Consensus-based secondary frequency control under denial-of-service attacks of distributed generations for microgrids

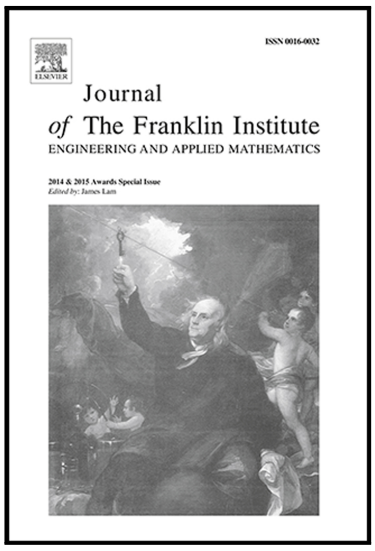
Wang, Bingyu; Sun, Qiuye; Han, Renke; Ma, Dazhong

Published in:
Journal of the Franklin Institute

DOI (link to publication from Publisher):
10.1016/j.jfranklin.2019.01.007

Publication date:
2021

Document Version
Accepted author manuscript, peer reviewed version



Consensus-Based Secondary Frequency Control under Denial-of-Service Attacks of Distributed Generations for Microgrids

Bingyu Wang, Qiuye Sun, Renke Han, Dazhong Ma

PII: S0016-0032(19)30035-3
DOI: https://doi.org/10.1016/j.jfranklin.2019.01.007
Reference: FI 3742

To appear in: *Journal of the Franklin Institute*

Received date: 31 March 2018
Revised date: 9 December 2018
Accepted date: 6 January 2019

Please cite this article as: Bingyu Wang, Qiuye Sun, Renke Han, Dazhong Ma, Consensus-Based Secondary Frequency Control under Denial-of-Service Attacks of Distributed Generations for Microgrids, *Journal of the Franklin Institute* (2019), doi: https://doi.org/10.1016/j.jfranklin.2019.01.007

Consensus-Based Secondary Frequency Control under Denial-of-Service Attacks of Distributed Generations for Microgrids

Bingyu Wang[a], Qiuye Sun[a,*], Renke Han[b], Dazhong Ma[a]

[a] *Northeastern University. Shenyang, Liaoning 110819, China*
[b] *Aalborg University. Aalborg, North Denmark, Denmark*

Abstract

In this paper, Denial-of-Service (DoS) attacks on a microgrid (MG), especially on service-provider-edge routers in the MG, are considered and analysed. To increase the tolerance of the MG for DoS attacks with decreased computing time, we present consensus-based secondary frequency controllers with dynamic P-f droop controllers. Then, with the consideration of the impact on these controllers caused by DoS attacks, a state-space model of the MG is established based on which the stability analysis is derived. Finally, the effectiveness of the method is verified by simulation and experimental results.

Keywords: Cyber-physical system, DoS attacks, Hierarchical control structure, Microgrid, Multi-agent systems

2010 MSC: 00-01, 99-00

1. Introduction

Microgrids (MGs), which facilitate deep integration of distributed generations (DGs), storage systems and modern load, have gained significant attention[1, 2]. And numerous research results have been reported in recent years, which include frequency regulation, power allocation, power control game, etc[3, 4, 5].

*Corresponding author

Email addresses: www.wwbbyy@qq.com (Bingyu Wang), sunqiuye@mail.neu.edu.cn (Qiuye Sun), hanrenke.neu@gmail.com (Renke Han), madazhong@ise.neu.edu.cn (Dazhong Ma)

Most of control strategies of the results are based on network system and technology, which makes MGs work as typical cyber-physical systems(CPSs). These strategies are aggregated into a hierarchical control architecture of these CPSs. However due to open communication in the control hierarchy, there is a potential risk that vulnerabilities in communication systems are maliciously exploited by some people, usually called attackers. For attackers who have full knowledge of MGs, secondary control of the control hierarchy relying on communication can be their targets, which may result in aberrant operation of systems.

Generally speaking, common attacks adopted by attackers mainly include False Data Injection (FDI) and Denial-of-Service (DoS) attacks. The former erode the trustworthiness of data by inputting false information to original data. Interested readers can find further information about FDI attacks in [6]. The latter are the main topic of this paper causing significant disruptions to communication networks by jamming spectrum bands by jammers, flooding target channels by malicious packets and so on[7, 8]. Further, some researches were carried out to analyze the impact on the systems' stability caused by DoS attacks,. Long *et al.*[9] established two queue models in order to analyze the impact on network-based control systems(NBCSs)caused by DoS attacks. Later Foroush *et al.* [10] proposed an event-triggered control method for linear systems under specific DoS attacks i.e., periodic/PWM jamming attacks. A more common model of DoS attacks with frequency and duration constraints was established by Persis and Tesi [11] for the sake of designing resilient control logics to reserve input-to-output stability of closed-loop systems. Under this model, an event-triggered control logic for NCBSs under attacks was proposed in [12]. Meanwhile in multi-area power systems under energy-limited DoS attacks, Peng *et al.* [13] proposed an algorithm to obtain the resilient event-triggering parameters for load frequency controllers. In addition, an optimal attack scheduling scheme was derived for networks with packet-dropping[7]. Although these researches are practical for their systems, few researches have been focused on secondary control in MGs under DoS attacks, which may result in instability of microgrids.

Motivated by this issue, we attempted to analyze stability of a MG under DoS attacks. The MG adopted a consensus-based secondary frequency control strategy with a dynamic P-f droop control method with the purpose of increasing the tolerance for DoS attacks. To achieve the above objectives, the main idea of this paper is capable of (i) regulating the droop parameter according to the differential of active power in primary control; (ii)transferring the model of the MG to a state-space representation including the model of the primary P-f controllers, consensus-based secondary controllers and DoS attacks; (iii) analyzing stability of the MG with a suitable Lyapunov-Krasovskii functional.

The paper is organized as follows. In section 2, preliminaries are defined. The structure and operation principle of the MG are in section 3. In section 4, the consensus-based frequency control strategy with a dynamic P-f control method is described and the model of the system is represented. The main theorem is given by modeling DoS attacks in section 5. Simulation and experiment results are presented in Section 6. Finally, the paper is concluded in Section 7.

2. Preliminaries

A finite set of ϑ is given and $|\vartheta|$ represents its cardinality. $G(\nu, \varepsilon, A)$ represents the MG, in which the set of nodes including DGs and loads, the set of edges and the adjacency matrix are represented by ν, $\varepsilon \subseteq \nu \times \nu$ and $A \in R^{|\nu|\times|\nu|}$, respectively. The graph G has a directed spanning tree if there exists a root node with a direct path from that node to every other node. The node-edge incidence matrix is defined as $B \in R^{|\nu|\times|\varepsilon|}$, where $B_{kl} = 1$ if node k is the sink node of edge l, $B_{kl} = -1$ if node k is the source of edge l, and other elements in the l-th column are zero. For $x \in R^{|\nu|}$, $B^T x \in R^{|\varepsilon|}$ is the vector expressing the component $x_i - x_j$ with $\{i, j\} \in \varepsilon$. For $\chi \in [0, \pi/2]$, let $\Delta_G(\chi) = \left\{\theta : \max_{\{i,j\}\in\varepsilon} |\theta_i - \theta_j| < \chi\right\}$ be a closed set about angles of voltage. And deviations between angles are no more than χ. Neighbors of node ν_i are represented by $N_i = \{v_j | (v_j, v_i) \in \varepsilon\}$. In this paper, it is assumed that the impedance is inductive. Here are some notations: purely inductive admittance

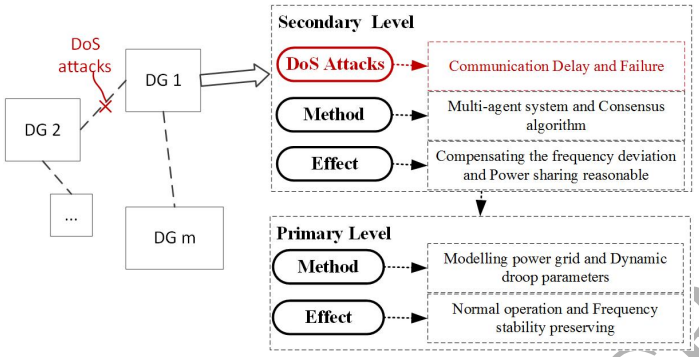


Figure 1: Control Structure of the MG.

matrix $Y \in jR^{n\times n}$, nodal voltage magnitudes $E_i > 0$, nodal voltage phase angle θ_i, the frequency ω_i is the differential of θ_i. Define the weighted matrix $C = diag\left(\{c_{ij}\}_{\{i,j\}\in\varepsilon}\right)$ where $c_{ij} = E_i E_j |Y_{ij}|$. The weighted Laplacian matrix L is defined as $L = BCB^T$ in primary control considering the physical connection and power flow. For $x \in R^n$, define $x^{\perp} \triangleq \{z \in R^n | x^T z = 0\}$. There exists a unique $\gamma \in R^{|\varepsilon|}$ representing the power flow for branch vector. According to the Kirchoofs Current Law, the branch vectors satisfy $P = B\gamma$.

3. Structure and Operating Principle of Microgrids

In this section, the hierarchical control structure is presented to analyze operation principle of the MG. Then based on operation principle, especially communication principle, vulnerabilities are analyzed which could be maliciously exploited by attackers.

There are two control levels in the microgrid shown in Fig. 1, in which the first level is primary control and the other is secondary control. Primary control can be seen as the physical part of the MG which contains the inner current control loop, the outer voltage control loop and the droop control loop. The droop controller in the droop control loop supplies reference inputs for the outer voltage control loop in an inverter of a DG which can rapidly regulate output current and voltage. For droop controllers in the MG, their parameters are

designed according to rated powers of DGs. Although these controllers can guarantee stability of the MG, they draw the bus voltages and frequencies of DGs from nominal values. So secondary control is applied to compensate the deviations completely by moving the droop curves up or down[14].

In secondary control, the consensus-based control frequency method was used to compensate frequency deviations. In this paper, it is assumed that the primary source can satisfy the load variation, and the total load does not surpass the upper limit. Then the intercept of droop curves can be regulated up and down within the stability range. By application of this method, deviations of frequency could be mitigated completely no matter whether the load power is constant or not.

In secondary control, DGs, regarded as agents, communicate frequency information with their neighbors. The communication between DGs in the MG is realized based on the UDP, a common and susceptible protocol. During the communication process, packets containing frequency information are transmitted over channels and received by data receivers of DGs. And then these packets would be holden by data buffers writing to be handled by frequency controllers in DGs. The data path from DG-i to DG-j is shown in Fig. 2.

It should be noted that, secondary control could easily be attacked by attackers, as the communication is open. As shown in Fig. 2, packets are transmitted through channels, service-provider-edge routers and other networking devices, which can utilize available communication resources. In this paper, we assume that DoS attackers launch DoS attacks to the service-provider-edge routers which are designed to route packets and can handle a relatively high packet arrival rate. This situation is highly possible as the routers are open for energy users, as well as the attackers. No matter which methods that DoS attackers take, the purpose of DoS attacks is to hinder data processing in the network. Then the timeliness of packets containing frequency information is affected. That is to say, the response rate of frequency controllers will be slowed. As one of methods to reduce the impact of DoS attacks is to improve the response rate of the whole control system[11], the response rate of the P-f control is

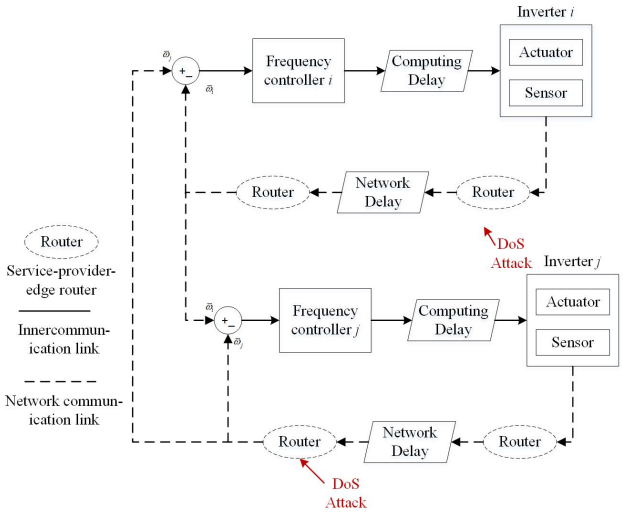


Figure 2: Data Path from DG-i to DG-j.

improved by regulating droop parameters according to the differential of active power. Details would be shown in the following.

4. Algorithm Designation and Model for the MG

In this section, control algorithms in both primary and secondary control were presented. Then by combining the primary P-f controllers and the secondary frequency controllers, a state-space model of the MG was established.

- A. A Droop Control Method with Dynamic Droop Coefficients

In this subsection, the P-f droop control method with dynamic droop coefficients was introduced. When two or more DGs are connected, conventional droop controllers are applied to generate reference inputs for the inner current and outer voltage control loops. For inductive lines, a P-f droop controller can be described as[15]

$$\omega_i = {\omega_i}^* - n_i \left(P_{e,i} - P_i^*\right) \tag{1}$$

where ω^* and P_i^* are nominal or reference value of frequency and rated active power, respectively, $P_{e,i}$ and ω_i are the active power injection at inverter i and reference frequency of the inner loop, respectively, and n_i is the droop control coefficient.

From equation (1), the conventional droop control is a pure proportion control which can deviate frequency from nominal value when active power is changed. When the MG is under large load change, the required damping active power to stabilize frequency for each DG is restricted[16]. This may lead to oscillation and even instability of the system. To overcome the difficulty, the improved droop controller was proposed

$$\omega_i = \omega^* - n_i\left(P\right)\left(P_{e,i} - P_i^*\right), \tag{2}$$

where $n_i\left(P\right)$ represented the dynamic droop coefficient which responded to the variant of active power of loads. And the coefficient was represented as

$$n_i\left(P\right) = \begin{cases} \min\left(n_i, \left(n_i - k_{n,i}\frac{dP}{dt}e^{a_{n,i}(t-t_d)}\right)\right) & \frac{dP}{dt} \geq 0 \\ \max\left(n_i, \left(n_i - k_{n,i}\frac{dP}{dt}e^{a_{n,i}(t_d-t)}\right)\right) & \frac{dP}{dt} < 0 \end{cases}, \tag{3}$$

where $k_{n,i}$ regulating variation influence, $a_{n,i}$ regulating the speed of variation of the droop parameter, and t_d was the last time that the systems demand was changed. For example, when the active load power was increased or decreased, the variation of $n_i\left(P\right)$ could be described as shown in Fig. 3(a) or Fig. 3(b), respectively. By the above method, the droop controller could respond to variant of power more quickly. However bus frequency of the DG utilizing this droop control method was also drawn from nominal value. So the consensus-based secondary frequency control method would be applied to secondary control.

- B. Consensus-based Secondary Frequency Control Method

Although the conventional droop control was improved into a new form, secondary control should be introduced to compensate deviation of frequency. In order to achieve the frequency recovery strategy, the consensus-based control algorithm is applied in secondary controllers. To illustrate the algorithm, some

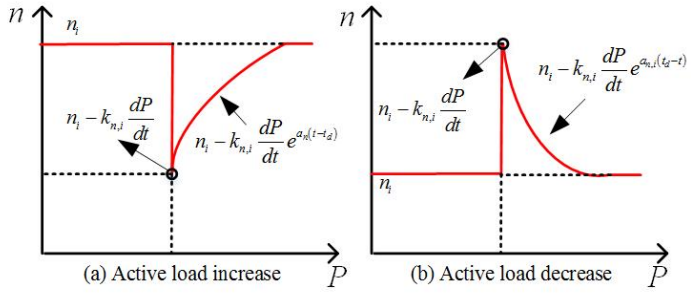


Figure 3: Variation of P-f droop parameters.

formula about DGs are given first. The output voltage angle of the i-DG can be written as:

$$\theta_i = \omega_i t + \delta_i. \tag{4}$$

Then derive the equation (4) as:

$$\dot{\theta}_i = \omega_i. \tag{5}$$

For convenience, the equation (5) can be rewritten as:

$$\dot{\theta}_i = \omega_i - \omega_* + \omega_* = \varpi_i + \omega_*, \tag{6}$$

where ω_* is the reference frequency given by secondary control.

For controllers in frequency control, frequency information is communicated between neighboring DGs. During this procedure, packets containing status information move from one DG to another through telecommunication network equipment. The common discipline for the service for each router in communication paths is first-come-first-serve. The queueing model can be used to abstract the mechanism governing packet transmission shown in Fig. 4. The newly arrived packet will be served for some time (i.e. the computing time from CPU) without delay if the CPU of network routers are idle. Otherwise, the packet will be holden in the queue to wait for service. The packet will be dropped if the queue of a finite size is full. For the packet, there exists an delay $\tau_d(t)$, i.e. the service time, which represents the total time spent in the queue before arriving

at the destination device (usually the controller of the neighboring DG). The delay $\tau_d(t)$ is the sum of waiting time, i.e. the transmission time of one packet in the each communication path, and service time i.e. the computing time of each controller, represented by $\tau_t(t)$ and $\tau_c(t)$, respectively.

Here we assume that $\tau_t(t)$ and $\tau_c(t)$ are deterministic,represented by τ_t and τ_c. It is also assumed that global clock synchronization has been achieved in the MG, and secondary frequency controllers and networking devices have identical performance. And for communication links, IP routing from a node to another presents symmetry. As ϖ from different DGs are different, the error between them can be used as inputs of frequency control. Then the control protocol of DG-i can be written as (7):

$$\dot{\varpi}_i(t) = -k\sum_{j=1}^{n} a_{ij}\left[\varpi_i(t-\tau_c) - \varpi_j(t-\tau_m)\right], \tag{7}$$

where k is the control coefficient and $\tau_m = \tau_c + \tau_t$. Then in the next section, the state-space model of the MG can be built with the consideration of the droop control method, the secondary frequency control method and the network structure.

- C. Model for the MG

In this section, the network structure of the MG is modeled firstly. The active power $P_{e,i}$ of DG-i injected into microgrid is shown as:

$$P_{e,i} = \sum_{j\in N_i} E_i E_j |Y_{ij}| \sin(\theta_i - \theta_j), \tag{8}$$

where E_i represents the output voltage of DG-i, Y_{ij} represents the inductive admittance of the line $i-j$ and θ_i represents the phase angle of DG-i.

Noting $D_i(P) = 1/n_i(P)$, the P-f droop controller can be rewritten as

$$0 = P_i^* - P_{e,i} - D_i(P)\varpi_i, i \in \nu_{DG}. \tag{9}$$

where ν_{DG} represents the set of DGs. Substituting equation (8) into (9), the equation (9) can be rewritten as

$$0 = P_i^* - \sum_{j\in N_i} E_i E_j |Y_{ij}| \sin(\theta_i - \theta_j) - D_i(P)\varpi_i, i \in \nu_{DG}. \tag{10}$$

According to the Kirchoffs Current Law, when the node is a constant power load, the equation can be written as

$$0 = P_i^* - \sum_{j \in N_i} E_i E_j \left| Y_{ij} \right| \sin\left(\theta_i - \theta_j\right), i \in \nu_L. \tag{11}$$

where ν_L represents the set of load nodes. Combining the equations (10) and (11) to form the matrix formula as

$$0 = P^* - BC \sin\left(B^T \theta\right) - D\left(P\right) \varpi. \tag{12}$$

where $\theta = [\theta_1, ..., \theta_n]$, $D\left(P\right) = diag\left(0_{|\nu_L|}, \{D_i\left(P\right)\}_{i \in \nu_{DG}}\right)$ and the vector of rated power is $P^* = (P_1^*, ...P_n^*)$.

Because the deviation between different angles is very small, the equation (12) can be rewritten as:

$$0 = P^* - BCB^T \theta - D\left(P\right) \varpi. \tag{13}$$

The matrix BCB^T can be seen as the physical part of microgrid which reflects the power flow features.

Through adding the secondary controller (7), the system can be described as

$$\dot{\varpi} = P^* - BCB^T \theta - D\left(P\right) \bar{\omega} - kD\varpi\left(t - \tau_c\right) + A\varpi\left(t - \tau_m\right). \tag{14}$$

where $\bar{\omega} = \left(\omega_1, ...\omega_n\right)^T$, $\varpi\left(t\right) = \left(\varpi_1\left(t\right), ..., \varpi_n\left(t\right)\right)^T$. However, the impact of DoS attacks is not considered in this model. In order to analyze stability of the system, the model will be changed into a new form considering the impact of DoS attacks.

5. Stability Analysis for MG under DoS Attacks

The idea of this paper is to find the condition which can maintain stability of the MG when DoS attacks occur. The impact of DoS attacks on the system state equation was discussed, and DoS attacks model was established. Then stability of the system was discussed based on Lyapunov stability.

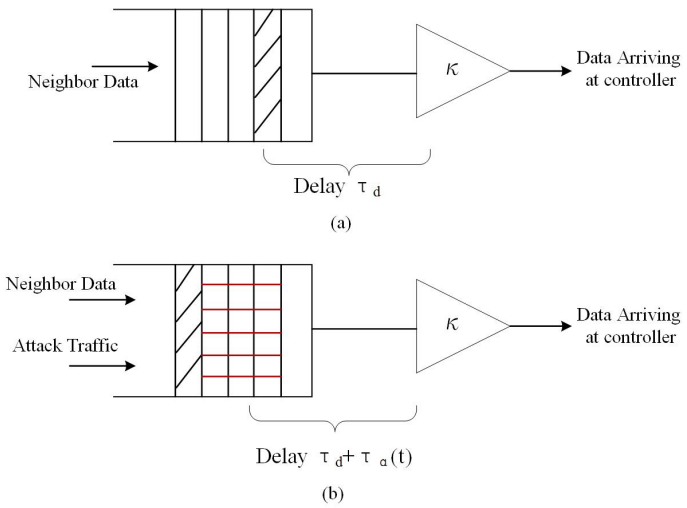


Figure 4: Queueing Model of Data Transmission Process.

- A. Model and Analysis of DoS Attacks

As it is assumed that DoS attackers launch DoS attacks to routers, i.e. massive malicious packets are injected to routers, a attack traffic is put into the queue shown in Fig. 4. As a result, the service time of newly arrived status packet is increased. Indeed, an additional service time in communication network is induced by DoS attacks[17]. Considering stochastic characterization of DoS attacks and characterization of data buffer in DGs, the impact of DoS attacks can be modeled by different types of time delays[18, 19], such as constant time delay[12, 20] and probabilistic time delay[21, 22]. In this paper, the service time $\tau_d(t)$ was represent as $\tau_d(t) = \tau_t + \tau_\alpha(t)$, where $\tau_\alpha(t)$ represented the additional delay induced by DoS attacks. And $\tau_\alpha(t) = g(\phi(t)\lambda(t), \kappa)$, where g represents the function of queue model, $\phi(t)$ represents the arriving rate of attack packets , $\lambda(t)$ is the arriving rate of state information packets and κ represents the service time of the controller [9]. Here we assume that the attacker adopts a same attack strategy to affect the routers and has a limited capability to increase network service time. So $\tau_\alpha(t)$ suffers a upper bound $\tau_{\max}$. As our

purpose is to find the control system's tolerance of DoS attacks, we rewrite the consensus-based controller as

$$\dot{\varpi}_i = -k\sum_{j=1}^{n} a_{ij}\left[\varpi_i\left(t-\tau_c\right)-\varpi_j\left(t-\tau_m-\tau_\alpha\left(t\right)\right)\right]. \tag{15}$$

The system can be rewritten as

$$\dot{\varpi} = P^* - BCB^T\theta - D\left(P\right)\bar{\omega} - kD\varpi\left(t-\tau_c\right) + kA\varpi\left(t-\tau_m-\tau_\alpha\left(t\right)\right) \tag{16}$$

- B. Condition to Keep Stability of the MG

Stability of primary control can be guaranteed by satisfying the power flow and frequency constraints shown in [23]. After that, the consensus-based frequency control method in secondary control would be proved to be stable. In order to prove stability of the system (15), it was rewritten into matrix as:

$$\dot{\varpi}\left(t\right) = -kD\varpi\left(t-\tau_c\right) + kA\varpi\left(t-\tau_m-\tau_\alpha\left(t\right)\right). \tag{17}$$

The free weighting matrices [24] were applied to Theorem 1 to prove the multi-delay multi-agent consensus algorithm.

Theorem 1: For given time-delays $\tau_c \geq 0$, $\tau_t > 0$ and $\tau_m = \tau_t + \tau_c > \tau_c$, the system (17) is asymptotically stable for the uncertain DoS time delay which lies in $[0, \tau_{\max}]$ and satisfies $\dot{\tau}_d\left(t\right) \leq \mu < 1$, if there exist symmetric positive, definite matrices $P = P^T > 0$ and $Q_i = Q_i^T > 0\,(i = 1, 2, 3)$ symmetric semi-positive definite matrices $W_l = W_l^T \geq 0$,

$$X_l = \begin{bmatrix} X_l^{11} & X_l^{12} & X_l^{13} & X_l^{14} \\ \left[X_l^{12}\right]^T & X_l^{22} & X_l^{23} & X_l^{24} \\ \left[X_l^{13}\right]^T & \left[X_l^{23}\right]^T & X_l^{33} & X_l^{34} \\ \left[X_l^{14}\right]^T & \left[X_l^{24}\right]^T & \left[X_l^{34}\right]^T & X_l^{44} \end{bmatrix} \geq 0, l = 1, 2, 3$$

and any appropriately dimensioned matrices $N_l^i, l = 1, 2, 3, i = 0, 1, 2, 3$ such that the following LMIs hold

$$\Phi = \begin{bmatrix} \phi_{11} & \phi_{12} & \phi_{13} & \phi_{14} \\ \phi_{12}^T & \phi_{22} & \phi_{23} & \phi_{24} \\ \phi_{13}^T & \phi_{23}^T & \phi_{33} & \phi_{34} \\ \phi_{14}^T & \phi_{24}^T & \phi_{34}^T & \phi_{44} \end{bmatrix} < 0. \tag{18}$$

$$\Psi_l = \begin{bmatrix} X_l^{11} & X_l^{12} & X_l^{13} & X_l^{14} & N_l^0 \\ \left[X_l^{12}\right]^T & X_l^{22} & X_l^{23} & X_l^{24} & N_l^1 \\ \left[X_l^{13}\right]^T & \left[X_l^{23}\right]^T & X_l^{33} & X_l^{34} & N_l^2 \\ \left[X_l^{14}\right]^T & \left[X_l^{24}\right]^T & \left[X_l^{34}\right]^T & X_l^{44} & N_l^3 \\ \left[N_l^0\right]^T & \left[N_l^1\right]^T & \left[N_l^2\right]^T & \left[N_l^3\right]^T & W_l \end{bmatrix} \geq 0, l = 1, 2, 3. \quad (19)$$

where

$$\phi_{11}=Q_1 + Q_2 + Q_3 + 2N_1^0 + X^{11},$$

$$\phi_{12} = -kPD + \left[N_1^1\right]^T + N_2^0 - N_1^0 + X^{12},$$

$$\phi_{13} = \left[N_1^2\right]^T + N_3^0 - N_2^0 + X^{13},$$

$$\phi_{14} = kPA + \left[N_1^3\right]^T - N_3^0 + X^{14},$$

$$\phi_{22} = -Q + k^2 D^T G D + 2N_2^1 - 2N_1^1 + X^{22},$$

$$\phi_{23} = \left[N_2^2\right]^T - \left[N_1^2\right]^T - N_2^1 + N_3^1 + X^{23},$$

$$\phi_{24} = -k^2 D^T G A + \left[N_2^3\right]^T - \left[N_1^3\right]^T - N_3^1 + X^{24},$$

$$\phi_{33} = -Q - 2N_2^2 + 2N_3^2 + X^{33},$$

$$\phi_{34} = \left[N_3^3\right]^T - \left[N_2^3\right]^T - N_3^2 + X^{34},$$

$$\phi_{44} = (1-\mu) Q_3 + k^2 A^T G A - 2N_3^3 + X^{44},$$

$$G = \tau_c W_1 + \tau_t W_2 + \tau_{\max} W_3,$$

$$X^{ij} = \tau_c X_1^{ij} + \tau_t X_2^{ij} + \tau_{\max} X_3^{ij}.$$

Proof: Denote that $\tau_d(t) = \tau_\alpha(t) + \tau_m$ and $\tau_{d\_\max} = \tau_{\max} + \tau_m$. Choose the following candidate Lyapunov-Krasovskii functional:

$$\begin{aligned} V(t) = {} & \varpi^T(t) P \varpi(t) + \int_{t-\tau_c}^{t} \varpi^T(s) Q_1 \varpi(s) ds + \int_{t-\tau_m}^{t} \varpi^T(s) Q_2 \varpi(s) ds \\ & + \int_{t-\tau_d(t)}^{t} \varpi^T(s) Q_3 \varpi(s) ds + \int_{-\tau_c}^{0} \int_{t+\theta}^{t} \dot{\varpi}^T(s) W_1 \dot{\varpi}(s) ds d\theta \\ & + \int_{-\tau_m}^{-\tau_c} \int_{t+\theta}^{t} \dot{\varpi}^T(s) W_2 \dot{\varpi}(s) ds d\theta + \int_{-\tau_{d\_\max}}^{-\tau_m} \int_{t+\theta}^{t} \dot{\varpi}^T(s) W_3 \dot{\varpi}(s) ds d\theta \end{aligned} \quad (20)$$

where $P = P^T > 0$, $Q_i = Q_i^T > 0\,(i = 1, 2, 3)$ and $W_l = W_l^T \geq 0\,(l = 1, 2, 3)$. The derivative of V_1 yields

$$\begin{aligned}\dot{V}(t) = 2\varpi^T(t) P\left[-kD\varpi(t-\tau_c) + kA\varpi(t-\tau_d(t))\right] + \varpi^T(t) Q_1 \varpi(t)\\ -\varpi^T(t-\tau_c) Q_1 \varpi(t-\tau_c) + \varpi^T(t) Q_2 \varpi(t) - \varpi^T(t-\tau_m) Q_2 \varpi(t-\tau_m)\\ +\varpi^T(t) Q_3 \varpi(t) - (1-\dot{\tau}_d(t))\varpi^T(t-\tau_d(t)) Q_3 \varpi(t-\tau_d(t)) + \tau_c \dot{\varpi}^T(t) W_1 \dot{\varpi}(t)\\ -\int_{t-\tau_c}^{t} \dot{\varpi}^T(s) W_1 \dot{\varpi}(s)\, ds + \tau_t \dot{\varpi}^T(t) W_2 \dot{\varpi}(t) - \int_{t-\tau_m}^{t-\tau_c} \dot{\varpi}^T(s) W_2 \dot{\varpi}(s)\, ds\\ +\tau_{\max} \dot{\varpi}^T(t) W_3 \dot{\varpi}(t) - \int_{t-\tau_{d\_\max}}^{t-\tau_m} \dot{\varpi}^T(s) W_3 \dot{\varpi}(s)\, ds\end{aligned} \tag{21}$$

Using the Leibniz-Newton formula, for any matrices $N_l^i, l = 1, 2, 3, i = 0, 1, 2, 3$, the followings are true

$$\begin{aligned}2\left[\varpi^T(t) N_1^0 + \varpi^T(t-\tau_c) N_1^1 + \varpi^T(t-\tau_m) N_1^2 + \varpi^T(t-\tau_d(t)) N_1^3\right]\\ \times\left[\varpi(t) - \varpi(t-\tau_c) - \int_{t-\tau_c}^{t} \dot{\varpi}(s)\, ds\right] = 0.\end{aligned} \tag{22}$$

$$\begin{aligned}2\left[\varpi^T(t) N_2^0 + \varpi^T(t-\tau_c) N_2^1 + \varpi^T(t-\tau_m) N_2^2 + \varpi^T(t-\tau_d(t)) N_2^3\right]\\ \times\left[\varpi(t-\tau_c) - \varpi(t-\tau_m) - \int_{t-\tau_m}^{t-\tau_c} \dot{\varpi}(s)\, ds\right] = 0.\end{aligned} \tag{23}$$

$$\begin{aligned}2\left[\varpi^T(t) N_3^0 + \varpi^T(t-\tau_c) N_3^1 + \varpi^T(t-\tau_m) N_3^2 + \varpi^T(t-\tau_d(t)) N_3^3\right]\\ \times\left[\varpi(t-\tau_m) - \varpi\left(t-\tau_{d(t)}\right) - \int_{t-\tau_{d(t)}}^{t-\tau_m} \dot{\varpi}(s)\, ds\right] = 0.\end{aligned} \tag{24}$$

Meanwhile, for any n*n dimensioned matrices $X_l^{ij}, l = 1, 2, 3, i = 1, 2, 3, 4, i < j \leq 4$, the following equation holds

$$\eta_1^T(t) \begin{bmatrix} \Lambda_{11} & \Lambda_{12} & \Lambda_{13} & \Lambda_{14} \\ \Lambda_{21} & \Lambda_{22} & \Lambda_{23} & \Lambda_{24} \\ \Lambda_{31} & \Lambda_{32} & \Lambda_{33} & \Lambda_{34} \\ \Lambda_{41} & \Lambda_{42} & \Lambda_{43} & \Lambda_{44} \end{bmatrix} \eta_1(t) = 0, \tag{25}$$

where Λ_{ij}=$\tau_c\left(X_1^{ij} - X_1^{ij}\right) + \tau_t\left(X_2^{ij} - X_2^{ij}\right) + \tau_{\max}\left(X_3^{ij} - X_3^{ij}\right)$ and $\eta_1(t) = \begin{bmatrix} \varpi^T(t) & \varpi^T(t-\tau_c) & \varpi^T(t-\tau_m) & \varpi^T(t-\tau_d(t)) \end{bmatrix}^T$.

Then adding the left terms in (22),(23),(24) and (25) to (21) , then the derivative of V_1 can be rewritten as

$$\begin{aligned}\dot{V}_1 < \eta_1^T(t)\Phi\eta(t) - \int_{t-\tau_c}^{t} \eta_2^T(t,s)\Psi_1\eta_2(t,s)\, ds\\ -\int_{t-\tau_m}^{t-\tau_c} \eta_2^T(t,s)\Psi_2\eta_2(t,s)\, ds - \int_{t-\tau_{d(t)}}^{t-\tau_m} \eta_2^T(t,s)\Psi_3\eta_2(t,s)\, ds\end{aligned} \tag{26}$$

where $\eta_2(t,s) = \left[\begin{array}{cc} \eta_1^T(t) & \dot{\varpi}^T(s) \end{array} \right]^T$.

Thus, if $\Phi < 0$ and $\Psi_l \geq 0, l = 1,2,3$, the $\dot{V}_1 < 0$ for any $\eta_1(t) \neq 0$. So the system (17) is asymptotically stable if LMIs (18)and (19) hold which can require the delay upper limit. The proof is completed.

6. Simulation and Experiment Study

In this section, the effectiveness of the method is verified by simulation and experimental results.

- A. Simulation of IEEE-34 nodes

As shown in Fig.(5), a microgrid system based on one-line 25kV IEEE-34 Node Test Feeder system[25, 26] has been simulated in MATLAB/Simulink environment to assess the tolerance of DoS attacks for the consensus-based frequency control method. Six DGs are represented by different colors in six regions. In this simulation study, only single-phase inverters are considered and all reactive power is provided by the main grid. The parameters of the system are listed in Table I.

Table 1: DG Type & Magnitude of Power Generated

Component Name	Type of Generation	Magnitude (KW)
DG-1	Wind Power	50
DG-2	Wind Power	50
DG-3	Solar Power	100
DG-4	Solar Power	100
DG-5	Solar Power	150
DG-6	Solar Power	150

The simulation process is shown as follows. The system is initially experiencing a total load demand of 360kW before t=1s. Then 16.2% nonlinear load and 16.2% linear load are increased in the whole system. At t=2s, the output

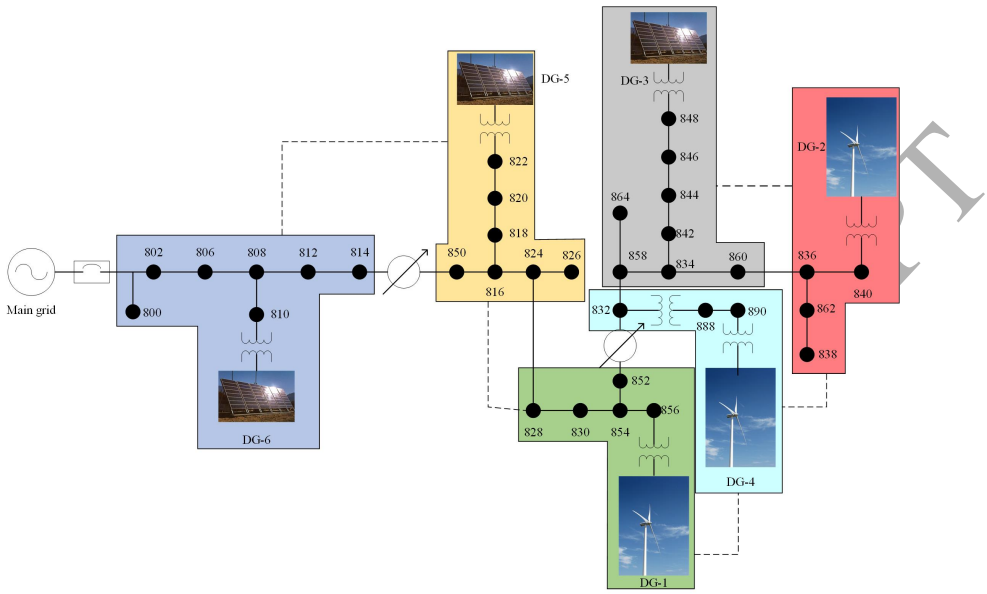
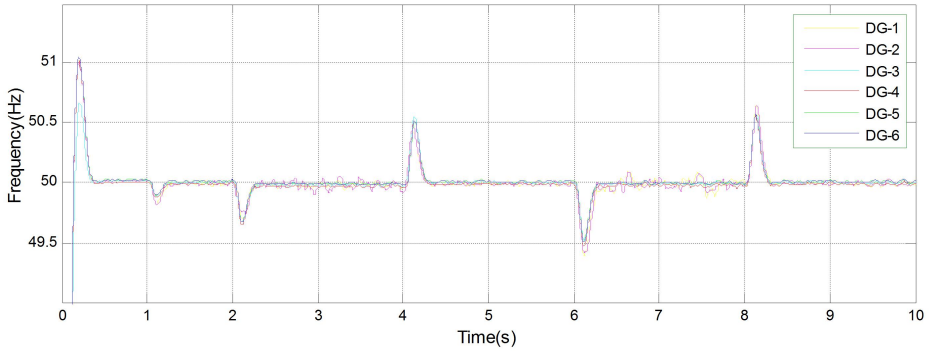


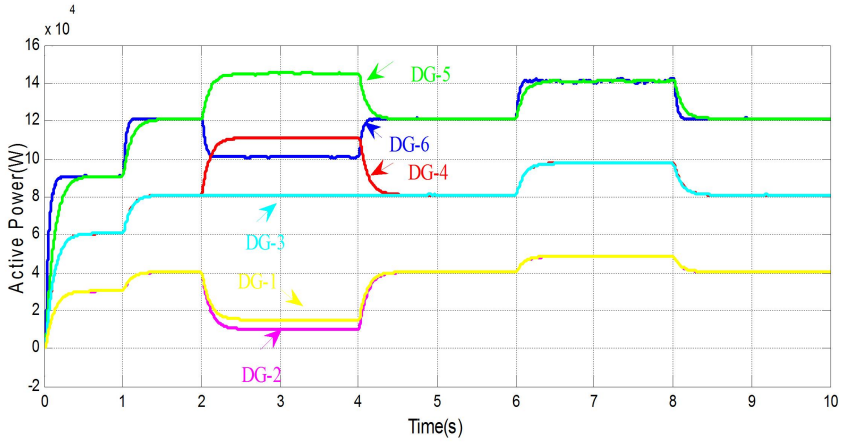
Figure 5: One-line Diagram of 34-bus Test Feeder System.

power of DG-1, DG-2, DG-3 and DG-6 are limited to 15kW, 10kW, 100kW and 100kW, respectively. This limitation is removed at t=4s. Two electric vehicles with charging levels of 50kW are charged during t=6-8s. According to system settings, the computing delay τ_c and the transmission delay τ_t are set to be 0.01s and 0.03s, respectively. Then the condition keeping stability of the system from Theorem 1 can be satisfied when the system is under DoS attacks which suffer the upper bound τ_{max}=0.09s. The simulation results are shown in Fig. 6.

As seen from Fig. 6 (a), frequency of the six DGs are regulated at the rated frequency at the steady state under different load conditions when the microgrid is under the DoS attack. And from Fig. 6 (b), the active power is shared in proportion among the six DGs. Especially, DGs' intermittent feature has been considered during t=2s-4s in this simulation. From the results, when the output power of some of the six DGs is confined, the residual load can be supplied by other DGs.



(a)



(b)

Figure 6: Simulation results: (a) frequency of six DGs; (b) active power of six DGs.

- B. Experiment Results

To verify stability of one system under DoS attacks in practice, the condition from Theorem 1 is implemented in the experimental testbed shown in Fig. 7. The experimental testbed is composed of DG1, DG2 and DG3 with the rated capacity of 1000W, 1000W and 2000W, respectively. In this case, the computing delay τ_c and the transmission delay τ_t are set to be 0.01s and 0.03s, respectively. The condition keeping stability of the system from Theorem 1 can be satisfied when the system is under DoS attacks which suffer the upper bound τ_{max}=0.09s. In Fig. 7, the red dotted lines represent control signals and the green dotted lines represent communication links between three DGs. The waveforms of frequency and active power are viewed through the digital-to-analog function. The values about frequency, active power are transformed into voltage value shown through oscilloscope.

Figs. 8 and 9 show experimental waveforms when the active power is varied from 0 to 7 kW and then to 3.5 kW. In Fig. 8, the active power can be shared by three DGs in proportion of 4:2:1 when the system is under the DoS attacks. In Fig. 9, during the load disturbance, the output frequency from three DGs can be kept constant after little disturbance when the system is under the DoS attacks.

7. Conclusion

The tolerance of DoS attacks for consensus-based secondary frequency controllers in one microgrid has been studied in this paper. The model of one microgrid is transferred to a state-space representation with the consideration of the impact of DoS attacks. Based on this model, the free weighted matrices and LMI tools are used to analyze the condition under which stability of the MG can be preserved. Considering that processors in most microgrids suffer from low communication abilities, how to extend the results to the case with event-driven communication [27] would be a useful and meaning research topic.

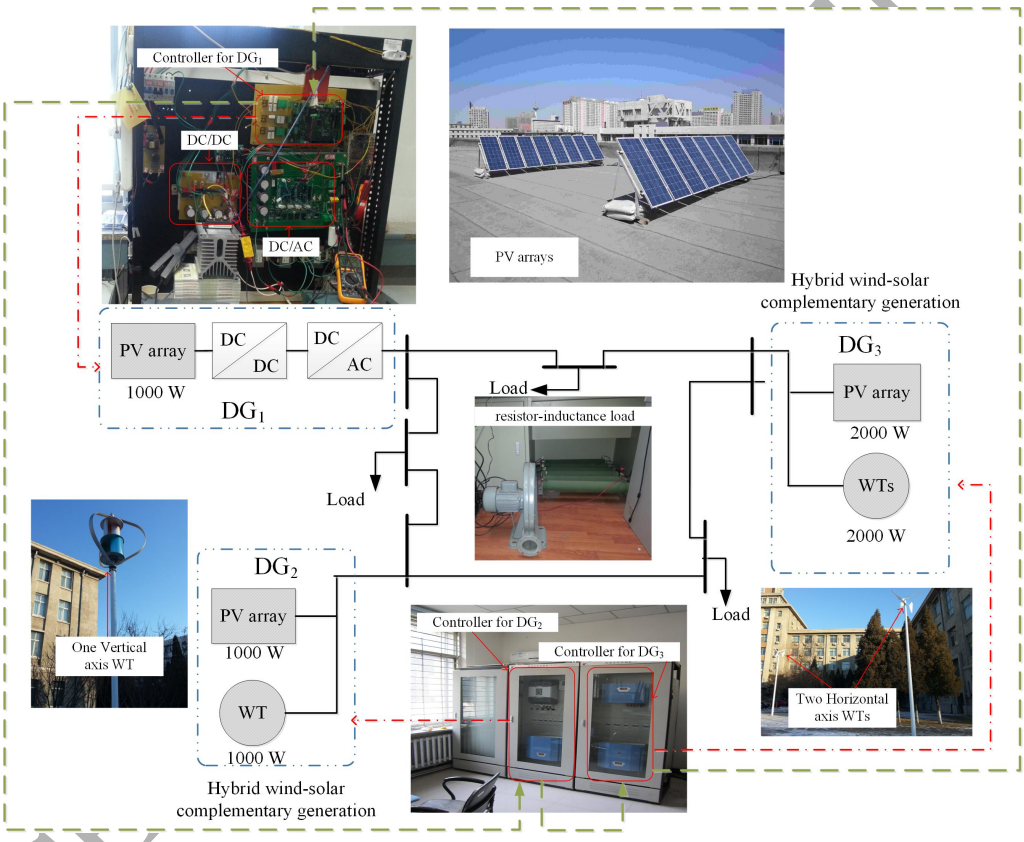


Figure 7: Experimental Testbed.

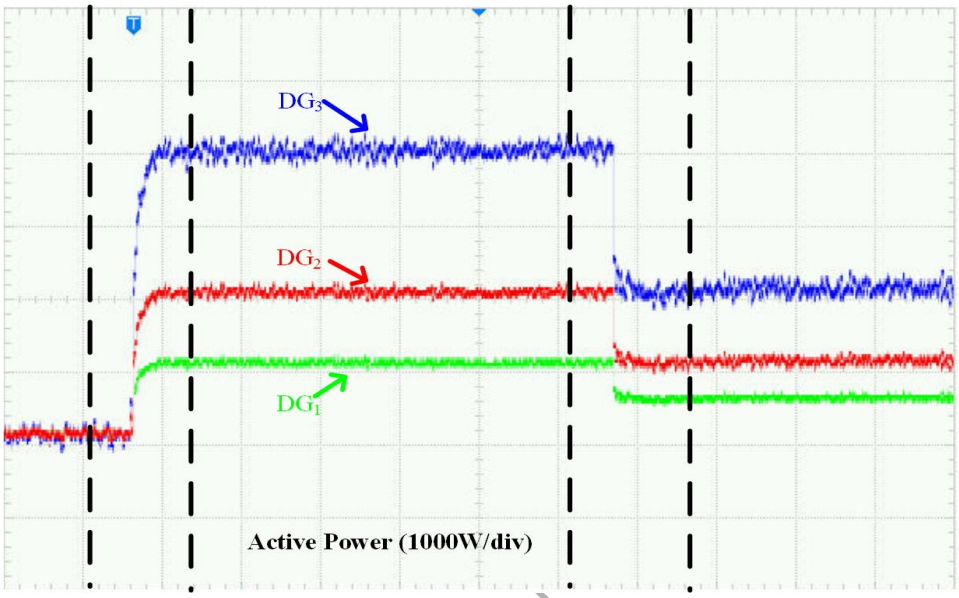


Figure 8: Output active power from DG1, DG2, DG3.

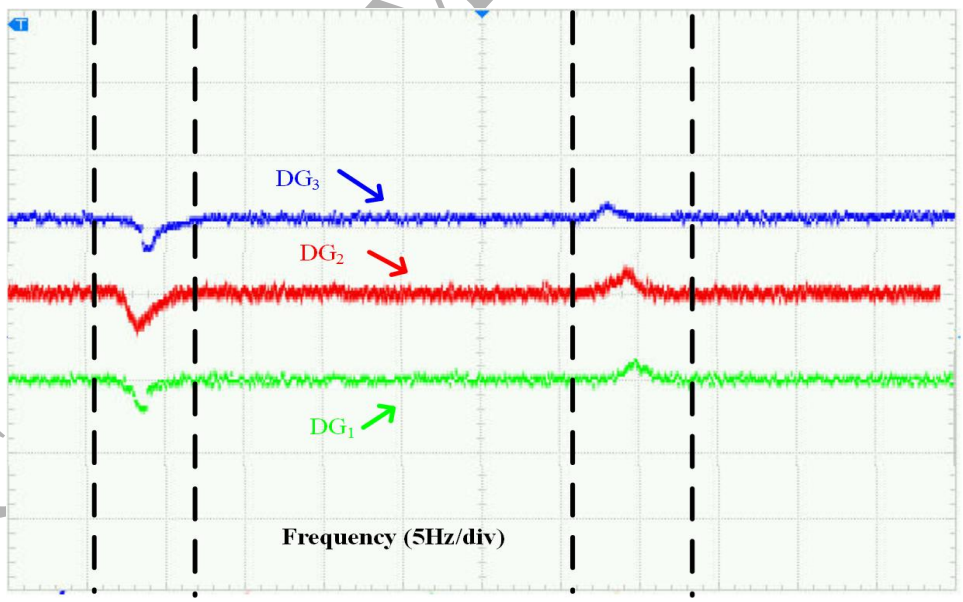


Figure 9: Output frequency from DG1, DG2, DG3.

And the extension of results on other kinds of cyber attacks, such as the replay and FDI attacks, should also be studied.

References

References

[1] R. Han, L. Meng, G. Ferrari-Trecate, E. A. A. Coelho, J. C. Vasquez, J. M. Guerrero, Containment and consensus-based distributed coordination control to achieve bounded voltage and precise reactive power sharing in islanded ac microgrids, IEEE Transactions on Industry Applications 53 (6) (2017) 5187–5199. doi:10.1109/TIA.2017.2733457.

[2] R. Han, L. Meng, J. M. Guerrero, J. C. Vasquez, Distributed nonlinear control with event-triggered communication to achieve current-sharing and voltage regulation in dc microgrids, IEEE Transactions on Power Electronics 33 (7) (2018) 6416–6433. doi:10.1109/TPEL.2017.2749518.

[3] J. Qin, Q. Ma, Y. Shi, L. Wang, Recent advances in consensus of multi-agent systems: A brief survey, IEEE Transactions on Industrial Electronics PP (99) (2016) 1–1.

[4] J. Qin, C. Yu, S. Hirche, Stationary consensus of asynchronous discrete-time second-order multi-agent systems under switching topology, IEEE Transactions on Industrial Informatics 8 (4) (2012) 986–994.

[5] Q. Sun, R. Han, H. Zhang, J. Zhou, J. M. Guerrero, A multiagent-based consensus algorithm for distributed coordinated control of distributed generators in the energy internet, IEEE Transactions on Smart Grid 6 (6) (2015) 3006–3019.

[6] H. Zhang, W. Meng, J. Qi, X. Wang, W. X. Zheng, Distributed load sharing under false data injection attack in inverter-based microgrid, IEEE Transactions on Industrial Electronics PP (99) (2018) 1–1.

[7] J. Qin, M. Li, L. Shi, X. Yu, Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks, IEEE Transactions on Automatic Control 63 (6) (2018) 1648–1663. doi:10.1109/TAC.2017.2756259.

[8] O. Osanaiye, A. S. Alfa, G. P. Hancke, Denial of service (dos) defence for resource availability in wireless sensor networks, IEEE Access PP (99) (2018) 1–1.

[9] M. Long, C. H. Wu, J. Y. Hung, Denial of service attacks on network-based control systems: impact and mitigation, IEEE Transactions on Industrial Informatics 1 (2) (2005) 85–96.

[10] H. S. Foroush, S. Martnez, On event-triggered control of linear systems under periodic denial-of-service jamming attacks, in: Decision and Control, 2013, pp. 2551–2556.

[11] C. D. Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Transactions on Automatic Control 60 (11) (2015) 2930–2944.

[12] V. S. Dolk, P. Tesi, C. D. Persis, W. P. M. H. Heemels, Event-triggered control systems under denial-of-service attacks, IEEE Transactions on Control of Network Systems 4 (1) (2017) 93–105.

[13] C. Peng, J. Li, M. R. Fei, Resilient event-triggered h_∞ load frequency control for networked power systems with energy-limited dos attacks, IEEE Transactions on Power Systems 32 (5) (2017) 4110–4118.

[14] L. Y. Lu, C. C. Chu, Consensus-based droop control of isolated micro-grids by admm implementations, IEEE Transactions on Smart Grid PP (99) (2017) 1–1.

[15] J. Chen, L. Wang, L. Diao, H. Du, Z. Liu, Distributed auxiliary inverter of urban rail trainload sharing control strategy under complicated operation

condition, IEEE Transactions on Power Electronics 31 (3) (2016) 2518–2529. doi:10.1109/TPEL.2015.2427381.

[16] Y. A. I. Mohamed, E. F. El-Saadany, Adaptive decentralized droop controller to preserve power sharing stability of paralleled inverters in distributed generation microgrids, IEEE Transactions on Power Electronics 23 (6) (2008) 2806–2816. doi:10.1109/TPEL.2008.2005100.

[17] Z. A. Biron, S. Dey, P. Pisu, Real-time detection and estimation of denial of service attack in connected vehicle systems, IEEE Transactions on Intelligent Transportation Systems (2018) 1–10doi:10.1109/TITS.2018.2791484.

[18] S. Feng, P. Tesi, Resilient control under denial-of-service: Robust design, in: 2016 American Control Conference (ACC), 2016, pp. 4737–4742. doi:10.1109/ACC.2016.7526102.

[19] J. Wu, T. Chen, Design of networked control systems with packet dropouts, IEEE Transactions on Automatic Control 52 (7) (2007) 1314–1319. doi:10.1109/TAC.2007.900839.

[20] A. Lu, G. Yang, Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service, IEEE Transactions on Automatic Control 63 (6) (2018) 1813–1820. doi:10.1109/TAC.2017.2751999.

[21] S. Amin, A. A. Crdenas, S. S. Sastry, Safe and secure networked control systems under denial-of-service attacks, in: International Conference on Hybrid Systems: Computation and Control, 2009, pp. 31–45.

[22] G. Befekadu, V. Gupta, P. Antsaklis, Risk-sensitive control under markov modulated denial-of-service (dos) attack strategies, IEEE Transactions on Automatic Control 60 (12) (2015) 3299–3304.

[23] J. W. Simpson-Porco, F. Drfler, F. Bullo, Synchronization and power sharing for droop-controlled inverters in islanded microgrids , Pergamon Press, Inc., 2013.

[24] Y. He, M. Wu, J. H. She, Delay-dependent stability criteria for linear systems with multiple time delays, IEE Proceedings - Control Theory and Applications 153 (4) (2006) 447–452.

[25] R. C. Dugan, W. H. Kersting, Induction machine test case for the 34-bus test feeder -description, in: Power Engineering Society General Meeting, 2006, p. 4 pp.

[26] N. Samaan, T. Mcdermott, B. Zavadil, J. Li, Induction machine test case for the 34-bus test feeder - steady state and dynamic solutions, in: Power Engineering Society General Meeting, 2006, p. 5 pp.

[27] W. Meng, X. Wang, S. Liu, Distributed load sharing of an inverter-based microgrid with reduced communication, IEEE Transactions on Smart Grid PP (99) (2016) 1–11.