SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

June 2022, Vol. 65 162202:1–162202:18
https://doi.org/10.1007/s11432-021-3290-3

Small-signal stability and robustness analysis for microgrids under time-constrained DoS attacks and a mitigation adaptive secondary control method

Qiuye SUN[1*], Bingyu WANG[1], Xiaomeng FENG[2] & Shiyan HU[2]

[1]*College of Information Science and Engineering, Northeastern University, Shenyang* 110819*, China;*
[2]*School of Electronics and Computer Science, University of Southampton, Southampton* SO17 1BJ*, UK*

Received 5 January 2021/Revised 1 May 2021/Accepted 2 June 2021/Published online 26 April 2022

Abstract With the close integration of cyber and power systems, the consensus-based secondary frequency control in a microgrid is increasingly vulnerable to communication failures such as transmission delays and denial-of-service (DoS) attacks, which can affect the efficiency of frequency recovery in the secondary frequency control. Leveraging the small-signal model, this paper develops a novel cyber-physical system model to analyze the cross-layer effect of DoS attacks on microgrids. In this way, the cross-layer impact on the microgrid from the cyber system to the physical system can be convincingly analyzed. Based on the root approximation method, the tolerant saving time is designed for the microgrid as the index to evaluate the tolerance margin of the time-constrained DoS attack, and then the relationship between the margin and secondary control coefficients is found. A mitigation adaptive secondary control technique is proposed so that the attacked microgrid can dynamically tune the secondary control gain according to the saving time and tolerant saving time (TST). The simulation results show that although the microgrid with high secondary control gain has good dynamic robustness, its TST is low. In addition, the proposed adaptive secondary control system is significantly better than the traditional control system in terms of the stability performance of the microgrid under a DoS attack.

Keywords microgrid, hierarchical control architecture, cyber-physical system security, denial-of-service attack, adaptive secondary frequency control

Citation Sun Q Y, Wang B Y, Feng X M, et al. Small-signal stability and robustness analysis for microgrids under time-constrained DoS attacks and a mitigation adaptive secondary control method. Sci China Inf Sci, 2022, 65(6): 162202, https://doi.org/10.1007/s11432-021-3290-3

1 Introduction

A microgrid integrates the communication system and the energy system generated by renewable or non-renewable resources [1], which can be viewed as a hierarchical control architecture including the primary and secondary control systems. The primary control, termed the droop control, can achieve power-sharing through adjusting the inverter-based distributed generation (DG). However, these droop controllers at each inverter make the grid frequency deviate from the nominal value. To remove these deviations, the secondary control system is designed for the recovery of global frequency in the microgrid. Since the secondary control system is based on the interaction and transmission of data among DGs, its effectiveness is closely related to the communication networks [2]. Thus, the microgrid, with characteristics of deeply integrated cyber information and physical power flow, can be seen as a typical cyber-physical system (CPS).

In general, the vulnerability of communication systems can degrade the performance of the secondary controllers, leading to the vulnerability of the microgrid in a cross-layer fashion [3]. From some studies, cyber attacks can cause the microgrid to operate on an erroneous level [4]. Thus it is a challenge to ensure the stability of the microgrid under a vulnerable communication system. To solve this problem, the first thing is to analyze the cyber and physical characteristics of the microgrid and then propose a

* Corresponding author (email: sunqiuye@ise.neu.edu.cn)

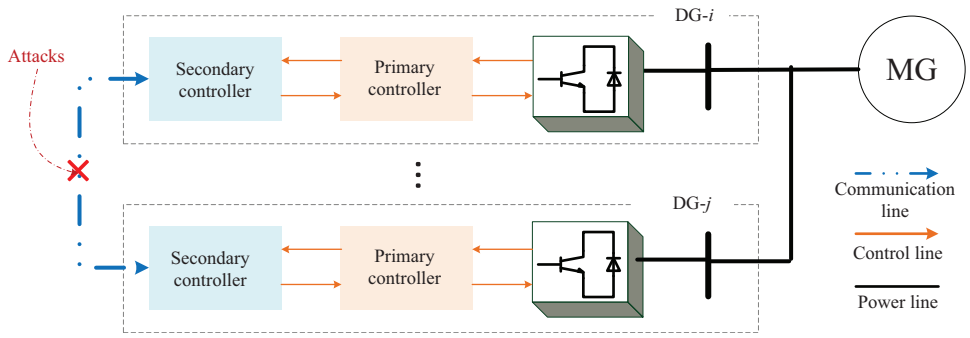

Figure 1 (Color online) Hierarchical control architecture on a microgrid.

proper control method based on the analysis results. Considering that power systems always operate at an equilibrium point, the small-signal stability analysis method is widely used in the corresponding research [5,6]. Thus, the small-signal stability of the microgrid with the hierarchical control architecture under denial-of-service (DoS) attacks is analyzed in this paper. Based on the analysis results, an adaptive secondary frequency control method is also proposed.

Currently, studies focus on the impact on the microgrid caused by DoS attacks [4,7] with consideration of potential communication failures in the microgrid, as shown in Figure 1. DoS attacks intend to affect timeliness and success rate of data exchange and then cause a time delay and packet loss [8, 9], for example [10, 11]. In the literature, it is difficult to discuss the damage caused by DoS attacks without the limitation of attack duration. This paper focuses on one DoS attack scenario that constrains attacker actions by limiting the duration of this attack in 0.3–4 s, referring to [12] due to attack resources. This DoS attack with limitation of duration can be viewed as a time-constrained DoS attack [10].

To analyze the stability of power systems under the DoS attack, the markovian DoS attack model is used to provide stochastic stability conditions [13,14]. However, based on this type of DoS attack model, the quantitative impact caused by failures of information flow on power flow cannot be obtained. A time delay model of DoS attacks [7, 12, 15] can be built to obtain the root distribution of the microgrid and then find the quantitative impact caused by DoS attacks according to the root distribution. In network control systems, data buffers and zero-order-holders (ZOHs) are applied to keep continuous inputs of actuators, and then systems can smoothly respond [8, 9]. As one type of network control systems, the microgrid with the distributed secondary control system suffers this property. In the microgrid with hierarchical control architecture, when the time-constrained DoS attack occurs, the communication links between neighboring DGs will be jammed. In this case, the real-time data transmission and exchange cannot be received on time, and these emergencies can cause frequency fluctuations and damage the stability and robustness of the microgrid. Take the packet transmitted from the first DG to the i-th DG in the communication system as an example. One packet containing the corresponding secondary control variable sent from the first DG is supposed to be received by the i-th DG at t_k. However, when the time-constrained DoS attack occurs, this packet is received by the i-th DG at t'_k instead of t_k. Therefore, the real-time secondary control variable cannot be available to the i-th DG, and there exists a delay $t'_k - t_k$ of the secondary control variable of the first DG in the i-th DG's controller.

By modeling the impact of the time-constrained DoS attack as the time delay, the model of the microgrid can be formulated as a set of delayed differential equations (DDEs). Some researchers [5,16–20] focus on small-signal stability analysis of time-delayed power system in recent time. However, due to the introduction of the distributed secondary control system, the information flow of the microgrid becomes more complex than the flow of the power system with centralized control, which is the subject in [16–19]. In the literature, the authors analyze the delay margin of the system with consideration of the delays of sampled state variables and control variables. These delays are caused by local measurement, control execution, and communication between controllers and corresponding actuators. After the secondary control system is introduced, delays of the distributed information flow between the DGs, should also be considered when analyzing the stability of the microgrid. Afterwards, different from [5, 19, 20] in which only the stability of the power system is analyzed, the robustness of the system is also one of the concerned properties because disturbances caused by DGs plug-and-play frequently happen in the microgrid. The rightmost pair of roots of the linearized DDEs must be found, and they are used to calculate the critical damping ratio of the system which is used to evaluate robustness of the microgrid.

In this process, characteristics of both the physical and cyber parts should be considered, while existing studies only consider the problem of convergence of the state variables related to the cyber part [7, 21]. Finally, communication channels between DGs are the targets of attackers when the microgrid is under the constrained DoS attack. The attack will impact sampled state variables that relate to off-diagonal elements of the cyber matrix in the linearized DDEs. Thus, the root loci of the DDEs with equivalent delays on the off-diagonal elements should be concerned.

To address the above challenges, the stability and robustness of the microgrid with the distributed secondary frequency control method under the time-constrained DoS attack are analyzed, and then an adaptive secondary frequency control method is proposed to mitigate the attack impact based on the analysis results in this paper. The contributions of this paper are as follows.

- This paper proposes a novel small-signal cyber-physical system (SSCPS) model, which separates the hierarchical control architecture of the microgrid into a cyber system and a physical system. During the model process, an improved power flow analysis method is proposed to find the changed operation equilibrium point of the microgrid caused by the variables of the cyber system. In this way, the cross-layer impact from the distributed information flow on the cyber system to the network power flow on the physical system can be convincingly analyzed.
- To analyze the robustness of the microgrid under the time-constrained DoS attack with consideration of characteristics of both the physical system and the cyber system, the impact caused by the attack is transformed to the time-varying delay in the SSCPS model. Thus, the SSCPS is formulated as a set of DDEs. Then, based on the root approximation method, the tolerant saving time (TST) is designed for the DDEs as the index to evaluate the tolerance margin of time-constrained DoS attack for the microgrid and find the relationship between the margin and the secondary control coefficient.
- To mitigate the impact on the microgrid caused by the time-constrained DoS attack, this paper proposes an adaptive frequency control method that can dynamically change the secondary control gain values according to the saving time and TST based on the relationship between the margin and the secondary control coefficient.
- The simulation shows that the performance of the microgrid with the proposed adaptive secondary control system is superior to that with the traditional secondary control system. In addition, the microgrid with high secondary control gain has low TST, e.g., when the control gain is 200 and 300, TST is 0.06 and 0.05 s, respectively.

The remainder of this paper is organized as follows. The preliminaries of hierarchical control architecture of microgrid and modeling techniques are presented in Section 2. The formulation of the improved small-signal model of microgrid under the time-constrained DoS attack is proposed in Section 3. In addition, Section 3 analyzes the stability and robustness of the microgrid and proposes an adaptive frequency control method to mitigate the impact caused by the time-constrained DoS attack. The performance of microgrid under the time-constrained DoS attack with the proposed strategy is shown in Section 4. Finally a conclusion is summarized in Section 5.

2 Preliminaries and related work

Some preliminary knowledge of the hierarchical control architecture of microgrid, AC power flow, and the small-signal model of the dynamical system is briefly presented first for completeness.

2.1 Hierarchical control architecture of microgrid

To address problems of the synchronization, power balance and load sharing in microgrids, the hierarchical control architecture proposed in [22] is widely used, which includes the primary droop control and the secondary frequency control.

2.1.1 *Primary P-ω droop control system*

The primary control is used to establish power sharing using the droop controller. For the i-th DG, the P-ω droop controller in the primary frequency control system can be written as [23, 24]

$$\omega_i(t) = \omega_i^* - m_i\left(P_i(t) - P_i^*\right) + \Omega_i(t), \tag{1a}$$

$$\dot{P}_i(t) = \eta\left(P_{ei}(t) - P_i(t)\right), \tag{1b}$$

where ω_i is the nodal frequency, ω_i^* is the nominal frequency, m_i is the droop coefficient, P_i is the filtered output power, P_i^* is the rated output power, P_{ei} is the output power of the inverter, and η is the low-pass time constant of power filter. Ω_i is the auxiliary power variable whose derivative is delivered to the primary control from the secondary control, which is used to compensate for the frequency deviation induced by the droop controller.

2.1.2 *Secondary frequency control system*

After the primary P-ω droop control, these droop controllers at each DG force the grid frequency to deviate from the nominal value. Therefore, the secondary control has been utilized to remove these deviations, in which control strategies range from centralized control to decentralized control.

Based on a piecewise-constant control law, the secondary control input Ω_i [23] is calculated as

$$\dot{\Omega}_i(t) = -k_\omega u_i(t_k) = -k_\omega \left((\omega_i(t_k) - \omega^*) + \sum_{j \in N_i} a_{ij} (\Omega_i(t_k) - \Omega_j(t_k)) \right), \quad t_k \leqslant t < t_{k+1}, \tag{2}$$

where k_ω is the control gain, u_i is the control input of secondary controller, N_i is the set of neighboring DGs of the i-th DG on a connected directed graph G, a_{ij} is the weight of the communication edge between the i-th DG and j-th DG, and $0 = t_0 < \cdots < t_k < \cdots$ are the control time instants. Commonly, when the information of all the neighbors is received by i-th DG's PC, the frequency control task is triggered at the control time instant. The communication graph G is defined as a triple pair $(V, E, \boldsymbol{D})$, where $V = \{\text{DG } 1, \text{DG } 2, \ldots, \text{DG } N\}$ is the DG set, $E \subseteq V \times V$ is the set of connections among DGs, and $\boldsymbol{D} = [a_{ij}]$ is the adjacency matrix. If the i-th DG receives information from its j-th neighboring DG, $a_{ij} = 1$; otherwise $a_{ij} = 0$. The corresponding Laplacian matrix is defined as $\boldsymbol{L} = [l_{ij}]$, where $l_{ii} = \sum_{j=1}^{N} a_{ij}$, $l_{ij} = -a_{ij}$ for $i \neq j$.

2.2 AC power flow analysis for islanded microgrid

According to the AC power flow presented in [25], the voltage phase angle δ_i and output power P_{ei} at the i-th DG are given as

$$\dot{\delta}_i(t) = \omega_i(t) - \omega_{\text{sys}}, \tag{3a}$$

$$P_{ei}(t) = \sum_{j=1}^{N} E_i E_j Y_{ij} \sin(\delta_i(t) - \delta_j(t)), \tag{3b}$$

where δ is the nodal voltage phase angle, ω_{sys} is the current system's frequency, $E_i > 0$ is the nodal voltage magnitude, and Y_{ij} is the inductive admittance for the inductive line between i-th DG and j-th DG.

The power flow analysis of islanded microgrid is used to estimate system's state which can be seen as the solution of nonlinear algebraic equations. Newton Raphson solution method in which variable vectors $\boldsymbol{y}$, mismatch matrix $\boldsymbol{\Phi}$ and Jacobian matrix $\boldsymbol{J}$ are commonly used is widely developed to solve the equations [26].

2.3 Time-constrained DoS attack

Normally, the communication network in the microgrid provides available and abundant communication resources for DGs. When a time-constrained DoS attack occurs, these communication resources might be overwhelmed and legitimate users are thus prevented from communicating. Through affecting the timeless of the exchanging information between the neighboring DGs, the time-constrained DoS attack can cause frequency fluctuations, impact the robustness of microgrid, and even destruct the stability of the system [11].

As shown in Figure 2, packets containing the values of secondary control variables Ω are transmitted periodically in the communication network. In the diagram, packets from the first DG to the second DG are transmitted in a communication channel. When a packet is received by the second DG at t_k, the information of secondary control variable of the first DG $\Omega_1(t_k)$ is used to compute the value of the control input u_i and saved in a memory. The control input u_i is held by the zero-order-holder to provide a continuous input for the physical system until the next control moment t_{k+1}. If the next packet from

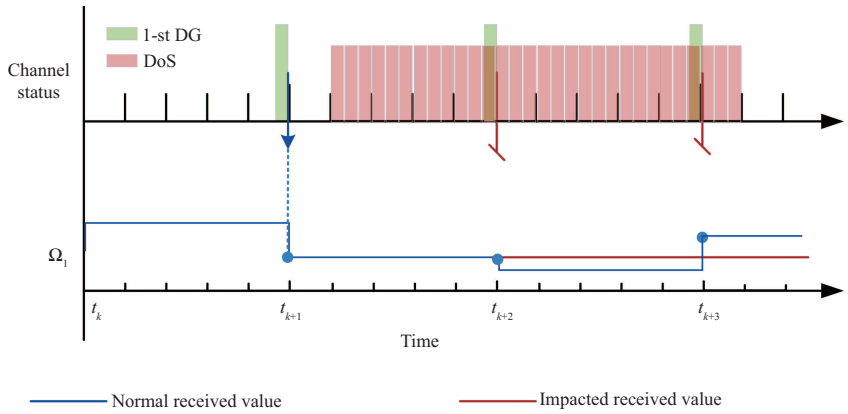

Figure 2 (Color online) Diagram of the impact on the communication channel and the second DG caused by the DoS attack.

the first DG is received at t_{k+1}, the value in the memory is updated as $\Omega_1(t_{k+1})$ and used to compute u_i. Otherwise, the value $\Omega_1(t_k)$ saved in the memory is used. Normally, there are N_i memories in the i-th DG and the time of a certain neighboring control value in each memory, named the saving time in this paper, equals the control period. When the time-constrained DoS attack occurs on the communication channel, lots of empty or useless packets are transmitted in the target channel. Communication traffic congestion happens as a brute of packets is crowded. It results in that normal packets cannot be transmitted in the target channel. During the congestion period, the last successful updated value of the impacted neighboring DGs is used to compute the inputs $\boldsymbol{u}$ of secondary controllers. In this way, a time delay is introduced for corresponding states in the system model.

We will use an example to illustrate why the impact induced by packet losses on the microgrid can be modeled as time-varying delay. For the control law $u_i(t_k)$, it can be represented as the delayed control during $[t_k, t_{k+1})$ as

$$u_i = u_i(t_k) = u_i(t-(t-t_k)) = u_i(t-\tau(t)), \quad t_k \leqslant t < t_{k+1}, \quad \tau(t) = t - t_k,$$

where $\tau(t)$ is piecewise-linear with the derivative $\dot{\tau}(t) = 1$ for $t \neq t_k$. When the system suffers from the time-constrained DoS attack, assume that the packets of the moments t_{k+1} and t_{k+2} are lost. Assume that the time-constrained DoS attack finishes due to the limitation of resources at the moment t_{k+3}. The packet of the moment t_{k+3} can be received by the controller. That is, the DoS attack is time-constrained and the impact period of the attack on the controller is from t_k to t_{k+3}. The control law during the impact period of the attack can be represent as

$$u_i = u_i(t_k) = u_i(t-(t-t_k)) = u_i(t-\tau_d(t)), \quad t_k \leqslant t < t_{k+3}, \quad \tau_d(t) = t - t_k,$$

where $\tau_d < t_{k+3} - t_k = \tau_{\text{cons}}$, and τ_{cons} is the time-constrain of the DoS attack.

3 Proposed model and analysis

The secondary control system is crucial to the frequency recovery in microgrid, which is based on the interactive communication among DGs. The interactive communication may not operate normally when time-constrained DoS attack occurs. More specifically, time-constrained DoS attack can bring invalid data packets so that the channel resources are consumed. In this way, the effective data packets cannot be timely transmitted into the controllers, i.e., there exists a transmission delay of second control variables. This delay leads to the deviation of frequency recovery through impacting the accuracy of the secondary control, and further impacts the stability of the microgrid. This paper proposes a secondary control model in microgrid, considering the control input delay of secondary control variable caused by the communication network. Afterwards, to tackle the difficulty of analyzing the stability of the non-linear system, the small-signal model at the equilibrium point is used to linearize the proposed model. Considering the time-constrained DoS attack, this paper proposes an improved small-signal model of microgrid which can evaluate the impact of time-constrained DoS attack. Based on this model, this paper designs TST and the critical damp-ratio as the index to analyze the stability and robustness of the microgrid

under time-constrained DoS attack, respectively. In addition, an adaptive secondary control method is proposed which can mitigate the consequence of the time-constrained DoS attack on the performance of the microgrid.

3.1 Small-signal model of microgrid

In this subsection, a novel model of microgrid is proposed to improve the modelling accuracy. Intuitively, it is difficult to analyze the stability of the proposed system, so the small-signal model is used to linearize the model of microgrid. To obtain the small-signal model, the equilibrium point needs to be calculated. Therefore, an improved power flow analysis method is proposed to calculate the equilibrium point, which takes the secondary control variable into consideration. Afterwards, the novel small-signal model of microgrid on this equilibrium point can be built and provides the basic model for the following analysis in Subsection 3.2.1.

3.1.1 *Model of microgrid*

Compared with the second-order model of microgrid in [23], a third-order model of microgrid is proposed with the consideration of the power filter coefficient η as indicated in Subsection 2.1.1. This coefficient is used to reduce the fluctuation of nodal frequency through providing a smooth output value P_i which is the input of the P-ω droop controller. The proposed model has one feather that it includes both continuous states and piecewise-constant control law, and thus it can be viewed as a sampled-data based system in one control period h. By substituting (1b), (2), and (3) into the derivative of (1a), the details of this model are as follows:

$$\dot{\delta}_i(t) = \omega_i(t) - \omega_{\text{sys}}, \tag{4a}$$

$$\dot{\omega}_i(t) = m_i\eta P_i^* - m_i\eta\sum_{j=1}^{N} E_iE_jY_{ij}\sin\left(\delta_i(t) - \delta_j(t)\right) + \eta\left(\omega_i^* - \omega_i(t)\right) + \eta\Omega_i(t) + \dot{\Omega}_i(t), \tag{4b}$$

$$\dot{\Omega}_i(t) = -k_\omega\left(\left(\omega_i(t_k) - \omega^*\right) + \sum_{j\in N_i} a_{ij}\left(\Omega_i(t_k) - \Omega_j(t_k)\right)\right), \tag{4c}$$

where N_i is the number of neighbors of i-th DG. In fact, it is difficult to intuitively analyze the stability of the proposed non-linear model, and thus the small-signal linear approximation method at the equilibrium point of (4) is used. To obtain the small-signal approximation, the equilibrium point needs to be calculated by the improved power flow analysis method, which is discussed as follows.

3.1.2 *Improved power flow analysis of microgrid with secondary frequency control*

In fact, the traditional power flow analysis methods do not take the secondary frequency control characteristics into account, and thus the equilibrium point of states $\boldsymbol{\Omega}$ cannot be calculated. To solve this problem, an improved power flow analysis method is proposed in this subsection, which considers the secondary frequency control variable and can calculate the equilibrium point of the microgrid with secondary frequency control.

The power flow analysis for islanded microgrids with droop control can be referenced in [26]. When considering the secondary frequency control characteristics, the variable vectors and mismatch matrix are modified as

$$\boldsymbol{y}' = \left[\begin{array}{cccc}\boldsymbol{\delta}^{\mathrm{T}} & |\boldsymbol{V}|^{\mathrm{T}} & \omega & |V_1| & \boldsymbol{\Omega}^{\mathrm{T}}\end{array}\right]^{\mathrm{T}}, \tag{5a}$$

$$\boldsymbol{\Phi}' = \left[\begin{array}{cccccc}\Delta\boldsymbol{P}^{\mathrm{T}} & \Delta\boldsymbol{Q}^{\mathrm{T}} & P_{\text{tot}} - P_{\text{sys}} & Q_{\text{tot}} - Q_{\text{sys}} & \Delta\boldsymbol{\Omega}\end{array}\right], \tag{5b}$$

where $\boldsymbol{\delta}$ and $|\boldsymbol{V}|$ are respectively the vectors of voltage angles and magnitudes of all the bus except the slack bus, ω is the system frequency, $|V_1|$ is the voltage magnitudes of the slack bus (assuming bus 1 to be the slack bus), $\boldsymbol{\Omega}$ is the vectors of the secondary control variables, $\Delta\boldsymbol{P}^{\mathrm{T}}$ and $\Delta\boldsymbol{Q}^{\mathrm{T}}$ are the vectors of difference between the real power P_i and reactive power Q_i and the calculated real power P_{ci} and reactive power Q_{ci}, respectively of all the bus, P_{tot} and Q_{tot} are the system consumption of real and reactive power, P_{sys} and Q_{sys} are the sum of real and reactive power of DGs, and $\Delta\boldsymbol{\Omega}$ is the difference between the control variables $\boldsymbol{\Omega}$ and the control calculated variables $\boldsymbol{\Omega}_c$.

When the system is stable, $k_\omega\left(\omega_i-\omega^*\right)+k_\omega(\sum_{j\in N_i}a_{ij}\left(\Omega_i-\Omega_j\right))=0$ for the i-th DG. Correspondingly, the Jacobian matrix is modified as

$$\boldsymbol{J}'=\left[\begin{array}{cccc|c}\boldsymbol{J}_{11} & \boldsymbol{J}_{12} & \boldsymbol{J}_{13} & \boldsymbol{J}_{14} & \boldsymbol{J}'_{15}\\ \boldsymbol{J}_{21} & \boldsymbol{J}_{22} & \boldsymbol{J}_{23} & \boldsymbol{J}_{24} & \boldsymbol{J}'_{25}\\ \boldsymbol{J}_{31} & \boldsymbol{J}_{32} & \boldsymbol{J}_{33} & \boldsymbol{J}_{34} & \boldsymbol{J}'_{35}\\ \boldsymbol{J}_{41} & \boldsymbol{J}_{42} & \boldsymbol{J}_{43} & \boldsymbol{J}_{44} & \boldsymbol{J}'_{45}\\ \hline \boldsymbol{J}'_{51} & \boldsymbol{J}'_{52} & \boldsymbol{J}'_{53} & \boldsymbol{J}'_{54} & \boldsymbol{J}'_{55}\end{array}\right], \tag{6}$$

where $\boldsymbol{J}_{ij},i,j=1,2,3,4$ are the Jacobian sub-matrices (the details can be found in [26]),

$$\boldsymbol{J}'_{15}=\left[\begin{array}{ccc}\frac{\partial P_{c2}}{\partial\Omega_1} & \cdots & \frac{\partial P_{c2}}{\partial\Omega_n}\\ \vdots & \ddots & \vdots\\ \frac{\partial P_{cn}}{\partial\Omega_1} & \cdots & \frac{\partial P_{cn}}{\partial\Omega_n}\end{array}\right],\quad \frac{\partial P_{ci}}{\partial\Omega_j}=\begin{cases}0, & i\neq j,\\ \frac{1}{m_j}, & i=j,\end{cases}$$

$\boldsymbol{J}'_{25}=[\boldsymbol{0}]_{(N-1)\times N}$, $\boldsymbol{J}_{35}=[\,\frac{\partial P_{\rm sys}}{\partial\Omega_1}\ \cdots\ \frac{\partial P_{\rm sys}}{\partial\Omega_n}\,]$, $\frac{\partial P_{\rm sys}}{\partial\Omega_j}=\frac{1}{m_j}$, $\boldsymbol{J}_{45}=[\boldsymbol{0}]_{1\times N}$, $\boldsymbol{J}_{51}=[\boldsymbol{0}]_{N\times(N-1)}$, $\boldsymbol{J}_{52}=[\boldsymbol{0}]_{N\times(N-1)}$, $\boldsymbol{J}_{53}=[\boldsymbol{0}]_{N\times1}$, $\boldsymbol{J}_{54}=[\boldsymbol{0}]_{N\times1}$, and $\boldsymbol{J}_{55}=\boldsymbol{I}_N-\boldsymbol{L}$. Once the Jacobian matrix is calculated, the equilibrium point $\bar{\boldsymbol{x}}=[\bar{\boldsymbol{\delta}},\bar{\boldsymbol{\omega}},\bar{\boldsymbol{\Omega}}]^{\rm T}$ can be calculated by Newton Raphson method, and then used to build the small-signal model of microgrid.

3.1.3 *Linearizing model of microgrid*

After obtaining the equilibrium point $\bar{\boldsymbol{x}}=[\bar{\boldsymbol{\delta}},\bar{\boldsymbol{\omega}},\bar{\boldsymbol{\Omega}}]$, the small-signal model is used to linearize the model of microgrid in (4), and the linearization process is as follows.

To simplify the notational expression, Eq. (4) can be represented as

$$\dot{\boldsymbol{\delta}}=\boldsymbol{f}(\boldsymbol{\delta},\omega,\Omega), \tag{7a}$$

$$\dot{\boldsymbol{\omega}}=\boldsymbol{g}(\boldsymbol{\delta},\omega,\Omega), \tag{7b}$$

$$\dot{\boldsymbol{\Omega}}=\boldsymbol{h}(\boldsymbol{\delta},\omega,\Omega). \tag{7c}$$

According to the small-signal method, the state transition matrix $\boldsymbol{A}$ can be obtained as

$$\boldsymbol{A}=\left[\begin{array}{ccc}\frac{\partial f}{\partial\delta}\Big|_{\bar\delta} & \frac{\partial f}{\partial\omega}\Big|_{\bar\omega} & \frac{\partial f}{\partial\Omega}\Big|_{\bar\Omega}\\ \frac{\partial g}{\partial\delta}\Big|_{\bar\delta} & \frac{\partial g}{\partial\omega}\Big|_{\bar\omega} & \frac{\partial g}{\partial\Omega}\Big|_{\bar\Omega}\\ \frac{\partial h}{\partial\delta}\Big|_{\bar\delta} & \frac{\partial h}{\partial\omega}\Big|_{\bar\omega} & \frac{\partial h}{\partial\Omega}\Big|_{\bar\Omega}\end{array}\right], \tag{8}$$

where $\bar\delta,\bar\omega,\bar\Omega$ are the state variables at the equilibrium point. Since only the information about the secondary control variables is exchanged between DGs, the variables $\boldsymbol{\Omega}$ are periodically updated in the cyber layer, instead of other variables $\boldsymbol{\delta}$ and $\boldsymbol{\omega}$. In this case, to respectively analyze the impact on microgrid of physical layer and cyber layer, the matrix $\boldsymbol{A}$ is decomposed into $\boldsymbol{A}_p$ and $\boldsymbol{A}_c$, and the corresponding model in a control period can be described as

$$\dot{\boldsymbol{x}}=\boldsymbol{A}_p\boldsymbol{x}+\boldsymbol{A}_c\boldsymbol{x}\left(t_k\right), \tag{9}$$

in which $\boldsymbol{x}=[\,\Delta\boldsymbol{\delta}\ \Delta\boldsymbol{\omega}\ \Delta\boldsymbol{\Omega}\,]^{\rm T}$, $M_i=m_i\eta_i$, $\boldsymbol{M}=\mathrm{diag}\left(M_i\right)$, $\boldsymbol{K}=\mathrm{diag}\left(k_\omega\right)$, $\boldsymbol{H}=\mathrm{diag}\left(\eta\right)$ and

$$\boldsymbol{A}_p=\left[\begin{array}{ccc}\boldsymbol{0}_{N\times N} & \boldsymbol{I}_{N\times N} & \boldsymbol{0}_{N\times N}\\ \boldsymbol{A}^{21}_{N\times N} & -\boldsymbol{H}_{N\times N} & \boldsymbol{H}_{N\times N}\\ \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N}\end{array}\right],\quad \boldsymbol{A}_c=\left[\begin{array}{ccc}\boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N}\\ \boldsymbol{0}_{N\times N} & -\boldsymbol{K} & -\boldsymbol{K}\boldsymbol{L}\\ \boldsymbol{0}_{N\times N} & -\boldsymbol{K} & -\boldsymbol{K}\boldsymbol{L}\end{array}\right],$$

in which $\boldsymbol{A}^{21}_{N\times N}=-\boldsymbol{M}\frac{\partial\boldsymbol{P_e}}{\partial\boldsymbol{\delta}}$. In (9), $\boldsymbol{A}_p$ models the physical connection and the control structure of microgrid, called the physical matrix, and $\boldsymbol{A}_c$ models the influence caused by network control in one control period, called the cyber matrix in this paper. A small example to illustrate the process of solving this small-signal model of microgrid is shown in Appendix A.

3.2 Stability and robustness analysis of small-signal model when the microgrid under the time-constrained DoS attack

In fact, the traditional model is not applied when the microgird suffers from time-constrained DoS attack, so in Subsection 3.2.1 an extended small-signal model of microgrid with the impact caused by time-constrained DoS attack is proposed, which is an improvement of the small-signal model mentioned in Subsection 3.1.3. Afterwards, in Subsection 3.2.2 a root approximation method is used to obtain root distribution of the extended small-signal model of microgrid. Through discussing the characteristics of the root distribution, the small-signal stability and robustness analysis for this microgrid under time-constrained DoS attack are analyzed in Subsection 3.2.3, respectively.

3.2.1 *Small-signal model of microgrid with the impact caused by the time-constrained DoS attack*

According to definition of the time-constrained DoS attack, this paper assumes that the d-th channel is the target of attack. During the congestion period of DoS attack, the normal packets from all of the DGs over the channel cannot be transmitted. The auxiliary value of impacted DGs is kept and used to calculate the secondary control input of their neighboring DGs.

In this way, the auxiliary power variables of the small-signal model of microgrid in (9), i.e., $\Delta\boldsymbol{\Omega}$, are the only values impacted by the communication fault or DoS attack. Therefore, to make the model of the microgrid suitable for the scenarios with the time-constrained DoS attack, an improved small-signal model of microgrid during the period of communication fault or DoS attack in a control period $(t_k, t_{k+1}]$ is described as

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}_p\boldsymbol{x}(t) + \boldsymbol{A}_c\boldsymbol{x}(t-\tau_k) + \sum_{d=1}^{N_d}\boldsymbol{A}_c^d\boldsymbol{x}(t-\tau_d), \tag{10}$$

where $\tau_k = t - t_k$, $t_k \leqslant t < t_{k+1}$, $\tau_d = t - t_d$, t_d is the last update moment of all impacted variables on the d-th channel, $t_d < t_k$, $\tau_d < \tau_{\max}$,

$$\boldsymbol{A}_c^d = \begin{bmatrix} \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} \\ \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} & -\boldsymbol{K}\boldsymbol{D}^d \\ \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} & -\boldsymbol{K}\boldsymbol{D}^d \end{bmatrix},$$

$\boldsymbol{D}^d$ is the impacted adjacency matrix in which $a_{ij} = 1$ if the i-th DG receives information from the j-th DG over the d-th channel, $\boldsymbol{A}_c = \boldsymbol{A}_c - \sum_{d=1}^{d_{\max}}\boldsymbol{A}_c^d$, and N_d is the number of attacked channels. The characteristic equation of the system is

$$\det(\Delta(\lambda)) = 0, \tag{11}$$

where $\Delta(\lambda) = \lambda\cdot\boldsymbol{I}_N - \boldsymbol{A}_p - \boldsymbol{A}_c\cdot \mathrm{e}^{-\lambda\tau_k} - \sum_{d=1}^{d_{\max}}\boldsymbol{A}_c^d\cdot\mathrm{e}^{-\lambda\tau_d}$ is the characteristic matrix. The stationary point of microgrid is stable if all roots of (11) have negative real part for each control period. Through solving (11), some characteristics of the dynamic performance of system can also be acquired by the root distribution.

3.2.2 *Root approximation method*

Since the number of roots for (11) is infinite, it is complicated and difficult to compute the root distribution. Therefore, a root approximation method proposed in [27] is used to find the approximate roots of microgrid shown in (10), which maps the set of infinite roots into the finite set of approximate roots.

In this way, the approximated characteristic roots can be used to analyze the performance of the system instead of the accurate roots. Rewrite (10) at $t = t_{k+1}$ as

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}_p\boldsymbol{x}(t) + \boldsymbol{A}_c\boldsymbol{x}(t-h) + \sum_{d=1}^{N_d}\boldsymbol{A}_c^d\boldsymbol{x}(t-\tau_d), \tag{12}$$

where $h = t_{(k+1)} - t_k$ is the control period, $\tau_d = t_{k+1} - t_d$, $h < \tau_1 < \cdots < \tau_d < \cdots < \tau_{N_d} = \tau_{\max}$. Let $\boldsymbol{\tau} = \{\tau_1, \ldots, \tau_{N_d}\}$ denote the set composed by the saving time caused by the DoS attack on all the communication channels in the microgrid. Discrete the interval $[-\tau_{\max}, 0]$ into M blocks using a constant stepsize $l = \tau_{\max}/M$. For the γ-th block, an s-stage Runge-Kutta method $(\boldsymbol{R}, \boldsymbol{b}, \boldsymbol{c})$ with order p is used

to approximate the solution of (12) on the $(\gamma+1)$-th block. Thus, the discretization matrix ($\boldsymbol{S}_M$) of the solution operator $T(l)$ of (12) can be obtained as

$$\boldsymbol{S}_M=\begin{pmatrix}\Psi\left(l\boldsymbol{A}_p\right)\left(\boldsymbol{1}_{1\times s}\boldsymbol{e}_{1\times s}^{\mathrm{T}}\otimes\boldsymbol{I}_N\right) & \cdots & \boldsymbol{S}^{\gamma} & \cdots & l\Psi\left(l\boldsymbol{A}_p\right)\left(\boldsymbol{R}\otimes\boldsymbol{A}_c^{N^d}\right)\\ \boldsymbol{I}_{N\times s} & \boldsymbol{0}_{N\times s} & \cdots & \boldsymbol{0}_{N\times s} & \boldsymbol{0}_{N\times s}\\ \boldsymbol{0}_{Ns} & \boldsymbol{I}_{N\times s} & \cdots & \boldsymbol{0}_{Ns} & \boldsymbol{0}_{N\times s}\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \boldsymbol{0}_{N\times s} & \boldsymbol{0}_{N\times s} & \cdots & \boldsymbol{I}_{N\times s} & \boldsymbol{0}_{N\times s}\end{pmatrix},\tag{13}$$

where $\Psi\left(l\boldsymbol{A}_p\right)=\left(\boldsymbol{I}_{N\times s}-\boldsymbol{R}\otimes l\boldsymbol{A}_p\right)^{-1}$, $\boldsymbol{e}_{1\times s}=(0,\ldots,0,1)^{\mathrm{T}}$, $\boldsymbol{1}_{1\times s}=(1,\ldots,1,1)^{\mathrm{T}}$. Based on $p+1$ points around point c_il-h and $c_il-\tau_d$, $i=1,\ldots,s$, $d=1,\ldots,N_d-1$, the sub-matrix $\boldsymbol{S}^{\gamma}$ can be constructed by the approximation value to these points through Langrange interpolation method as $\boldsymbol{S}^{\gamma}=l\Psi(l\boldsymbol{A}_p)\sum_{i=1}^{s}\left(l_{\gamma}^{h}(c_i)\,\boldsymbol{R}\otimes\boldsymbol{A}_c^{n}\right)+l\Psi(l\boldsymbol{A}_p)\sum_{d=1}^{N_d-1}\left(\sum_{i=1}^{s}\left(l_{\gamma}^{\tau_d}(c_p)\,\boldsymbol{R}\otimes\boldsymbol{A}_c^{d}\right)\right)$, where $l_{\gamma}^{h}(c_i)$ and $l_{\gamma}^{\tau_d}(c_i)$ are the Langrange coefficients corresponding with point c_il-h and $c_il-\tau_d$, respectively.

For the system (12),

$$\lambda_s=\frac{1}{l}\ln\mu\tag{14}$$

is an approximation to characteristic roots where $\mu\in\sigma(S_M)\setminus\{\boldsymbol{0}\}$ ($\sigma(S_M)$ denotes the set of eigenvalue of $\boldsymbol{S}_M$).

3.2.3 *Stability and robustness analysis*

In this subsection, the stability and the robustness of the small-signal model of microgrid are evaluated according to the root distribution of (12), calculated by the parameters including the control period h and $\boldsymbol{\tau}$. More specifically, the root locus can be used to evaluate the stability of the system, and the critical damping ratio, which is determined according to this root distribution, is an evaluation of the system robustness against disturbance, such as the load variation.

For a vector $\boldsymbol{\tau}$, let $\boldsymbol{d}=\{d_1,\ldots,d_{N_d}\}$ denote the corresponding Boolean vector, where $d_i=1$ if the i-th channel is suffering from DoS attacks; otherwise, $d_i=0$. To evaluate the time-constrained DoS attack, an index, TST, is defined. The TST is the critical saving time if the roots of the corresponding characteristic equation are all in the open left-hand plane for $\tau_{\max}<\mathrm{TST}$ and the root trace intersects the imaginary axis for $\tau_{\max}>\mathrm{TST}$. The procedure of the proposed analysis approach is shown in Algorithm 1.

Algorithm 1 Analysis approach when the microgrid suffers from the time-constrained DoS attack

For $i=1:1:\bar{N}_d$
  Establish the small-signal model of microgrid, i.e., (9), at the control point $t=t_1$ in which $t_1=h$;
  For $k=1:1:k_{\max}$ ($k_{\max}$ is the default cease value of the approach)
    1. Solve the root locus of characteristic equation corresponding with (12) at $t=t_k$ in which $t_k=kh$ using the root approximation method;
    2. Save the corresponding most critical damping ratio according to the root locus;
    if the roots cross the imaginary axis
      3. Save the TST $=kh$ in this channel;
      Break
    End if
  End for
  4. Save the TST $=k_{\max}h$ in this channel;
End for

In this way, the relationship between the secondary control gain and the TST of each channel can be found by a series of tests with different gains. According to this relationship, a mitigation method can be proposed for the secondary frequency control system of microgrid with time-constrained DoS attack.

3.3 Adaptive secondary frequency control

According to the analysis results in Subsection 4.3, it shows that the value of TST is inversely linked to the secondary control gain. That is, the TST increases with the decrease of secondary control gain. Based on this conclusion, a gain scheduler $\beta_{\tau(z)}^{j}$ relating with the saving time for each neighboring DG is stored in the i-th DG. The gain scheduler is determined by the discretized relationship between secondary

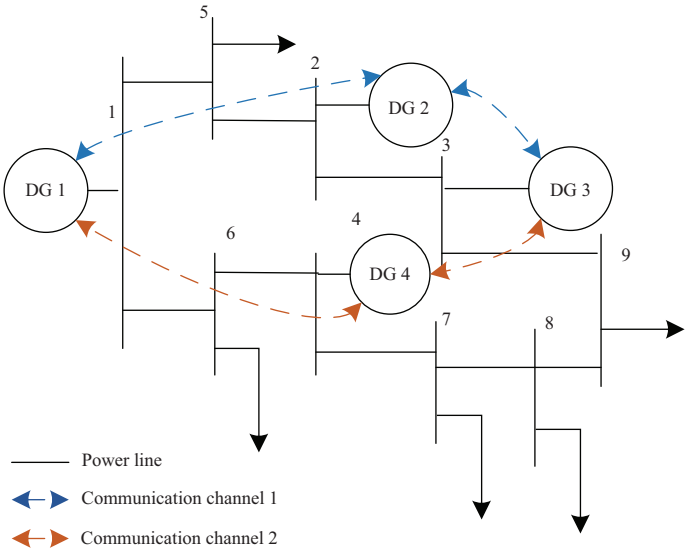

Figure 3 (Color online) The structure of the simulated microgrid.

control gains and the TST. Thus, $\beta^j_{\tau(z)}$ is a piecewise-constant function of the delay time $\tau_{ij} = t - T_j$, where T_j is the time stamp, and

$$\tilde{k}_{\omega,ij} = \beta^j_{\tau(z)} k_\omega, \quad \tau_{ij} \in \tau(z), \tag{15}$$

where $\tau(z)$ is the time interval $z = 1, 2, \ldots, N_\tau$ and N_τ is number of the intervals which is obtained by the relationship between the secondary control gain and the TST. In details, the method in the i-th DG includes the following steps:

(1) First, the j-th DG samples the secondary control variable $\Omega_j^{T_j}$ at time T_j, and sends it with the time stamp T_j to its neighboring DGs.

(2) After the i-th neighboring DG receives the secondary control variable from the j-th DG, it will store this variable.

(3) When the controller in the i-th DG is periodically triggered, the saving time $\tau_{ij} = t - T_j$ is calculated for each neighboring DG, and the input of secondary control u_i is calculated according to (15) and the variables stored in neighboring DGs.

4 Simulation and analysis results

As mentioned above, the stability and robustness of microgrid will be impacted or even destructed by the time-constrained DoS attack. In this section, the validation of the improved power flow method is tested. After that, a small example is used to analyze the stability and robustness of system under the time-constrained DoS attack. Subsequently, the performance of the microgrid under the normal communication is illustrated. Otherwise, when a time-constrained DoS attack occurs, the effectiveness of the microgrid with the proposed adaptive control method and the traditional method is tested, respectively. It shows the effectiveness of the proposed control method.

4.1 Simulation setup

A microgrid architecture shown in Figure 3 is used to perform the proposed control approach. The system parameters are reported in Table 1, where the communication network is configured with a data rate of 100 Mbps and a minimum message size of 512 bits. In order to provide a better simulation of real communication networks, two communication channels are set and simulated using Truetime Tools in the simulation. The information on the first channel and the second channel delivers the information from the 1-st, 2-nd and 4-th DG, and the information from the 2-nd, 3-rd and 4-th DG, respectively. The control period of secondary control in DGs is set as $h = 1$ ms and for all DGs $k_\omega = 200$.

Table 1 Electrical and control parameters

Parameter	Symbol	Value	Parameter	Symbol	DG 1	DG 2&3&4
Rated frequency	$\omega^*/2\pi$	50 Hz	Rated active power	P_{ratei}	66 kW	33 kW
DC votlage	V_{dc}	800 V	Rated reactive power	Q_{ratei}	0 kVAr	0 kVAr
Nominal voltages	E_*	220 V	Current loop P-coefficient	K_{CP}	6.72	10.5
Filter capacitance	C_f	40 μF	Current loop I-coefficient	K_{CI}	3360	3360
Filter inductance	L_f	0.2 mH	Voltage loop P-coefficient	K_{VP}	0.2	0.2
Output inductance	L_0	0.2 mH	Voltage loop I-coefficient	K_{VI}	480	480
Power filter coefficient	τ_P	0.0318	P-f droop coefficient	m_i	7.5E−6 $\frac{\text{Hz}}{\text{W}}$	1.5E−5 $\frac{\text{Hz}}{\text{W}}$
Line impedance	Z	0.1+0.31j Ω	Q-E droop coefficient	n_i	2E−4 $\frac{\text{V}}{\text{VAr}}$	2E−4 $\frac{\text{V}}{\text{VAr}}$

Table 2 Validation results for IPFM

Bus	Voltage magnitude		Voltage angle		Active power		Secondary input	
	IPFM	MAT	IPFM	MAT	IPFM	MAT	IPFM	MAT
DG 1	1.0059	1.0132	0	0	0.9665	0.9012	−0.1061	−0.1885
DG 2	0.9955	0.9977	−0.0021	−0.0063	0.4833	0.4510	−0.1061	−0.1885
DG 3	0.9800	0.9895	−0.0034	−0.0089	0.4833	0.4510	−0.1061	−0.1885
DG 4	0.9814	0.9895	−0.0018	−0.0071	0.4833	0.4510	−0.1061	−0.1885
Maximum error	0.0095		0.0053		0.0653		0.0824	

4.2 Validation of the improved power flow method

To validate the improved power flow method (IPFM), the results from the proposed method are compared with the steady state values obtained from the simulated microgrid, shown in Table 2. All the related value is turned to the per-unit form to give an intuitive view. The results of the IPFM closely match the results obtained from the time domain model in MATLAB/Simulink. It means that the improved power flow method can find the equilibrium point of microgrid with secondary frequency control.

4.3 Stability and robustness analysis of a small example

The accuracy of the root approximation method is discussed in this subsection before the details of the stability analysis. When the communication system is in normally operation with $k_\omega = 100$, the small-signal model of microgrid at $t = t_{k+1}$ can be written as

$$\dot{\boldsymbol{x}} = \boldsymbol{A}_p\boldsymbol{x} + \boldsymbol{A}_c\boldsymbol{x}\left(t-h\right), \tag{16}$$

where $h = 1 \times 10^{-3}$. Components of $\boldsymbol{A}_p$ and $\boldsymbol{A}_c$ are given in Appendix A. The 2-stage and 3-order Runge-Kutta method with $\boldsymbol{R} = \left[\begin{smallmatrix} 5/12 & -1/12 \\ 3/4 & 1/4 \end{smallmatrix}\right]$ is used and $M = 6$ in this case. Generally, when the control period is small, some of approximated roots of 16 are close to precise roots of the continuous system $\dot{\boldsymbol{x}} = \left(\boldsymbol{A}_p + \boldsymbol{A}_c\right)\boldsymbol{x}$. The eigenvalue of system (16) and the continuous system is shown in Figure 4. It shows that the approximated roots are close to the precise roots. That is to say, the selected coefficients of the root approximation method can ensure the accuracy. It also illustrates that the microgrid achieves small-signal stability and has a good robustness as the critical damp-ratio is 10%.

Assume the communication failure is launched on the first communication channel. With the increase of the saving time in the related memories caused by failures, the root locus of the system at $t = t_{k+1}$ is shown in Figure 5. Most of the roots move towards the imaginary axis and some of them cross the imaginary axis when $\tau_1 = 0.102$ which means that the small-signal stability is destructed by time-constrained DoS attack if the saving time is over 0.102 s and in this scenario, the TST is 0.102 s. Afterwards, the relationship between TST and secondary control gains under different directions of time-constrained DoS attack is illustrated in Figure 6. It shows that the TST decreases with the increase of the secondary control gain k_ω no matter the DoS attack is launched on which direction. Otherwise, the TSTs are almost same for a secondary control gain when the attack is launched on the 1st or 2nd channel. This is because the 1st and 2nd channels are symmetrical in the communication topology. It is interesting that when both the two channels are under DoS attacks, the TST is larger than that in the scenario that a single channel suffering from the DoS attack. This is the characteristic of the undirected topology.

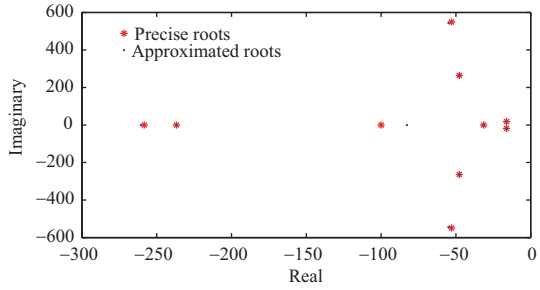

Figure 4 (Color online) Zooming in on the imaginary axis of the root loci of system (16) and the corresponding continuous system.

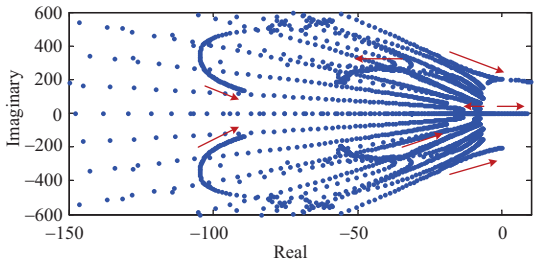

Figure 5 (Color online) Zooming in on the imaginary axis of the root loci of system (12) with the increase of the saving time caused by the DoS attack on the first channel.

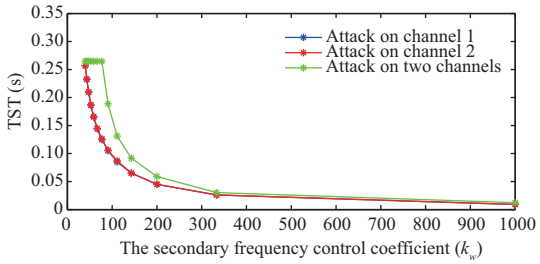

Figure 6 (Color online) The relationship of the secondary control gain k_w and the tolerant saving time when the attack launched on the channels.

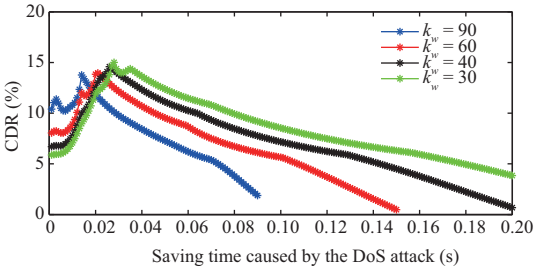

Figure 7 (Color online) The relationship of the critical damping ratio and the saving time for different k_w when the attack launched on the first channel.

The relationship of the critical damping ratio and the saving time caused by time-constrained DoS attack with different secondary control gains is shown in Figure 7. It shows that with the increasing saving time, the critical damp ratio (CDR) increases and then decreases stably. Otherwise, it also shows that when the saving time is set as 0, i.e., the cyber system is in normal operation, the CDR decreases with the increase of the secondary control gain. However, when the saving time increases, it will cross the critical time point, as the critical damp ratio is below 5%. After that, with the increasing of the secondary control gain, the CDR decreases, i.e., the dynamic robustness becomes worse. It concludes that with the increasing secondary control gains, the dynamic robustness of system will increase if the delay time is small and decrease if the delay time crosses over a critical point.

In conclusion, the microgrid with high secondary control gain has good dynamic robustness and has low TST.

4.4 Simulation results

Time-domain simulation results are performed to validate the analysis results in this subsection, which include three parts. The performance of the microgrid under normal operation and time-constrained DoS attack is tested in Subsections 4.4.1 and 4.4.2, respectively. Subsequently, the proposed adaptive control method is proved to be effective to weaken the impact caused by the time-constrained DoS attack in Subsection 4.4.3.

4.4.1 *Study 1: the cyber system is in normal operation*

The performance of microgrid with normal communication system is tested in this study. The schedule of the first channel during $t = [1, 1.01]$ s is shown in Figure 8(a). In this diagram, the state of the i-th DG increases by 0.25 when the packet containing its information arrives the transmission queue of the channel. In addition, the corresponding state increases by 0.5 when the packet is transmitted in the channel. The schedule of the second channel of the whole simulation time is shown in Figure 8(b). The saving time that the neighbor's information in the corresponding memory in the first DG is shown in Figure 8(c). In this diagram, the saving time is up to twice as the control period, $h = 1$ ms, caused by the occurrence of the packet loss. The packet loss probability of each channel is set as 0.3%. The three

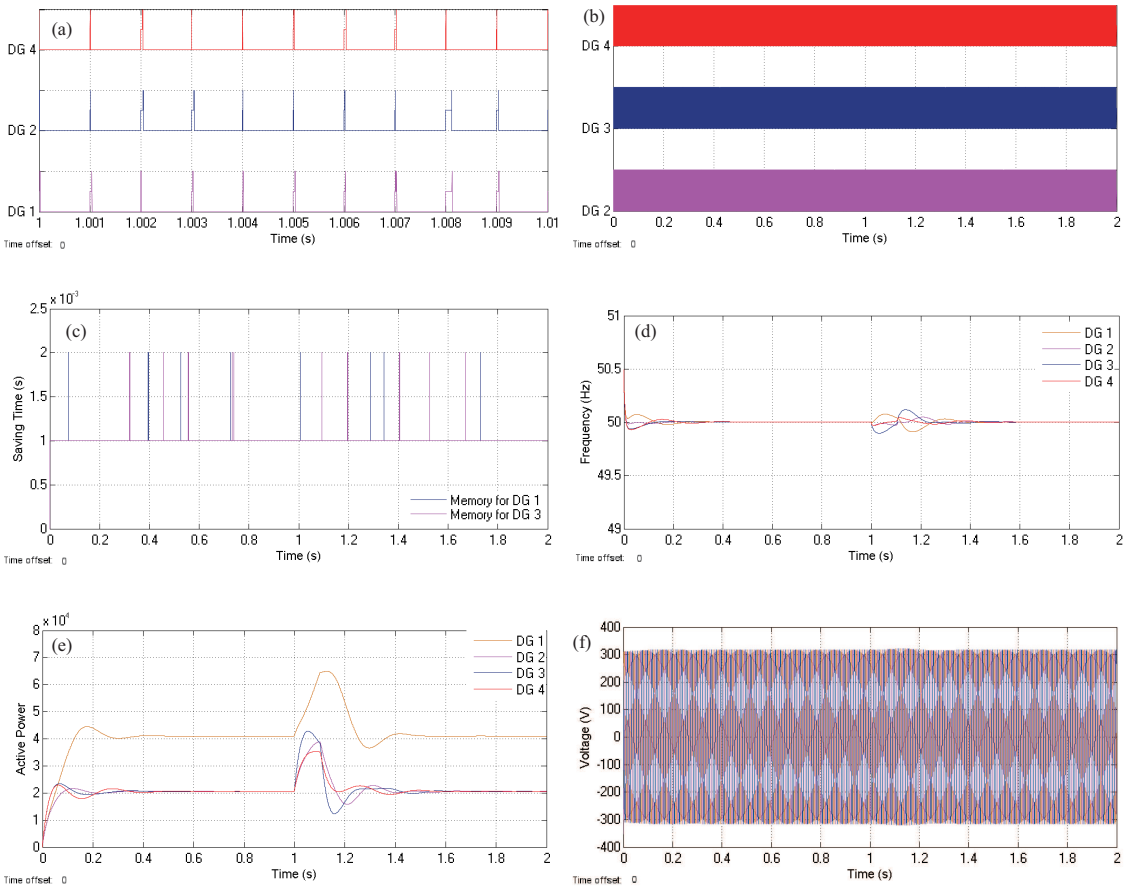

Figure 8 (Color online) Cyber and physical performance of microgrid in normal operation. (a) Zooming in on the schedule of the first channel; (b) schedule of the first channel; (c) diagram of saving time in the second DG; (d) output frequencies of DGs; (e) output active powers of DGs; (f) output voltage of the first DG.

diagrams show that the network bandwidth is enough and packets between DGs are transmitted every 1 ms. It concludes that the system achieves small-signal stability and has a good robustness, as shown in Figure 4. When a 45-kW load is plugged into the microgrid at node 9 at $t = 1$ s and plugged out at $t = 1.1$ s to simulate the disturbance, the output voltage of the first DG, the frequencies and the active power shares are shown in Figures 8(d)–(f), respectively. It also concludes that during the normal operation, the microgrid keeps stable and the active power shares perfectly when there exists load changing, i.e., the disturbance.

4.4.2 *Study 2: microgrid with communication failure*

To study the impact caused by communication failure on the microgrid, three cases are investigated in our simulation system, shown as the following. Case 1: a communication failure resulting in loss probability of two channels is up to 70% when $k_\omega = 200$. Case 2: a DoS attack of 24 MB/s is launched when $k_\omega = 200$. Case 3: a DoS attack of 24 MB/s is launched when $k_\omega = 10$. In all cases, the attack is launched on the first channel at $t = 0.5$ s and a 45-kW load is plugged in at $t = 1$ s and plugged out at $t = 1.1$ s. The corresponding results are shown in Figures 9–11, respectively.

When the packet loss probability of two channels caused by communication fault is set as 70%, the saving time of the neighbor's information increases, as shown in Figure 9(a). The output frequencies of DGs in Case 1 are shown in Figure 9(b). When the network is with 70% loss probability, the output frequencies can still reach the rated value but have a small fluctuation. That is, when the packet loss happens, the saving time in memories does not reach to the margin, which is caused by the abundant communication resources in this system.

When the attacker launches the attack of 24 MB/s on the first channel at $t = 0.5$ s, the normal communication between DGs is denied as cyber resources are consumed by the malicious packets, as

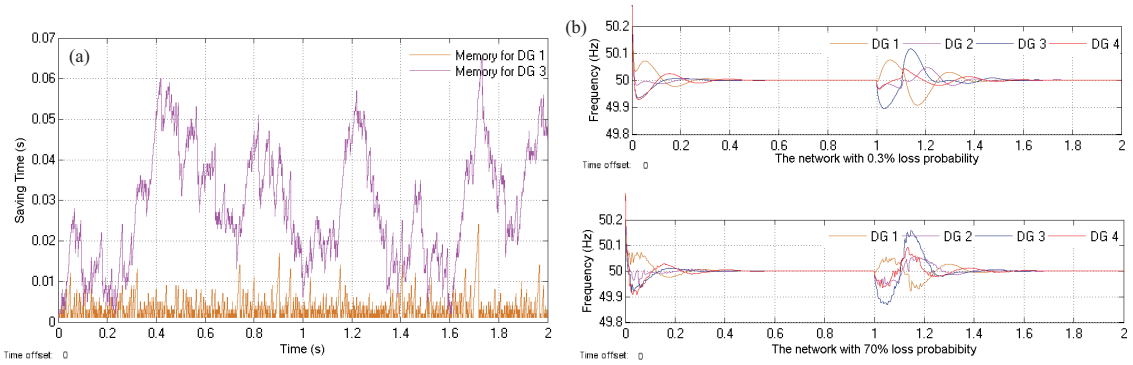

Figure 9 (Color online) Cyber and physical performance of microgrid when the packet loss probability of the network is 70%. (a) Diagram of saving time in the second DG; (b) output frequencies of DGs.

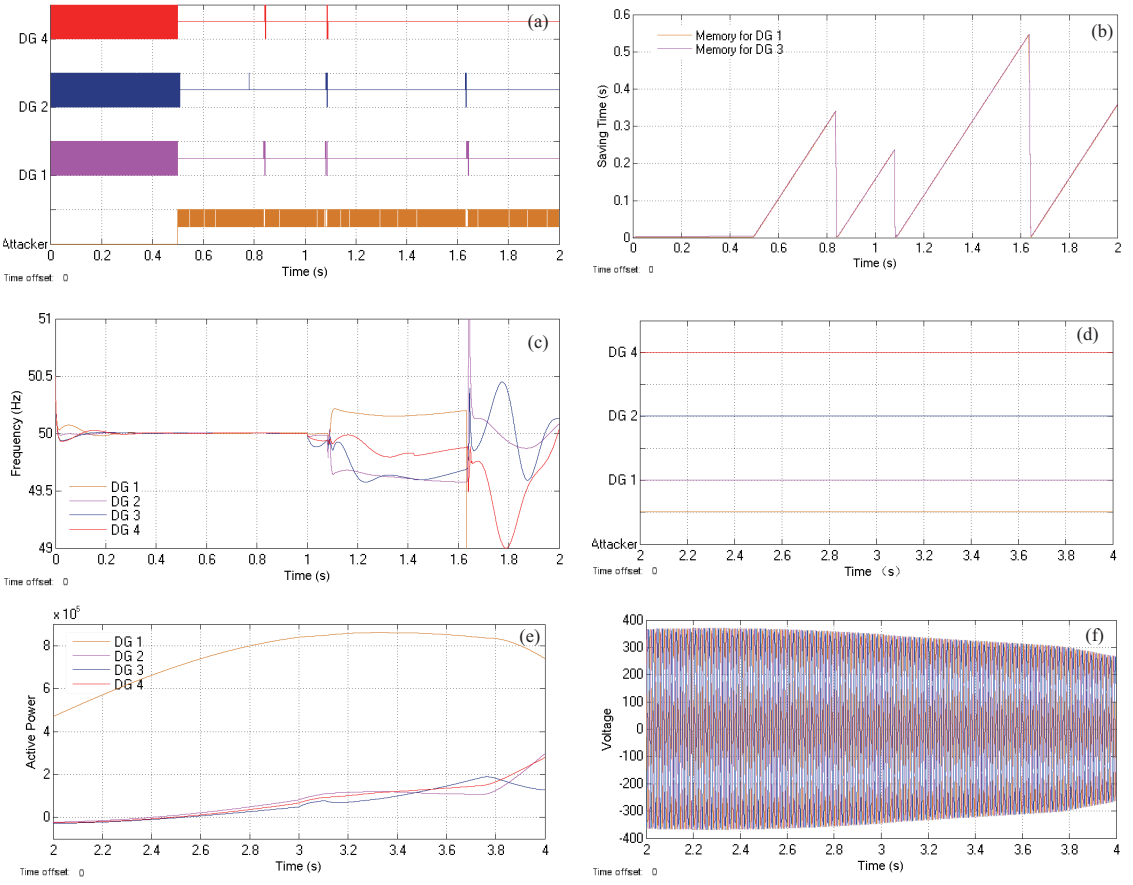

Figure 10 (Color online) Cyber and physical performance of microgrid suffering from the DoS attack when $k_\omega = 200$. (a) Schedule of the first channel; (b) diagram of saving time in the second DG; (c) output frequencies of DGs; (d) schedule of the first channel during $t = [2, 4)$; (e) output active powers for $t = [2, 4)$; (f) output voltage of the first DG for $t = [2, 4)$.

shown in Figure 10(a). As a result, the saving time of the neighbor's information becomes longer compared with Case 2, as shown in Figure 10(b). When the disturbance happens, the frequencies and output active powers fluctuate significantly, as shown in Figures 10(c) and (e). It concludes that the microgrid becomes unstable as the saving time for neighbors in the second DG is more than the tolerance margin, i.e., 0.102 s which is obtained in Subsection 4.3. As shown in Figure 10(d), during the continuous DoS attacks ($t = [2, 4)$ s), the attack impact increases so that the communication between the DGs on the first channel will be banned. The output active powers of DGs are shown in Figure 10(e) where the ordinate axis ranges from $P = -100$ kW to $P = 900$ kW during $t = [2, 4)$ s. The output powers of the DGs are out of the maximum output powers which are normally several times of the rated output active

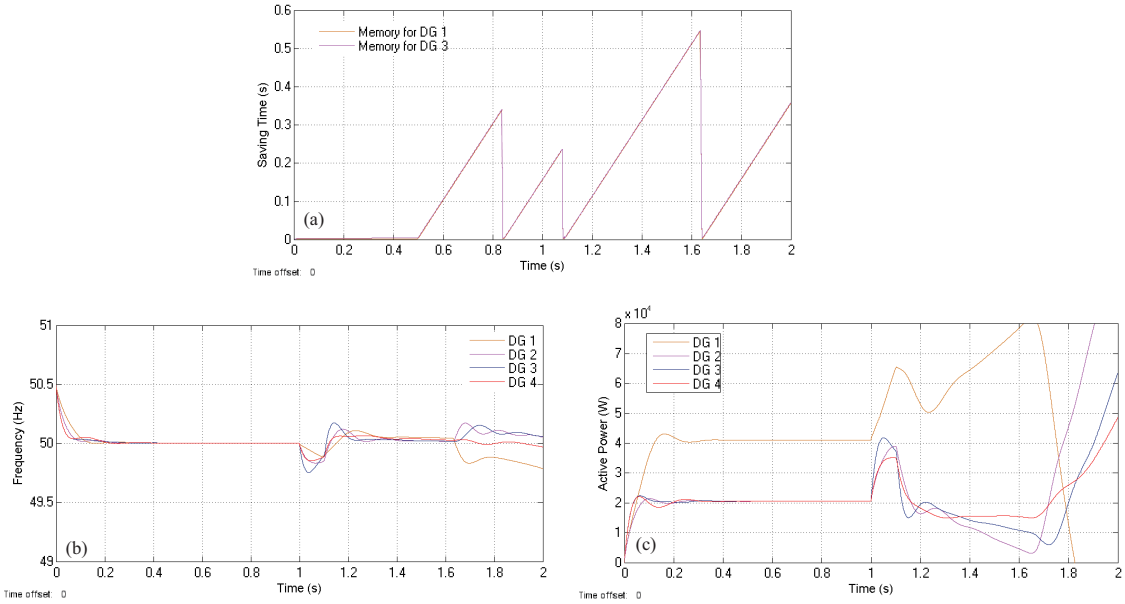

Figure 11 (Color online) Cyber and physical performance of the microgrid suffering from the DoS attack when $k_\omega = 10$. (a) Diagram of saving time in the second DG; (b) output frequencies of DGs; (c) output active powers of DGs.

power. It will cause the unstability of the microgrid which is shown in Figure 10(f). In this case, the output voltage of the first DG cannot keep the constant amplitude value which will result in damages of electric devices.

In Case 3, the control gain k_ω of secondary frequency control is set as 10 to show the impact of different control coefficients when the cyber system suffering from the same attack with Case 2. The performance of the cyber system is similar with Case 2. Comparing Figure 11(b) with Figure 10(c), we can find that fluctuations of the frequencies are smaller than Case 2. This case shows that the performance of physical system is improved if the control gain decreases when the time-constrained DoS attack happens.

4.4.3 *Study 3: the microgrid with the mitigation method*

From Figure 6, the adaptive coefficient $\beta(\tau_{ij})$ is added in the front of k_ω for each DG as

$$k_{\omega,ij} = \beta(\tau_{ij})\, k_\omega, \tag{17}$$

where

$$\beta(\tau_{ij}) = \begin{cases} 1, & \tau_{ij} < 0.05, \\ 0.025, & 0.05 \leqslant \tau_{ij} < 0.1, \\ 0.01, & 0.1 \leqslant \tau_{ij} < 0.25, \\ 0, & 0.25 \leqslant \tau_{ij}, \end{cases}$$

$\tau_{ij} = t - T_j$, t is the internal current time and T_j is the stamp time of the nearest received packet from the neighboring DG. From Figure 6, the TST is smaller than 0.05 s when the secondary control gain is lower than 180. Considering the basic control gain $k_\omega = 100$, when the delay time $\tau_{ij} < 0.05$, choose $\beta = 1$ to provide some control margins for the controllers. The TST is in the range of $[0.05, 0.1)$ when the secondary control gain is in the range of $[90, 180)$. Thus, when the delay time $0.05 \leqslant \tau_{ij} < 0.1$, choose $\beta = 0.025$. The other parameters are similarly chosen.

In this study, the cyber system is also launched with the attack of 24 MB/s when the adaptive coefficients $\boldsymbol{\beta}$ are adopted in the microgrid. The change of the real-time secondary control gain $k_{\omega,12}$ with the saving time caused by the DoS attack is shown in Figure 12(a). The $k_{\omega,12}$ decreases with the increase of saving time τ_{ij}. The performance of physical system is shown in Figures 12(b) and (c). Comparing Figures 10(b) and (c), we can find that although the speed of active power sharing becomes slow, the performance of physical system is improved when the adaptive coefficients are employed in the system.

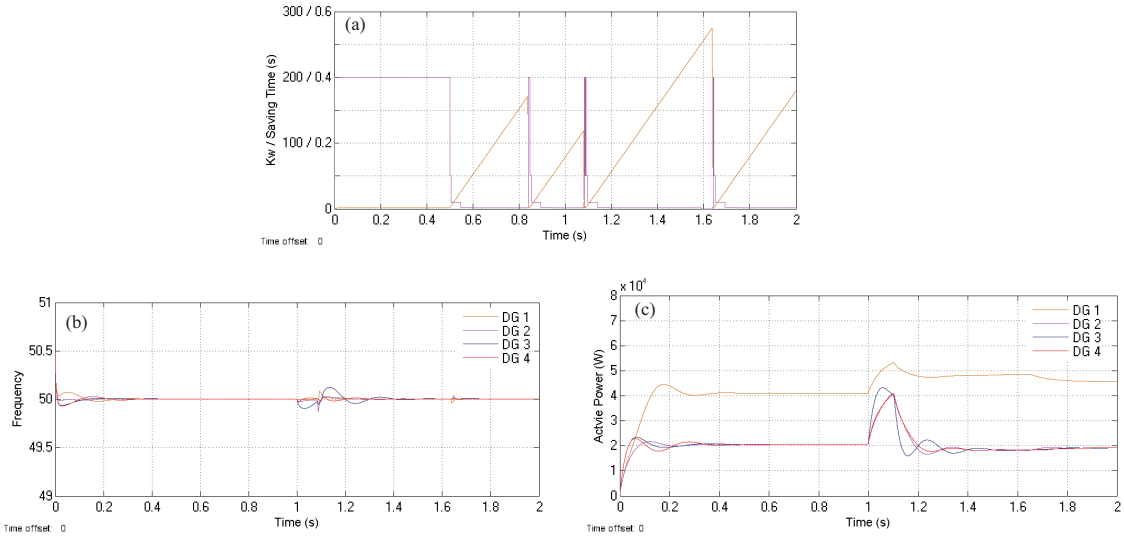

Figure 12 (Color online) Cyber and physical performance of microgrid with the adaptive secondary frequency control method. (a) Diagram of saving time in the second DG for the first DG and the real-time secondary control gain $k_{\omega,12}$ with the adaptive coefficient; (b) output frequencies of DGs; (c) output active powers of DGs.

5 Conclusion

In this paper, the time-constrained DoS attack targeting the microgrid is illustrated in detail. In this type of attack, invalid data packets are generated and thus the communication channel resources are consumed, so there exists a transmission delay of the effective data packets. Thus, through considering these transmission delays as the time delays delivered into the secondary controllers, this paper proposes an improved system for the microgrid which is applicable during time-constrained DoS attacks. To tackle the difficulty of analyzing the stability and robustness of the nonlinear system, the small-signal method is used to linearize this system and qualitatively evaluate its stability and robustness. In addition, to evaluate the impact of the delay time on a microgrid, TST is defined as the critical time that if the delay time, caused by the time-constrained DoS attack, exceeds this critical time, the microgrid system cannot achieve small-signal stability. To improve the performance of the microgrid system, the adaptive secondary control is proposed, which can dynamically change the secondary control gain values according to the saving time and TST. As shown in simulation results, it concludes that although the microgrid with high secondary control gain has good dynamic robustness, it has low TST. Thus, an adaptive secondary control method is proposed. Moreover, compared with the microgrid with a traditional control system under the time-constrained DoS attack, the microgrid with the proposed method has better performance, and it concludes that the proposed adaptive secondary control is effective.

In the simulation, the microgrid suffers a net structure in the physical system, and the DGs are plugged into the microgrid at different bus in this paper. That is to say, there is no circulating current among DGs, and then the stability of the system cannot be destroyed by the output currents distortion in the microgrid without the voltage recovery [28]. However, the voltage recovery should be applied when the microgrid suffers from the parallel structure of DGs, i.e., all the DGs are plugged into the system through the same bus. Thus, it is a challenge to analyze the stability of the microgrid with the voltage recovery with consideration of the complex information flow when the DoS attack happens for future research directions. Besides, the analysis method is based on the small-signal method, which can only be used to analyze the stability of the microgrid at the equilibrium point. We are also interested in whether the system can escape from the current equilibrium point to another equilibrium point when the equivalent delay time caused by the DoS attack crosses a certain margin. The possible solution may be found from building the Kuramoto-type model of microgrid, and it is also one of our future research directions.

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2018YFA0702200) and National Natural Science Key Foundation of China (Grant No. U20A20190).

References

1 Kashem S B A, de Souza S, Iqbal A, et al. Microgrid in military applications. In: Proceedings of IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering, Doha, 2018. 1–5
2 Sun Q Y, Han R K, Zhang H G, et al. A multiagent-based consensus algorithm for distributed coordinated control of distributed generators in the energy internet. IEEE Trans Smart Grid, 2015, 6: 3006–3019
3 Du D J, Li X, Li W T, et al. ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks. IEEE Trans Syst Man Cybern Syst, 2019, 49: 1698–1711
4 Danzi P, Stefanovic C, Meng L, et al. On the impact of wireless jamming on the distributed secondary microgrid control. In: Proceedings of IEEE GlobeCom Workshops (GC Wkshps), Washington, 2016. 1–6
5 Ye H, Liu K H, Mou Q Y, et al. Modeling and formulation of delayed cyber-physical power system for small-signal stability analysis and control. IEEE Trans Power Syst, 2019, 34: 2419–2432
6 Wang R, Sun Q Y, Ma D Z, et al. The small-signal stability analysis of the droop-controlled converter in electromagnetic timescale. IEEE Trans Sustain Energy, 2019, 10: 1459–1469
7 Wang B Y, Sun Q Y, Han R K, et al. Consensus-based secondary frequency control under denial-of-service attacks of distributed generations for microgrids. J Franklin Institute, 2021, 358: 114–130
8 Long M, Wu C H, Hung J Y. Denial of service attacks on network-based control systems: impact and mitigation. IEEE Trans Ind Inf, 2005, 1: 85–96
9 Wu J, Chen T W. Design of networked control systems with packet dropouts. IEEE Trans Automat Contr, 2007, 52: 1314–1319
10 Beg O A, Johnson T T, Davoudi A. Detection of false-data injection attacks in cyber-physical DC microgrids. IEEE Trans Ind Inf, 2017, 13: 2693–2703
11 Foroush H S, Martinez S. On event-triggered control of linear systems under periodic denial-of-service jamming attacks. In: Proceedings of IEEE 51st Annual Conference on Decision & Control, Maui, 2012. 2551–2556
12 de Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service. IEEE Trans Automat Contr, 2015, 60: 2930–2944
13 Liu S C, Hu Z J, Wang X Y, et al. Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks. IEEE Trans Ind Inf, 2019, 15: 4066–4075
14 Qin J H, Li M L, Shi L, et al. Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks. IEEE Trans Automat Contr, 2018, 63: 1648–1663
15 Lu A Y, Yang G H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. IEEE Trans Automat Contr, 2018, 63: 1813–1820
16 Milano F, Anghel M. Impact of time delays on power system stability. IEEE Trans Circuits Syst I, 2012, 59: 889–900
17 Liu S C, Wang X Y, Liu P X. Impact of communication delays on secondary frequency control in an islanded microgrid. IEEE Trans Ind Electron, 2015, 62: 2021–2031
18 Dong C Y, Jia H J, Xu Q W, et al. Time-delay stability analysis for hybrid energy storage system with hierarchical control in DC microgrids. IEEE Trans Smart Grid, 2018, 9: 6633–6645
19 Lou G N, Gu W, Xu Y L, et al. Stability robustness for secondary voltage control in autonomous microgrids with consideration of communication delays. IEEE Trans Power Syst, 2018, 33: 4164–4178
20 Xu L, Guo Q L, Wang Z G, et al. Modeling of time-delayed distributed cyber-physical power systems for small-signal stability analysis. IEEE Trans Smart Grid, 2021, 12: 3425–3437
21 Zhou J G, Sun H B, Xu Y L, et al. Distributed power sharing control for islanded single-/three-phase microgrids with admissible voltage and energy storage constraints. IEEE Transactions on Smart Grid, 2021, 14: 2760–2775
22 Guerrero J M, Vasquez J C, Matas J, et al. Hierarchical control of droop-controlled AC and DC microgrids-a general approach toward standardization. IEEE Trans Ind Electron, 2011, 58: 158–172
23 Simpson-Porco J W, Dörfler F, Bullo F. Synchronization and power sharing for droop-controlled inverters in islanded microgrids. Automatica, 2013, 49: 2603–2611
24 Guo F H, Wen C Y, Mao J F, et al. Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids. IEEE Trans Ind Electron, 2015, 62: 4355–4364
25 Saadat H. Power System Analysis. Hoboken: Wiley, 2002
26 Mumtaz F, Syed M H, Hosani M A, et al. A novel approach to solve power flow for islanded microgrids using modified Newton Raphson with droop control of DG. IEEE Trans Sustain Energy, 2016, 7: 493–503
27 Breda D. Solution operator approximations for characteristic roots of delay differential equations. Appl Numer Math, 2006, 56: 305–317
28 Wu Y, Guerrero J M, Wu Y P. Distributed coordination control for suppressing circulating current in parallel inverters of islanded microgrid. IET Gener Transm Distrib, 2019, 13: 968–975

Appendix A A small example to illustrate the small-signal model of microgrid

The process of solving the small-signal model and parameters is illustrated on a small microgrid in Figure 3.

First, the nonlinear system of this microgrid can be obtained by substituting the parameters into (4).

Second, through improved power flow analysis algorithm, an approximate solution of the proposed microgrid system, called the equilibrium point $\bar{x}$ can be calculated as

$$\begin{aligned}\bar{\boldsymbol{x}} &= [\bar{\boldsymbol{\delta}}, \bar{\boldsymbol{\omega}}, \bar{\boldsymbol{\Omega}}]^{\mathrm{T}} \\ &= [0, -0.081, -0.149, -0.114, 314.15, 314.15, 314.15, 314.15, -9.65, -9.65, -9.65, -9.65].\end{aligned}$$

Third, by taking the partial derivatives of $\boldsymbol{\delta}, \boldsymbol{\omega}, \boldsymbol{\Omega}$ from the left part of (4), it yields to the state transition matrices $\boldsymbol{A}_p$ and $\boldsymbol{A}_c$ with variables $\boldsymbol{x} = [\boldsymbol{\delta}, \boldsymbol{\omega}, \boldsymbol{\Omega}]^{\mathrm{T}}$. Then, by setting x as $\bar{x}$, the corresponding $\boldsymbol{A}_p$ and $\boldsymbol{A}_c$ are as

$$\boldsymbol{A}_p = \begin{bmatrix} \boldsymbol{0}_{N\times N} & \boldsymbol{I}_{N\times N} & \boldsymbol{0}_{N\times N} \\ A^{21}_{N\times N} = \begin{cases} ME_iE_iY_{ij}\cos(\delta_i-\delta_j), & i\neq j \\ -M\sum\limits_{i\neq j} E_iE_iY_{ij}\cos(\delta_i-\delta_j) & i=j \end{cases} & -\boldsymbol{H}_{N\times N} & \boldsymbol{H}_{N\times N} \\ \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ -5.9\times10^{4} & 331.5 & 0 & 5.9\times10^{4} & -31.4 & 0 & 0 & 0 & -31.4 & 0 & 0 & 0 \\ 663.1 & -663.1 & 1.1\times10^{-11} & 0 & 0 & -31.4 & 0 & 0 & 0 & -31.4 & 0 & 0 \\ 0 & 1.3\times10^{-11} & -1.2\times10^{5} & 1.2\times10^{5} & 0 & 0 & -31.4 & 0 & 0 & 0 & -31.4 & 0 \\ 1.2\times10^{5} & 0 & 1.2\times10^{5} & -2.3\times10^{5} & 0 & 0 & 0 & -31.4 & 0 & 0 & 0 & -31.4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\boldsymbol{A}_c = \begin{bmatrix} \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} \\ \boldsymbol{0}_{N\times N} & -\boldsymbol{K} & -\boldsymbol{K}\boldsymbol{L} \\ \boldsymbol{0}_{N\times N} & -\boldsymbol{K} & -\boldsymbol{K}\boldsymbol{L} \end{bmatrix} = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&-100&0&0&0&-200&100&0&100 \\ 0&0&0&0&0&-100&0&0&100&-200&100&0 \\ 0&0&0&0&0&0&-100&0&0&100&-200&100 \\ 0&0&0&0&0&0&0&-100&100&0&100&-200 \\ 0&0&0&0&-100&0&0&0&-200&100&0&100 \\ 0&0&0&0&0&-100&0&0&100&-200&100&0 \\ 0&0&0&0&0&0&-100&0&0&100&-200&100 \\ 0&0&0&0&0&0&0&-100&100&0&100&-200 \end{bmatrix}.$$

Finally, the small-signal model at the equilibrium point $\bar{x}$ can be obtained.