Small-signal Stability and Robustness Analysis for Microgrids under Time-constrained DoS Attack 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, University Road,* SO17 1BJ, *United Kingdom*

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 micorgrid 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

1   Introduction

The 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 system. 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, it can be seen that 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).

---

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

In general, the vulnerability of communication systems can degrade the performance of the secondary controllers, and then lead to vulnerability of the microgrid in a cross-layer fashion [3]. From some works, 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 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 DoS attacks is analyzed in this paper. Based on the analysis results, an adaptive secondary frequency control method is also proposed.
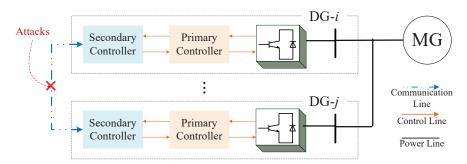

Figure 1   Hierarchical control architecture on a microgrid

Currently, research works 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 Fig. (1). DoS attacks intend to affect timeliness and success rate of data exchange and then cause a time delay and packet loss [8,9], see 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 0.3-4s, 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. Time delay model of DoS attack [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, 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 focus on small-signal stability analysis of time-delayed power system in recent time [5,16–20]. 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 distribution generations (DGs), should also be considered when analyzing stability of the microgrid. Afterwards, different from [5,19,20] in which only 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 happens 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 part should be considered, unlike existing studies which only consider the problem of convergence of the state variables related to the cyber part is considered [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 secondary control coefficient.

• The simulation shows that the performance of microgrid with the proposed adaptive secondary control system is superior to it with the traditional secondary control system as noted in Fig. 10. 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 0.05s, 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 time-constrained DoS 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 time-constrained DoS attack. The performance of microgrid under time-constrained DoS attack with proposed strategy is shown in Section 4. Finally, conclusions are summarized in Section 5.

2 Preliminaries and Related Work

Some preliminary knowledge of hierarchical control architecture of microgrid, AC power flow and small-signal model of 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 $P - \omega$ droop Control System

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

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

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

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 $P - \omega$ 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 :

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

where k_ω is the control gain, u_i is the control input of secondary controller, N_i is the set of neighbor 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 $V = \{DG - 1, DG - 2, \ldots, DG - N\}$ 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 neighbor j-th 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:

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

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

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 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 Fig. (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 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.
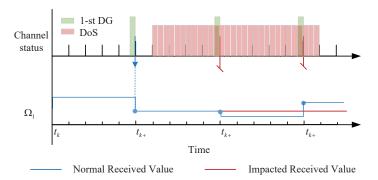

Figure 2   Diagram of the impact on the communication channel and the second DG caused by the DoS attack

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

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

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

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

where $\tau_d < t_{k+3} - t_k = \tau_{cons}$, 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 section, 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 section 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 section 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 $P - \omega$ 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 Eqn. (1b), Eqn. (2), and Eqn. (3) into the derivative of Eqn. (1a), the details of this model are as follows:

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

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

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

where N_j 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 Eqn. (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 $\mathbf{\Omega}$ cannot be calculated. To solve this problem, an improved power flow analysis method is proposed in this section, 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 is modified as:

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

$$\boldsymbol{\Phi}' = \left[\Delta \boldsymbol{P}^T \ \Delta \boldsymbol{Q}^T \ P_{tot} - P_{sys} \ Q_{tot} - Q_{sys} \ \Delta \boldsymbol{\Omega} \right] \tag{5b}$$

where $\boldsymbol{\delta}$ and $|\boldsymbol{V}|$ are respectively the vectors of voltage angels and magnitudes of all the buses 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, $\Delta \boldsymbol{P}^T$ and $\Delta \boldsymbol{Q}^T$ 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 buses, 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, $k_\omega (\omega_i - \omega^*) + k_\omega \left(\sum_{j \in N_i} a_{ij}(\Omega_i - \Omega_j) \right) = 0$ 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]),

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

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

3.1.3 Small-Signal 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 Eqn. (4), and the linearization process is as follows.

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

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

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

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

. .

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

$$\boldsymbol{A} = \begin{bmatrix} \frac{\partial f}{\partial \delta}\big|_{\bar{\delta}} & \frac{\partial f}{\partial \omega}\big|_{\bar{\omega}} & \frac{\partial f}{\partial \Omega}\big|_{\bar{\Omega}} \\ \frac{\partial g}{\partial \delta}\big|_{\bar{\delta}} & \frac{\partial g}{\partial \omega}\big|_{\bar{\omega}} & \frac{\partial g}{\partial \Omega}\big|_{\bar{\Omega}} \\ \frac{\partial h}{\partial \delta}\big|_{\bar{\delta}} & \frac{\partial h}{\partial \omega}\big|_{\bar{\omega}} & \frac{\partial h}{\partial \Omega}\big|_{\bar{\Omega}} \end{bmatrix}, \tag{8}$$

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

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

in which $\boldsymbol{x} = \begin{bmatrix} \Delta\boldsymbol{\delta} & \Delta\boldsymbol{\omega} & \Delta\boldsymbol{\Omega} \end{bmatrix}^T$, $M_i = m_i\eta_i$, $\boldsymbol{M} = diag(M_i)$, $\boldsymbol{K} = diag(k_\omega)$, $\boldsymbol{H} = diag(\eta)$ and

$$\boldsymbol{A}_p = \begin{bmatrix} \boldsymbol{0}_{N\times N} & \boldsymbol{I}_{N\times N} & \boldsymbol{0}_{N\times N} \\ \boldsymbol{A}^{21}_{N\times N} & -\boldsymbol{H}_{N\times N} & \boldsymbol{H}_{N\times N} \\ \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} \end{bmatrix}, \boldsymbol{A}_c = \begin{bmatrix} \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} & \boldsymbol{0}_{N\times N} \\ \boldsymbol{0}_{N\times N} & -\boldsymbol{K} & -\boldsymbol{KL} \\ \boldsymbol{0}_{N\times N} & -\boldsymbol{K} & -\boldsymbol{KL} \end{bmatrix},$$

in which $\boldsymbol{A}^{21}_{N\times N} = -\boldsymbol{M}\frac{\partial \boldsymbol{P}_e}{\partial \boldsymbol{\delta}}$. In Eqn. (9), $\boldsymbol{A}_p$ models the physical connection and the control structure of microgrid, called as 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.

3.2 Stability and Robustness Analysis of Small-signal model when the Microgrid under 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 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 Eqn. (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, $t_d < t_k$, and $\tau_d < \tau_{max}$,

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

$\boldsymbol{D}^d$ 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

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

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

3.2.2 *Root Approximation Method*

Since the number of roots for Eqn. (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 Eqn. (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 Eqn. (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, $\tau_d = t_{k+1} - t_d$, $h < \tau_1 < ... < \tau_d < ... < \tau_{N_d} = \tau_{max}$. Denote $\boldsymbol{\tau} = \{\tau_1, \cdots, \tau_{N_d}\}$ is 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 Eqn. (12) on the $(\gamma + 1)$-th block. Thus, the discretization matrix $(\boldsymbol{S}_M)$ of the solution operator $T(l)$ of Eqn. (12) can be obtained as

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

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

For the system Eqn. (12),

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

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

3.2.3 *Stability and Robustness Analysis of Small-Signal model of Microgrid under time-constrained DoS attack*

In this subsection, the stability and the robustness of the small-signal model of microgrid are evaluated according to the root distribution of Eqn. (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 $\boldsymbol{\tau}$, denote $\vec{d} = \{d_1,\cdots,d_{N_d}\}$ as the corresponding Boolean vector, where $d_i = 1$ if the i-th channel is suffering from DoS attack; otherwise, $d_i = 0$. To evaluate the time-constrained DoS attack, an index, tolerant saving time (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 $\tau_{max} < TST$ and the root trace intersects the imaginary axis for $\tau_{max} > TST$. The procedure of the proposed analysis approach is shown in Algorithm. 1.

Algorithm 1 Analysis Approach When the Microgrid Suffer from time-constrained DoS attack

    for $i = 1:1:\bar{N}_d$

        Establish the small-signal model of microgrid, i.e. Eqn. (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 Eqn. (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 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 section 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 DGs is stored in i-th DG. The gain scheduler is determined by the discretized relationship between secondary control gains and the TST. Thus, $\beta_{\tau(z)}^j$ is a piecewise-constant function of the delay time $\tau_{ij} = t - T_j$, where T_j is the time stamp, and

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

where $\tau(z)$ is the time interval $z = 1, 2, \cdots, N_\tau$ 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:
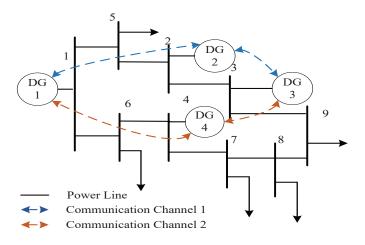
1. First, the j-th DG samples the secondary control variable $\Omega^{T_j}_j$ at time T_j, and sends it with the time stamp T_j to its neighboring DGs.

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

3. When the controller in i-th DG is periodically triggered, the saving time $\tau_{ij} = t - T_j$ is calculated for each neighboring DGs, and the input of secondary control u_i is calculated according to Eqn. (15) and the variables stored from 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 performances of the microgrid under the normal communication is illustrated. Otherwise, when time-constrained DoS attack occur, the effectiveness of the microgrid with the proposed adaptive control method and the traditional method are tested, respectively. It shows the effectiveness of the proposed control method.

4.1 Simulation Setup

A microgrid architecture shown in Fig. 3 is used to perform the proposed control approach. The system parameters are reported in Tab. 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 network, two communication channels are set and simulated using Truetime Tools in the simulation. The information on the first channel and the second channel deliver the information from the first, second and 4-th DG, and the information from the second, thrid and 4-th DG, respectively. The control period of secondary control in DGs is set as $h = 1$ms and for all DGs, and $k_\omega = 200$.

Figure 3 The structure of the simulated microgrid

Table 1 Electrical and Control Parameters

Parameter	Symbol	Value	Parameter	Symbol	DG-1	DG-2&3&4
Rated Frequency	$\omega^*/2\pi$	50Hz	Rated Active Power	P_{ratei}	66 kW	33 kW
DC Votlage	V_{dc}	800V	Rated Reactive Power	Q_{ratei}	0 kVAr	0 kVAr
Nominal Voltages	E_*	220V	Current Loop P-Coeff.	K_{CP}	6.72	10.5
Filter Capacitance	C_f	40 μF	Current Loop I-Coeff.	K_{CI}	3360	3360
Filter Inductance	L_f	0.2mH	Voltage Loop P-Coeff.	K_{VP}	0.2	0.2
Output Inductance	L_0	0.2mH	Voltage Loop I-Coeff.	K_{VI}	480	480
Power Filter Coeff.	τ_P	0.0318	$P - f$ Droop Coeff.	m_i	7.5e-6 $\frac{Hz}{W}$	1.5e-5 $\frac{Hz}{W}$
Line Impedance	Z	0.1+0.31j Ω	$Q - E$ Droop Coeff.	n_i	2e-4 $\frac{V}{VAr}$	2e-4 $\frac{V}{VAr}$

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 Tab. 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.

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	

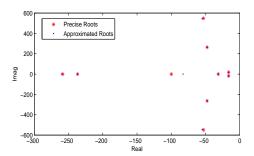## 4.3 Stability and Robustness Analysis of a Small Example

The accuracy of the root approximation method is discussed in this section 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 can be written at $t = t_{k+1}$ 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. The 2-stage and 3-order Runge-Kutta method with $\boldsymbol{R} = \begin{bmatrix} 5/12 & -1/12 \\ 3/4 & 1/4 \end{bmatrix}$ is used and $M = 6$ in this case. Generally, when the control period is small, some of approximated roots of Eqn. 16 are close to precise roots of the continuous system $\dot{\boldsymbol{x}} = \left(\boldsymbol{A}_p + \boldsymbol{A}_c\right)\boldsymbol{x}$. A zoom of the eigenvalue of System Eqn. (16) and the continuous system is shown in Fig. 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 is small-signal stable 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
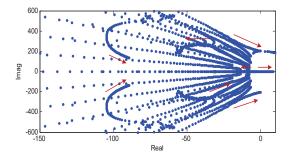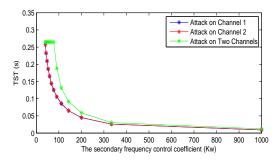
Figure 4 Zoom close to the imaginary axis of the root loci of System Eqn. (16) and the corresponding continuous system

Figure 5 Zoom close to the imaginary axis of the root loci of System Eqn. (12) with the increase of the saving time caused by the DoS attack on the first channel

in Fig. (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 $0.102s$ and in this scenario, the TST is $0.102s$. Afterwards, the relationship between TST and secondary control gains under different directions of time-constrained DoS attack is illustrated in Fig. (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 first or second channel. This is because the first and second channel are symmetrical in the communication topology. What's interesting is that when both the two channels are under DoS attack, the TST is larger than the one while a single channel suffering from the DoS attack. This is the characteristic of the undirected topology.
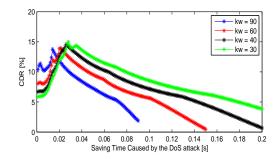

Figure 6 The relationship of the secondary control gain k_w and the tolerant saving time when the attack launched on the channels

Figure 7 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 Fig. (7). It shows that with the increasing saving time, the 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 critical damp ratio (CDR) decreases with the increase of the secondary control gain. However, when the saving time is 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, it has low TST.

4.4 Simulation Results

Time-domain simulation results are performed to validate the analysis results in this section, which include three parts. The performance of the microgrid under normal operation and time-constrained DoS

attack is tested in subsection4.4.1 and subsection4.4.2, respectively. Subsequently, the proposed adaptive control method is proved to be effective to weaken the impact caused by time-constrained DoS attack in subsection4.4.3.

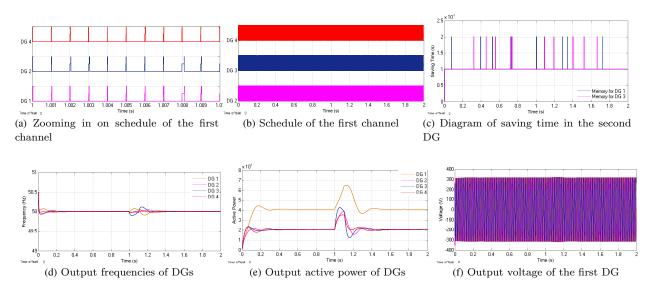### 4.4.1 *Study 1: The cyber system is in normal operation*

(a) Zooming in on 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 power of DGs

(f) Output voltage of the first DG

Figure 8 Cyber and physical performance of microgrid 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 Fig. (8a). In this diagram, the state of 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 transmitting in the channel. The schedule of the second channel of the whole simulation time is shown in Fig. (8b). The saving time that the neighboring's information in the corresponding memory in the first DG is shown in Fig. (8c). 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 diagrams show that the network bandwidth is enough and packets between DGs are transmitted every 1ms. It concludes that the system is small-signal stable and has a good robustness, as shown in Fig. (4). When a 45-kW Load is plugged into the microgrid at node 9 at t = 1s and plugged out at t = 1.1s to simulate the disturbance, the output voltage of the first DG , the frequencies and the active power shares are shown in Fig. (8) (d)-(f), respectively. It also concludes that during the normal operation, the microgrid keeps stable and the active power shares perfectly when there exits 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: 1) Case 1: a communication failure resulting in loss probability of two channels is up to 70% when $k_\omega = 200$; 2) Case 2: a DoS attack of 24MB/s is launched when $k_\omega = 200$; 3) Case 3: a DoS attack of 24MB/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 = 1s and plugged out at t = 1.1s. The corresponding results are shown in Fig. (9), (10) and (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 Fig. (9a). The output frequencies of DGs in Case 1 are zoomed in Fig. (9b). 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
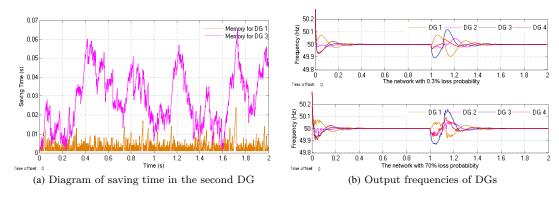
(a) Diagram of saving time in the second DG

(b) Output frequencies of DGs

Figure 9 Cyber and physical performance of microgrid when the packet loss probability of the network is 70%

saving time in memories is not reach to the margin, which is cause by the abundant communication resources in this system.
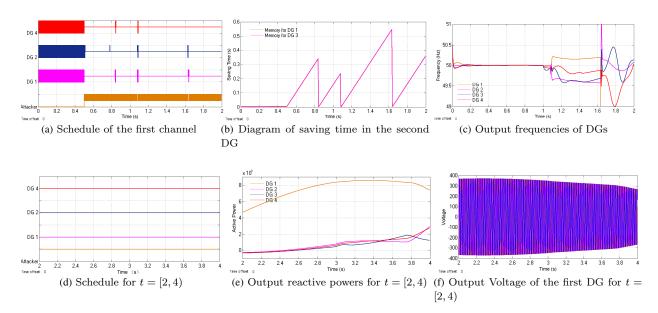

(a) Schedule of the first channel

(b) Diagram of saving time in the second DG

(c) Output frequencies of DGs

(d) Schedule for $t = [2, 4)$

(e) Output reactive powers for $t = [2, 4)$

(f) Output Voltage of the first DG for $t = [2, 4)$

Figure 10 Cyber and physical performance of microgrid suffering from the DoS attack when $k_\omega = 200$

When the attacker launches the attack of 24MB/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 shown in Fig. (10a). As a result, the saving time of the neighbor's information becomes longer compared with Case 2, as shown in Fig. (10b). When the disturbance happens, the frequencies and output active powers fluctuate significantly, as shown in Fig. (10c) and Fig. (10d). 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., 0.102s which is obtained in Section 4.3. As shown in Fig. (10d), during the continuous DoS arrack ($t = [2, 4)s$), 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 Fig. (10e) where the ordinate axis ranges from $P = -100kW$ to $P = 900kW$ 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 power. It will cause the unstability of the microgrid which is shown in Fig. (10f). 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 coefficient when the cyber system suffering from the same attack with Case 2. The performance
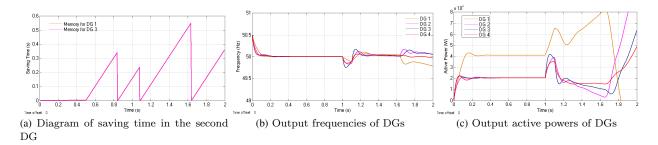
(a) Diagram of saving time in the second DG

(b) Output frequencies of DGs

(c) Output active powers of DGs

Figure 11 Cyber and physical performance of microgrid suffering from the DoS attack when $k_\omega = 10$

of the cyber system is similar with Case 2. Compared Fig. (11b) with Fig. (10c), 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 time-constrained DoS attack happens.

4.4.3 *Study 3: The microgrid with the mitigation 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

Figure 12 Cyber and physical performance of microgrid with the adaptive secondary frequency control method

From Fig. (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 Fig. 6, the TST is smaller than 0.05s 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 24MB/s when the adaptive coefficients β 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 Fig. (12a). The $k_{\omega,12}$ decreases with the increase of saving time τ_{ij}. The performance of physical system is shown in Fig. (12b) and Fig. (12c). Compared with Fig. (10b) and Fig. (10c), 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.

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 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 is not small signal stable. 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 buses 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 also interest 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.

Appendix

A Small Example to Illustrate the Small-signal Model of Microgrid

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

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

$$\bar{\boldsymbol{x}} = [\bar{\boldsymbol{\delta}}, \bar{\boldsymbol{\omega}}, \bar{\boldsymbol{\Omega}}]^T$$

$$= [0 - 0.081, -0.149, -0.114, 314.15, 314.15, 314.15, 314.15, -9.65, -9.65, -9.65, -9.65].$$

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

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

$$= \begin{bmatrix}
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
-5.9 \times 10^4 & 331.5 & 0 & 5.9 \times 10^4 & -31.4 & 0 & 0 & 0 & -31.4 & 0 & 0 & 0 \\
663.1 & -663.1 & 1.1 \times 10^{-11} & 0 & 0 & -31.4 & 0 & 0 & 0 & -31.4 & 0 & 0 \\
0 & 1.3 \times 10^{-11} & -1.2 \times 10^5 & 1.2 \times 10^5 & 0 & 0 & -31.4 & 0 & 0 & 0 & -31.4 & 0 \\
1.2 \times 10^5 & 0 & 1.2 \times 10^5 & -2.3 \times 10^5 & 0 & 0 & 0 & -31.4 & 0 & 0 & 0 & -31.4 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix},$$

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

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

References

1 Saad Bin Abul Kashem, Stephanie De Souza, Atif Iqbal, and et al. Microgrid in military applications. In *Proceedings of 2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering*, Doha, Qatar, 2018. 1-5.

2 Qiuye Sun, Renke Han, Huaguang Zhang, and et al. A multiagent-based consensus algorithm for distributed coordinated control of distributed generators in the energy internet. *IEEE Transactions on Smart Grid*, 2015. 6:3006-3019.

3 Dajun Du, Xue Li, Wenting Li, and et al. Admm-based distributed state estimation of smart grid under data deception and denial of service attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019. 49:1698-1711.

4 Pietro Danzi, Cedomir Stefanovic, Lexuan Meng, and et al. On the impact of wireless jamming on the distributed secondary microgrid control. In *Proceedings of 2016 IEEE Globecom Workshops (GC Wkshps)*, Washington, DC, United states, 2016. 1-6.

5 Hua Ye, Kehan Liu, Qianying Mou, and et al. Modeling and formulation of delayed cyber-physical power system for small-signal stability analysis and control. *IEEE Transactions on Power Systems*, 2019. 34:2419 - 2432.

6   Rui Wang, Qiuye Sun, Dazhong Ma, and et al. The small-signal stability analysis of the droop-controlled converter in electromagnetic timescale. *IEEE Transactions on Sustainable Energy*, 2019. 10:1459 - 1469.

7   Bingyu Wang, Qiuye Sun, Renke Han, and et al. Consensus-based secondary frequency control under denial-of-service attacks of distributed generations for microgrids. *Journal of the Franklin Institute*, 2021. 358:114 - 130.

8   Men Long, Chwan-Hwa Wu, and John Y. Hung. Denial of service attacks on network-based control systems: Impact and mitigation. *IEEE Transactions on Industrial Informatics*, 2005. 1:85-96.

9   Jing Wu and Tongwen Chen. Design of networked control systems with packet dropouts. *IEEE Transactions on Automatic Control*, 2007. 52:1314-1319.

10 Omar Ali Beg, Taylor T. Johnson, and Ali Davoudi. Detection of false-data injection attacks in cyber-physical dc microgrids. *IEEE Transactions on Industrial Informatics*, 2017. 13:2693 - 2703.

11 Hamed Shisheh Foroush and Sonia Martinez. On event-triggered control of linear systems under periodic denial-of-service jamming attacks. In *IEEE 51st Annual Conference on Decision & Control*, Hawaii, USA, 2012. 2551-2556.

12 Claudio De Persis and Pietro Tesi. Input-to-state stabilizing control under denial-of-service. *IEEE Transactions on Automatic Control*, 2015. 60:2930 - 2944.

13 Shichao Liu, Zhijian Hu, Xiaoyu Wang, and et al. Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks. *IEEE Transactions on Industrial Informatics*, 2019. 15:4066 - 4075.

14 Jiahu Qin, Menglin Li, Ling Shi, and et al. Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks. *IEEE Transactions on Automatic Control*, 2018. 63:1648 - 1663.

15 Anyang Lu and Guanghong Yang. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. *IEEE Transactions on Automatic Control*, 2018. 63:1813 - 1820.

16 Federico Milano and Marian Anghel. Impact of time delays on power system stability. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2012. 59:889 - 900.

17 Shichao Liu, Xiaoyu Wang, and Peter Xiaoping Liu. Impact of communication delays on secondary frequency control in an islanded microgrid. *IEEE Transactions on Industrial Electronics*, Apr. 2015. 62:2021 - 2031.

18 Chaoyu Dong, Hongjie Jia, Qianwen Xu, and et al. Time-delay stability analysis for hybrid energy storage system with hierarchical control in dc microgrids. *IEEE Transactions on Smart Grid*, 2018. 9:6633 - 6645.

19 Guannan Lou, Wei Gu, Yinliang Xu, and et al. Stability robustness for secondary voltage control in autonomous microgrids with consideration of communication delays. *IEEE Transactions on Power Systems*, 2018. 33:4164-4178.

20 Luo Xu, Qinglai Guo, Zhongguan Wang, and et al. Modeling of time-delayed distributed cyber-physical power systems for small-signal stability analysis. *IEEE Transactions on Smart Grid*, 2021. Published online. Doi:10.1109/TSG.2021.3052303.

21 Jianguo Zhou, Hongbin Sun, Yinliang Xu, and 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. Published online. Doi:10.10.1109/TSG.2021.3057899.

22 Josep M. Guerrero, Juan C. Vasquez, Jose Matas, and et al. Hierarchical control of droop-controlled ac and dc microgrids - a general approach toward standardization. *IEEE Transactions on Industrial Electronics*, 2011. 58:158 - 172.

23 John W. Simpson-Porco, Florian Dorfler, and Francesco Bullo. Synchronization and power sharing for droop-controlled inverters in islanded microgrids. *Automatica*, 2013. 49:2603 - 2611.

24 Fanghong Guo, Changyun Wen, Jianfeng Mao, and et al. Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids. *IEEE Transactions on Industrial Electronics*, 2015. 62:4355 - 4364.

25 Hadi Saadat. *Power System Analysis*. Wiley, 2002.

26 Faisal Mumtaz, M.H. Syed, Mohamed Al Hosani, and et al. A novel approach to solve power flow for islanded microgrids using modified newton raphson with droop control of dg. *IEEE Transactions on Sustainable Energy*, 2016. 7:493-503.

27 Dimitri Breda. Solution operator approximations for characteristic roots of delay differential equations. *Applied Numerical Mathematics*, 2006. 56:305-317.

28 Ying Wu, Josep M. Guerrero, and Yanpeng Wu. Distributed coordination control for suppressing circulating current in parallel inverters of islanded microgrid. *IET Generation, Transmission and Distribution*, 2019. 13:968 - 975.