Distributed Load Sharing Under False Data Injection Attack in an Inverter-Based Microgrid

Heng Zhang, *Member, IEEE*, Wenchao Meng, Junjian Qi, *Senior Member, IEEE*, Xiaoyu Wang, *Senior Member, IEEE*, and Wei Xing Zheng, *Fellow, IEEE*

***Abstract*—In microgrids, distributed load sharing plays an important role in maintaining the supply–demand balance of power. Because false data injection (FDI) is one of the crucial threats faced by future microgrids, the study of the impact of FDI on distributed load sharing is both of theoretical merit and practical value. In this paper, we consider the distributed load sharing problem of the microgrids operating in autonomous mode under FDI. Each bus is assumed to be equipped with an agent. Under a well-developed distributed load sharing protocol based on multiagent systems, we first construct an FDI attack model, where the attacker is capable of injecting false data into the bus agents. Then, a utilization level is introduced for coordinating generators, and its variation is evaluated in the presence of FDI attacks with given injection strategies. The stable region of the microgrid is defined, and conditions are given to determine stability. Finally, theoretical results are validated on the Canadian urban distribution system.**

***Index Terms*—Cyberattacks, distributed load sharing, false data injection (FDI), microgrids.**

Nomenclature

λ_m^{ω} Droop control gain of the mth distributed generation (DG).

$\lambda_m^{i\omega}$ Integral control gain of the mth DG for the secondary frequency control.

λ_m^{ii} Integral current control gain of the mth DG.

λ_m^{ip} Integral power control gain of the mth DG.

$\lambda_m^{p\omega}$ Proportional control gain of the mth DG for the secondary frequency control.

λ_m^{pi} Proportional current control gain of the mth DG.

λ_m^{pp} Proportional power control gain of the mth DG.

$\lambda_{\omega,m}$ Frequency droop control gain of the mth DG.

ω_0 Nominal frequency reference.

ω_m Instantaneous frequency obtained from a phase-locked loop.

$i_{d,m}$ Instantaneous currents on d-axis of the mth DG.

$i_{d,m}^{\text{ref}}$ Set point of the d-axis (direct) component of the current for the mth DG.

$i_{q,m}$ Instantaneous currents on q-axis of the mth DG.

$i_{q,m}^{\text{ref}}$ Set point of the q-axis (quadrature) component of the current for the mth DG.

m DG number.

P_m Instantaneous real power of the mth DG.

$P_{\text{DC},m}^{\text{ref}}$ Corrective realpower set point generated by the power control of the mth DG.

$P_{\text{SF},m}^{\text{ref}}$ mth DG supplementary real-power set point assigned by the secondary frequency controller of MGCC.

Q_m Instantaneous reactive power of the mth DG.

Q_m^{ref} Reactive power set point of the mth DG.

$v_{d,m}$ Components of the voltage set points on d-axis of the mth DG.

$v_{q,m}$ Components of the voltage set points on q-axis of the mth DG.

Manuscript received August 23, 2017; revised November 4, 2017; accepted December 19, 2017. Date of publication January 17, 2018; date of current version September 28, 2018. This work was supported in part by the National Nature Science Foundation of China under Grant 61503147 in part by the Australian Research Council under Grant DP120104986, in part by the National Nature Science Foundation of Jiangsu Province under Grant BK20171264, in part by the University Science Research General Project of Jiangsu Province under Grant 15KJB510002, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant Y16F030011, and in part by the Lianyungang Science and Technology Project under Grant CG1501. The work of J. Qi was supported by the U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability. *(Corresponding author: Wei Xing Zheng.)*

H. Zhang is with the School of Science, Huaihai Institute of Technology, Lianyungang 222005, China, and also with the School of Computing, Engineering and Mathematics, Western Sydney University, Sydney, NSW 2751, Australia (e-mail: Dr.Zhang.Heng@ieee.org).

W. Meng and X. Wang are with the Department of Electronics, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: wmengzju@gmail.com; xiaoyuw@doe.carleton.ca).

J. Qi is with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816-2362 USA (e-mail: Junjian.Qi@ucf.edu).

W. X. Zheng is with School of Computing, Engineering and Mathematics, Western Sydney University, Sydney, NSW 2751, Australia (e-mail: w.zheng@westernsydney.edu.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIE.2018.2793241

I. Introduction

Microgrids refer to small distributed power systems that integrate DG, energy storing devices, energy converters, load monitors, etc. [1]. They can either be connected to the main grid or operate autonomously. When connected with the main grid, they can not only consume power from the main grid, but also can feed their redundant energy to the main grid. In the autonomous mode, they have to balance their own supply and demand by load sharing control. The proposed structure of microgrids is beneficial to take full advantage of the distributed energy and maintain the synchronization of various forms of distributed power [2]–[4].

Security of power systems is a matter of great concern for system design and management [5], [6]. Recently, it has become even more crucial from both technological and economic perspectives, especially for system operators due to the recent introduction of performance-based rules [7], [8]. Because of an increasing number of cyberattacks, the power systems, specifically microgrids, are becoming more and more vulnerable. The performances of microgrids may be seriously deteriorated in the presence of attacks. Typical cyberattacks in microgrids include false data injection (FDI) attacks and denial-of-service (DoS) attacks [9]–[11]. FDI attacks can maliciously destroy the system performance by injecting false information into the original data, whereas DoS attacks may damage the system operations by breaking communications between the agents. Chlela *et al.* provided an example to show the effect of these attacks on the distributed energy resources active power, network frequency, and load active power [10]. An implementation example of FDI attacks in smart grid can be found in [9].

FDI attacks in microgrids have attracted considerable attention in recent years [12]–[19]. The existing literature has mainly focused on the evaluation of FDI attack effect [12], [13], intrusion detection technologies [14]–[16], and defense strategies [17]–[19]. Zhang *et al.* [12] studied the effect of FDI attacks on the dynamic microgrid partitioning process. Chlela *et al.* [13] developed a hardware platform to examine the impact of an FDI attack on the microgrid performance indices, including the total load lost, the frequency nadir, and latency time to achieve frequency stability. Li *et al.* [14] provided a conjunctive policy-based majority voting approach to detect the smart FDI attack actions in microgrids. Yang *et al.* [15] proposed a Gaussian-mixture model-based detection method to discover FDI attacks. A major advantage of this method is that there is no need to predefine a detection threshold. Based on recognizing the variations of inferred candidate invariants, Beg *et al.* [16] designed an intrusion detection method to judge the presence or the absence of FDI attacks. Hao *et al.* [17] considered the scenario that an FDI attacker injects false data into the intelligent voltage controller in a substation, which can negatively influence the performances of the microgrid. They provided an adaptive Markov strategy to defend against FDI attacks with unpredictable and dynamic behaviors. In order to eliminate an FDI attack that injects false data into the measurements of a microgrid, Rana *et al.* [18] presented a recursive systematic convolutional code to append redundancy in the states of microgrid, and a semidefinite-programming-based optimal control policy to defend against FDI attacks. Wang *et al.* [19] designed a topology switch scheme to reduce the effect of FDI attacks on the measurements of microgrid. However, the intrusion detection of cyberattacks and the implementation of defense strategies may result in the loss of economy and the sacrifice of system performances. Therefore, it would be important to be able to evaluate the effect of FDI attacks and decide whether it is necessary to implement defense measures.

A major problem that has not been carefully studied is the theoretical analysis of FDI attacks on the stability of microgrids. Motivated by this, we investigate the system stability of inverter-based microgrid under FDI attacks. Specifically, in this paper, we introduce the structure of inverter-based microgrid and then present the model of FDI attacks that have access to inject false data into the bus agents (BAs). We then adopt a utilization level to define a stable region and theoretically investigate the stability of microgrids with respect to the utilization level.

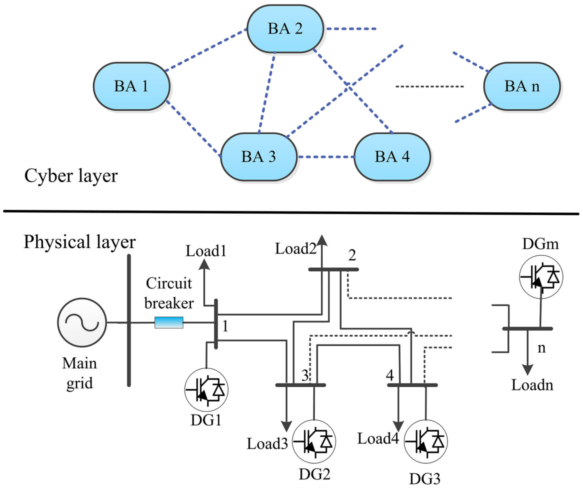


Fig. 1. Framework of microgrid.

In brief, the main contributions of this paper can be summarized as follows.

1) We construct an FDI attack model in which the attacker is able to inject false data into the BAs.
2) We define a utilization level of the microgrid and evaluate the variation of the utilization level in the presence of FDI attacks with a given injection strategy.
3) We define a stable region for the microgrid under FDI attack and provide sufficient conditions for the system stability.

The remainder of this paper is organized as follows. Section II introduces the inverter-based microgrid structure. Section III presents the system dynamic model. Section IV investigates the microgrid system performance under FDI attacks. Section V provides a simulation example to study the system stability in the presence of an FDI attack with given attack strategies. Section VI concludes this paper.

II. Inverter-Based Microgrid Structure

As shown in Fig. 1, the proposed microgrid structure is composed of two layers, i.e., a physical layer and a cyber communication layer. The physical layer is an interconnected power grid that delivers power from the grid to consumers. The cyber communication layer consists of a sparse communication network, which is the medium for exchanging data between physical elements in the physical layer.

A. Physical Layer

There are a number of distributed generators (DGs) and local loads in the microgrid. In this study, we consider inverter-based DGs because their operation and control is more flexible as opposed to the conventional rotational machine-based generators. In fact, the inverter is an interface between the system and the DG, which can be photovoltaic panels, fuel cells, or

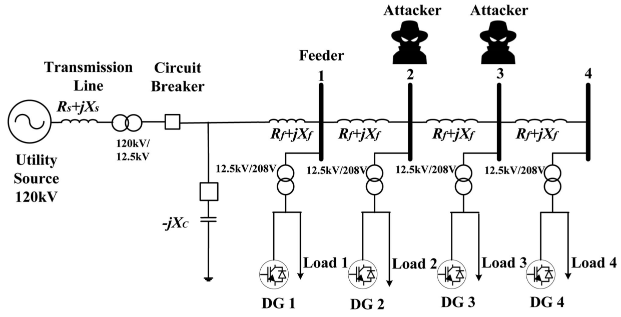


Fig. 2. Canadian urban benchmark distribution system [23].

microturbines [20]. As shown in Fig. 2, a circuit breaker is usually utilized to connect the main grid and the microgrid. Hence, the microgrid can operate in either a grid-connected model or an autonomous mode. In the autonomous mode, the microgrid has to maintain the power balance for safe operation.

Assume that the microgrid has n buses. If a bus is not equipped with DG, it can be viewed as the one having a DG with zero available power generation. Similarly, if a bus is not equipped with load, it can be viewed as the one having load with zero demand. Therefore, the microgrid has n DGs and n loads.

B. Cyber Communication Layer

BA, which is installed in each bus, exchanges local information with its neighboring agents and runs a distributed load sharing algorithm to collect the global microgrid information. The computing process of the distributed algorithm requires only a sparse communication network and very limited data. An apparent advantage of the proposed solution is the flexibility and adaptability to different operating conditions [21].

The communication network of the agents can be formulated as an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ is the set of nodes that are the agents in the microgrid, and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of edges [22]. The edge $e_{ij} = (i, j) \in \mathcal{E}$ means that there is a communication link between nodes i and j. For an undirected graph $\mathcal{G}$, the statement $e_{ij} \in \mathcal{E} \iff e_{ji} \in \mathcal{E}$ is true. The nodes i and j are called adjacent if $e_{ij} \in \mathcal{E}$. Let $A = (a_{ij})_{n\times n}$ be the adjacent matrix, in which $a_{ij} = 1$ if $e_{ij} \in \mathcal{E}$ and $a_{ij} = 0$ otherwise. Define $\mathcal{N}_i = \{j \in \mathcal{V} \mid e_{ij} \in \mathcal{E}\}$ as the neighbor set of node i. The Laplacian operation of a graph $\mathcal{G}$ is defined as the positive semidefinite matrix $\mathbf{L} = D - A$, where $D = \mathrm{diag}\{d_1, d_2, \ldots, d_n\}$ with $d_i = \sum_{j=1}^{n} a_{ij}$. It can be easily seen that $\mathbf{L1}_n = 0$, where $\mathbf{1}_n = [1, 1, \ldots, 1]^T$.

A representative inverter-based microgrid is the Canadian urban benchmark distribution system (see Fig. 2) [23], which will be used as an example in this study.

III. System Dynamic Model

A. Small Signal Model

For a microgrid in an autonomous mode, the small-signal model consists of three parts, namely, the DG block, the network block, and the interface block [23].

The inverter-based DG block includes a local primary control loop and a secondary frequency control loop [23]. The local primary control loop is working with a power controller and an inner current loop (see Fig. 3). It can manage the output power in terms of the preset power points. The controllers in the local primary loop follow the proportional-integral (PI) control law. The DG controller is given by

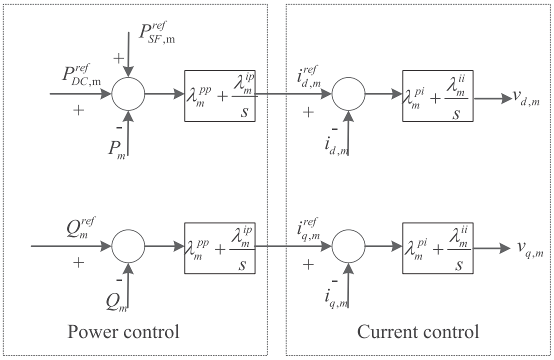

$P^{ref}_{SF,m}$
$P^{ref}_{DC,m}$
+
+
-
P_m
$\lambda^{pp}_m + \frac{\lambda^{ip}_m}{s}$
$i^{ref}_{d,m}$
+
-
$i_{d,m}$
$\lambda^{pi}_m + \frac{\lambda^{ii}_m}{s}$
$v_{d,m}$
Q^{ref}_m
+
-
Q_m
$\lambda^{pp}_m + \frac{\lambda^{ip}_m}{s}$
$i^{ref}_{q,m}$
+
-
$i_{q,m}$
$\lambda^{pi}_m + \frac{\lambda^{ii}_m}{s}$
$v_{q,m}$
Power control
Current control

Fig. 3. Block diagram of local primary DG control loops.

$$i^{\mathrm{ref}}_{q,m} = \left(\lambda^{pp}_m + \frac{\lambda^{ip}_m}{s}\right)\left(Q^{\mathrm{ref}}_m - Q_m\right) \tag{1}$$

$$i^{\mathrm{ref}}_{d,m} = \left(\lambda^{pp}_m + \frac{\lambda^{ip}_m}{s}\right)\left(P^{\mathrm{ref}}_{\mathrm{SF},m} + P^{\mathrm{ref}}_{\mathrm{DC},m} - P_m\right) \tag{2}$$

$$v_{d,m} = \left(\lambda^{pi}_m + \frac{\lambda^{ii}_m}{s}\right)\left(i^{\mathrm{ref}}_{d,m} - i_{d,m}\right) \tag{3}$$

$$v_{q,m} = \left(\lambda^{pi}_m + \frac{\lambda^{ii}_m}{s}\right)\left(i^{\mathrm{ref}}_{q,m} - i_{q,m}\right) \tag{4}$$

where $P^{\mathrm{ref}}_{\mathrm{DC},m}$ refers to the $\omega - P$ characteristic of the frequency droop control and can be calculated by $P^{\mathrm{ref}}_{\mathrm{DC},m} = \lambda_{\omega,m}(\omega_0 - \omega_m)$, and $P^{\mathrm{ref}}_{\mathrm{SF},m}$ is the supplementary power set point of the mth DG assigned by the secondary frequency controller and can be obtained by $P^{\mathrm{ref}}_{\mathrm{SF},m} = \left(\lambda^{p\omega}_m + \frac{\lambda^{i\omega}_m}{s}\right)(\omega_0 - \omega_m)$.

Network block, the second part of the microgrid model, can be presented in a common reference frame x–y as follows:

$$\begin{bmatrix}\Delta\mathbf{i}_x\\ \Delta\mathbf{i}_y\end{bmatrix} = \begin{bmatrix} G & -B\\ B & G\end{bmatrix}\begin{bmatrix}\Delta\mathbf{V}_x\\ \Delta\mathbf{V}_y\end{bmatrix}$$

where $\mathbf{i}_x = [i_{x1}, i_{x2}, \ldots, i_{xn}]^T$ and $\mathbf{i}_y = [i_{y1}, i_{y2}, \ldots, i_{yn}]^T$ with $i_{xm}, i_{ym}, m = 1, \ldots, n$ being the terminal current of the mth DG in the common x-axis and y-axis, respectively, $\mathbf{V}_x = [V_{x1}, V_{x2}, \ldots, V_{xn}]^T$ and $\mathbf{V}_y = [V_{y1}, V_{y2}, \ldots, V_{yn}]^T$ with $V_{xm}, V_{ym}, m = 1, \ldots, n$ being the terminal voltage of the mth DG in the common x-axis and y-axis, respectively, and the matrices G and B are obtained from the network admittance matrix [23].

The third part, interface block, can be modeled as follows:

$$\begin{aligned}
\Delta\mathbf{V}_d &= C_0\Delta\mathbf{V}_x - \mathbf{V}_{x0}S_0\Delta\boldsymbol{\delta} + S_0\Delta\mathbf{V}_y + \mathbf{V}_{y0}C_0\Delta\boldsymbol{\delta}\\
\Delta\mathbf{V}_q &= S_0\Delta\mathbf{V}_x - \mathbf{V}_{x0}C_0\Delta\boldsymbol{\delta} + C_0\Delta\mathbf{V}_y + \mathbf{V}_{y0}S_0\Delta\boldsymbol{\delta}\\
\Delta\mathbf{i}_x &= C_0\Delta\mathbf{i}_d - \mathbf{i}_{d0}S_0\Delta\boldsymbol{\delta} - S_0\Delta\mathbf{i}_q - \mathbf{i}_{q0}C_0\Delta\boldsymbol{\delta}\\
\Delta\mathbf{i}_y &= S_0\Delta\mathbf{i}_d + \mathbf{i}_{d0}C_0\Delta\boldsymbol{\delta} + C_0\Delta\mathbf{i}_q - \mathbf{i}_{q0}S_0\Delta\boldsymbol{\delta}
\end{aligned}$$

where δ_i is the individual-inverter terminal-voltage phase angle in the x–y reference frame, and the matrices $C_0 = \text{diag}\{\cos(\delta_{i0})\}$ and $S_0 = \text{diag}\{\sin(\delta_{i0})\}$.

Then, according to [23], the whole system model can be expressed as follows:

$$E\Delta\dot{\boldsymbol{x}} = A\Delta\boldsymbol{x} + F\boldsymbol{r}_0 \tag{5}$$

where $\boldsymbol{x} = [\boldsymbol{\delta}, \boldsymbol{\omega}, \mathbf{i}_d, \mathbf{i}_q, \mathbf{i}_{dref}, \mathbf{i}_{qref}, \mathbf{u}_d, \mathbf{u}_q, P, Q, P_{\text{ref}}, \mathbf{V}_d, \mathbf{V}_q, \mathbf{i}_{\boldsymbol{x}}, \mathbf{i}_{\boldsymbol{y}}, \mathbf{V}_{\boldsymbol{x}}, \mathbf{V}_{\boldsymbol{y}}]^T$, $\boldsymbol{r}_0 = [\boldsymbol{\omega}_0]^T$, and the system matrix E is singular. Due to the limitation of space, the expressions of matrices E and A are omitted here, and they can be found in [23, App. A].

B. Active Power Reference

The active power setting depends on the total power demand and power generation. The total active power demand is representable as $P_d = \sum_{m=1}^{n} P_{mL} + P_{\text{Loss}}$, where P_{mL} is the active power demand of load at bus m, and P_{Loss} is the total loss of active power, which is only a small proportion of the total active power demand. Denote by $P_{mG}^{\max}$ the maximum power generation of the mth DG. Then, we can present the total available power generation as $P_G^{\max} = \sum_{m=1}^{n} P_{mG}^{\max}$. Let

$$U = \min\left\{\frac{P_d}{P_G^{\max}}, 1\right\} \tag{6}$$

be a common utilization level for all DGs [24], [25]. We assume that the load is less than the maximum available power generation. It can be seen that the supply and demand are balanced if the active power generation reference of the mth DG, i.e., P_{mG}^{ref}, satisfies $P_{mG}^{\text{ref}} = UP_{mG}^{\max}$.

In fact, the balance of supply and demand can be achieved when the load demand P_d is less than the maximum available power generation $P_G^{\max}$. We have $U = P_d/P_G^{\max} \leq 1$. Furthermore, we can see that

$$\sum_{m=1}^{n} P_{mG}^{\text{ref}} = \sum_{m=1}^{n} UP_{mG}^{\max} = \frac{P_d}{P_G^{\max}} \sum_{m=1}^{n} P_{mG}^{\max} = P_d.$$

However, if the load demand is more than the maximum available power generation, i.e., $P_d > P_G^{\max}$, then DGs should operate in the maximum peak power tracking mode, and the power storage needs to compensate for the power shortage.

IV. System Performance Under Attack

A. FDI Attack Against Distributed Load Sharing Control

The global microgrid information includes the average power demands and available power generations of all BAs. It is the basis of designing the active power references of DGs. However, each BA only has its local information and cannot directly obtain the global information. Each agent can only exchange information with its neighbors. Hence, a distributed information processing law must be properly designed for the agents in order to obtain the global information.

In the cyberlayer, the computing process of information discovery at agent m can be represented by a linear time-invariant model

$$\begin{bmatrix} P_{mL}(k+1) \\ P_{mG}(k+1) \end{bmatrix} = \begin{bmatrix} P_{mL}(k) \\ P_{mG}(k) \end{bmatrix} + \begin{bmatrix} u_{mL}(k) \\ u_{mG}(k) \end{bmatrix}$$

where $u_{mL}(k)$ and $u_{mG}(k)$ are the control inputs of load and generation, respectively. The objective of information discovery is to find a distributed control law such that all the states converge to the average value of initial states, i.e.,

$$\lim_{k\to\infty} P_{mL}(k) = \bar{P}_L, \lim_{k\to\infty} P_{mG}(k) = \bar{P}_G, m = 1, 2, \ldots, n \tag{7}$$

where $\bar{P}_L = \frac{1}{n}\sum_{m=1}^{n} P_{mL}(0), \bar{P}_G = \frac{1}{n}\sum_{m=1}^{n} P_{mG}(0)$.

Smart grid often suffers from FDI attacks [26], [27]. To analyze the impact of FDI attacks, we assume that the attacker has full knowledge of the power system [9]. The FDI attack on the information discovery processes can be modeled as follows:

$$\begin{bmatrix} P_{mL}^a(k) \\ P_{mG}^a(k) \end{bmatrix} = \begin{bmatrix} P_{mL}(k) \\ P_{mG}(k) \end{bmatrix} + \begin{bmatrix} a_{mL}(k) \\ a_{mG}(k) \end{bmatrix} \tag{8}$$

where $a_{mL}(k)$ and $a_{mG}(k)$ are the FDI data that is injected into the state of agent m at time k, $P_{mL}^a(k)$ and $P_{mG}^a(k)$ denote the state of agent m at time k when the FDI attack is present. We focus on the discrete average consensus algorithm [28] under the FDI attack. It can be seen that

$$\begin{aligned} P_{mL}^a(k+1) &= P_{mL}^a(k) + \sum_{j\in\mathcal{N}_m(k)} w_{mjL}[P_{jL}^a(k) - P_{mL}^a(k)] \\ &= P_{mL}(k) + a_{mL}(k) + \sum_{j\in\mathcal{N}_m(k)} w_{mjL}[P_{jL}(k) \\ &\quad + a_{jL}(k) - P_{mL}(k) - a_{mL}(k)] \\ &= \sum_{j=1}^{n} w_{mjL}P_{jL}(k) + \sum_{j=1}^{n} w_{mjL}a_{jL}(k) \end{aligned}$$

where $\mathcal{N}_m(k)$ is the set of agent m's neighbors at time k, w_{mjL} is a positive weight with respect to load for $j \in \mathcal{N}_m(k)$, which represents importance degree of agent j's information from the viewpoint of agent m, and $w_{mmL}(k) = 1 - \sum_{j\in\mathcal{N}_m(k)} w_{mjL}$. Its equivalent matrix form is given by

$$\mathbf{P}_L^a(k+1) = \mathbf{W}_L(k)[\mathbf{P}_L(k) + \mathbf{A}_L(k)]. \tag{9}$$

This means that the information discovery for the load under an FDI attack at time $k+1$ is the linear combination of the information discovery without the attack and the attack vector at time k.

Similarly, we have

$$P_{mG}^a(k+1) = \sum_{j=1}^{n} w_{mjG}P_{jG}(k) + \sum_{j=1}^{n} w_{mjG}a_{jG}(k)$$

and the equivalent matrix form

$$\mathbf{P}_G^a(k+1) = \mathbf{W}_G(k)[\mathbf{P}_G(k) + \mathbf{A}_G(k)] \tag{10}$$

for the power generation.

Notice that $\mathbf{W}_L(k)$ and $\mathbf{W}_G(k)$ are predefined Perron matrices, which depend on the structure of graph $\mathcal{G}$, i.e.,

$$\mathbf{W}_L(k) = E - \epsilon_L(k)\mathbf{L}, \text{ and } \mathbf{W}_G(k) = E - \epsilon_G(k)\mathbf{L}$$

where $\epsilon_L(k), \epsilon_G(k)$ are the given parameters that satisfy $\epsilon_L(k) \in (0, 1/\rho), \epsilon_G(k) \in (0, 1/\rho)$ with $\rho = \max\{\sum_{j\neq i} a_{ij}\}$ (more details can be found in [29, Sec. II.C]).

Before investigating the impact of an FDI attack on the microgrid, two basic assumptions are presented.

Assumption 1 (Nondegeneracy [28]): There exists $w > 0$ such that $w_{mm}(k) \geq w$ for all m and $w \leq w_{mj}(k) \leq 1$, or $w = 0$, for all $m \neq j$ at any time k.

Assumption 2 (Balanced Communication [30]): For any time k, $\mathbf{1}^T\mathbf{W}(k) = \mathbf{1}^T$, and $\mathbf{W}(k)\mathbf{1} = \mathbf{1}$.

Notice that Assumption 1 can guarantee that each agent updates the states with its neighbors' information, and Assumption 2 makes sure that all agents converge to the average initial states [31].

Lemma 1: If Assumptions 1 and 2 hold for $\mathbf{W}_L$ and $\mathbf{W}_G$, $\sum_{k=1}^{\infty} |a_{mL}(k)| \leq \bar{B}_L$, and $\sum_{k=1}^{\infty} |a_{mG}(k)| \leq \bar{B}_G$, where $\bar{B}_L$ and $\bar{B}_G$ are constant FDI bounds on the load and generation of arbitrary agent m, respectively, then

$$\lim_{k\to\infty} \left| \frac{1}{n}\sum_{m=1}^{n} P^a_{mL}(k) - \bar{P}_L \right| \leq n\bar{B}_L \tag{11}$$

$$\lim_{k\to\infty} \left| \frac{1}{n}\sum_{m=1}^{n} P^a_{mG}(k) - \bar{P}_G \right| \leq n\bar{B}_G. \tag{12}$$

Proof: This is the direct result from [32, Ths. 2 and 3]. ■

Lemma 1 shows the property of difference between the convergence value of load under the FDI attack and that without the attack. The difference bound for load (generation) depends on the agents' number, and the bound of the false data injected into the BA.

When an FDI attack is present, the utilization level is

$$U^a = \frac{\bar{P}^a_L}{\bar{P}^a_G} = \frac{\lim_{k\to\infty}\frac{1}{n}\sum_{m=1}^{n} P^a_{mL}(k)}{\lim_{k\to\infty}\frac{1}{n}\sum_{m=1}^{n} P^a_{mG}(k)}. \tag{13}$$

Theorem 1: If Assumptions 1 and 2 hold for $\mathbf{W}_L$ and $\mathbf{W}_G$, $\sum_{k=1}^{\infty} |a_{mL}(k)| \leq \bar{B}_L$, and $\sum_{k=1}^{\infty} |a_{mG}(k)| \leq \bar{B}_G$, and then

$$\frac{\bar{P}_L - n\bar{B}_L}{\bar{P}_G + n\bar{B}_G} \leq U^a \leq \frac{\bar{P}_L + n\bar{B}_L}{\bar{P}_G - n\bar{B}_G}. \tag{14}$$

Proof: According to Lemma 1, we have

$$|\bar{P}_L - \bar{P}^a_L| \leq n\bar{B}_L, |\bar{P}_G - \bar{P}^a_G| \leq n\bar{B}_G$$

which is equivalent to

$$\bar{P}_L - n\bar{B}_L \leq \bar{P}^a_L \leq \bar{P}_L + n\bar{B}_L \tag{15}$$

$$\bar{P}_G - n\bar{B}_G \leq \bar{P}^a_G \leq \bar{P}_G + n\bar{B}_G. \tag{16}$$

Then, (14) can be obtained from (15) and (16). ■

B. Effects of FDI Attack on the Microgrid Performance

The characteristic equation of system (5) is $\det(\lambda E - A) = 0$, where λ is the eigenvalue to indicate the stability of system (5), i.e., the system is stable if the real part of λ is less than 0, and it is unstable otherwise.

TABLE I
SYSTEM PARAMETERS

Parameters	Value	Parameters	Value
S_{base}	10 (MVA)	R_s	1.73×10^{-6} (p.u.)
$V_{\text{base},1}$	$120\sqrt{2}/\sqrt{3}$ (kV)	X_s	3.47×10^{-5} (p.u.)
$V_{\text{base},2}$	$12.5\sqrt{2}/\sqrt{3}$ (kV)	R_f	0.0029 (p.u.)
$V_{\text{base},3}$	$208\sqrt{2}/\sqrt{3}$ (kV)	X_f	0.0041 (p.u.)

The characteristic equation is often used to investigate the performance of microgrid systems [23]. In this paper, we study the impact of FDI attacks on the microgrid performance with respect to the utilization level.

Definition 1: A critical utilization interval denoted by $\mathcal{U} = (\underline{U}, \overline{U})$ is called a *stable region* if system (5) is stable for $U \in \mathcal{U}$, and it is unstable for $U \notin \mathcal{U}$.

Now, it is ready to show the stability of a microgrid under the FDI attack.

Theorem 2: If Assumptions 1 and 2 hold for $\mathbf{W}_L$ and $\mathbf{W}_G$, $\sum_{k=1}^{\infty} |a_{mL}(k)| \leq \bar{B}_L$, and $\sum_{k=1}^{\infty} |a_{mG}(k)| \leq \bar{B}_G$, then

1) system (5) is stable, if

$$\left(\frac{\bar{P}_L - n\bar{B}_L}{\bar{P}_G + n\bar{B}_G}, \frac{\bar{P}_L + n\bar{B}_L}{\bar{P}_G - n\bar{B}_G}\right) \subset \mathcal{U} \tag{17}$$

2) system (5) is unstable, if

$$\frac{\bar{P}_L - n\bar{B}_L}{\bar{P}_G + n\bar{B}_G} \geq \overline{U}, \text{ or } \frac{\bar{P}_L + n\bar{B}_L}{\bar{P}_G - n\bar{B}_G} \leq \underline{U}. \tag{18}$$

Proof: It can be directly obtained from Theorem 1 and Definition 1. ■

Theorem 2 provides an important theoretical result for both the attacker and the defender. From the viewpoint of an FDI attacker, if they know the initial load information and generation information, they can design proper injection data to achieve their objective. If they want to make the system unstable, they can adopt the second statement of Theorem 2 to design an attack strategy. If they only aim at changing the average consensus values of load and power generation, the FDI attack strategy should satisfy the first statement of Theorem 2. From the viewpoint of a defender, if they have learned the attack quantitative characteristics satisfying boundedness assumption in this theorem, then they can design a new control policy to relieve the impact of the FDI attack.

V. Case Studies

In order to show the performance of distributed load sharing under FDI attacks, we provide an illustrative example based on the Canadian urban distribution system (see Fig. 2) and implemented it in MATLAB/SimPowerSystems. The main parameters of this microgrid are given in Table I. In our simulation, the microgrid is disconnected with the main grid from time $t = 0.2$ s.

A. Stable Region

An illustrative example of a stable region is shown in Fig. 4. In this example, the utilization levels of all agents in Fig. 2 are varying in interval $[0.1,0.7]$. It can be observed that the stable

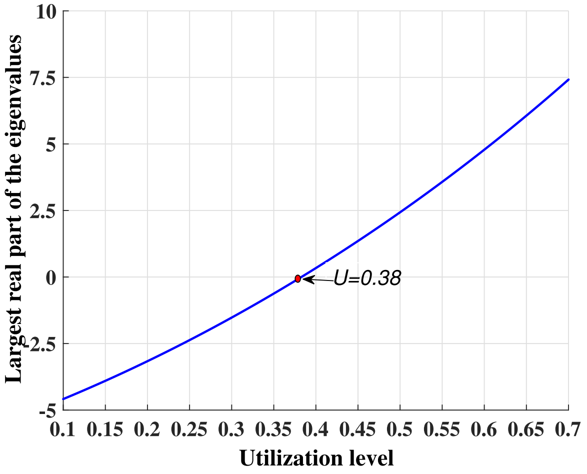


Fig. 4. Variation of maximal real value of eigenvalues with respect to utilization level.

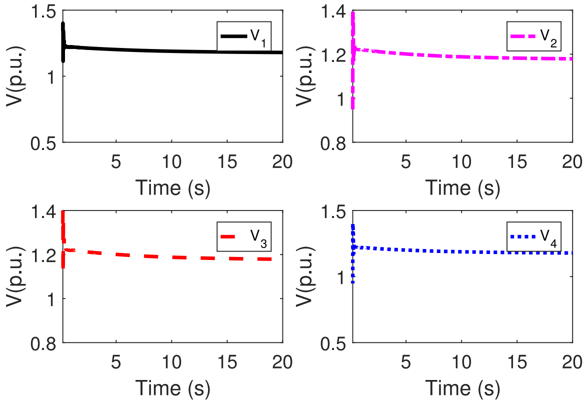


Fig. 5. Variations of voltage magnitudes under attack strategy 1.

region is $\mathcal{U} = (0, 0.38)$. In other words, when $U \in \mathcal{U}$, the maximal real value of eigenvalues is less than 0, and therefore, the system is stable. When $U \notin \mathcal{U}$, the system will become unstable. In general, the stable region is determined by the system parameters, and it is still challenging to find the analytical expression of the stable region. At the moment, we can only derive the stable region for the given system by numerical computation.

B. System Performance Under Attack Strategy 1

In this section, we study the system performances under an FDI attack with *Strategy 1*

$$a_{mL}(k) = 0.05e^{-k-1}|\sin[2\pi\xi_m(k)]|$$
$$a_{mG}(k) = 0.1e^{-k-1}|\cos[2\pi\eta_m(k)]|$$

where $\xi_m(k)$and $\eta_m(k)$ are with independent identical uniform distribution $\mathcal{U}(0,1)$.

It is clear that

$$|a_{mL}(k)| \le 0.05e^{-k-1}, \ |a_{mG}(k)| \le 0.1e^{-k-1}, k = 1, 2, \ldots.$$

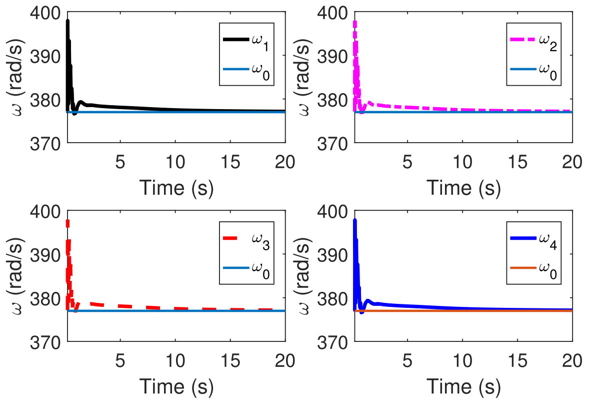


Fig. 6. Variations of frequency under attack strategy 1.

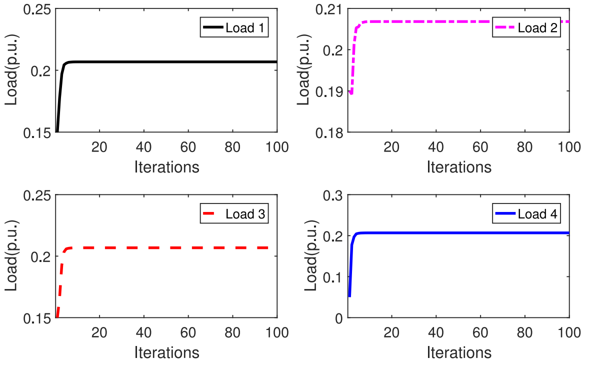


Fig. 7. Average load information discovery under attack strategy 1.

Thus, we can verify that

$$\sum_{k=1}^{\infty} |a_{mL}(k)| \le \bar{B}_L = \sum_{k=1}^{\infty} 0.05e^{-k-1} = \frac{0.05e^{-2}}{1-e^{-1}}$$
$$\sum_{k=1}^{\infty} |a_{mG}(k)| \le \bar{B}_G = \sum_{k=1}^{\infty} 0.1e^{-k-1} = \frac{0.1e^{-2}}{1-e^{-1}}.$$

This means that the conditions in Theorems 1 and 2 hold for this strategy.

We now investigate the microgrid system performances under an FDI attack with strategy 1. According to the simulation results, we have $\bar{P}_L = 0.1418$, $\bar{P}_G = 0.9137$, and then it can be easily verified that

$$\left(\frac{\bar{P}_L - n\bar{B}_L}{\bar{P}_G + n\bar{B}_G}, \frac{\bar{P}_L + n\bar{B}_L}{\bar{P}_G - n\bar{B}_G}\right) = (0.0991, 0.2230) \subset \mathcal{U}.$$

Thus, condition (17) holds when attack strategy 1 is implemented. Figs. 5–8 present the variations of voltage magnitudes, frequencies, loads, and generations under attack strategy 1, respectively. It can be seen that the indices can still reach steady states in a short time even when the agents are under FDI attacks. Our simulation results in Figs. 5–8 confirm the first statement of Theorem 2. In contrast to microgrid performances in the absence of the attack (see Figs. 9–12), although the performance indices, i.e., voltage magnitudes, frequencies, loads, and powers, are still convergent under attack strategy 1, the convergence values are different from those in the absence of the attack.

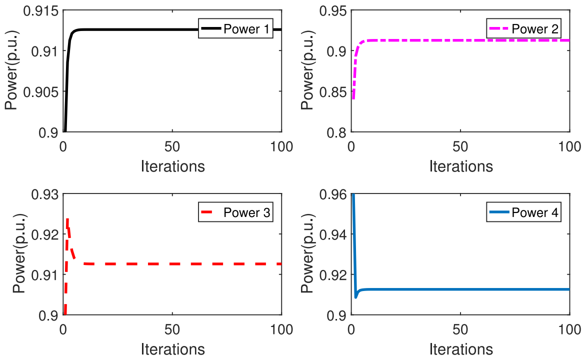


Fig. 8. Average power generation information discovery under attack strategy 1.

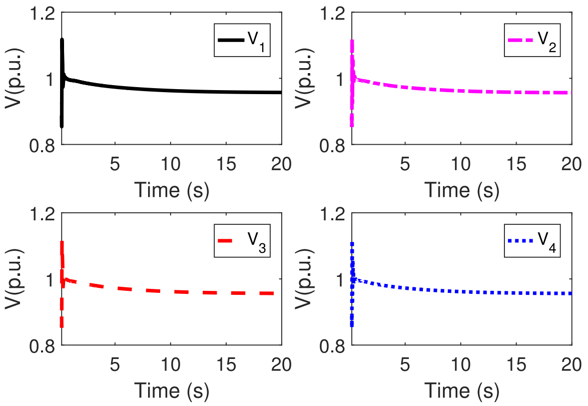


Fig. 9. Variations of voltage magnitudes in the absence of attack.

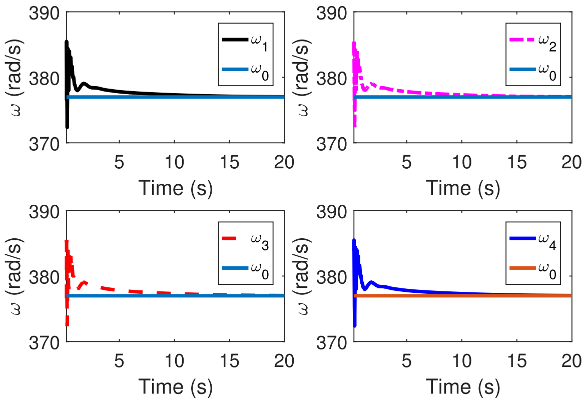


Fig. 10. Variations of frequency in the absence of attack.

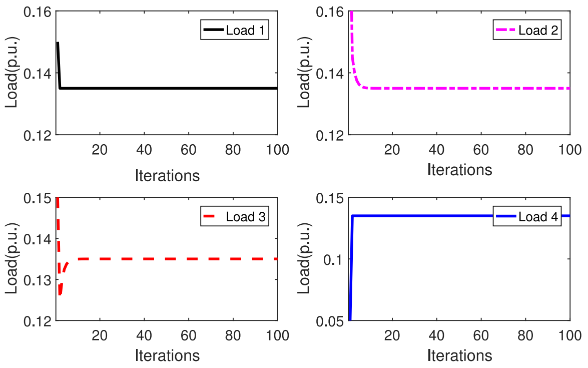


Fig. 11. Average load information discovery in the absence of attack.

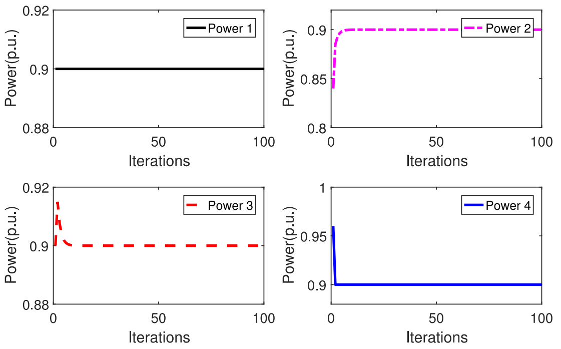


Fig. 12. Average power generation information discovery in the absence of attack.

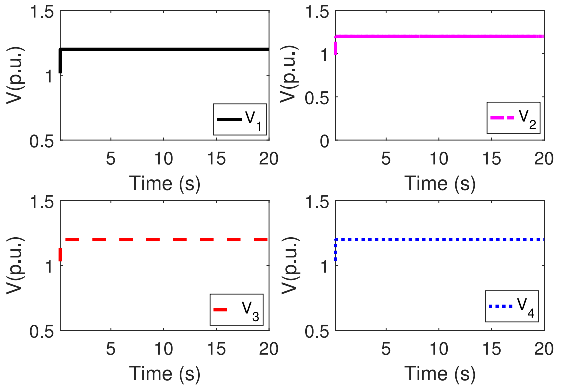


Fig. 13. Variations of voltage magnitudes under attack strategy 2.

C. System Performance Under Attack Strategy 2

In this section, we study the system performances under an FDI attack with *Strategy 2*

$$a_{m\,L}(k) = 4.5e^{-k-1}|\sin[2\pi\xi_m(k)]|$$
$$a_{m\,G}(k) = 0.1e^{-k-1}|\cos[2\pi\eta_m(k)]|.$$

Similar to attack strategy 1, we have

$$\sum_{k=1}^{\infty}|a_{m\,L}(k)| \le \bar{B}_L = \sum_{k=1}^{\infty}4.5e^{-k-1} = \frac{4.5e^{-2}}{1-e^{-1}}$$
$$\sum_{k=1}^{\infty}|a_{m\,G}(k)| \le \bar{B}_G = \sum_{k=1}^{\infty}0.1e^{-k-1} = \frac{0.1e^{-2}}{1-e^{-1}}.$$

For this attack strategy, we can derive $\frac{\bar{P}_L - n\bar{B}_L}{\bar{P}_G + n\bar{B}_G} = 1 > \overline{U} = 0.38$. Thus, condition (18) holds. Figs. 13–16 show the variations of voltage magnitudes, frequencies, loads and generations under attack strategy 2, respectively. From Figs. 15 and 16, it can be observed that the loads and generations can still reach steady states when all the agents are under FDI attacks with strategy 2. However, the performances of voltage magnitudes and frequencies are prominently influenced. Figs. 13 and 14 indicate that the voltage magnitudes and frequencies still drastically run up and down. Thus, the microgrid cannot achieve the steady states when attack strategy 2 is launched. In practice, per unit (p.u.) voltage is around one and will usually

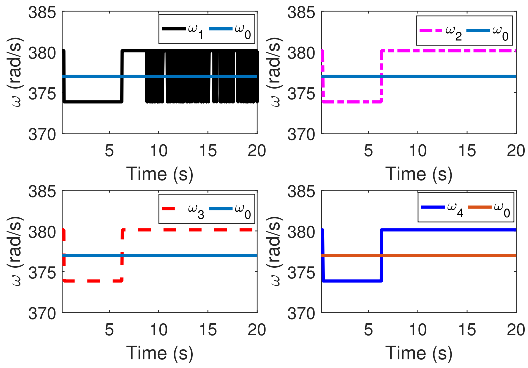


Fig. 14. Variations of frequency under attack strategy 2.

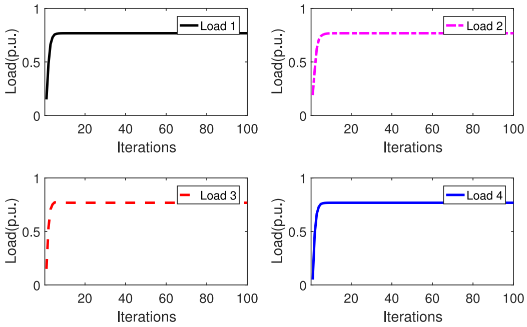


Fig. 15. Average load information discovery under attack strategy 2.

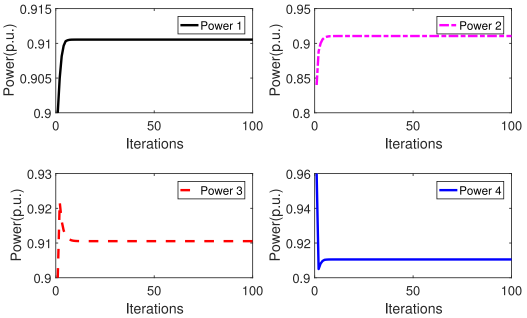


Fig. 16. Average power generation information discovery under attack strategy 2.

not get to a state with a p.u. voltage greater than 1.2. Since the frequency is usually maintained within a tight bound, the DG may have already been tripped after getting out of the bound, either instantaneously or after a certain time delay depending on the actual frequency [33]. Thus, we can set a limit for voltage and frequency to stop the simulation when hitting that limit.

D. Discussion

An FDI attacker may inject arbitrary false data to any node. However, the sufficiently large injected data may result in the false information seriously deviating from the real value and the attacked nodes would be suspected by their neighbors [34], [35]. Thus, in the case study, we assume that the injected data is decayed exponentially. Although the attack strength is very weak, the voltage magnitudes and frequency under attack strategy 2 are still becoming unstable. This simulation demonstrates that the distributed microgrid is very vulnerable to FDI attacks. Intuitively, a sustained attack may destroy the microgrid system even more significantly.

Our simulations have evaluated the effect of FDI attacks on distributed load sharing. It is still challenging to design a proper active defense strategy to defeat FDI attacks. As is well known, a centralized operation system can equip with an intrusion detector at the fusion center side to detect FDI attacks. Unfortunately, every node in our considered distributed microgrids only knows its neighboring information and does not understand the global information. Therefore, the traditional intrusion detection methods cannot be applied to distributed microgrids. Inspired by a trust-aware defending method for distributed operation systems [36], we will design a trust-based distributed load sharing protocol against FDI attacks in the future.

VI. Conclusion

In this paper, we investigated the effect of FDI attacks on distributed load sharing of microgrids operating in the autonomous mode. Each bus was supposed to be equipped with an agent and the power balance was achieved by a well-developed consensus protocol of multiagent systems. Under FDI attacks, the information among agents can be corrupted by attackers. Meanwhile, the impact of FDI attacks on the utilization level was investigated under different injection strategies. We also defined the stable region and sufficient conditions for microgrids operating in stable regions. The theoretical results were validated in MATLAB/SimPowerSystems on the Canadian urban distribution system. Future works include investigation of the impact of FDI attacks in a more general form on the microgrid performance, and designing proper active defense strategies against FDI attacks in the microgrid.

References

[1] D. Chen, Y. Xu, and A. Q. Huang, "Integration of DC microgrids as virtual synchronous machines into the AC grid," *IEEE Trans. Ind. Electron.*, vol. 64, no. 9, pp. 7455–7466, Sep. 2017.

[2] J. M. Guerrero, M. Chandorkar, T.-L. Lee, and P. C. Loh, "Advanced control architectures for intelligent microgrids Part I: Decentralized and hierarchical control," *IEEE Trans. Ind. Electron.*, vol. 60, no. 4, pp. 1254–1262, Apr. 2013.

[3] A. Ovalle, G. Ramos, S. Bacha, A. Hably, and A. Rumeau, "Decentralized control of voltage source converters in microgrids based on the application of instantaneous power theory," *IEEE Trans. Ind. Electron.*, vol. 62, no. 2, pp. 1152–1162, Feb. 2015.

[4] P. Sreekumar and V. Khadkikar, "Direct control of the inverter impedance to achieve controllable harmonic sharing in the islanded microgrid," *IEEE Trans. Ind. Electron.*, vol. 64, no. 1, pp. 827–837, Jan. 2017.

[5] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746–4756, Oct. 2013.

[6] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 28–39, 2016.

[7] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2013-5472, 2013.

[8] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5107–5117, Jun. 2017.

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, 2011.

[10] M. Chlela, G. Joos, and M. Kassouf, "Impact of cyber-attacks on islanded microgrid operation," in *Proc. Workshop Commun. Comput. Control Resilient Smart Energy Syst.*, 2016, pp. 1–5.

[11] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017, doi: 10.1109/TSG.2015.2495133.

[12] X. Zhang, X. Yang, J. Lin, and W. Yu, "On false data injection attacks against the dynamic microgrid partition in the smart grid," in *Proc. IEEE Int. Conf. Commun.*, 2015, pp. 7222–7227.

[13] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *Proc. Power Energy Soc. General Meeting*, 2016, pp. 1–5.

[14] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *J. Parallel Distrib. Comput.*, vol. 103, pp. 32–41, May 2017.

[15] X. Yang, P. Zhao, X. Zhang, J. Lin, and W. Yu, "Toward a Gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 147–161, Feb. 2017.

[16] O. Beg, T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans. Ind. Inform.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017, doi: 10.1109/TII.2017.2656905.

[17] J. Hao *et al.*, "An adaptive Markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2016.2610582.

[18] M. M. Rana, L. Li, and S. W. Su, "Cyber attack protection and control in microgrids using channel code and semidefinite programming," in *Proc. Power Energy Soc. Gen. Meeting.*, 2016, pp. 1–5.

[19] S. Wang and W. Ren, "Stealthy false data injection attacks against state estimation in power systems: Switching network topologies," in *Proc. Amer. Control Conf.*, 2014, pp. 1572–1577.

[20] A. Pilloni, A. Pisano, and E. Usai, "Robust finite-time frequency and voltage restoration of inverter-based microgrids via sliding-mode cooperative control," *IEEE Trans. Ind. Electron.*, vol. 65, no. 1, pp. 907–917, Jan. 2018, doi: 10.1109/TIE.2017.2726970.

[21] W. Meng, X. Wang, and S. Liu, "Distributed load sharing of an inverter-based microgrid with reduced communication," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2016.2587685.

[22] Q. Li *et al.*, "Networked and distributed control method with optimal power dispatch for islanded microgrids," *IEEE Trans. Ind. Electron.*, vol. 64, no. 1, pp. 493–504, Jan. 2017.

[23] S. Liu, X. Wang, and P. X. Liu, "Impact of communication delays on secondary frequency control in an islanded microgrid," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2021–2031, Apr. 2015.

[24] W. Zhang, Y. Xu, W. Liu, F. Ferrese, and L. Liu, "Fully distributed coordination of multiple DFIGs in a microgrid for load sharing," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 806–815, Jun. 2013.

[25] Y. Xu *et al.*, "Distributed subgradient-based coordination of multiple renewable generators in a microgrid," *IEEE Trans. Power Syst.*, vol. 29, no. 1, pp. 23–33, Jan. 2014.

[26] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[27] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar. 2013.

[28] V. Blondel, J. M. Hendrickx, A. Olshevsky, and J. Tsitsiklis, "Convergence in multiagent coordination, consensus, and flocking," in *Proc. IEEE Conf. Decis. Control*, 2005, pp. 2996–3000.

[29] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, Jan. 2007.

[30] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1520–1533, Sep. 2004.

[31] A. Olshevsky and J. N. Tsitsiklis, "Convergence speed in distributed consensus and averaging," *SIAM J. Control Optim.*, vol. 48, no. 1, pp. 33–55, 2009.

[32] J. He, M. Zhou, P. Cheng, L. Shi, and J. Chen, "Consensus under bounded noise in discrete network systems: An algorithm with fast convergence and high accuracy," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 2874–2884, Dec. 2016.

[33] *IEEE Standard for Interconnecting Distributed Resources With Electric Power Systems*, IEEE Std. 1547-2003, 2003.

[34] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[35] R. Tan *et al.*, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

[36] C. Rosinger, M. Uslar, and J. Sauer, "Using information security as a facet of trustworthiness for self-organizing agents in energy coalition formation processes," in *Proc. EnviroInfo*, 2014, pp. 373–380.

Heng Zhang (M'16) received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2015.

He is currently an Associate Professor with the School of Science, Huaihai Institute of Technology, Lianyungang, China. He is also a Research Fellow with Western Sydney University, Sydney, NSW, Australia. His research interests include security and privacy in cyber-physical systems, control, and optimization theory.

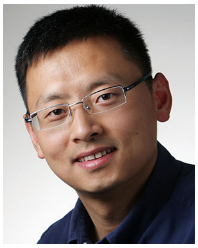
Wenchao Meng received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2015.

He is currently a Postdoctoral Scholar with Carleton University, Ottawa, ON, Canada. His research interests include intelligent control and smart grids.

Junjian Qi (S'12–M'13–SM'17) received the B.E. degree from Shandong University, Jinan, China, in 2008 and the Ph.D. degree from Tsinghua University, Beijing, China, in 2013, both in electrical engineering.

He was a Visiting Scholar with Iowa State University, Ames, IA, USA, in 2012; a Research Associate with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA, from 2013 to 2015; and a Postdoctoral Appointee with the Energy Systems Division, Argonne National Laboratory, Argonne, IL, USA, from 2015 to 2017. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL, USA. His research interests include cascading blackouts, power system dynamics, state estimation, synchrophasors, voltage control, and cybersecurity.

Dr. Qi is the Secretary of the IEEE Task Force on Voltage Control for Smart Grids.



Xiaoyu Wang (M'08–SM'13) received the B.Sc. and M.Sc. degrees from Tsinghua University, Beijing, China, and the Ph.D. degree from the University of Alberta, Edmonton, AB, Canada, in 2000, 2003, and 2008, respectively, all in electrical engineering.

He is currently an Associate Professor with the Department of Electronics, Faculty of Engineering and Design, Carleton University, Ottawa, ON, Canada. His research interests include the integration of distributed energy resources and power quality.

Wei Xing Zheng (F'14) received the Ph.D. degree in electrical engineering from Southeast University, Nanjing, China, in 1989.

He has held various Faculty/Research/Visiting positions with several universities in China, the U.K., Australia, Germany, and the USA. He is currently a Full Professor with Western Sydney University, Sydney, NSW, Australia.

Prof. Zheng is an Associate Editor for *Automatica*, the IEEE TRANSACTIONS ON AUTOMATIC CONTROL, the IEEE TRANSACTIONS ON CYBERNETICS, and the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, among others. He was named a Thomson Reuters' Highly Cited Researcher in 2015, 2016, and 2017, consecutively.