packets and the occurrence of cyber attacks as Bernoulli stochastic processes, which are somewhat limited in practical applications. Secondly, the stability criterion obtained from the generalized function chosen in this paper is somewhat conservative when dealing with time delay systems. In the future, the simultaneous consideration of input and output packet dropouts described by other efficient stochastic processes and time-varying signal delays deserves further study.

Author Contributions: Y.G., G.L. and J.S. contributed to developing the ideas of this research, Y.G., G.L., G.Z. and H.L. performed the research. All of the authors were involved in preparing this manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant 62003168, Natural Science Foundation of Jiangsu Province under Grant BK20210569, and Natural Science Research Project of Jiangsu Higher Education Institutions under Grant 20KJB120003, 20KJB470025.

Data Availability Statement: Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

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

References

1. Wu, Z.; Mo, H.; Xiong, J.; Xie, M. Adaptive event-triggered observer-based output feedback L_∞ load frequency control for networked power systems. *IEEE Trans. Ind. Inform.* **2019**, *16*, 3952–3962. [CrossRef]
2. Singh, V.; Kishor, N.; Samuel, P. Load frequency control with communication topology changes in smart grid. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1943–1952. [CrossRef]
3. Jiang, L.; Yao, W.; Wen, J.; Chen, S.; Wu, Q. Delay-dependent stability for load frequency control with constant and time-varying delays. *IEEE Trans. Power Syst.* **2012**, *27*, 932–941. [CrossRef]
4. Zhang, Y.; Li, X. A note on L_2-gain analysis for power systems with delayed load frequency control schemes. *J. Frankl. Inst.* **2021**, *358*, 7586–7602. [CrossRef]
5. Zhang, H.; Liu, J.; Xu, S. H_∞ load frequency control of networked power systems via an event-triggered scheme. *IEEE Trans. Ind. Electron.* **2020**, *67*, 7104–7113. [CrossRef]
6. Zhang, Y.; Yang, T. Decentralized switching control strategy for load frequency control in multi-area power systems with time delay and packet losses. *IEEE Access* **2020**, *8*, 15838–15850. [CrossRef]
7. Pradhan, S.; Das, D. H_∞ controller design for frequency control of delayed power system with actuator saturation and wind source integration. *Arab. J. Sci. Eng.* **2022**, *67*. [CrossRef]
8. Feng, W.; Xie, Y.; Luo, F.; Zhang, X.; Duan, W. Enhanced stability criteria of network-based load frequency control of power systems with time-varying delays. *Energies* **2021**, *14*, 5820. [CrossRef]
9. Zhao, F.; Yuan, J.; Wang, N.; Zhang, Z.; Wen, H. Secure load frequency control of smart grids under deception attack: A piecewise delay approach. *Energies* **2019**, *12*, 2266. [CrossRef]
10. Zhao, X.; Zou, X.; Wang, N.; Zhong, M. Decentralized resilient H_∞ load frequency control for cyber-physical power systems under DoS attacks. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1737–1751. [CrossRef]
11. Fayek, H. 5G Poor and Rich Novel Control Scheme Based Load Frequency Regulation of a Two-Area System with 100% Renewables in Africa. *Fractal Fract.* **2021**, *5*, 2. [CrossRef]
12. Zhang, C.; Jiang, L.; Wu, Q.; He, Y.; Wu, M. Delay-dependent robust load frequency control for time delay power systems. *IEEE Trans. Power Syst.* **2013**, *28*, 2192–2201. [CrossRef]
13. Sargolzaei, A.; Kang, K.; Lghani, M.; Mehbodniya, A.; Sargolzaei, S. A novel technique for detection of time delay switch attack on load frequency control. *Intell. Control Autom.* **2015**, *6*, 205–214. [CrossRef]

14. Pradhan, S.; Das, D. H_∞ load frequency control design based on delay discretization approach for interconnected power systems with time delay. *J. Mod. Power Syst. Clean Energy* **2021**, *9*, 1468–1477. [CrossRef]
15. Sun, Y.; Wang, Y.; Wei, Z.; Sun, G.; Wu, X. Robust H_∞ load frequency control of multi-area power system with time delay: A sliding mode control approach. *IEEE/CAA J. Autom. Sin.* **2018**, *5*, 610–617. [CrossRef]
16. Ahuja, A.; Narayan, S.; Kumar, J. Two degrees of freedom observer controller for load frequency control with communication delay. *J. Control Instrum.* **2017**, *8*, 35–44.
17. Wang, Y.; Yan, W.; Zhang, H.; Xie, X. Observer-based dynamic event-triggered H_∞ LFC for power systems under actuator saturation and deception attack. *Appl. Math. Comput.* **2022**, *420*. [CrossRef]
18. Sathishkumar, M.; Liu, Y. Resilient annular finite-time bounded and adaptive event-triggered control for networked switched systems with deception attacks. *IEEE Access* **2021**, *9*, 92288–92299. [CrossRef]
19. Tian, E.; Peng, C. Memory-based event-triggering H_∞ load frequency control for power systems under deception attacks. *IEEE Trans. Cybern.* **2020**, *50*, 4610–4618. [CrossRef]
20. Shen, Z.; Yang, F.; Chen, J.; Zhang, J.; Hu, A.; Hu, M. Adaptive event-triggered synchronization of uncertain fractional order neural networks with double deception attacks and time-varying delay. *Entropy* **2021**, *23*, 1291. [CrossRef]
21. Tapin, L.; Mehta, R. An integral with feed forward control for primary load frequency control loop using pole-placement design. *Int. J. Electr. Electron. Data Commun.* **2014**, *2*, 38–45.
22. Vrdoljak, K.; Peri, N.; Petrovi, I. Sliding mode based load-frequency control in power systems. *Electr. Power Syst. Res.* **2010**, *80*, 514–527. [CrossRef]
23. Fernando, T.; Emami, K.; Yu, S.; Iu, H.; Wong, K. A novel quasi-decentralized functional observer approach to LFC of interconnected power systems. *IEEE Power Energy Soc. Gen. Meet.* **2016**, *31*, 3139–3151.
24. Pham, T.; Trinh, H.; Le, V. Load frequency control of power systems with electric vehicles and diverse transmission links using distributed functional observers. *IEEE Trans. Smart Grid* **2015**, *7*, 238–252. [CrossRef]
25. Wang, Z.; Liu, Y.; Yang, Z.; Yang, W. Load Frequency Control of Multi-Region Interconnected Power Systems with Wind Power and Electric Vehicles Based on Sliding Mode Control. *Energies* **2021**, *14*, 2288. [CrossRef]
26. Liu, J.; Gu, Y.; Zha, L.; Liu, Y.; Cao, J. Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1665–1678. [CrossRef]
27. Wang, J.; Xia, J.; Shen, H.; Xing, M.; Park, J. H_∞ synchronization for fuzzy Markov jump chaotic systems with piecewise-constant transition probabilities subject to PDT switching rule. *IEEE Trans. Fuzzy Syst.* **2021**, *29*, 3082–3092. [CrossRef]
28. Liu, J.; Wu, Z.; Yue, D.; Park, J. Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 943–953. [CrossRef]
29. Yan, H.; Zhang, H.; Zhan, X.; Li, Z.; Yang, C. Event-based H_∞ fault detection for buck converter with multiplicative noises over network. *IEEE Trans. Circuits Syst. Regul. Pap.* **2019**, *66*, 2361–2370. [CrossRef]
30. Tian, E.; Wang, K.; Zhao, X.; Shen, S.; Liu, J. An improved memory-event-triggered control for networked control systems. *J. Frankl. Inst.* **2019**, *356*, 7210–7223. [CrossRef]
31. Zhou, Q.; Shi, P.; Xu, S.; Li, H. Observer-based adaptive neural network control for nonlinear stochastic systems with time delay. *IEEE Trans. Neural Netw. Learn. Syst.* **2013**, *23*, 71–80. [CrossRef] [PubMed]
32. Yan, H.; Su, Z.; Zhang, H.; Yang, F. Observer-based $\mathcal{H}_\infty$ control for discrete-time stochastic systems with quantisation and random communication delays. *IET Control Theory Appl.* **2013**, *7*, 372–379. [CrossRef]
33. Zhao, Y.; Duan, Z.; Wen, G.; Zhang, Y. Distributed finite-time tracking control for multi-agent systems: An observer-based approach. *Syst. Control. Lett.* **2013**, *62*, 22–28. [CrossRef]
34. Tan, F.; Zhou, L. Analysis of random synchronization under bilayer derivative and nonlinear delay networks of neuron nodes via fixed time policies. *ISA Trans.* **2022**. [CrossRef] [PubMed]