Switching Method Based Load Frequency Control for Power System with Energy-Limited DoS Attacks ⋆

Xingchen Shang-Guan [*,**,***] Li Jin [*,**,***] Yong He [*,**,‡]
Chuan-Ke Zhang [*,**] Lin Jiang [***]
Joseph William Spencer [***] Min Wu [*,**]

[*] *School of Automation, China University of Geosciences, Wuhan 430074, China*
[**] *Hubei Key Laboratory of Advanced Control and Intelligent Automation for Complex Systems, Wuhan, 430074, China*
[***] *Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom*

Abstract: A load frequency control (LFC) scheme for modern power systems employs an open communication network to transmit control/measurement signals. The usage of the open communication network in power system makes the LFC scheme more vulnerable to communication network attacks, for example, a denial-of-service (DoS) attack. This attack will prevent a certain amount of transmission of the signals so as to degrade the performance of LFC scheme, or even lead to instability of power system. Therefore, this paper concerns LFC scheme for single-area power system with energy-limited DoS attack based on switching method. Compared with the latest schemes only considering duration of a DoS attacks, the proposed LFC takes fully into account both the duration and attack frequency of the DoS attack. A switching LFC model for a single-area power system is firstly constructed based on the characteristic of periodical sampling and DoS attacks. Then, an exponential stability criterion is developed in terms of the duration and frequency of a DoS attack. Next, a feasible controller of LFC scheme is derived by solving linear matrix inequalities in the criterion. Finally, a detailed design algorithm of LFC scheme is presented for a known DoS attack or an unknown DoS attack. The effectiveness of the proposed LFC scheme is evaluated on a single-area power system under DoS attacks. The proposed LFC scheme is compared with a robust LFC scheme and an event-triggered H_∞ LFC scheme. The obtained contrasting results demonstrate that the proposed LFC scheme can defend DoS attacks with limited energy, and can perform better control effect in the presence of load fluctuations.

Keywords: Power system, Load frequency control, Open communication network, Switching system, DoS attacks, Exponential stability.

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]). In an interconnected power system, the main objective of LFC is to restore the balance between load and generation in each control area (Shayeghi et al. [2009]). Traditionally, an LFC scheme employs dedicated channels to transmit control signals and measurements. Yet, 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 widely studied in LFC scheme to support the increasingly decentralized property of control services (referring to Shayeghi et al. [2007] and Zhang et al. [2013b]). However, the application of open network technology in the power grid makes the LFC system more vulnerable to various network attacks. Such attacks may cause a serious impact on system stability and even social stability. Typical cases are that the management system of supervisory control and data acquisition distribution in Ukrainian was attacked by a foreign attacker as noted in Lee et al. [2016] and an Iranian nuclear power station at Natanz was attacked by StuxNet virus as reported in Farwell et al. [2011]. The Ukrainian blackout affected approximately 225, 000 customers, while the attacks in the Iranian resulted in 60% hosts damaged. Therefore, it is urgent to solve the adverse effects caused by network attacks for an effective LFC scheme.

A denial-of-Service (DoS) attack is one of network attacks. DoS attacks corrupt the availability by blocking the transmission medium, which results in the loss of useful information. Up to date, many researchers have made significant effort on the LFC scheme to defend DoS attacks. Regarding DoS attacks as networked induced sent disturbances, some robust LFC schemes for interconnected power system have been developed in Dong et al. [2012]

⋆ This work was supported in part by the National Natural Science Foundation of China under Grants 61973284 and 61873347, by the Hubei Provincial Natural Science Foundation of China under Grants 2019CFA040, by the 111 project under Grant B17040, and by the Program of China Scholarship Council under Grant 201706410012 and 201706410037.

[**‡] Corresponding author: Yong He (e-mail: heyong08@cug.edu.cn).

and Zhang et al. [2013a]. Yet, such robust schemes did not consider the detailed model of DoS attack to design LFC scheme. Different from the above scheme, by introducing DoS attacks into modeling of LFC scheme, Liu et al. [2013] proved that the existence of DoS attacks make the dynamics of a power system unstable, including convergence and steady-state errors, based on switched system theories. By considering the effect of energy-limited DoS attacks, Peng et al. [2016] designed a resilient event-triggered communication scheme that allows a degree of packet losses induced by 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 in Peng et al. [2016] employ single loop LFC scheme without the additional control, and thus a resilient design of additional control law for a multi-area power system is proposed. An unknown input functional observer based optimal LFC approach was presented to handle network attacks in Alhelou et al. [2019]. To detect and defend the DoS attacks, Wang et al. [2019] established a co-simulation technology-based platform. A deep auto-encoder extreme learning machine algorithm was introduced to predict and supplement lost data, and thus to ensure the normal operation of the LFC system in Li et al. [2019]. However, most of the above methods focus on the stability analysis of LFC scheme, considering only the durations of DoS attacks. The useful and significant information of DoS attacks, attack frequency, has not yet been introduced to design an LFC scheme. The analysis of attack frequency is helpful for the detection of DoS attack in LFC process. Therefore, the stability and design of LFC scheme under DoS attacks have not been fully investigated, which motivates this research effort.

Based on the above discussions, this paper explores the stability analysis and the controller design of LFC scheme for a single-area power system under energy-limited DoS attacks. The proposed LFC scheme considers fully the attack frequency of DoS attack, which is different from the existing schemes considering only the attack duration in Peng et al. [2016] and Cheng et al. [2020]. Considering both the frequency and the duration can more accurately characterize the process of DoS attacks, so that the stability analysis and controller design of LFC scheme are more effective. An exponential stability criterion and a controller design algorithm are developed for LFC scheme with the aid of the switching method in Zhang et al. [2008]. The usage of the exponential stability theory can not only ensure the stable operation of the LFC scheme under DoS attacks, but also provide better performance in system frequency response than the schemes in Dong et al. [2012] and Liu et al. [2019].

The remainder of this paper is organized as follows. Section 2 gives the switching system model of LFC for a single-area power system. Section 3 proposes an LFC design algorithm. In Section 4, a case study based on a single-area power system is shown to verify effectiveness of the proposed LFC scheme. Conclusion is given in Section 5.

2. SWITCHING LFC MODEL FOR A SINGLE-AREA POWER SYSTEM

This section describes a switching LFC model for single-area power system. At first, a linear LFC model for single-area power system is introduced under open communication network. Then, a detailed descriptions of modeling a switching LFC model is illustrated under the DoS attacks.

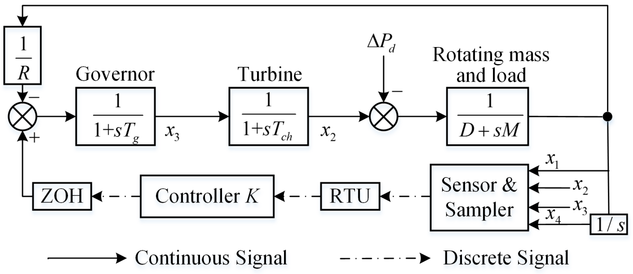

Fig. 1. LFC structure of a single-area power system.

2.1 Single-area power system

As shown in Fig. 1, the dynamic LFC model of single-area power system can be expressed as follows (Zhang et al. [2013a]):

$$\dot{x}(t) = \bar{A}x(t) + \bar{B}u(t) + \bar{F}\omega(t) \tag{1}$$

where

$$x^T = [\Delta f,\ \Delta P_m,\ \Delta P_v],\quad u = \Delta P_C,\quad \omega = \Delta P_d$$

$$\bar{A} = \begin{bmatrix} -\frac{D}{M} & \frac{1}{M} & 0 \\ 0 & -\frac{1}{T_{ch}} & \frac{1}{T_{ch}} \\ -\frac{1}{RT_g} & 0 & -\frac{1}{T_g} \end{bmatrix}, \bar{B} = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{T_g} \end{bmatrix}, \bar{F} = \begin{bmatrix} -\frac{1}{M} \\ 0 \\ 0 \end{bmatrix},$$

and $\Delta f, \Delta P_m, \Delta P_v, \Delta P_d$ and ΔP_C are the deviation of frequency, generator mechanical output, valve position, load and control input, respectively; M, D, T_g, T_{ch}, R represent the moment of inertia of generator unit, generator unit damping coefficient, time constant of the governor, time constant of the turbine, and speed droop, respectively.

In the LFC scheme, in order to force the steady state of Δf to tend to zero, the integral of Δf is used as an additional state. It is defined as $\Delta E = K_I \int \Delta f d(t)$, where K_I is the gain of integral controller. Redefine the state vector as $x^T = [\Delta f\ \Delta P_m\ \Delta P_v\ \Delta E]$. Then system (1) is written as

$$\dot{x}(t) = Ax(t) + Bu(t) + F\omega(t) \tag{2}$$

where

$$A = \begin{bmatrix} \bar{A} & 0 \\ [K_I\ 0\ 0] & 0 \end{bmatrix},\ B = \begin{bmatrix} \bar{B}^T & 0 \end{bmatrix}^T,\ F = \begin{bmatrix} \bar{F}^T & 0 \end{bmatrix}^T.$$

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 studied in this paper can be summarized as follows

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{3}$$

2.2 Modeling for LFC under energy-limited DoS attacks

Firstly, we assume that the actuator is periodical time-triggered, while the controller is event-triggered. Assume that the LFC system is subjected to DoS attacks under $[kT, (k+m)T]$, where T is the sampling period of the sensor and $m \in M \triangleq \{1, 2, \cdots, \bar{M}\}$, $\bar{M}$ is the largest integer in the finitely set M. The value m describes the duration of the DoS attacks, and the $\bar{M}$ is the largest one of the durations. Here, a new sampling time $t_0, t_1, \cdots, t_l, l \in N$ is defined as the updated time of controller signals, then the set of new sampling period of system (3) is $h_k = t_{k+1} -$

$t_k \in MT$ with $k \in N$. Then, the LFC system (3) can be rewritten as follows:

$$\dot{x}(t)=Ax(t)+\xi Bu(t_k)+(1-\xi)Bu(t_{k-1}), t = [t_k, t_{k+1}) \quad (4)$$

where, $\xi = 0$ or 1, and $\xi = 0$ denotes the system is subjected to DoS attacks; $\xi = 1$ denotes the system is not subjected to DoS attacks.

In order to alleviate the impact of DoS attacks, we will reconstruct LFC system model in terms of execution period of the actuator. Assume that $T_0 = T/n$ and T_0 is the execution period of the actuator. Then, the sampling period of system (4) is mnT_0. The detailed time slots under DoS attacks are shown in Fig. 2. From this diagram, it can be seen that two control signals $u\left(t_{k-1}\right)$ and $u\left(t_k\right)$ 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 $h_k = \varpi_1(k)T_0 + \varpi_0(k)T_0 = mnT_0$.

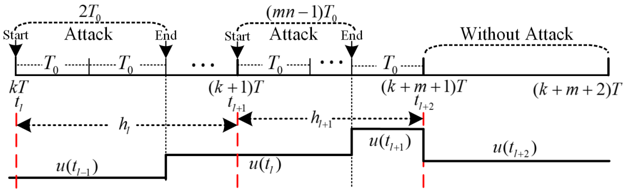

Fig. 2. Time slots of an LFC process under DoS attacks

Then, based on the above analysis, the system (4) can be rewritten the following discrete model.

$$x\left(t_{k+1}\right)=A(h_k)x(t_k)+B\left(h_k\right)u\left(t_k\right)+B(h_{k-1})u(t_{k-1}) \quad (5)$$

where $A\left(h_k\right) = e^{Ah_k}$, $B\left(h_k\right) = \int_{\varpi_1(k)T_0}^{h_k} e^{As}Bds$, $B\left(h_{k-1}\right) = \int_0^{\varpi_1(k)T_0} e^{As}Bds$. Defining $A_0{=}e^{AT_0}$, $B_0{=}\int_0^{T_0} e^{As}Bds$, we can obtain $A\left(h_k\right) = e^{AmnT_0} = \left(e^{AT_0}\right)^{mn} = A_0^{mn}$, $B\left(h_k\right) = \int_{\varpi_1(k)T_0}^{h_k} e^{As}Bds = A_0^{\varpi_1(k)} \sum_{j=0}^{\varpi_0(k)-1} \int_{jT_0}^{(j+1)T_0} \times e^{As}Bds = A_0^{\varpi_1(k)} \sum_{j=0}^{\varpi_0(k)-1} A_0^j B_0 = \sum_{i=\varpi_1(k)}^{mn-1} A_0^i B_0$, and $B\left(h_{k-1}\right) = \int_0^{\varpi_1(k)T_0} e^{As}Bds = \sum_{i=0}^{\varpi_1(k)-1} \int_{i_0}^{(i+1)T_0} e^{As}Bds = \sum_{i=0}^{\varpi_1(k)-1} A_0^i B_0$. Then, the system (5) is equivalent to

$$x\left(t_{k+1}\right)=A_0^{mn}x\left(t_k\right) + \sum_{i=\varpi_1(k)}^{mn-1} A_0^i B_0 u\left(t_k\right) + \sum_{i=0}^{\varpi_1(k)-1} A_0^i B_0 u\left(t_{k-1}\right) \quad (6)$$

In the above model, when $m \in M, n$ is given, $\varpi_1(k)$ can take different values in the set $\mathbb{H} = \{0, 1, 2, \cdots, Mn\}$ to make the system (6) exist in different forms. Therefore, the above system can be rewritten as the following switching system model.

$$S_{o\sigma(t_k)}\colon x\left(t_{k+1}\right)=A_0^{mn}x\left(t_k\right)+B_{o\sigma(t_k)}u\left(t_k\right)+\tilde{B}_{o\sigma(t_k)}u\left(t_{k-1}\right) \quad (7)$$

where $B_{o\sigma(t_k)} = \sum_{i=\varpi_1(k)}^{mn-1} A_0^i B_0$, $\tilde{B}_{o\sigma(t_k)}{=}\sum_{i=0}^{\varpi_1(k)-1} A_0^i B_0$, and $\sigma\left(t_k\right) = \varpi_1(k) \in \mathbb{H}$ is the switching signal. Noted that if $\sigma\left(t_k\right) = 0$, the subsystem is not subjected to DoS attacks, and meanwhile $B_{o0} = \sum_{i=0}^{n-1} A_0^i B_0$ and $\tilde{B}_{o0} = 0$. Also, when $\varpi_1(k) = mn$, the subsystem will be subjected to DoS attacks with the whole duration of mnT_0, and $B_{omn} = 0$, $\tilde{B}_{omn} = \sum_{i=0}^{mn-1} A_0^i B_0$.

Lastly, we choose the following state-feedback control law as shown in Fig. 1.

$$u\left(t_k\right) = Kx\left(t_k\right) \quad (8)$$

Combining the system (7) and control law (8), the closed switching system of LFC for single-area power system can be obtained as follows:

$$S_{c\sigma(t_k)} : x\left(t_{k+1}\right) = A_{\sigma(t_k)}x\left(t_k\right) + B_{\sigma(t_k)}x\left(t_{k-1}\right) \quad (9)$$

where $A_{\sigma(t_k)} = A_{o\sigma(t_k)} + B_{o\sigma(t_k)}K, B_{\sigma(t_k)} = \tilde{B}_{o\sigma(t_k)}K$.

Under the impact of switching law $\sigma\left(t_k\right)$, assume the subsystem with $\sigma\left(t_k\right) = 0$, which is not subjected to DoS attacks, is stable. When $\sigma\left(t_k\right) = 1, 2, \cdots$, the system will become more unstable. Assume that the total activation number of stable and unstable subsystems over the time $[t_0, t_k)$ are denoted $\mathbb{G}_s$ and $\mathbb{G}_u$, respectively. Meanwhile, denoting $f_s = \frac{\mathbb{G}_s}{t_k}$ and $f_u = \frac{\mathbb{G}_u}{t_k}$ are the existing frequencies of the stable and unstable subsystems, respectively. Assume that system (9) has $s+1$ stable subsystems, and S_j, $j = \mathbb{H}_s = \{0, 1, \cdots, s\}$ are the stable ones. So, the system has $mn - s$ unstable subsystems, and S_j, $j = \mathbb{H}_u = \{s+1, s+2, \cdots, mn\}$ are the unstable ones. Then, we can derive the following theorems (Zhang et al. [2008]).

3. DESIGN OF LFC SCHEME WITH DOS ATTACKS

In this section, a design method of a LFC scheme for a single-area power system with DoS attacks is introduced. An exponential stability conditions are presented to assure the stability of the LFC of power system. Then, a theorem of controller design is proposed based on the above stability conditions. At last, a design procedure for LFC scheme is summarised.

3.1 Stability criterion and controller design method of LFC scheme for a single-area power system

Theorem 1. Consider system (9), for given scalars $\lambda_j > 0$, $\lambda_a = \max(\lambda_j | j \in \mathbb{H}_s)$, $\lambda_b = \max(\lambda_j | j \in \mathbb{H}_u)$, $\mu \geq 1$, and $\lambda < 1$ with $\lambda_a < \lambda < \lambda_b$, if there exist appropriate matrixes $P_j \geq 0$, $Q_j \geq 0$, $j \in \mathbb{H}$ such that the following inequalities hold

$$\Xi_j = \begin{bmatrix} A_j^T P_j A_j - \lambda_j^2 P_j + Q_j & A_j^T P_j B_j \\ B_j^T P_j A_j & B_j^T P_j B_j - \lambda_j^2 Q_j \end{bmatrix} < 0 \quad (10)$$

$$P_\alpha \leq \mu P_\beta, Q_\alpha \leq \mu Q_\beta, \alpha, \beta \in \mathbb{H} \quad (11)$$

$$\frac{f_s}{f_u} \geq \frac{\ln \lambda_b - \ln \lambda}{\ln \lambda - \ln \lambda_a} \quad (12)$$

$$T_a > \bar{t}_a \triangleq \frac{\ln \mu}{2\ln(1/\lambda)} \quad (13)$$

where T_a is the average dwell time as defined in Lemma 4 in Appendix A. Then, the system (9) is exponentially stable with exponential decay rate $\rho\left(\lambda, T_a\right) = \lambda\mu^{1/(2T_a)}$.

The proof is shown in Appendix A.

Remark 1: In real power system, the average dwell time T_a cannot be determined in advance due to the variation of 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

$$\frac{\ln u}{2\ln(1/\lambda)} < T \quad (14)$$

then it can guarantee inequality (13) holds no matter how DoS attacks change.

Due to $f_s + f_u = 1$, the inequality (12) can be rewritten as follows:

$$f_u \leq \bar{f}_u \triangleq \frac{1}{\left(\ln \lambda_b - \ln \lambda\right) / \left(\ln \lambda - \ln \lambda_a\right) + 1} \quad (15)$$

When controller K in system (9) is unknown, Theorem 1 is no longer an LMI-based condition due to a product of $A_j^T P_j B_j$. In order to obtain a feasible controller K, the following Theorem 2 is shown to derive the controller parameters.

Theorem 2. For preset scalars $\lambda_j > 0$, $\lambda_a = \max(\lambda_j | j \in \mathbb{H}_s)$, $\lambda_b = \max(\lambda_j | j \in \mathbb{H}_u)$, $\mu \geq 1$, and $\lambda < 1$ with $\lambda_a < \lambda < \lambda_b$, if there exist appropriate matrices X, Υ, $R_j \geq 0$, $S_j \geq 0$, $j \in \mathbb{H}$, such that (14), (15) and the following inequalities hold

$$\begin{bmatrix} -\lambda_j^2 R_j + S_j & 0 & X^T A_{oj}^T + \Upsilon^T B_{oj}^T \\ * & -\lambda_j^2 S_j & \Upsilon^T \tilde{B}_{oj}^T \\ * & * & -X - X^T + R_j \end{bmatrix} < 0 \quad (16)$$

$$R_\alpha \leq \mu R_\beta,\ S_\alpha \leq \mu S_\beta,\ \alpha, \beta \in \mathbb{H} \quad (17)$$

then system (9) is exponentially stable with a decay rate $\rho(\lambda, t_a) = \lambda \mu^{1/(2T_a)}$, and the controller gains can be calculated by

$$K = \Upsilon X^{-1} \quad (18)$$

The proof is shown in Appendix B.

3.2 Design procedure of LFC scheme for single-area power system under energy-limited DoS attacks

In this subsection, we will introduce an algorithm to present the design procedure of LFC scheme for single-area power system under DoS attacks. The objective is to find feasible controller gains K and λ. The detailed procedure is shown as the following Algorithm 1.

```
Algorithm 1: Find $K$ and $\lambda$

Step 1: Preset system (4) parameters $A$, $B$, and sampling period
        $T_0$ of actuator and $T = nT_0$ of sensor.
Step 2: Evaluate the largest duration and frequency of DoS attack,
        denote $mnT_0$ and $f_{\max}$, respectively.
Step 3: Preset $s + 1$ stable subsystem; set $\lambda_j$ with $j \in$
        $\{0, 1, \cdots, mn\}$ and $\mu$; then determine $\lambda_a = \max(\lambda_j | j \in$
        $\mathbb{H}_s)$ and $\lambda_b = \max(\lambda_j | j \in \mathbb{H}_u)$.
Step 4: Find $K$.
    1) Check the feasibility of LMIs (16) and (17) under the given
       $\mu$ and $\lambda_j$.
    2) If (16) and (17) are true, determine feasible solutions of
       $X$ and $\Upsilon$; else, go to Step 3 and modify $\lambda_j$.
    3) Calculate $K$ based on (18).
Step 5: Find $\lambda$.
    1) Initialize $\lambda_{\min} = \lambda_a$, $\lambda_{\max} = 1$, and select the accuracy
       coefficient $\lambda_{ac} = 0.0001$.
    2) Check the feasibility of inequalities (14) and $\bar{f}_u \geq f_{\max}$ in
       (15) under $\lambda_{test} = (\lambda_{\min} + \lambda_{\max})/2$.
    3) If (14) and $\bar{f}_u \geq f_{\max}$ are feasible, set $\lambda_{\min} = \lambda_{test}$; else,
       set $\lambda_{\max} = \lambda_{test}$.
    4) If $|\lambda_{\min} - \lambda_{\max}| \leq \lambda_{ac}$, set $\lambda = \lambda_{\min}$.
    5) If $\lambda > \lambda_a$, obtain $\lambda$; else, go to Step 3 and modify $\lambda_j$.
Step 6: Output $K$ and $\lambda$.
```

Remark 2: The selection of λ_j determines the control performance of the designed frequency controller for the single-area power system. In the Steps 4 and 5 of this algorithm, we can design a feasible controller to resist the possible DoS attack by adjusting appropriate values of λ_j.

4. CASE STUDIES

To illustrate the effectiveness of the proposed approach, the case study has been carried out based on a single-area power system. The dynamic model of LFC scheme for the single-area power system is described in subsection 2.1 and is governed by (2). The standard nominal values of the parameters are shown in Table 1 as reported in Liu et al. [2019]. The updated period of measurements and control signals in LFC process is set to $T = 3s$. That is, the sampling period of the sensor of this system is 3s. Also, the execution period of the actuator in LFC process is set to $T_0 = 1s$, which means that $n = T/T_0 = 3$. Moreover, we simulate the system for load disturbance (in pu)

$$\Delta P_d(t) = \begin{cases} 0.06, & 0s \leq t < 100s \\ 0.003\sin(0.3t), & 100s \leq t < 200s \\ -0.02, & 200s \leq t \leq 300s \end{cases} \quad (19)$$

Table 1. Parameters of LFC scheme of single-area power system

D	M	R	T_g	T_{ch}	K_I
1 pu/Hz	10 pu·s	0.05 Hz/pu	0.1s	0.3s	1

4.1 LFC scheme design under known DoS attacks

In the following design procedure, the LFC schemes for single-area power system are designed based on a known DoS attack model. Assume that the LFC of the single-area power system is subjected to the known DoS attack, as shown in Fig. 3. Based on this diagram, one can obtain that the largest durations is $9T_0 = 3T$. Also, the activated switching subsystems consist of S_0, S_1, S_3, S_4, S_5, S_6, S_7, S_8, and S_9, and their detailed activated times are 59, 16, 1, 1, 2, 2, 3, 1 and 1, respectively. Then, we can represent the interval of DoS attack in terms of new sampling time $[t_0, t_{86})$, and obtain $M = \{1, 2, 3\}$, $\bar{M} = 3$ and $H = \{0, 1, \cdots, 9\}$. Choose the stable subsystems is S_0. Next, based on the procedure of the algorithm in section 3.2 and by setting $\mu = 1.001$, $\lambda_0 = 0.40$, $\lambda_1 = 1.2$, $\lambda_2 = 2.4$, $\lambda_3 = 3.5$, $\lambda_4 = 4.1$, $\lambda_5 = 4.52$, $\lambda_6 = 5.8$, $\lambda_7 = 5.9$, $\lambda_8 = 6.3$, and $\lambda_9 = 6.95$ in every subsystem, respectively, we can determine $\lambda_a = 0.4$ and $\lambda_b = 6.95$. Then, based on Step 4 in Algorithm 1, we obtain a feasible controller gain matrix K_1 for the LFC scheme, and

$$K_1 = [-2.7997 - 0.0840 - 0.0280 - 5.8795]. \quad (20)$$

Based on Step 5 in Algorithm 1, we can get $\lambda = 0.9998$. Also, the maximum acceptable DoS attack frequency is $\bar{f}_u = 32.09\%$. From the detailed attacks durations in Fig. 3, we can obtain the real attack frequency is $f = 27/86 \approx 31.40\% < \bar{f}_u$. Thus, by Theorem 2, the LFC scheme for the single-area power system controlled by the designed K_1 is exponentially stable. Moreover, choose $N_0 = 0$, and the average dwell time $T_a = 300/54 \approx 5.3571s > T = 3s > \bar{t}_a = 2.2742$ in (13) of Theorem 1. Thus, the system has an exponential decay rate $\rho = \lambda\mu^{1/(2T_a)} = 0.9999$.

4.2 Simulation Verification

To illustrate the effectiveness and superiority of the proposed LFC scheme, we compared three LFC schemes to defend DoS attacks:

1) the event-triggered H_∞ LFC scheme considering only the duration of DoS attacks in Liu et al. [2019], and the proposed PI controller $K_2 = [-0.0571, -0.0109]$;

2) the robust LFC scheme without considering DoS attacks in Dong et al. [2012], and the proposed PI controller $K_3 = [-3.27e-4, -0.3334]$;

3) the proposed LFC scheme considering the duration and frequency of DoS attacks in this paper, the designed state-feedback controller K_1 as shown in equation (20).

The system controlled by the above three controllers is tested under load disturbances $\Delta P_d(t)$ in (19). Deviations of frequency of the power system are depicted in Fig. 4. It

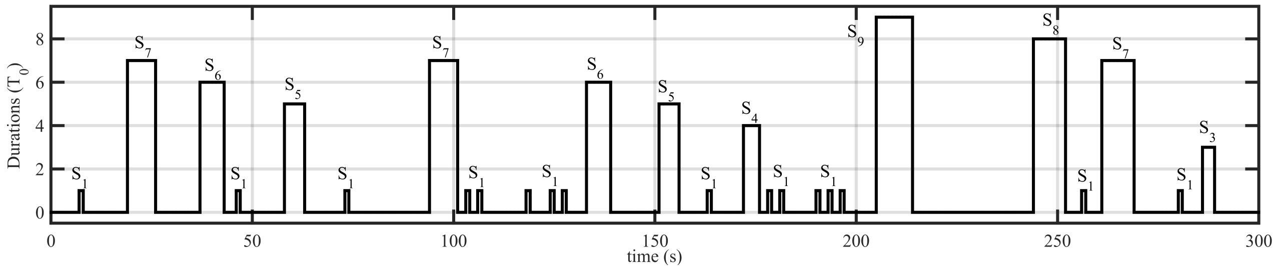

Fig. 3. Detailed time slots of the known DoS attack

can be seen that K_1 can drive the system frequency back to the scheduled frequency under load disturbances, and it takes shorter time and shows smaller frequency deviation than controllers K_2 and K_3.

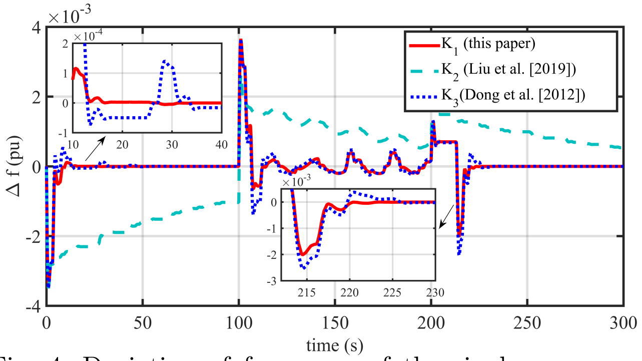

Fig. 4. Deviation of frequency of the single-area power system under controllers K_1, K_2, and K_3.

4.3 LFC scheme design under unknown DoS attacks

The diagram of DoS attacks can not be always determined precisely. In this case, we can roughly estimate the maximum durations and frequency of DoS attacks to design feasible LFC scheme based on Algorithm 1. Similarly, some feasible parameters of λ_j can be selected to develop controller gains of LFC scheme. Subsystem S_0 is considered as stable switching subsystem.With the aid of Theorem 2, we calculated the maximum acceptable DoS attack frequency of LFC scheme under different DoS attack durations and actuator execution periods. The detailed results are shown in Table 2. From this table, we can determine the feasibility of the LFC scheme to defend certain DoS attacks as long as the DoS attacks meet the calculated maximum durations and attack frequency. The feasible controller gains of the LFC scheme can be developed by Algorithm 1.

Table 2. Maximum acceptable DoS attack frequency of LFC scheme under different DoS attack durations and actuator execution periods

Durations	m=1	m=2	m=3	m=4	m=5
$T/T_0 = 3$	49.95%	39.25%	32.09%	24.90%	22.33%

Remark 3: The proposed method can be easily extended into multi-area power based on the decentralised strategy. As noted in Dong et al. [2012] and Zhang et al. [2013a] that the interactions between different areas can be treated as disturbances. Therefore, the design of multi-area LFC schemes under DoS attacks can be simplified to a repetitive single-area design problem.

Remark 4: In this paper, the design of an LFC scheme ignores the presence of communication delays in the transmission of control signals and measurements. Yet the delays are inevitable, and may affect the performance of LFC scheme as noted in Zhang et al. [2013a] and Zhang et al. [2013b]. So, in the future, we will improve the proposed LFC scheme by considering communication delays.

5. CONCLUSION

In this paper, an LFC scheme for single-area power system has been investigated to defend an energy-limited DoS attack based on a switching method. By considering the durations and frequency of DoS attacks, an exponential stability criterion has been developed. A detailed procedure has been proposed to design a feasible LFC scheme by evaluating the durations and frequency of DoS attacks. The proposed scheme has been tested on a single-area power system under a known DoS attack. The obtained results have illustrated the effectiveness of the proposed LFC on defending the DoS attack. Also, the results have shown that the proposed scheme took a shorter time to recover system frequency to the scheduled value and performed a smaller frequency deviation than other schemes.

REFERENCES

Alhelou H. H., Golshan M. E. H. 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.

Dong L., Zhang Y. and Gao Z. (2012). A robust decentralized load frequency controller for interconnected power systems. *ISA trans.*, 51, 410–419.

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

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

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 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.

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

Wang Q., Tai W., Tang Y., Zhu H., Zhang M. and Zhou D. (2019). Coordinated defense of distributed denial of service attacks against the multi-area load frequency control services. *Energies*, 12, 2493.

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.

Appendix A. PROOF FOR THEOREM 1

Firstly, some lemmas are shown as follows.

Lemma 3. System (9) is said to be exponentially stable with exponential decay rate λ 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 te chatter bound.

The subsystem of system (9) is $S_j : x(t_{k+1}) = A_j x(t_k) + B_j x(t_{k-1}), j \in \mathbb{H}$. Choose the following Lyapunov functional for the subsystem.

$$V_j(t_k) = x^T(t_k) P_j x(t_k) + x^T(t_{k-1}) Q_j x(t_{k-1}) \tag{A.2}$$

Denote $\eta(t_k) = [x^T(t_k), x^T(t_{k-1})]^T$. Then by using inequality (10), one can obtain that $V_j(t_{k+1}) - \lambda_j^2 V_j(t_k) = x^T(t_{k+1}) P_j x(t_{k+1}) + x^T(t_k) Q_j x(t_k) - \lambda^2 x^T(t_k) P_j x(t_k) - \lambda^2 x^T(t_{k-1}) \Xi_j x(t_{k-1}) = \eta^T(t_k) \Omega_j \eta(t_k) < 0$. 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 (9), we choose the Lyapunov functional: $V_{\sigma(t_k)}(t_k) = x^T(t_k) P_{\sigma(t_k)} x(t_k) + x^T(t_{k-1}) Q_{\sigma(t_k)} x(t_{k-1})$. For the switching signal $\sigma(t_k)$, we let $t_{k1} < \cdots < t_{ki}, i \ge 1$ denote the switching points of $\sigma(t_k)$ during the time interval $[t_0, t_k)$. Note that the state of system (9) does not jump at the switching points. Then by applying inequality (11), one can obtain

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

Based on the definitions of f_s and f_u, the inequality (12) can be rewritten as follows:

$$\frac{\mathbb{G}_s}{\mathbb{G}_u} = \frac{\sum_{j=0}^{s} n_j}{\sum_{j=s+1}^{mn} n_j} \ge \frac{\ln\lambda_b - \ln\lambda}{\ln\lambda - \ln\lambda_a} \tag{A.5}$$

Combining $\lambda_a < \lambda$ and (A.5), one can obtain that $\sum_{j=0}^{mn} n_j \ln\lambda_j = \sum_{j=0}^{r} n_j \ln\lambda_j + \sum_{j=r+1}^{mn} n_j \ln\lambda_j \le \left(\sum_{j=0}^{r} n_j\right) \ln\lambda_a + \left(\sum_{j=r+1}^{mn} n_j\right) \ln\lambda_b = \mathbb{G}_s \ln\lambda_a + \mathbb{G}_u \ln\lambda_b \le (\mathbb{G}_s + \mathbb{G}_u) \ln\lambda = \sum_{j=0}^{mn} n_j \ln\lambda$, where n_j denotes the number of activation of subsystem S_j over $[t_0, t_k)$. Such inequality implies $\prod_{j=1}^{mn} \lambda_j^{2n_j} \le \lambda^{2t_k}$. By combining (A.3)–(A.5) and Lemma 5, obtain by induction $V_{\sigma(t_k)}(t_k) < \lambda_{\sigma(t_{ki})}^{2(t_k - t_{ki})} V_{\sigma(t_{ki})}(t_{ki}) \le \mu \lambda_{\sigma\left(t_{k_i}\right)}^{2\left(t_k - t_{k_i}\right)} V_{\sigma\left(t_{k(i-1)}\right)}(t_{ki}) \cdots \le \mu^{N_\sigma[t_0,t_k)} \lambda_{\sigma\left(t_{k_i}\right)}^{2(t_k - t_{ki})} \lambda_{\sigma\left(t_{k(i-1)}\right)}^{2\left(t_{ki} - t_{k(i-1)}\right)} \cdots \lambda_{\sigma(t_0)}^{2(t_{k1} - t_0)} V_{\sigma(t_0)}(t_0) = \mu^{N_\sigma[t_0,t_k)} \prod_{j=1}^{mn} \lambda_j^{2n_j} V_{\sigma(t_0)}(t_0) \le \mu^{N_\sigma[t_0,t_k)} \lambda^{2t_k} V_{\sigma(t_0)}(t_0) = \rho^{2t_k}(\lambda, T_a) V_{\sigma(t_0)}(t_0)$, where $\rho(\lambda, T_a) = \lambda\mu^{1/(2T_a)}$. Then, we can obtain that $\xi_1 \|x(t_k)\|^2 \le V_{\sigma(t_k)}(t_k) < \rho^{2t_k}(\lambda, t_a) \xi_2 \|x(t_0)\|^2$, where $\xi_1 = \min_{j\in\mathbb{H}} \lambda_{\min}(P_j)$ and $\xi_2 = \max_{j\in\mathbb{H}}(\lambda_{\max}(P_j) + \lambda_{\max}(Q_j))$, and $\lambda_{\min}(\Delta)$ and $\lambda_{\max}(\Delta)$ are, respectively, the maximum and minimum eigenvalues of Δ. 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 (13) and $\lambda < 1$ guarantee $\rho(\lambda, T_a) < 1$. Therefore, based on the Lemma 3, system (9) 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 Γ, $P > 0$, 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 (10) holds if there exists a matrix Y such that the following inequality holds

$$\begin{bmatrix} -\lambda^2 P_j + Q_j & \theta & A_j^T Y \\ * & -\lambda_j^2 Q_j & B_j^T Y \\ * & * & -Y - Y^T + P_j \end{bmatrix} < 0 \tag{B.2}$$

Inequality (B.2) implies that Y is invertible. Denote $X = Y^{-1}$, $\Upsilon = KX$, $R_j = X^T P_j X$, 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, (10) holds. Also, Pre and post multiply inequalities $P_\alpha \le \mu P_\beta$ and $Q_\alpha \le \mu Q_\beta$ by X^T and X, respectively. Then, inequality (17) is obtained. If inequality (17) is true, (11) holds. Therefore, based on Theorem 1, as long as (13), (15), (16), and (17) hold, system (9) is exponentially stable. This completes the proof.