# Switching System-Based Load Frequency Control for Multi-Area Power System Resilient to Denial-of-Service Attacks

Xing-Chen ShangGuan[a,b,c,d], Yong He[a,b,c], Chuan-Ke Zhang[a,b,c], Li Jin[a,b,c,d], Lin Jiang[d,*], Min Wu[a,b,c], Joseph William Spencer[d]

[a] *School of Automation, China University of Geosciences, Wuhan 430074, China*
[b] *Hubei Key Laboratory of Advanced Control and Intelligent Automation for Complex Systems, Wuhan 430074, China*
[c] *Engineering Research Center of Intelligent Technology for Geo-Exploration, Ministry of Education, Wuhan 430074, China*
[d] *Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3GJ, United Kingdom*

## Abstract

Load frequency control (LFC) scheme of modern power systems tends to employ open communication networks to transmit control/measurement signals, which makes the LFC scheme more vulnerable to cyber-attacks such as a denial-of-service (DoS) attack. The DoS attack prevents signal transmission and degrades the performance of or even results in instability in the LFC scheme. This paper proposes a switching system-based approach to the LFC scheme of a multi-area power system that is resilient to DoS attacks. After modelling the LFC scheme under DoS attacks as switching subsystems based on the duration of DoS attacks, a new stability criterion in terms of the duration and frequency of DoS attacks is developed. The derived criterion can be used to calculate the maximum duration and frequency of DoS attacks that the LFC system with a given proportional-integral (PI)-type controller can tolerate and to determine the control gains of the PI-type controller for a given duration and frequency of DoS attack. Moreover, a resilient LFC scheme is proposed based on a dual-loop communication channel equipped with the designed PI controller. The effectiveness of the proposed LFC scheme is evaluated on a traditional three-area power system and a deregulated three-area power system under DoS attacks.

*Keywords:* Power system, Load frequency control, Open communication network, DoS attacks, Switching system theory.

## 1. Introduction

As one of the most essential operational functions of power systems, load frequency control (LFC) is widely used for frequency regulation (Kudur [1994], Sharma et al. [2019]). In an interconnected power system, the main objective of LFC is to restore the balance between load and generation in each control area (Khodabakhshian et al. [2008], Jiang et al. [2012]). The configuration of power system becomes complex with the advancement and usage of distributed generators, and the conventional power system is evolving towards a deregulated and competitive power system (Shayeghi et al. [2009]). The changes in the power system introduce new challenges to the operation of LFC system. The primary problem is the stability of the LFC system under an open communication network (Zhang et al. [2013a]), which is investigated in this paper. In addition, uncertainties and low inertia due to the intermitted and uncertain generation of renewable energy sources (Alhelou et al. [2018]) and the high penetration of renewable energy sources(ShangGuan et al. [2020]), respectively, are challenges.

Traditionally, an LFC scheme employs dedicated channels to transmit control signals and measurements (Zhang et al. [2013b]). However, with the existence of geographically distributed generators and the increased competition among third party or bilateral contracts in a modern electricity market, an open communication infrastructure has been suggested for the LFC scheme to support the increasingly decentralized property of control services (referring to Shayeghi et al. [2007] and Jin et al. [2019]). However, the use of information and communication technologies in the power system makes the system more vulnerable to various network attacks, as reported in Teumim [2010]. Such attacks may have a serious impact on power system stability and even social stability. Typical cases include when the management system of supervisory control and data acquisition distribution in Ukraine was attacked by a foreign attacker, as noted in Lee et al. [2016], and when an Iranian nuclear power station at Natanz was attacked by the StuxNet virus, as reported in Farwell et al. [2011]. The Ukrainian blackout affected approximately $225,000$ customers, while the attacks in Iran resulted in $60\%$ of the hosts being damaged. Therefore, it is urgent to address the adverse effects caused by network attacks with an effective LFC scheme.

A denial-of-service (DoS) attack is a network attack. The attack corrupts availability by blocking the transmission medium, which results in the loss of useful information. To date, many

[☆] This work was supported in part by the National Natural Science Foundation of China under Grants 62022074, 61973284 and 61873347, by the Hubei Provincial Natural Science Foundation of China under Grants 2019CFA040, by the 111 project, China under Grant B17040, by the Program of China Scholarship Council under Grant 201706410012 and 201706410037, and by the Fundamental Research Funds for National Universities, China University of Geosciences (Wuhan) under Grant 2201610296.

[*] Corresponding author

*Email address:* ljiang@liv.ac.uk (Lin Jiang)

researchers have applied significant effort to the LFC scheme regarding defence against DoS attacks. Regarding DoS attacks as networked induced sent disturbances, some robust LFC schemes for interconnected power systems have been developed in Zhang et al. [2013a], Liu et al. [2016], Saxena et al. [2017] and Alhelou et al. [2019]. Zhang et al. [2013a] proposed a delay-dependent $H_\infty$ LFC scheme so that the scheme can withstand certain time delays caused by data packet dropout and/or disordering in communication channels. Liu et al. [2016] and Saxena et al. [2017] presented a robust distributed model predictive control-based LFC scheme against power system dynamic uncertainties. Additionally, an unknown input functional observer-based optimal LFC approach was introduced to handle network attacks in Alhelou et al. [2019]. However, such robust schemes did not consider the detailed model of a DoS attack in the design of the LFC scheme.

Different from the above schemes, some literature has suggested the introduction of DoS attacks into the modeling of LFC schemes. For example, by modelling DoS attacks as a switching on/ off event of a switch system, Liu et al. [2013] proved that the existence of DoS attacks makes the dynamics of a power system unstable, including convergence and steady-state errors. By considering the effect of energy-limited DoS attacks, Peng et al. [2016] designed a resilient event-triggered-based LFC scheme that allows a degree of packet loss from DoS attacks. Further work can be found in Zhou et al. [2019] and Liu et al. [2019]. Cheng et al. [2020] noted that both studies in Liu et al. [2013] and Peng et al. [2016] employ a single loop LFC scheme without additional control, and thus, a resilient design of an additional control law for a multi-area power system is proposed. However, the above methods focus on the stability analysis of the LFC scheme, considering only the durations of the DoS attacks. The useful and significant information of DoS attacks, the attack frequency, has not yet been introduced in the design of an LFC scheme. As reported in Help Net Security [2018], the distributed DoS attack frequency experienced 40% year-on-year growth in 2018 according to Corero Network Security. Therefore, both the frequency and duration of DoS attacks need to be considered in the LFC.

For this, Shang-Guan et al. [2020] investigated the stability and controller design of LFC for a simple single area power system under DoS attacks. However, the modeling and analysis method of a single-area power system is only applicable to situations where the entire power system is regarded as a control region, such as an independent small power grid or an isolated power grid. Additionally, modern power systems are often interconnected and controlled through different control areas. In a single-area power system, maintaining frequency at a prescribed value is the only goal of LFC, while except for the frequency, the power exchanges through tie lines between different areas also need to be maintained at a prescribed value in a multi-area power system (Pandey et al. [2013]). Moreover, from the single-area power system to the multi-area power system, the dimensions of the system have increased significantly, and there are also inter-area coupling connections. This greatly increases the difficulty of modelling and design. Therefore, extending the research scheme of a single-area power system in Shang-Guan et al. [2020] to a multi-area power system represents a more realistic power system situation and also exists more challenges.

Most importantly, a resilient LFC scheme should be able to defend against a serious DoS attack. However, most of the above proposed schemes can only withstand a certain level of DoS attack according to stability analysis, for example Peng et al. [2016]. For this purpose, a deep auto-encoder extreme learning machine algorithm was introduced in Li et al. [2019] to predict and supplement lost data and thus to ensure the normal operation of the LFC system. Such a scheme, however, requires numerous computing spaces to predict the lost data based on historical frequency records. Additionally, the scheme executes actions for any DoS attack, and thus wastes communication and computing resources and lacks of flexibility. Peng et al. [2016] employed a dual-loop communication network, including a main channel and a standby channel, for the LFC scheme. When the main channel suffers a serious DoS attack, the main channel is switched to the standby channel. However, the attack frequency has not been investigated in this work. Therefore, how to design a resilient LFC scheme, that can defend against certain levels of duration and frequency in DoS attacks and can execute extra actions to face some serious DoS attacks has not been fully investigated. This motivates this research effort.

Based on the above discussion, this paper investigates a switching system-based resilient LFC scheme for a multi-area power system against DoS attacks. The originality and contributions of this paper can be summarized as follows:

1) The LFC of a multi-area power system is divided into different switching subsystems based on different durations of DoS attacks. With the aid of the connection between adjacent subsystems, the switching system-based LFC scheme model is established.
2) Based on Lyapunov stability theory, a novel stability condition for a switching system-based LFC scheme for a multi-area power system is proposed in terms of the duration and frequency of DoS attacks. The proposed criterion fully considers the attack frequency. This is different from the existing methods in Peng et al. [2016] and Cheng et al. [2020], which consider only the attack duration.
3) Based on the linear matrix inequality (LMI) technique, the margins of the duration and frequency of a DoS attack for an LFC scheme with a given proportional-integral (PI)-type controller can be derived from the stability condition. Additionally, the PI-type controller gains of the LFC scheme can be determined under a given frequency and duration of DoS attack.
4) A resilient LFC scheme to defend against DoS attacks is proposed for a multi-area power system. The scheme is equipped with a dual-loop communication network including the main and standby channels, where the designed PI controller is installed. When the duration and frequency of DoS attack detected by the main channel exceed the scheduled values obtained for the stability condition, the main communication channel is switched to the standby channel to mitigate the impact of the serious DoS attack.

The remainder of this paper is organized as follows. Section 2 presents the switching LFC system model for a multi-area power system. Section 3 proposes stability analysis and controller design methods of the LFC scheme, and introduces a DoS attack defence LFC scheme. In Section 4, case studies based on a traditional three-area power system and a deregulated three-area power system under DoS attacks are shown to verify the effectiveness of the proposed scheme. The conclusion is given in Section 5.

## 2. Switching LFC Model for Multi-Area Power System Under Decentralized Control Strategy

This section introduces a switching LFC model for a multi-area power system. To simplify the LFC design, the decentralized control strategy is applied. Additionally, the exchange of tie-line power in each area is regarded as a disturbance. That is, only the local system information is related to the design LFC scheme in every control area, and the LFC scheme design for a multi-area power system can be treated as a repetitive LFC scheme design for a single area power system. Therefore, at first, a linear LFC model for a single control area in a multi-area power system is introduced under an open communication network. Then, a detailed description of modelling a switching LFC model is illustrated under DoS attacks.

### *2.1. Modelling for multi-area power system*

A multi-area power system includes $N$ subareas, and these subareas are interconnected by tie-lines. Each subarea has a similar structure, including governor, turbine, rotating mass and load, controller, and double-loop communication network. For a modern power system under a deregulated environment, the power system comprises generation companies(Gencos) and distribution companies (Discos). Each Genco can contract with various Discos located in or out of the area to which the Genco belongs. These bilateral contracts are visualized by an augmented generation participation matrix (AGPM) Shayeghi et al. [2006]. For an LFC scheme under a deregulated environment including $p$ Discos and $q$ Gencos in the $i_{th}$ control area, the AGPM is given by

$$\mathrm{AGPM} = \begin{bmatrix} \mathrm{AGPM}_{11} & \cdots & \mathrm{AGPM}_{1N} \\ \vdots & \ddots & \vdots \\ \mathrm{AGPM}_{N1} & \cdots & \mathrm{AGPM}_{NN} \end{bmatrix} \tag{1}$$

where

$$\mathrm{AGPM}_{ij} = \begin{bmatrix} \mathcal{LP}_{s_i+1,z_j+1} & \cdots & \mathcal{LP}_{s_i+1,z_j+p} \\ \vdots & \ddots & \vdots \\ \mathcal{LP}_{s_i+q,z_j+1} & \cdots & \mathcal{LP}_{s_i+q,z_j+p} \end{bmatrix}$$

with $s_i = q(i-1)$ and $z_j = p(j-1)$. $\mathcal{LP}_{ij}$ shows the participation factor of Genco $i$ in the total load following requirement of Disco $j$ based on the possible contracts. As shown in Fig. 1, the dotted lines in $v_{1i}$, $v_{3i}$ and $v_{4i}$ show the new load demand signals related to the possible bilateral contracts. The details are as follows: $v_{1i} = \Delta P_{Li} + \Delta P_{di} = \sum_{j=1}^{p} \Delta P_{Lj-i} + \sum_{j=1}^{p} \Delta P_{ULj-i}$, $v_{3i} = \sum_{k=1,k\neq i}^{N} \Delta P_{tie,ik,sch}$, $\Delta P_{tie,ik,sch} = \sum_{j=1}^{q} \sum_{t=1}^{p} \mathcal{LP}_{s_i+j,z_k+t} \Delta P_{Lt-k} - \sum_{j=1}^{q} \sum_{t=1}^{p} \mathcal{LP}_{s_k+j,z_i+t} \Delta P_{Lt-i}$ $v_{4i}^T = \left[v_{4i,1} \cdots v_{4i,k} \cdots v_{4i,q}\right]$, $v_{4i,k} = \sum_{j=1}^{N} \sum_{t=1}^{p} \mathcal{LP}_{s_i+k,z_j+t} \Delta P_{Lt-j}$, and $\Delta P_{mk-i} = v_{4i,k} + \alpha_{ki} \sum_{j=1}^{p} \Delta P_{ULj-i}$, where $\Delta P_{Li}$ and $\Delta P_{di}$ are the total contracted and un-contracted demands in subarea $i$, respectively; $\Delta P_{Lj-i}$ and $\Delta P_{ULj-i}$ are the contracted and un-contracted demands of Disco $j$ in subarea $i$, respectively; $\Delta P_{tie,ik,sch}$ is the scheduled tie-line power exchange between subareas $i$ and $k$; and $\Delta P_{m,k-i}$ is the desired total power generation of Genco $k$ in subarea $i$.

Then, we assume that all generators are equipped with a non-reheat turbine. Treating $v_{1i}$, $v_{2i}$, $v_{3i}$ and $v_{4i}$ as disturbances in the LFC scheme, we can express the LFC state-space model of subarea $i$ as follows (Zhang et al. [2013a]):

$$\begin{cases} \dot{\bar{x}}_i(t) = \bar{A}_i \bar{x}_i(t) + \bar{B}_i u_i(t) + \bar{F}_i \bar{\omega}_i(t) \\ \bar{y}_i(t) = \bar{C}_i \bar{x}_i(t) \end{cases} \tag{2}$$

where

$$\begin{aligned}
&\bar{x}_i^T = \left[\Delta f_i \; \Delta P_{tie-i} \; \Delta P_{m1i} \; \cdots \; \Delta P_{mqi} \; \Delta P_{v1i} \; \cdots \; \Delta P_{vqi}\right] \\
&u_i = \Delta P_{ci}, \bar{\omega}_i = [v_{1i}; v_{2i}; v_{3i}; v_{4i}], \bar{y}_i = ACE_i \\
&\bar{A}_i = \begin{bmatrix} A_{11i} & A_{12i} & 0 \\ 0 & A_{22i} & A_{23i} \\ A_{31i} & 0 & A_{33i} \end{bmatrix}, \bar{F}_i = \begin{bmatrix} -\frac{1}{M_i} & 0 & 0 & 0 \\ 0 & -2\pi & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -A_{33i} \end{bmatrix} \\
&\bar{B}_i = \begin{bmatrix} 0 \\ 0 \\ B_{3i} \end{bmatrix}, A_{11i} = \begin{bmatrix} -\frac{D_i}{M_i} & -\frac{1}{M_i} \\ 2\pi \sum_{j=1,j\neq i}^{N_i} T_{ij} & 0 \end{bmatrix} \\
&A_{12i} = \begin{bmatrix} \frac{1}{M_i} & \cdots \frac{1}{M_i} \\ 0 & \cdots 0 \end{bmatrix}, B_{3i} = \left[\frac{\alpha_{1i}}{T_{g1i}} \cdots \frac{\alpha_{qi}}{T_{gqi}}\right], \bar{C}_i = [\beta_i \; 1 \; 0 \; 0] \\
&A_{22i} = -A_{23i} = \mathrm{diag}\left\{\frac{-1}{T_{ch1i}} \cdots \frac{-1}{T_{chqi}}\right\}, v_{2i} = \sum_{j=1,j\neq i}^{N} T_{ij} \Delta f_j \\
&A_{31i} = \begin{bmatrix} \frac{-1}{RT_{g1i}} & \cdots & \frac{-1}{RT_{gqi}} \\ 0 & \cdots & 0 \end{bmatrix}^T, A_{33i} = \mathrm{diag}\left\{\frac{-1}{T_{g1i}} \cdots \frac{-1}{T_{gqi}}\right\}
\end{aligned}$$

and $\Delta f_i, \Delta P_{mki}, \Delta P_{vki}$ and $\Delta P_{ci}$ are deviations of frequency, generator mechanical output, valve position, and control input in subarea $i$, respectively; $\beta_i$, $M_i, D_i, T_{gki}, T_{chki}, R_{qi}$ and $\alpha_{ki}$ represent the frequency bias factor, moment of inertia of the generator unit, generator unit damping coefficient, time constant of the governor, time constant of the turbine, speed droop and participation factor for generator $k$ in subarea $i$, respectively; $\Delta P_{tie-i}$ represents the tie-line power exchange; $T_{ij}$ is the tie-line synchronizing coefficient between subareas $i_{th}$ and $j_{th}$; and $ACE_i$ represents the ACE of the $i_{th}$ area of the power system and is the linear combination of $\Delta f_i$ and $\Delta P_{tie-i}$, i.e., $ACE_i = \beta_i \Delta f_i + \Delta P_{tie-i}$.

Different from the deregulated LFC scheme, a traditional LFC scheme does not require contracts between Gencos and Discos. Therefore, the LFC structure in the traditional power system is represented by Fig. 1 without the dotted lines in $v_{1i}$, $v_{3i}$ and $v_{4i}$. Therefore, the main difference between the traditional and deregulated LFC schemes is $\bar{w}_i(t)$ and $\bar{F}_i$. In the traditional LFC scheme, $\bar{w}_i(t) = [\Delta P_{di}; v_{2i}]$ and $\bar{F}_i = \begin{bmatrix} -\frac{1}{M_i} & 0 & 0 & 0 \\ 0 & -2\pi & 0 & 0 \end{bmatrix}^T$. The balance point's inner stability of the system (2) is equivalent to the origin's stability with $\omega(t) = 0$. Thus, the state-space model of subarea $i$ studied in

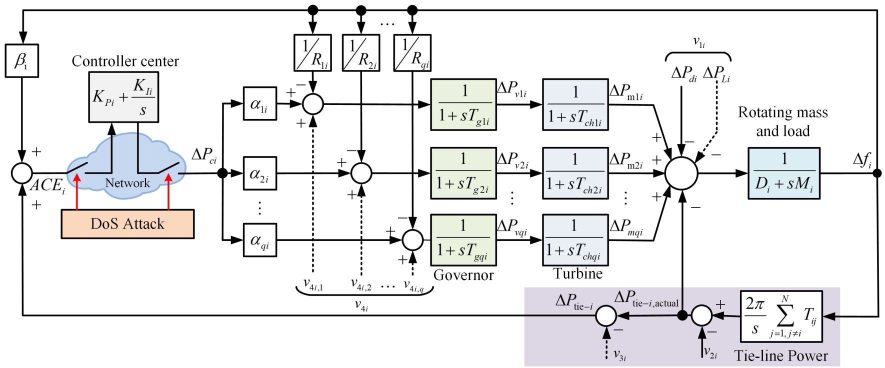

Figure 1: Structure of the $i_{th}$ control area of LFC scheme for a multi-area power system.

this paper can be summarized as follows

$$\begin{cases} \dot{\bar{x}}_i(t) = \bar{A}_i\bar{x}_i(t) + \bar{B}_iu_i(t) \\ \bar{y}_i(t) = \bar{C}_i\bar{x}_i(t) \end{cases} \tag{3}$$

### 2.2. *Modelling for LFC under DoS attacks*

The control action $u_i(t)$ in system (3) is implemented over a sensor/acuator network. We assume that the sensor and actuator are periodically time-triggered, while the controller is event-triggered when sensor data are received. The control signal is sampled using a zero-order holder device. $kT_{k=0,1,2\cdots}$ with sampling period $T$ of the sensor represents the sequence of time instants at which it is desired to update the control action. In the ideal situation where data can be sent and received at any desired instant of time, the ideal control input applied to the process is given by

$$u_i(t) = K_i\bar{x}_i(kT) \tag{4}$$

where $K_i$ is the controller gains.

#### 2.2.1. *DoS attacks*

DoS attack is a cyber-attack, in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet. In a sampled-data control system, DoS attacks are referred to as the phenomenon that prevents sampled data from being transmitted to the intended users at each sampling time $kT$. Assume that the system is subjected to a DoS attack as shown in Fig. 2. The DoS attack is represented by the attack duration and the attack frequency based on Assumption 1 and Assumption 2, respectively.

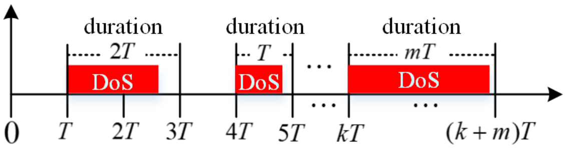

Figure 2: Time slots of a sampled-data system with DoS attacks

**Assumption 1:** For a sampled-data system with a sampling period $T$, the system is subjected to a DoS attack under $[kT,(k+m)T)$ with $m \in \{1,2,\cdots,m_{\max}\}$ and the sampled data at sampling time $\{kT,(k+1)T,\cdots,(k+m-1)T\}$ is prevented from being transmitted. Then, the durations of this attack are defined as $mT$, and $m_{\max}T$ is the largest of the durations.

**Assumption 2:** During a certain time period, $\ell_1$ is the number of DoS attacks on the system, and $\ell_2$ is the number of normal transmissions without DoS attacks. Then, the frequency of DoS attacks is defined as $\frac{\ell_1}{\ell_1+\ell_2}$ over this period.

#### 2.2.2. *LFC model with DoS attacks*

In the LFC scheme, DoS attacks are referred to as the phenomenon that prevents (4) from being executed at each desired time $kT$. We assume that a case of DoS attack simultaneously affecting both measurement and control channels is considered, which means that data can neither sent nor received in the presence of the DoS attack. When the system is under a DoS attack, the ideal control input $u_i(t)$ of the actuator cannot be guaranteed to be updated in a timely manner. Assume that the actuator executes the input $u_i(kT)$ when the DoS attacks end during $[kT,(k+m)T)$.

Considering the influence of DoS attacks on the updating of the actuator, a new sampling time $t_0,t_1,\cdots,t_l, l = 0,1,2\cdots$ is defined as the updated time of the controller signals. Then, the new sampling period of system (3) is $h_k = t_{k+1} - t_k = mT$ with $m \in \{1,2,\cdots,m_{\max}\}$ and $k = 0,1,2\cdots$. Then, the LFC state-space model (3) of subarea $i$ can be rewritten as follows:

$$\begin{cases} \dot{\bar{x}}_i(t) = \bar{A}_i\bar{x}_i(t) + \eta\bar{B}_iu_i(t_k) + (1-\eta)\bar{B}_iu_i(t_{k-1}) \\ \bar{y}_i(t) = \bar{C}_i\bar{x}_i(t) \qquad\qquad t \in [t_k,t_{k+1}) \end{cases} \tag{5}$$

where, $\eta = 0$ or $1$, $\eta = 0$ denotes that the system is subjected to DoS attacks, and $\eta = 1$ denotes that the system is not subjected to DoS attacks. To alleviate the impact of DoS attacks, we reconstruct the LFC system model in terms of the execution period of the actuator. Assume that $T_0 = \frac{1}{n}T$ with $n = 1,2,3,\cdots$ and $T_0$ is the execution period of the actuator. Then, the sampling period of system (5) is $mnT_0$. The detailed time slots under DoS attacks are shown in Fig. 3. From this diagram, it can be seen that two control signals $u(t_{k-1})$ and $u(t_k)$ exist simultaneously in the time interval of $h_k$. Assume the durations of the two control signals are $\varpi_1(k)T_0$ and $\varpi_0(k)T_0$, respectively. That is $h_k = \varpi_1(k)T_0 + \varpi_0(k)T_0 = mnT_0$.

Then, system (5) can be rewritten the following discrete model.

$$\begin{cases} \bar{x}_i(t_{k+1}) = \bar{A}_i(h_k)\bar{x}_i(t_k) + \bar{B}_i(h_k)u_i(t_k) + \bar{B}_i(h_{k-1})u_i(t_{k-1}) \\ \bar{y}_i(t_k) = \bar{C}_i\bar{x}_i(t_k) \end{cases} \tag{6}$$

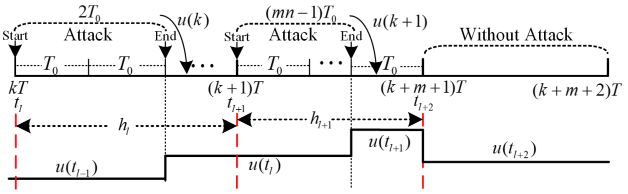

Figure 3: Time slots of an LFC process under DoS attacks

where $\bar{A}_i(h_k) = e^{\bar{A}_i h_k}$, $\bar{B}_i(h_k) = \int_{\varpi_1(k)T_0}^{h_k} e^{\bar{A}_i s}\bar{B}_i ds$, $\bar{B}_i(h_{k-1}) = \int_0^{\varpi_1(k)T_0} e^{\bar{A}_i s}\bar{B}_i ds$. Defining $\bar{A}_{oi}=e^{\bar{A}_i T_0}$, $\bar{B}_{oi}=\int_0^{T_0} e^{\bar{A}_i s}\bar{B}_i ds$, we can obtain $\bar{A}_i(h_k) = \bar{A}_{oi}^{mn}$, $\bar{B}_i(h_k) = \sum_{j=\varpi_1(k)}^{mn-1} \bar{A}_{oi}^{j}\bar{B}_{oi}$, and $\bar{B}_i(h_{k-1}) = \sum_{j=0}^{\varpi_1(k)-1} \bar{A}_{oi}^{j}\bar{B}_{oi}$. Then, system (6) is equivalent to

$$\begin{cases} \bar{x}_i(t_{k+1}) = \bar{A}_{oi}^{mn}\bar{x}_i(t_k) + \sum_{j=\varpi_1(k)}^{mn-1} \bar{A}_{oi}^{j}\bar{B}_{oi}u_i(t_k) \\ \qquad + \sum_{j=0}^{\varpi_1(k)-1} \bar{A}_{oi}^{j}\bar{B}_{oi}u_i(t_{k-1}) \\ \bar{y}_i(t_k) = \bar{C}_i\bar{x}_i(t_k) \end{cases} \tag{7}$$

In the above model, $\varpi_1(k)$ can take different values from an integral set $\{0, 1, 2, \cdots, m_{\max}n\}$ to make the system (7) exist in different forms under sampling period $h_k$. Taking $\sigma(t_k) = \varpi_1(k)$ as a switching signal under interval $[t_k, t_{k+1})$, we can rewrite the above system as the following switching system model.

$$S_{oi-\sigma(t_k)}\colon \begin{cases} \bar{x}_i(t_{k+1}) = \bar{A}_{oi}^{mn}\bar{x}_i(t_k) + \bar{B}_{oi-\sigma(t_k)}u_i(t_k) + \hat{\bar{B}}_{oi-\sigma(t_k)}u_i(t_{k-1}) \\ \bar{y}_i(t_k) = \bar{C}_i\bar{x}_i(t_k) \end{cases} \tag{8}$$

where $\bar{B}_{oi-\sigma(t_k)} = \sum_{j=\varpi_1(k)}^{mn-1} A_{oi}^{j}\bar{B}_{oi}$ and $\hat{\bar{B}}_{oi-\sigma(t_k)}=\sum_{j=0}^{\varpi_1(k)-1} \bar{A}_{oi}^{j}\bar{B}_{oi}$, and $\sigma(t_k) = \{0, 1, 2, \cdots, m_{\max}n\}$. Note that if $\sigma(t_k) = 0$, the subsystem is not subjected to DoS attacks, and additionally, $\bar{B}_{oi-0} = \sum_{j=0}^{n-1} A_{oi}^{j}\bar{B}_{oi}$ and $\hat{\bar{B}}_{oi-0} = 0$. Moreover, when $\sigma(t_k) = mn$, the subsystem is subjected to DoS attacks during the duration of $mnT_0$ with $m \in M$, and now $\bar{B}_{oi-mn} = 0$ and $\hat{\bar{B}}_{oi-mn} =\sum_{j=0}^{mn-1} \bar{A}_{oi}^{j}\bar{B}_{oi}$.

Under the impact of switching law $\sigma(t_k)$, assume the subsystem with $\sigma(t_k) = 0$, meaning it is not subjected to DoS attacks, is stable. When $\sigma(t_k) = 1, 2, \cdots$, the system becomes more unstable. Assume that the total activation numbers of stable and unstable subsystems over $[t_0, t_k)$ are denoted $n_0$ and $\Sigma_{j=1}^{mn} n_j$, respectively, where $n_{\sigma(t_k)}$ represents the activation number of subsystem $\sigma(t_k)$ over $[t_0, t_k)$. $f_u = \frac{\Sigma_{j=1}^{mn} n_j}{n_0+\Sigma_{j=1}^{mn} n_j}$ denotes the existing frequency of the unstable subsystems; then, the frequency of the stable subsystem is $1 - f_u$. Combining the definition of the DoS attack frequency, we regard the existing frequency $f_u$ of unstable subsystems as the DoS attack frequency.

Finally, choose the following PI-type controller:

$$u_i(t_k) = -K_{Pi}\bar{y}_i(t_k) - K_{Ii}\int \bar{y}_i(t_k) \tag{9}$$

where $K_{Pi}$ and $K_{Ii}$ are the proportional gain and integral gain, respectively.

Redefining $x_i(t) = \left[\bar{x}_i^T(t) \quad \int_0^t \bar{y}_i^T(s)ds\right]^T$ and $y_i(t) = \left[\bar{y}_i^T(t) \quad \int_0^t \bar{y}_i^T(s)ds\right]^T$ and then combining the system (8) and control law (9), we obtain the closed switching system for the LFC scheme of subarea $i$ as follows:

$$S_{ci\sigma(t_k)} : \begin{cases} x_i(t_{k+1}) = A_{i-\sigma(t_k)}x_i(t_k) - B_{i-\sigma(t_k)}x_i(t_{k-1}) \\ y_i(t_k) = C_i x_i(t_k) \end{cases} \tag{10}$$

where $A_{i-\sigma(t_k)} = \bar{A}_{oi}^{mn} - \bar{B}_{oi-\sigma(t_k)}K_iC_i$, $B_{i-\sigma(t_k)} = \hat{\bar{B}}_{oi-\sigma(t_k)}K_iC_i$, $K_i = [K_{Pi}\ K_{Ii}]$, $C_i = \begin{bmatrix} \bar{C}_i & 0 \\ 0 & 1 \end{bmatrix}$, and $\bar{A}_i$ and $\bar{B}_i$ are changed to

$$\bar{A}_i = \begin{bmatrix} A_{11i} & A_{12i} & 0 & 0 \\ 0 & A_{22i} & A_{23i} & 0 \\ A_{31i} & 0 & A_{33i} & 0 \\ \beta_i & 1 & 0 & 0 \end{bmatrix}, \bar{B}_i = \begin{bmatrix} 0 \\ 0 \\ B_{3i} \\ 0 \end{bmatrix}.$$

## 3. Design of The Resilient LFC Scheme with DoS Attacks

In this section, a resilient design method of the LFC scheme for a multi-area power system with DoS attacks is introduced. The schematic diagram of the proposed scheme is shown in Fig. 4. The scheme is equipped with a dual-loop communication network including the main (S1) and the standby (S2) channels. The resilience to DoS attacks is revealed in two parts. The first part is that the LFC centre installs a designed PI controller that can withstand a certain degree of DoS attack. The second part is the switch of the communication channel. When the duration and frequency of the DoS attack detected by channel S1 exceed the preset values of duration and frequency, channel S1 is switched to channel S2 to mitigate the impact of the serious DoS attack. To achieve the aims of the proposed scheme, an exponential stability criterion that considers the frequency and duration of DoS attacks and the updating period of ACE is first presented to ensure the stability of the LFC scheme. Then, a theorem of controller design is proposed based on the above stability condition. Finally, a design procedure for the resilient LFC scheme is described.

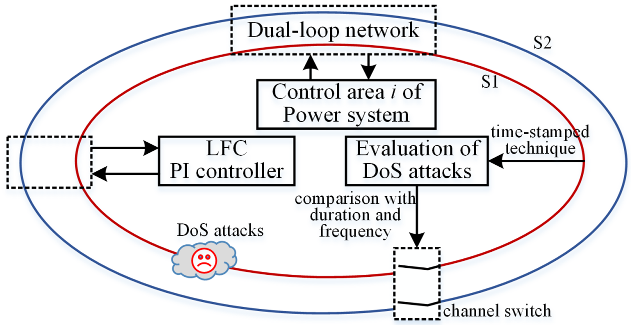
Dual-loop network
S2
S1
Control area $i$ of Power system
LFC PI controller
Evaluation of DoS attacks
time-stamped technique
comparison with duration and frequency
DoS attacks
channel switch

Figure 4: Schematic diagram of the proposed LFC scheme resilient to DoS attacks

### 3.1. Exponential stability criterion of LFC scheme with DoS attacks

Zhang et al. [2008] stated that the switching system allows both stable and unstable subsystems to exist simultaneously. As long as the frequency of the unstable subsystem is not greater than an upper bound, switching system (10) can be guaranteed to be stable. When the system is subjected to DoS attacks with $mnT_0$ durations, assume that system (10) has one stable subsystem with switching signal $\sigma(t_k) = 0$ and has $mn$ unstable subsystems with $\sigma(t_k) = \{1, 2, \cdots, mn\}$. Then, we can derive the following theorems.

**Theorem 1.** *Considering system (10), given the PI controller gains $K_i = [K_{Pi}\ K_{Ii}]$, sampling period of the actuator $T_0$, sampling period of the sensor $T = nT_0$, maximal duration of DoS attacks $mT$, exponential decay rate of stable subsystem $\lambda_0$ with $\sigma(t_k) = 0$, exponential decay ratesof unstable subsystem $\lambda_p | p \in \{1, 2, \cdots, mn\}$ with $\sigma(t_k) = \{1, 2, \cdots, mn\}$ and $\lambda_b = \max(\lambda_p)$, and prescribed scalars $\mu \geq 1$ and $\lambda < 1$ with $\lambda_0 < \lambda < \lambda_b$, if there exist appropriate matrixes $P_j \geq 0$, $Q_j \geq 0$, and $j \in \{0, 1, 2, \cdots, mn\}$ such that the following inequalities hold*

$$\Xi_j = \begin{bmatrix} A^T_{i-j} P_j A_{i-j} - \lambda_j^2 P_j + Q_j & A^T_{i-j} P_j B_{i-j} \\ B^T_{i-j} P_j A_{i-j} & B^T_{i-j} P_j B_{i-j} - \lambda_j^2 Q_j \end{bmatrix} < 0 \tag{11}$$

$$P_\alpha \leq \mu P_\beta, Q_\alpha \leq \mu Q_\beta, \alpha, \beta \in \{0, 1, 2, \cdots, mn\} \tag{12}$$

$$f_u \leq \frac{\ln \lambda - \ln \lambda_0}{\ln \lambda_b - \ln \lambda_0} \tag{13}$$

$$\frac{\ln \mu}{2 \ln(1/\lambda)} < T_a \tag{14}$$

*where $T_a$ is the average dwell time as defined in Lemma 4 in Appendix A, then system (10) is exponentially stable with an exponential decay rate of $\rho(\lambda, T_a) = \lambda \mu^{1/(2T_a)}$.*

The proof is shown in Appendix A.

Remark 1: In a real power system, the average dwell time $T_a$ cannot be determined in advance due to the variation in DoS attacks. However, based on the definition of $T_a$ in Lemma 4, we can obtain $T_a > T$. Therefore, if the following inequality holds

$$\frac{\ln u}{2 \ln(1/\lambda)} < T \tag{15}$$

then it can guarantee inequality (14) holds no matter how the DoS attacks change.

Theorem 1 provides a condition to evaluate the stability of the LFC system. This condition fully considers the updating period of ACE signals and the frequency and duration of DoS attacks. To analyse the stability margin of the DoS attack frequency and duration, Algorithm 1 is introduced to find the maximum attack frequency for a given PI controller and known maximum attack duration.

Remark 2: DoS attacks are often considered as transmission delays and then analysed by using the time-delay system theory, as stated in Zhang et al. [2013b]. However, this method does not fully consider the uncertainties of DoS attacks, that is, the frequency of attacks and the uncertainty in the duration of the attacks. Moreover, to analyse the margin of the time delay, transmission delays are assumed to always exist in the communication channel. However, the signal transmission is not always affected by DoS attacks, and DoS attacks are not always in the most severe state. Therefore, compared with the method in Zhang et al. [2013b], the method proposed in this paper, which takes into account the frequency and duration of DoS attacks, can more accurately analyse the impact of DoS attacks on system stability and design an effective LFC scheme against DoS attacks.

*Algorithm 1:* Find maximum attack frequency $f_{u_{max}}$

```
Step 1: Preset system parameters $\bar{A}_i$, $\bar{B}_i$, sampling periods $T_0$ of actuator
        and $T = nT_0$ of sensor, largest attack duration $m_{\max}T$, scalar $\mu$, and
        $\lambda_0 = 0.05$. Initialize $f_{u_{max}} = 0$
Step 2: While ($\lambda_0 < 1$)
            For k=1:$m_{\max}n$
                Set $\lambda_{min} = 1$, $\lambda_{max} = 10$, $\lambda_{ac} = 0.001$, $\rho = 0$.
                while ($\lambda_{max} - \lambda_{min} \geq \lambda_{ac}$)
                    $\lambda_k = (\lambda_{min} + \lambda_{max})/2$
                    For j=1:k
                    Obtain LMIs (11) and (12) under $\lambda_j$.
                    End
                    If LMIs hold, $\lambda_{max} = \lambda_k$, $\rho = 1$; else $\lambda_{min} = \lambda_k$.
                End
                If $\rho = 1$, save $\lambda_k = \lambda_{max}$; else, break.
            End
            If $\rho = 1$, $\lambda_b = \max\{\lambda_k, k = 1, 2, ..., m_{\max}n\}$, then based
            on (13) and (15) , calculate $f_u$, $\lambda$.
            If $f_u > f_{u_{max}}$, set $f_{u_{max}} = f_u$ and save $\lambda$, $\lambda_0$.
            Clear array $\lambda_k$ and set $\lambda_0 = \lambda_0 + 0.05$.
        End
Step 3: Output $f_{u_{max}}$, $\lambda$, $\lambda_0$.
```

### 3.2. Controller design for LFC scheme with DoS attacks

When PI controller $K_i$ in system (10) is unknown, Theorem 1 is no longer an LMI-based condition due to a product of $A^T_{i-j} P_j A_{i-j}$. To develop the gains of controller $K_i$, the following Theorem 2 is constructed.

**Theorem 2.** *Considering system (10), given sampling period of the actuator $T_0$ , sampling period of the sensor $T = nT_0$, maximal duration of DoS attacks $mT$, exponential decay rate of stable subsystem $\lambda_0$ with $\sigma(t_k) = 0$, exponential decay rates of unstable subsystem $\lambda_p | p \in \{1, 2, \cdots, mn\}$ with $\sigma(t_k) = \{1, 2, \cdots, mn\}$ and $\lambda_b = \max(\lambda_p)$, and prescribed scalars $\mu \geq 1$ and $\lambda < 1$ with $\lambda_0 < \lambda < \lambda_b$, if there exist appropriate matrices $X$, $\Upsilon$, $R_j \geq 0$, $S_j \geq 0$, $j \in \{0, 1, 2, \cdots, mn\}$, such that (13), (15) and the following inequalities hold*

$$\begin{bmatrix} -\lambda_j^2 R_j + S_j & 0 & X^T \bar{A}^T_{oi-j} + \Upsilon^T \bar{B}^T_{oi-j} \\ * & -\lambda_j^2 S_j & \Upsilon^T \hat{\bar{B}}^T_{oi-j} \\ * & * & -X - X^T + R_j \end{bmatrix} < 0 \tag{16}$$

$$R_\alpha \leq \mu R_\beta,\ S_\alpha \leq \mu S_\beta,\ \alpha, \beta \in \{0, 1, 2, \cdots, mn\} \tag{17}$$

*then system (10) is exponentially stable with an exponential decay rate of $\rho(\lambda, T_a) = \lambda \mu^{1/(2T_a)}$, and the PI controller gains can be calculated by*

$$K_i = \Upsilon X^{-1} C_i^T (C_i C_i^T)^{-1} \tag{18}$$

*The proof is given in Appendix B.*

To design a resilient LFC scheme, we want the designed PI controller to tolerate the maximal margins of attack frequency and duration. However, if the values of the exponential decay rate $\lambda_j$ are artificially selected, it is not guaranteed that the designed controller can tolerate the maximal frequency and duration of DoS attacks. Here, similar to Algorithm 1, the desired controller can be developed by finding a maximum attack frequency. The corresponding Algorithm 2 is presented as follows.

*Algorithm 2:* Find resilient controller $K_i$

```
Step 1: Preset system parameters $\bar{A}_i$, $\bar{B}_i$, $C_i$, sampling periods $T_0$ of actuator and $T = nT_0$ of sensor, largest attack duration $m_{\max}T$, scalar $\mu$, and $\lambda_0 = 0.05$. Initialize $f_{u_{max}} = 0$
Step 2: While ($\lambda_0 < 1$)
          For k=1: $m_{\max}n$
            $\lambda_{min} = 1$, $\lambda_{max} = 10$, $\lambda_{ac} = 0.001$, $\rho = 0$.
            while ($\lambda_{max} - \lambda_{min} \geq \lambda_{ac}$)
              $\lambda_k = (\lambda_{min} + \lambda_{max})/2$
                For j=1:k
                Obtain LMIs (16) and (17) under $\lambda_j$.
                End
              If LMIs hold, $\lambda_{max} = \lambda_k$, $\rho = 1$, and calculate
              $\bar{K}_i = \Upsilon X^{-1} C_i^T (C_i C_i^T)^{-1}$; else, $\lambda_{min} = \lambda_k$.
            End
            If $\rho = 1$, save $\lambda_k = \lambda_{max}$ and $\bar{K}_i$; else, break.
          End
          If $\rho = 1$, $\lambda_b = \max\{\lambda_k, k = 1, 2, ..., m_{\max}n\}$, then based
          on (18) and (20), calculate $f_u$, $\lambda$.
          If $f_u > f_{u_{max}}$, set $K_i = \bar{K}_i$, $f_{u_{max}} = f_u$, and save $f_u$, $\lambda$, $\lambda_0$.
          Clear array $\lambda_k$ and set $\lambda_0 = \lambda_0 + 0.05$.
        End
Step 3: Output $K_i$, $f_{u_{max}}$, $\lambda$, $\lambda_0$.
```

### 3.3. Design of the resilient LFC scheme for a multi-area power system under DoS attacks

In this subsection, we introduce an algorithm to present the design of a resilient LFC scheme for a multi-area power system under DoS attacks. The details are shown in Algorithm 3. To explain the procedure of the application of this algorithm, a flow chart is also shown in Fig. 5.

*Algorithm 3:* Design resilient LFC scheme for multi-area power system

Step 1: Divide the power system into $N$ control areas. Preset system parameters $\bar{A}_i$, $\bar{B}_i$ and $C_i$ with $i = 1, 2, ..., N$.

Step 2: Based on Algorithm 2, design PI controllers in each control area, and record the corresponding maximum attack duration $m_{\max-i}$ and frequency $f_{u-i}$ that controllers can tolerate in each control area. Then, equip the designed controllers to each control area.

Step 3: Install a double looped communication network in power system.

Step 4: A time-stamped technique is deployed to detect whether the triggered packet is lost or not. During a certain period, detect and record the real maximum duration $m_{r-i}$ and frequency $f_{r-i}$ of packet loss.

Step 5: Compare $m_{r-i}$ and $f_{r-i}$ with $m_{\max-i}$ and $f_{u-i}$ respectively. If $m_{r-i} \leq m_{\max-i}$ and $f_{r-i} > f_{u-i}$, or $m_{r-i} > m_{\max-i}$, the communication channel is switched from the main channel to the standby channel. Also, an alarm is triggered. When $m_{r-i} \leq m_{\max-i}$ and $f_{r-i} \leq f_{u-i}$, the communication channel is switched to the main channel.

Remark 3: A dual-loop communication network is suggested to be installed into the power system to improve the reliability of the LFC scheme. Assume that the main channel and the standby channel are set exactly the same, and data are simultaneously transmitted over both channels. Also, assume that the two channels can switch seamlessly when the main channel suffers severe DoS attacks.

Remark 4: A time-stamped technique (referring to Peng et al. [2016]) is used to detect information about DoS attacks. The time-stamped technique can analyse the system data packet loss due to the impact of DoS attacks and then obtain information about the duration and frequency of DoS attacks. In addition, information on DoS attacks can be obtained by evaluating the feedback data from the field. For example, machine learning algorithm (referring to Kumar et al. [2013]) is used to detect the anomaly data, and then the information of DoS attacks can be estimated by these anomaly data.

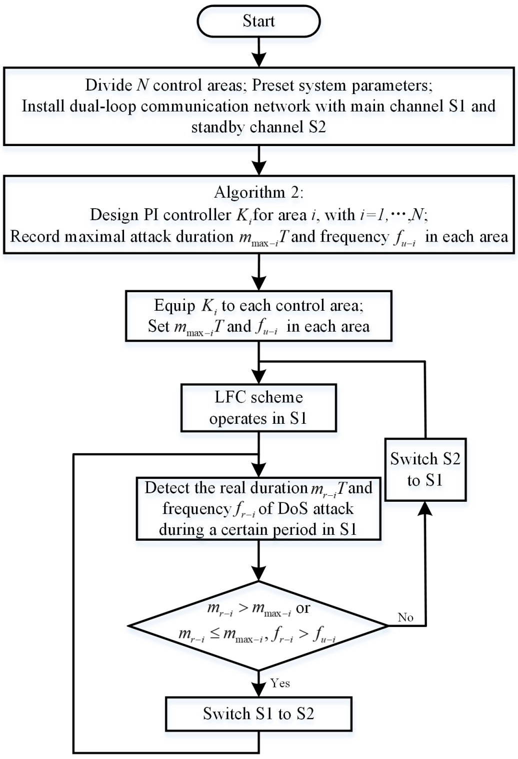
Start
Divide $N$ control areas; Preset system parameters;
Install dual-loop communication network with main channel S1 and standby channel S2
Algorithm 2:
Design PI controller $K_i$ for area $i$, with $i=1,\cdots,N$;
Record maximal attack duration $m_{\max-i}T$ and frequency $f_{u-i}$ in each area
Equip $K_i$ to each control area;
Set $m_{\max-i}T$ and $f_{u-i}$ in each area
LFC scheme operates in S1
Switch S2 to S1
Detect the real duration $m_{r-i}T$ and frequency $f_{r-i}$ of DoS attack during a certain period in S1
$m_{r-i} > m_{\max-i}$ or
$m_{r-i} \leq m_{\max-i}, f_{r-i} > f_{u-i}$
No
Yes
Switch S1 to S2

Figure 5: Procedure of application of the proposed LFC scheme resilient to DoS attack

## 4. Case Studies

In this section, to illustrate the effectiveness of the proposed approach, case studies have been carried out based on a traditional three-area power system and a deregulated three-area power system. In each case, we focus on three aspects of the proposed scheme, including the stability analysis, the controller design, and the test of the DoS attack defence LFC scheme. The details are as follows. The results of stability analysis and controller design are calculated based on the MATLAB/YALMIP toolbox, and the test of the DoS attack defence is simulated based on the Simulink environment in MATLAB.

### 4.1. A traditional three-area power system

To illustrate the principle of the proposed method, first, a case study is undertaken on a traditional three-area power system. The detailed LFC structure is shown in Fig. 1 excluding the dotted line connections, and its parameters are listed in Table 1 as reported in Zhou et al. [2019]. Moreover, we simulate the system for load disturbances (in pu) in three areas as follows:

$$\begin{cases} \Delta P_{d1} = 0.1, \Delta P_{d2} = -0.08 & t \in [0, 100s) \\ \Delta P_{d2} = 0.006\sin(0.3t), \Delta P_{d3} = 0.1 & t \in [100s, 200s) \\ \Delta P_{d1} = -0.02, \Delta P_{d3} = -0.04 & t \in [200s, 300s] \end{cases} \tag{19}$$

Table 1: Parameters of LFC scheme of the traditional three-area power system

| Control Area | $T_{ch}$(s) | $T_g$ (s) | $R$(Hz/pu) | D(pu/Hz) | M (pu·s) | $\beta$ (pu/Hz) | $\alpha$ | $T_{ij}$(pu/rad) |
|---|---|---|---|---|---|---|---|---|
| 1 | 0.30 | 0.10 | 0.05 | 1.0 | 10 | 21.0 | 1.0 | $T_{12} = 0.20$ |
| 2 | 0.40 | 0.17 | 0.05 | 1.5 | 12 | 21.5 | 1.0 | $T_{23} = 0.12$ |
| 3 | 0.35 | 0.20 | 0.05 | 1.8 | 12 | 21.8 | 1.0 | $T_{13} = 0.25$ |

### *4.1.1. Stability analysis*

The stability of the LFC scheme is analysed in terms of the attack frequency, attack durations and sampling periods. Due to the usual update period of $2 - 4s$ in the LFC process in real power system, we choose the sensor sampling period $2s$, $3s$, and $4s$ to analyse the stability.

Table 2: Acceptable frequencies of DoS attacks for different durations of DoS attacks in Area 1 under different sampling periods

| Duration | $1T$ | $2T$ | $3T$ | $4T$ | $5T$ |
|---|---|---|---|---|---|
| T=0.002s | 33.34% | 14.12% | 6.90% | 3.95% | 2.52% |
| T=0.2s | 37.26% | 15.71% | 8.26% | 5.28% | 3.83% |
| T=2s | 40.42% | 21.96% | 15.64% | 12.64% | 10.93% |
| T=3s | 44.54% | 25.94% | 18.99% | 15.64% | 13.67% |
| T=4s | 46.06% | 28.18% | 21.37% | 17.89% | 15.83% |

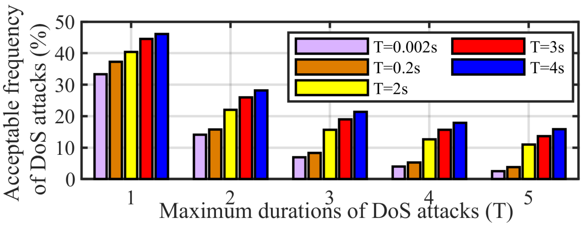

Figure 6: Acceptable frequencies of DoS attacks in Area 1 for given PI controller

First, for a given PI controller $[K_{Pi}, K_{Ii}] = [0.1, 0.1]$ with $i = 1, 2, 3$, the acceptable frequencies of DoS attacks of area 1 are calculated and listed in Table 2 based on Algorithm 1 with $n = 1$ and $\mu = 1.001$. For comparison with the proposed LFC scheme in Peng et al. [2016], we give the results under smaller sampling periods of $T = 0.002s$ and $0.2s$. The results for areas 2 and 3 are similar and omitted due to space limitations. To analyse the data more intuitively, the results of area 1 are displayed as a bar chart in Fig. 6. It can be seen from the results of Table 2 and Fig. 6 that the acceptable attack frequencies of the given PI controller decrease with increasing maximum attack duration. In addition, as the sampling period increases, the frequency of DoS attacks that the controller can tolerate increases under the unified attack duration. The results show that the proposed method can simultaneously analyse the relationship between the duration and frequency of DoS attacks under smaller or larger sampling periods. However, the method proposed in Peng et al. [2016] can only analyse the relationship between the attack duration and system stability. By substituting the system parameters into the method in Peng et al. [2016], we obtain that the maximum DoS attack duration is $4T$ under $T = 0.002\ s$, while the maximum DoS attack durations are shorter than $1T$ under $T \geq 0.02\ s$. Therefore, with a larger sampling period, the method in Peng et al. [2016] becomes unfeasible, while the method proposed in this paper is still feasible. This illustrates the effectiveness and superiority of the proposed method.

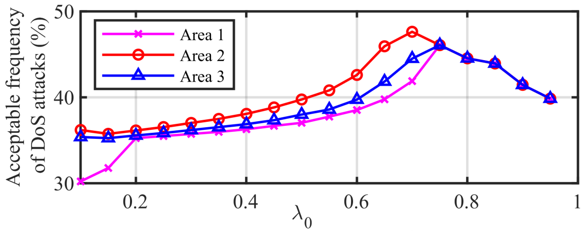

Figure 7: Relationship between the maximum attack frequencies and $\lambda_0$ in three areas under the sensor sampling period of $T = 3s$ and the maximal attack duration of $1T$

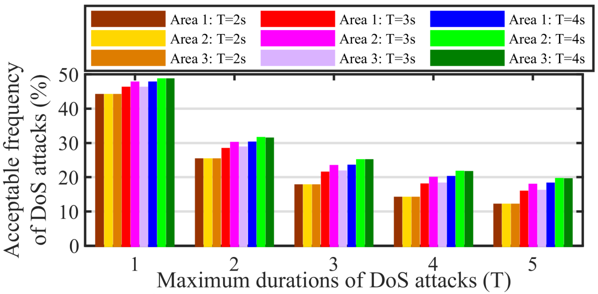

Figure 8: Maximum frequencies of DoS attacks in traditional three-area power system for unknown PI controllers

Second, when the PI controllers are unknown, the maximum acceptable attack frequencies are obtained by adjusting the exponential decay rate $\lambda_0$ of the stable subsystem with switching signal $\sigma(t_k) = 0$. Specifically, we give the relationship between the maximum acceptable frequencies and $\lambda_0$ for three areas under a sensor sampling period of $T = 3s$ and maximal attack duration of $1T$, as shown in Fig. 7. From this figure, it can be seen that with increasing $\lambda_0$, the maximum attack frequencies of the three areas increase first and then decrease. Area 2 reaches the maximum value at $\lambda_0 = 0.7$, while areas 1 and 3 are maximized at $\lambda_0 = 0.75$. In general, the results obtained in the three areas are the same when $\lambda_0 \geq 0.75$, while the results of area 2 are the highest and the results of area 1 are the lowest. The results under $T = 1\ s$ and $T = 2\ s$ are similar and omitted due to space limitations. Through the repetition of the above method, the results of the acceptable frequencies of DoS attacks in three areas are developed based on Algorithm 2, which are listed in Table 3. Additionally, these results are presented in Fig. 8 in a bar chart form. From these results, it can be found that as the maximum duration of the DoS attack increases, the maximum attack frequencies in the three areas all decrease. Additionally, when the sampling period changes from 2 s to 4 s, the maximum attack frequencies obtained in the three area increase slightly. The maximum attack frequencies in the three areas are almost the same under identical sampling periods and attack durations. These results can be used to guide the following controller design.

Table 3: Acceptable frequency of DoS attacks for different durations of DoS attacks in traditional three-area power system under different sampling periods

| Duration | 1T | | | 2T | | | 3T | | | 4T | | | 5T | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Period | T=2s | T=3s | T=4s | T=2s | T=3s | T=4s | T=2s | T=3s | T=4s | T=2s | T=3s | T=4s | T=2s | T=3s | T=4s |
| Area 1 | 43.92% | 46.06% | 47.61% | 25.16% | 28.18% | 30.07% | 17.58% | 21.31% | 23.31% | 13.95% | 17.83% | 20.00% | 11.97% | 15.76% | 18.12% |
| Area 2 | 43.92% | 47.61% | 48.49% | 25.16% | 29.96% | 31.42% | 17.58% | 23.22% | 24.88% | 13.95% | 19.79% | 21.54% | 11.97% | 17.78% | 19.45% |
| Area 3 | 43.92% | 46.06% | 48.49% | 25.16% | 28.59% | 31.24% | 17.58% | 21.59% | 24.88% | 13.95% | 18.11% | 21.45% | 11.97% | 15.99% | 19.38% |

### *4.1.2. Controller design*

The updated period of measurements and control signals in the LFC process is set to $T = 3s$. That is the sampling period of the sensor of this system is 3 s. Additionally, the execution period of the actuator in the LFC process is set to $T_0 = 1s$, which means that $n = T/T_0 = 3$. Based on the above stability analysis, to develop a maximum acceptable frequency for DoS attacks, the PI controller gains are calculated by selecting the exponential decay rates $\lambda_0 = 0.75, 0.7, 0.75$ of the stable subsystem in the three areas based on Algorithm 2. The obtained controller gains in the three areas are $K_1 = [0.0741\ 0.1379]$, $K_2 = [0.0893\ 0.1623]$, and $K_3 = [0.0741\ 0.1379]$, respectively.

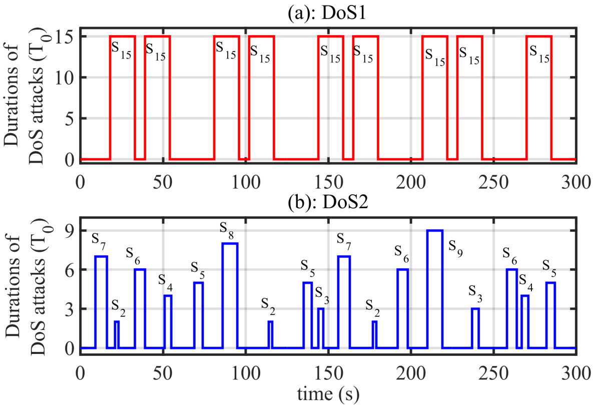

Figure 9: Detailed diagram of DoS attacks, DoS1 and DoS2

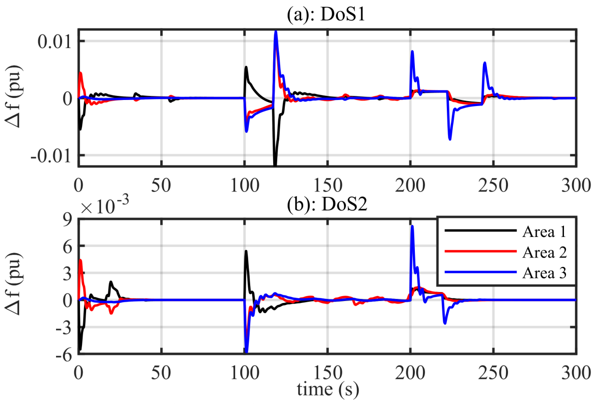

Figure 10: Responses of system frequency deviation in three areas under two DoS attacks and load disturbances

To validate the effectiveness of the proposed controller, assume that two DoS attacks, as shown in Fig. 9, are applied in each control area. In Fig. 9(a), the maximum duration of the DoS attack (named DoS1) is $5T$ during a period of 300 s. The frequency of DoS1 can be calculated by $f_u = \frac{\Sigma_{j=1}^{mn} n_j}{n_0+\Sigma_{j=1}^{mn} n_j} = \frac{9}{9+(300-9\times15)/3} = 14.06\%$. Similarly, these parameters are $3T$ and 20.24%, respectively, in Fig. 9 (b) (called DoS2). The three-area power system is tested under these two DoS attacks and load disturbances (19). The responses of frequency $\Delta_f$ and control input $\Delta P_c$ of the system are shown in Figs. 10 and 11, respectively. Sub-figures (a) and (b) represent the impacts of DoS1 and DoS2 on the power system, respectively. From Figs. 10 and 11, it can be found that the system frequency deviation is driven to zero under the action of the designed controller, and the control input deviation tends to a constant value. This illustrates that the controller designed in this paper can maintain the balance between generation and load under these two DoS attacks and load disturbances (19).

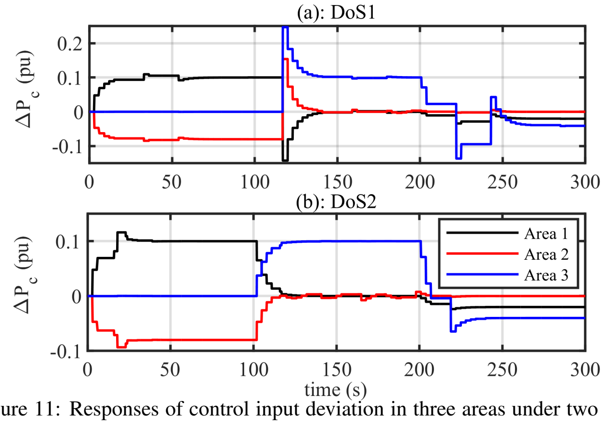

Figure 11: Responses of control input deviation in three areas under two DoS attacks and load disturbances

### *4.1.3. Test of DoS attack defence*

Based on the above designed controller, we test the scheme of DoS attack defence as introduced in Algorithm 3. Assume that the sampling period of the sensor of this system is $T = 3\ s$, and the execution period of the actuator in the LFC process is set to $T_0 = 1\ s$, which means $n = T/T_0 = 3$. Additionally, the detection period is set to 60 $s$, and the DoS attack shown in Fig. 12 occurs in the LFC process. The DoS attack has real maximum duration of $4T$ and frequency of $f_r = 38.45\%$ during interval $[0, 60]$ s, $5T$ and $f_r = 30.00\%$ in $[60, 180]$ s, and $5T$ and $f_r = 12.50\%$ in $[180, 240]$ s, and there are no DoS attacks during $[240, 300]$ s. A comparison of the results obtained in Table 3 shows that the detected attack frequencies exceed the scheduled values at $t = 60$, 120, 180 s. Therefore, the main communication channel (S1) is switched to the standby communication channel (S2) at times 60, 120, 180 s, and the standby channel is switched to the main channel at $t = 240$ s. When the power system is subjected to load disturbances (19), the responses of the system frequency deviation in the three areas are shown in Fig. 13. To highlight the effectiveness of the proposed scheme, we also show the responses of the system frequency deviation under no DoS attack defence action in Fig. 13. Compared to the two responses in Fig. 13, it is not difficult to find that when the

Table 4: Parameters of LFC scheme of deregulated three-area power system

| | k-i: the $k_{th}$ generator of area i | | | | | | | Control area | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1-1 | 2-1 | 1-2 | 2-2 | 1-3 | 2-3 | | 1 | 2 | 3 |
| $T_{ch}$(s) | 0.32 | 0.30 | 0.30 | 0.32 | 0.31 | 0.34 | M (pu·s) | 0.1667 | 0.2084 | 0.1600 |
| $T_g$ (s) | 0.06 | 0.08 | 0.06 | 0.07 | 0.08 | 0.06 | D(pu/Hz) | 0.0084 | 0.0084 | 0.0080 |
| $R$(Hz/pu) | 2.4 | 2.5 | 2.5 | 2.7 | 2.8 | 2.4 | $\beta$ (pu/Hz) | 0.4250 | 0.3966 | 0.3522 |
| $\alpha$ | 0.5 | 0.5 | 0.5 | 0.5 | 0.6 | 0.4 | $T_{ij}$(pu/rad) | $T_{12} = 0.245, T_{13} = 0.212, T_{23} = 0$ | | |

load fluctuates at $t = 100$ s, the strategy of switching the channel to the standby channel without a DoS attack significantly improves the control performance, which reduces the duration and peak value of the frequency fluctuation.

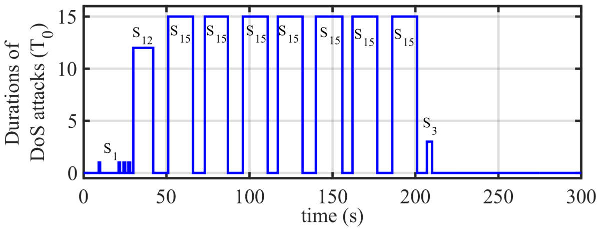

Figure 12: Detailed diagram of DoS attacks

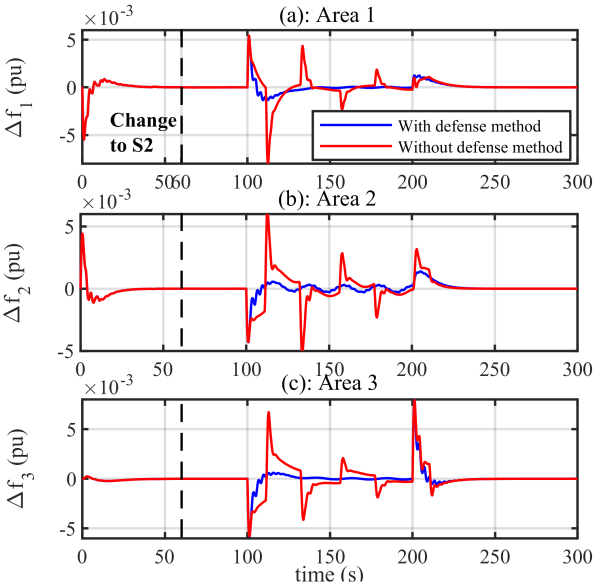

Figure 13: Responses of system frequency deviation in three areas with and without DoS attack defense scheme

### 4.2. A deregulated three-area power system

To investigate the feasibility of the proposed approach on a deregulated power market environment, a case study is undertaken based on a deregulated three-area power system. The LFC structure for the three-area power system is shown in Fig. 1 with dotted line connections. Each area of the power system comprises two Gencos and two Discos, and their parameters are listed in Table 4 (Shayeghi et al. [2006]).

#### 4.2.1. Stability analysis

The Parameters are set to sensor sampling periods of $T = 2$ s, 3 s and 4s , $n = 1$ and $\mu = 1.001$. First, the stability of the power system is analysed under a given PI controller $[K_{Pi}, K_{Ii}] = [0.1, 0.1]$ with $i = 1, 2, 3$. The acceptable frequencies of DoS attacks in area 2 are developed based on Algorithm 1. These results are given in Table 5, and are shown as a bar chart in Fig. 14. The results of areas 1 and 3 are similar and omitted due to space limitations. Similar to the results in traditional three-area power systems, the values of acceptable maximum attack frequency increase slightly under the same maximum attack duration when the sampling period changes from 2 s to 4 s. In addition, with increasing maximum attack duration, the values of the acceptable maximum attack frequency decrease under the same sampling period.

Table 5: Acceptable frequency of DoS attacks for different durations of DoS attacks in Area 2 under different sampling periods

| Durations | $1T$ | $2T$ | $3T$ | $4T$ | $5T$ |
|---|---|---|---|---|---|
| T=2s | 40.42% | 21.96% | 15.57% | 12.61% | 10.88% |
| T=3s | 44.54% | 25.94% | 19.05% | 15.67% | 13.69% |
| T=4s | 46.06% | 28.32% | 21.37% | 17.92% | 15.85% |

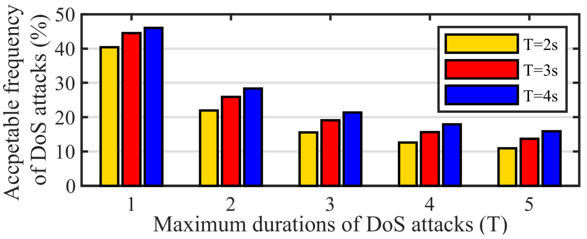

Figure 14: Acceptable frequency of DoS attacks in Area 2 under given PI controller

Second, the stability of power system is analysed under an unknown PI controller. With the aid of Algorithm 2, the acceptable frequencies of DoS attacks in three areas are calculated and are shown in Table 6 and as a bar chart in Fig. 15. From these results, the relationship among the system stability and the attack frequency, attack durations and sampling periods is similar to the relationship obtained in the above analysis for a given PI controller.

#### 4.2.2. Controller Design

The sampling period of the sensor and the execution period of the actuator in the LFC process are set to $T = 3$ s and $T_0 = 1$ s, respectively, which means $n = T/T_0 = 3$. With the maximum attack duration set to $5T$ and with the use of the method in Algorithm 2, PI controller gains of $K_1 = [0.0411\ 0.2304]$, $K_2 = [0.0758\ 0.2653]$, and $K_3 = [0.0894\ 0.2654]$ in three areas are derived where the exponential decay rates of the stable subsystem in three areas$\lambda_0$ are 0.55, 0.45, and 0.45, respectively.

To show the effectiveness of the proposed controller, the power system is tested in combination with Poolco

Table 6: Acceptable frequency of DoS attacks for different durations of DoS attacks in deregulated three-area power system under different sampling periods

| Duration | 1T | | | 2T | | | 3T | | | 4T | | | 5T | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Period | T=2s | T=3s | T=4s | T=2s | T=3s | T=4s | T=2s | T=3s | T=4s | T=2s | T=3s | T=4s | T=2s | T=3s | T=4s |
| Area 1 | 48.49% | 49.49% | 49.88% | 31.42% | 33.88% | 36.13% | 24.96% | 27.94% | 30.74% | 21.56% | 24.74% | 27.73% | 19.47% | 22.69% | 25.76% |
| Area 2 | 49.49% | 49.88% | 49.93% | 33.88% | 36.13% | 36.13% | 27.94% | 30.72% | 30.74% | 24.74% | 27.68% | 27.73% | 22.69% | 25.74% | 25.76% |
| Area 3 | 49.49% | 49.88% | 49.88% | 33.70% | 36.13% | 36.13% | 27.91% | 30.72% | 30.74% | 24.74% | 27.68% | 27.73% | 22.67% | 25.74% | 25.76% |

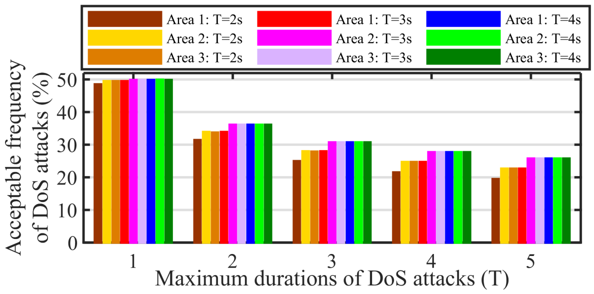

Figure 15: Acceptable frequencies of DoS attacks in deregulated three-area power system under unknown PI controllers

and bilateral-based transactions in a deregulated environment Shayeghi et al. [2006]. The generation rate constraints of each control area are assumed to be ±0.1 pu/min as given in Shayeghi et al. [2006]. Additionally, we assume that all the Discos contract with the Gencos as the following AGPM:

$$\text{AGPM} = \begin{bmatrix} 0.25 & 0 & 0.25 & 0 & 0.5 & 0 \\ 0.5 & 0.25 & 0 & 0.25 & 0 & 0 \\ 0 & 0.5 & 0.25 & 0 & 0 & 0 \\ 0.25 & 0 & 0.5 & 0.75 & 0 & 0 \\ 0 & 0.25 & 0 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Assume that the contracted demands of the Discos $\Delta P_{Lj-i}$ with $i = 1, 2, 3$ and $j = 1, 2$ exist in each area, and their values change from 0.05 pu in $t \in [60, 150]$ s to 0.1 pu in $t \in [150, 300]$ s. Additionally, Disco 1 in area 1 and area 2 and Disco 2 in area 3 demand 0.05 pu, 0.04 pu, and 0.03 pu, respectively, as an uncontracted load in $t \in [0, 150]$s, and their values change to -0.05 pu, -0.04 pu, and -0.03pu, respectively, in $t \in [150, 300]$s.

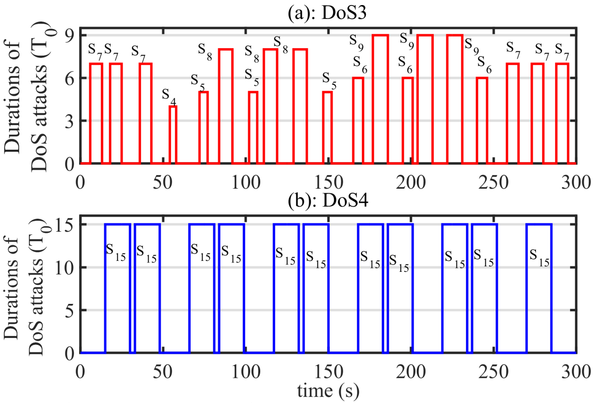

Figure 16: Detailed diagram of DoS attacks in deregulated power system

Then, the closed-loop system is tested for two DoS attacks shown in Fig. 16. The responses of the frequency deviation $\Delta f$, control input $\Delta P_c$, and generator mechanical output $\Delta P_m$ of the power system are shown in Figs. 17-19. In Fig. 16(a), the maximum durations and frequencies of the DoS attack (named DoS3) are $3T$ and 27.53% respectively, while they are $5T$ and 19.64%, respectively, in Fig. 16(b) (called DoS4) during the period of 300 s. Sub-figures (a) and (b) in Figs. 17-19 represent the impacts of DoS3 and DoS4 on the power system, respectively. From the results, it can be found that the frequency deviations of the three areas are driven back to zero after unbalanced generation and load, and the control input deviations of the three areas are adjusted to constant values. Additionally, the actual generated powers of the Gencos properly reach their desired values as calculated by the definition of $\Delta P_{mk-i}$. Specifically, $\Delta_{Pm1-1} = \Delta_{Pm2-1} = 0.075$ pu, $\Delta_{Pm1-2} = 0.065$ pu, $\Delta_{Pm2-2} = 0.140$ pu, $\Delta_{Pm1-3} = 0.057$ pu, and $\Delta_{Pm2-3} = 0.088$ pu after $t > 150$ $s$. Noted that the values of maximum durations and frequencies of the two DoS attacks are no greater than the corresponding theoretical margin obtained in Table 6.These results show the effectiveness of the designed controller and the accuracy of the stability analysis in Table 6.

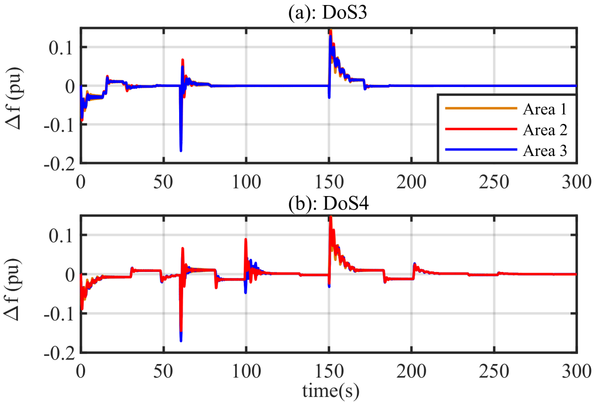

Figure 17: Frequency deviation of deregulated three-area power system under two DoS attacks. (a): DoS3; (b): DoS4.

### 4.2.3. *Test of DoS attack defence*

Here, based on the above designed controller, the LFC scheme of DoS attack defence proposed in Algorithm 3 is tested in a deregulated three-area power system. Similarly, the sampling period of the sensor and the execution period of the actuator are set to $T = 3$ s and $T_0 = 1$ s, respectively, which means $n = T/T_0 = 3$. The detection period is set to 60 s. Additionally, assume that the power system is subjected to DoS attack, as shown in Fig. 20. The DoS attack has a maximum duration of $3T$ and frequency of $f_r = 54.55\%$ during interval $[0, 60]$ s, then $5T$ and $f_r = 28.57\%$ in $[60, 120]$ s, $5T$ and $f_r = 33.33\%$ in $[120, 180]$ s, and $5T$ and $f_r = 12.50\%$ in $[180, 240]$ s, and there no DoS attack during $[240, 300]$ s. Note that the scheduled maximum durations and frequencies are $3T$, $f_u = 27.94\%$

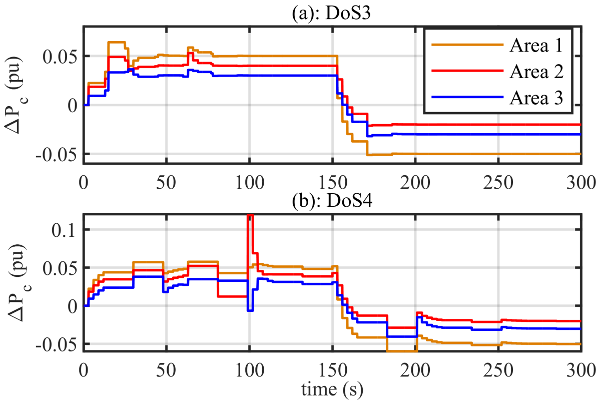

Figure 18: Control input deviation of deregulated three-area power system under two DoS attacks. (a): DoS3; (b): DoS4.

and $5T$, $f_u = 22.64\%$, as listed in Table 6. Therefore, the detected attack frequencies of this DoS attack are greater than the scheduled values at times $t = 60, 120, 180$ s. According to Algorithm 3, the communication channel switches from main channel (S1) to standby channel (S2) during interval $[60, 240]$ s. Then, the standby channel (S2) is switched to the main channel (S1) at $t = 240$ s.

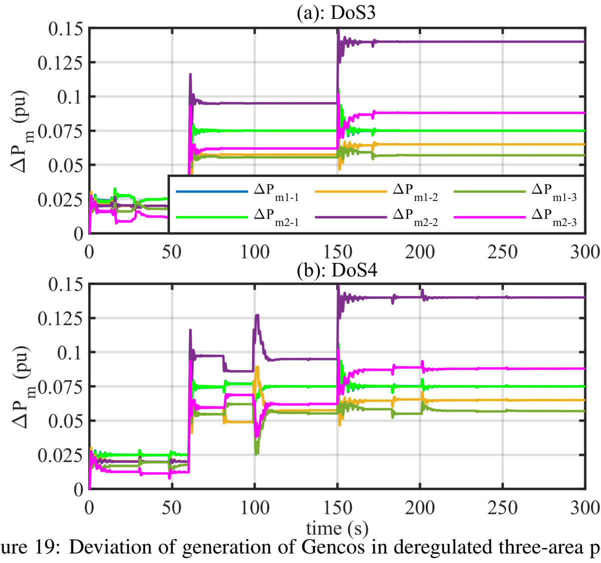

Figure 19: Deviation of generation of Gencos in deregulated three-area power system under two DoS attacks. (a): DoS3; (b): DoS4.

When the power system is subjected to the contracted and uncontracted demands of the Discos as described in the above controller design, the responses of system frequency deviation are given by using and not using the proposed defence scheme. The responses are shown in Fig. 21. When the demand fluctuates at 60 s and 150 s, the system frequency deviation is quickly driven back to zero after using the proposed LFC scheme. However, when the proposed LFC scheme is not used, it is difficult to restore the balance between power generation and demand during [60, 150] s. Additionally, after the change in demand at 150 s, it takes more time to drive the frequency back to zero and the frequency fluctuation is severe. Therefore, the difference in the control performance with and without  shows the advantages of the proposed LFC scheme in defending against DoS attacks. In addition, it can be found that the system frequency still changes significantly at the time instants of 0, 60 and 150 s. The obvious spur in the frequency is caused by the changes in the contracted and un-contracted demands of the Discos. At these points, regardless of whether the DoS attack defence scheme is used, there is a large frequency change.

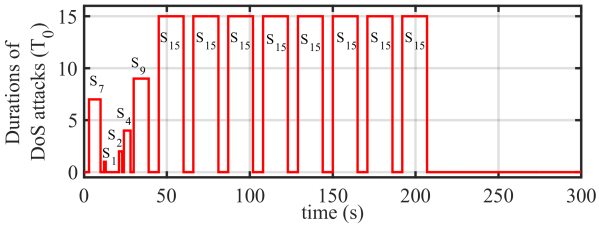

Figure 20: Detailed diagram of DoS attack in deregulated power system

### *4.3. Discussion*

1) The stability analysis results of the LFC scheme obtained through switching system theory are still conservative. In the tests of the DoS attacks defence in the above two cases, when the communication channel is not switched, it is not difficult to find that although the detected DoS attack frequency exceeds the scheduled value, resulting in a drastic frequency response and a long recovery time, the system remains stable. This shows that the upper bound calculated in this paper is not an accurate margin of what that the LFC scheme can withstand.

2) In this paper, the design of an LFC scheme ignores the presence of communication delays in the transmission of control signals and measurements. However, the delays are inevitable and may affect the performance of the LFC scheme, as noted in Zhang et al. [2013a] and Zhang et al. [2013b]. Therefore, in the future, we will improve the proposed LFC scheme by considering communication delays.

3) In the test of the DoS attacks defence in the deregulated three-area power system, if the DoS attack is detected with a period of 300 s, it can obtain the maximum attack duration and frequency with $5T$ and 20.63%, respectively. As listed in Table 6, the values of the attack duration and frequency do not exceed the scheduled value. There is no action to switch channels at this time. This worsens the effect of the proposed LFC, but the whole system can still maintain the frequency stability. However, when 60 s is used as the detection period in the simulation, the impact of the doS attacks on the frequency response is largely mitigated. Therefore, the selection of the detection period affects the control performance of the proposed control scheme. A small detection period may cause frequent channel switching, while a large detection period may degrade the frequency response performance.

4) As stated in Sun et al. [2020a], the event-triggered communication scheme has significant impacts on the reduce of the communication burden of the communication network. It has been used to conserve network sources in the LFC scheme in Peng et al. [2018]. In the future, how to effectively defend against DoS attacks in LFC schemes based on event-triggered communication scheme deserves further study. Moreover, the finite-time control method has been widely used to ensure the

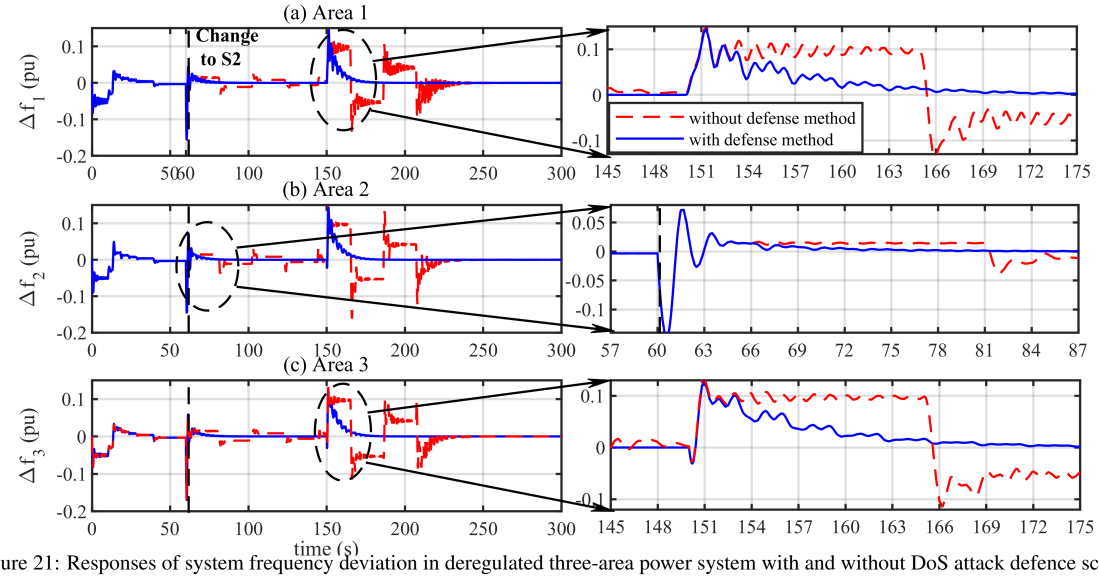

Figure 21: Responses of system frequency deviation in deregulated three-area power system with and without DoS attack defence scheme

control performance of the system within the finite time (Sun et al. [2019, 2020b]). In practical power systems, the regulation of frequency and voltage needs to be adjusted to a prescribed value in a limited time. Ensuring the frequency stability of the system in a limited time under DoS attacks needs to be further studied in the future.

## 5. Conclusion

In this paper, a resilient LFC scheme for a multi-area power system for defence against DoS attacks was investigated based on switching system theory. By analysing the duration and frequency of DoS attacks, we developed the stability condition of the LFC scheme under DoS attacks. Additionally, the PI controller gains of the LFC scheme that can resist DoS attacks with a certain duration and frequency could be determined based on this stability condition. To be able to defend against serious DoS attacks, the resilient LFC scheme was proposed based on the designed PI controller and the dual-loop communication network equipped with this controller. When there is a serious DoS attack in the main communication channel, the communication channel is switched from the main channel to the standby channel to mitigate the impact of the DoS attack. Simulation tests have been undertaken on the traditional three-area power system and the deregulated three-area power system. The simulation results have shown that the LFC scheme with the designed PI controller can tolerate DoS attacks with a certain degree of duration and frequency. Additionally, when a serious DoS attack occurs on the main communication channel, the proposed resilient LFC scheme can be implemented to switch the main communication channel to a standby channel to mitigate the impact of DoS attacks.

In the future, combined with the proposed method, the event-triggered communication scheme and finite-time control method will be considered as potential future research directions for LFC schemes under DoS attacks.

## Appendix A. Proof for theorem 1

Firstly, some lemmas are shown as follows.

**Lemma 3:** System (10) is said to be exponentially stable with exponential decay rate $\lambda$ if for every finite initial state $x(t_0) \in \Re^n$, there exist positive constants $c$ and $\lambda < 1$ such that the following inequality holds

$$\|x(t_k)\| \le c\lambda^{t_k} \|x(t_0)\|. \tag{A.1}$$

**Lemma 4:** [Zhai et al. [2002]]For any switching signal $\sigma(t_k)$ and any $t_k \ge 1$, let $N_\sigma[t_0, t_k)$ denote the number of switching points of $\sigma(t_k)$ over the time interval $[t_0, t_k)$. If $N_\sigma[t_0, t_k) \le N_0 + (t_k - t_0)/T_a$ holds for $N_0 \ge 0$ and $T_a > 0$, then $T_a$ is called the average dwell time and $N_0$ the chatter bound.

The subsystem with switching signal $\sigma(t_k) = j$ of system (10) is $S_{ci-j} : x_i(t_{k+1}) = A_{i-j}x_i(t_k) + B_{i-j}x_i(t_{k-1}), j \in \mathbb{H}$. Choose the following Lyapunov functional for subsystem $j$.

$$V_{i-j}(t_k)=x_i^T(t_k)P_jx_i(t_k) + x_i^T(t_{k-1})Q_jx_i(t_{k-1}) \tag{A.2}$$

Denote $\eta(t_k) = [x_i^T(t_k), x_i^T(t_{k-1})]^T$. Then by using inequality (11), one can obtain that $V_{i-j}(t_{k+1}) - \lambda_j^2 V_{i-j}(t_k) = x_i^T(t_{k+1})P_jx_i(t_{k+1}) + x_i^T(t_k)Q_jx_i(t_k) - \lambda_j^2 x_i^T(t_k)P_jx_i(t_k) - \lambda_j^2 x_i^T(t_{k-1})Q_jx_i(t_{k-1}) = \eta^T(t_k)\Xi_j\eta(t_k) < 0$. That is to say

$$V_j(t_{k+1}) < \lambda_j^2 V_j(t_k). \tag{A.3}$$

Then, for the whole switching system (10), we choose the Lyapunov functional: $V_{i-\sigma(t_k)}(t_k) = x_i^T(t_k)P_{\sigma(t_k)}x_i(t_k) + x_i^T(t_{k-1})Q_{\sigma(t_k)}x_i(t_{k-1})$. For the switching signal $\sigma(t_k)$, we let $t_{k1} < \cdots < t_{kl}$, $l \ge 1$ denote the switching points of $\sigma(t_k)$ during the time interval $[t_0, t_k)$. Noted that the state of system (10) does not jump at the switching points. Then by applying inequality (12), one can obtain

$$V_{i-\sigma(t_{kl})}(t_{kl}) \le \mu V_{i-\sigma\left(t_{k(l-1)}\right)}(t_{kl}). \tag{A.4}$$

The inequality (13) can be rewritten as follows:

$$\frac{n_0}{\sum_{j=1}^{mn} n_j} \ge \frac{\ln\lambda_b - \ln\lambda}{\ln\lambda - \ln\lambda_0} \tag{A.5}$$

Combining $\lambda_0 < \lambda$ and (A.5), one can obtain that $\sum_{j=0}^{mn} n_j \ln \lambda_j = \sum_{j=0}^{0} n_j \ln \lambda_j + \sum_{j=1}^{mn} n_j \ln \lambda_j$ $\leq n_0 \ln \lambda_0 + \left(\sum_{j=1}^{mn} n_j\right) \ln \lambda_b \leq \sum_{j=0}^{mn} n_j \ln \lambda$. Such inequality implies $\prod_{j=0}^{mn} \lambda_j^{2n_j} \leq \lambda^{2t_k}$. By combining (A.3)–(A.5) and Lemma 5, obtain by induction $V_{i-\sigma(t_k)}(t_k) < \lambda_{\sigma(t_{kl})}^{2(t_k - t_{kl})} V_{i-\sigma(t_{kl})}(t_{kl}) \leq$ $\mu \lambda_{\sigma(t_{kl})}^{2(t_k - t_{kl})} V_{i-\sigma\left(t_{k(l-1)}\right)}(t_{kl}) \cdots \leq$ $\mu^{N_\sigma[t_0, t_k)} \lambda_{\sigma\left(t_{k_l}\right)}^{2(t_k - t_{kl})} \lambda_{\sigma\left(t_{k(l-1)}\right)}^{2\left(t_{kl} - t_{k(l-1)}\right)} \cdots \lambda_{\sigma(t_0)}^{2(t_{k1} - t_0)} V_{i-\sigma(t_0)}(t_0) =$ $\mu^{N_\sigma[t_0, t_k)} \prod_{j=0}^{mn} \lambda_j^{2n_j} V_{i-\sigma(t_0)}(t_0) \leq \mu^{N_\sigma[t_0, t_k)} \lambda^{2t_k} V_{i-\sigma(t_0)}(t_0)$ $= \rho^{2t_k}(\lambda, T_a) V_{i-\sigma(t_0)}(t_0)$, where $\rho(\lambda, T_a) = \lambda \mu^{1/(2T_a)}$. Then, we can obtain that $\xi_1 \|x(t_k)\|^2 \leq V_{i-\sigma(t_k)}(t_k) < \rho^{2t_k}(\lambda, T_a) \xi_2 \|x(t_0)\|^2$, where $\xi_1 = \min \lambda_{\min}\left(P_j\right)$ and $\xi_2 = \max(\lambda_{\max}\left(P_j\right) + \lambda_{\max}\left(Q_j\right))$, and $\lambda_{\min}(\Delta)$ and $\lambda_{\max}(\Delta)$ are, respectively, the maximum and minimum eigenvalues of $\Delta$. Calculating the above inequality, we obtain $\|x(t_k)\| < \sqrt{\xi_2/\xi_1} \rho^{t_k}(\lambda, T_a) \|x(t_0)\|$. Also, the inequality (14) and $\lambda < 1$ guarantee $\rho(\lambda, T_a) < 1$. Therefore, based on the Lemma 3, system (10) is exponentially stable with an exponential decay rate $\rho(\lambda, T_a)$. This completes the proof.

## Appendix B. Proof for theorem 2

The following lemma is used to derive the theorem.

**Lemma 5:** [Hu et al. [2007]]For matrices $\Gamma$, $P > 0$, and $Q > 0$, the inequality $\Gamma^T Q \Gamma - P < 0$ holds if and only if there exists a matrix $Y$ such that

$$\begin{bmatrix} -P & \Gamma^T Y^T \\ Y\Gamma & -Y - Y^T + Q \end{bmatrix} < 0 \tag{B.1}$$

Based on Lemma 5, inequality (11) holds if there exists a matrix $Y$ such that the following inequality holds

$$\begin{bmatrix} -\lambda_j^2 P_j + Q_j & 0 & A_{i-j}^T Y \\ * & -\lambda_j^2 Q_j & B_{i-j}^T Y \\ * & * & -Y - Y^T + P_j \end{bmatrix} < 0 \tag{B.2}$$

Inequality (B.2) implies that $Y$ is invertible. Denote $X = Y^{-1}$, $\Upsilon = K_i C_i X$, $R_j = X^T P_j X$, and $S_j = X^T Q_j X$. Pre and post multiply (B.2) by $diag\{X^T, X^T, X^T\}$ and $diag\{X, X, X\}$, respectively. Then inequality (16) is obtained. So, if inequality (16) is true, (11) holds. Also, Pre and post multiply inequalities $P_\alpha \leq \mu P_\beta$ and $Q_\alpha \leq \mu Q_\beta$ by $X^T$ and $X$, respectively. Then, inequality (17) is obtained. If inequality (17) is true, (12) holds. Therefore, based on Theorem 1, as long as (13), (15), (16), and (17) hold, system (10) is exponentially stable. Moreover, the gain of $K_i$ can be calculated by $K_i = \Upsilon X^{-1} C_i^T (C_i C_i^T)^{-1}$. This completes the proof.

## Appendix C. References

Alhelou, H. H., Hamedani-Golshan, M. E., Zamani, R., Heydarian-Forushani, E., and Siano, P. (2018). Challenges and opportunities of load frequency control in conventional, modern and future smart power systems: A comprehensive review. *Energies*, 34, 2497.

Alhelou H. H., Hamedani-Golshan M. E. and Hatziargyriou N. D. (2019). A decentralized functional observer based optimal LFC considering unknown inputs, uncertainties, and cyber-attacks. *IEEE Trans. Power Syst.*, 34, 4408-4417.

Cheng Z., Yue D., Hu S., Huang C., Dou C. and Chen L. (2020). Resilient load frequency control design: DoS attacks against additional control loop. *Int. J. Electr. Power Energy Syst.*, 115, 105496.

Farwell J. P. and Rohozinski R. (2011). Stuxnet and the future of cyber war. *Survival*, 53, 23–40.

Help Net Security(2018). DDoS attack frequency grows 40%, low volume attacks dominate. *https://www.helpnetsecurity.com/2018/09/13/ddos-attack-frequency-grows/.*

Hu, L. S., Bai, T., Shi, P. and Wu, Z. (2007). Sampled-data control of networked linear control systems. *Automatica*, 43, 903–911.

Jiang L., Yao W., Wu Q. H., Wen J. Y. and Cheng S. J. (2012). Delay-dependent stability for load frequency control with constant and time-varying delays. *IEEE Trans. Power Syst.*, 27, 932–941.

Jin L., Zhang C. K., He Y., Jiang L., Wu M. (2019) Delay-dependent stability analysis of multi-area load frequency control with enhanced accuracy and computation efficiency. *IEEE Trans. Power Syst.*, 34, 3687–3696.

Khodabakhshian, A., Edrisi M. (2008). A New Robust PID Load Frequency Controller. *Control Eng. Pract.*, 16, 1069–1080.

Kumar P. A. R., Selvakumar S. (2013). Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. *Comput. Commun.*, 36, 303–319.

Kundur P. (1994). *Power System Stability and Control*. New York: Mc Graw Hill.

Lee R., Assante M. and Conway T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid *Electr. Inf. Sharing Anal. Center*.

Li Y., Zhang P. and Ma L. (2019). Denial of service attack and defense method on load frequency control system. *J. Franklin Inst.*, 356, 8625–8645.

Liu S., Liu X. P. and Saddik A. (2013). Denial-of-service (DoS) attacks on load frequency control in smart grids. *IEEE PES Innovative Smart Grid Technol. Conf.*, 1–6.

Liu X., Zhang Y., Lee K.Y. (2016). Robust distributed MPC for load frequency control of uncertain power systems. *Control Eng. Pract.*, 56, 23–47.

Liu J., Gu Y., Zha L. and Cao J. (2019). Event-triggered load frequency control for multiarea power systems under hybrid cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.*, 49, 1665–1678.

Peng C., Li J. and Fei M. (2016). Resilient event-triggering load frequency control for multi-area power systems with energy-limited DoS attacks. *IEEE Trans. Power Syst.*, 32, 4110–4118.

Pandey S. K., Mohanty S. R., Kishor N. (2013). A literature survey on load-frequency control for conventional and distribution generation power systems. *Renewable Sustainable Energy Rev.*, 25, 318-334.

Peng C., Zhang J., Yan H. (2018). Adaptive event-triggering $H_\infty$ load frequency control for network-based power systems. *IEEE Trans. Ind. Electron.*, 65, 1685–1694.

Saxena S., Hote Y. V. (2017). Stabilization of perturbed system via IMC: An application to load frequency control. *Control Eng. Pract.*, 64, 61-73.

Sun K., Qiu J., Karimi H. R. and Gao H. (2019). A novel finite-time control for nonstrict feedback saturated nonlinear systems with tracking error constraint. *IEEE Trans. Syst. Man Cybern.: Syst.*, to be publised. Doi: 10.1109/TSMC.2019.2958072.

Sharma J., Hote Y. V., Prasad R. (2019). PID controller design for interval load frequency control system with communication time delay. *Control Eng. Pract.*, 89, 154-168.

Shayeghi H., Shayanfar H. A., and Jalili A. (2006) Multi-stage fuzzy PID power system automatic generation controller in deregulated environments *Energy Convers. Manage.* 47, 2829–2845.

Shayeghi H., Jalili A. and Shayanfar H. A. (2007). Robust modified GA based multi-stage fuzzy LFC. *Energy Convers. Manage.*, 48, 1656-1670.

Shayeghi H., Shayanfar H. A., Jalili A. (2009). Load frequency control strategies:A state-of-the-art survey for the researcher. *Energy Convers. Manage.*, 50, 344-353.

Shang-Guan X., Jin L., He Y., Zhang C. K., Jiang L., Wu M. (2020) Switching method based load frequency control for power system with energy-limited dos attacks. *Proceedings of the 21st IFAC World Congress*, 2020, to be published.

Sun K., Qiu J., Karimi H. R. and Fu Y. (2020a). Event–triggered robust fuzzy adaptive finite-time control of nonlinear systems with prescribed performance. *IEEE Trans. Fuzzy Syst.*, to be published. Doi: 10.1109/TFUZZ.2020.2979129.

Sun K., Liu L., Qiu J. and Feng G. (2020b). Fuzzy adaptive finite–time fault-tolerant control for strict-feedback nonlinear systems. *IEEE Trans. Fuzzy*

*Syst.*, to be pubulished. Doi: 10.1109/TFUZZ.2020.2965890.

Teumim D. J. (2010). *Industrial network security*. ISA.

Zhai, G., Hu B., Yasuda K. and Michel A. N. (2002). Qualitative analysis of discrete-time switched systems. *2002 Am. Control Conf.*, 3, 1880–1885.

Zhang, W. A., Yu L. (2008). New approach to stabilisation of networked control systems with time-varying delays. *IET Control Theory Appl.*, 2, 1094–1104.

Zhang C. K., Jiang L., Wu Q. H., He Y. and Wu M. (2013a). Delay-dependent robust load frequency control for time delay power systems. *IEEE Trans. Power Syst.*, 28, 2192-2201.

Zhang C. K., Jiang L., Wu Q. H., He Y., Wu M. (2013b). Further results on delay-dependent stability of multi-area load frequency control. *IEEE Trans. Power Syst.*, 28, 4465–4474.

Zhou X., Gu Z., Yang F.. (2019) Resilient event-triggered output feedback control for load frequency control systems subject to cyber attacks. *IEEE Access*, 7, 58951–58958.