This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

Detection and Mitigation of Data Manipulation Attacks in AC Microgrids

Aquib Mustafa, *Student Member, IEEE*, Binod Poudel, *Student Member, IEEE*, Ali Bidram, *Member, IEEE*, and Hamidreza Modares, *Senior Member, IEEE*

***Abstract*— This paper presents a resilient control framework for distributed frequency and voltage control of AC microgrids under data manipulation attacks. In order for each distributed energy resource (DER) to detect any misbehavior on its neighboring DERs, an attack detection mechanism is first presented using a Kullback-Liebler (KL) divergence-based criterion. An attack mitigation technique is then proposed that utilizes the calculated KL divergence factors to determine trust values indicating the trustworthiness of the received information. Moreover, DERs continuously generate a self-belief factor and communicate it with their neighbors to inform them of the validity level of their own outgoing information. DERs incorporate their neighbors' self-belief and their own trust values in their control protocols to slow down and mitigate attacks. It is shown that the proposed cyber-secure control effectively distinguishes data manipulation attacks from legitimate events. The performance of proposed secure frequency and voltage control techniques is verified through the simulation of microgrid tests system implemented on IEEE 34-bus test feeder with six DERs.**

***Index Terms*— Data Manipulation attacks, distributed control, Kullback-Liebler divergence, microgrids, secondary control.**

I. Introduction

Microgrids, as the main building block of smart grids, are a controllable group of interconnected loads and Distributed Energy Resources (DERs) with the ability to operate autonomously in both grid-connected and islanded modes [1]. This unique feature of microgrids is a critical factor in enhancing the resilience of power systems under extreme events and is enabled through a hierarchical control architecture consisting of primary, secondary, and tertiary control levels [2]-[3]. The primary control level maintains the voltage and frequency stability of the microgrid. The secondary control level restores the microgrid voltage and frequency to their nominal values. The tertiary control level manages the active and reactive power flow between microgrid and upstream grid in grid-connected mode [2]. Among these hierarchies, the secondary control level plays a vital role in guaranteeing the reliable operation of microgrid critical customers at the nominal voltage and frequency values after the microgrid loses the support from the upstream grid. The secondary control level can adopt either centralized or distributed communication architectures. Compared to conventional centralized secondary control architecture, distributed secondary control offers more reliability, flexibility, and scalability [4]-[12], as well as improved transient performance as demonstrated in [13].

Despite significant advantages of the distributed secondary control, similar to other cyber-physical systems, due to the extensive deployment of communication and control technologies, it is vulnerable to attacks [14]. Attacks can target individual DERs as well as the communication links among them to corrupt the data transfer [14]-[30]. False data injection (FDI) attacks corrupt the data transferred through the communication links and impact the microgrid data integrity [15]-[17]. Denial-of-Service (DOS) attacks endanger the availability of communication system services [19]. The distributed control approach proposed in [20] requires limited communication capability which helps with the resilience of control system in the presence of DOS attacks. Both FDI and DOS attacks can adversely disrupt the voltage and frequency synchronization of the microgrid which in turn may result in cascading failures of its components and outage of power delivered to the critical customers during the emergency conditions [21].

The bulk of the research in cybersecurity of power systems focuses mainly on attack detection techniques [22]-[31]. Different techniques, including, adaptive cumulative sum using Markov-chain analysis [22], Kalman filter [23], graphical method [24], model-based scheme [25], matrix separation technique [26], Chi-square detector and cosine similarity matching approach [27], and nonlinear internal observer [28] are introduced for the attack detection in power systems with centralized control structure. The proposed attack detection filter in [29] and systematic detection and localization strategy in [31] tackle the attack detection in distributed control systems. In [32], signal temporal logic has been utilized for attack detection in a distributed control system. Attack mitigation has also recently been considered in power systems. In [33], sensor fault detection and mitigation schemes are proposed to mitigate the impacts of cyber-attacks in DC power systems with centralized control structure. Reference [34] proposes a trust/confidence-based approach for cyber-attack mitigation in the distributed control system of DC microgrids. In [35], a two-fold strategy is proposed to mitigate the impacts of FDI attacks on the control system of shipboard power system. In [36], a trust/confidence-based control protocol is proposed to mitigate the impact of attacks on the distributed secondary control of AC

Binod Poudel and Ali Bidram are supported by the National Science Foundation EPSCoR Program under Award #OIA-1757207.

Aquib Mustafa, and Hamidreza Modares are with the Department of Mechanical Engineering, Michigan State University, East Lansing, MI, (e-mail: {mustaf15, modaresh}@msu.edu).

Binod Poudel and Ali Bidram are with the Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM, (e-mail: {binodpoudel309, bidram}@unm.edu).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

microgrids. This approach, however, only considers the secondary frequency control and does not address attack mitigation of secondary voltage control. The objective of this paper is to present FDI-attack detection and mitigation approaches for distributed secondary control of microgrids that are not limited to any specific type of attack with only mild restrictions on network connectivity.

This paper proposes data manipulation attack detection and mitigation techniques to increase the resilience of distributed control of microgrids with respect to FDI attacks. The attack detection mechanism deploys Kullback-Liebler (KL) divergence to measure the discrepancy between the Gaussian distributions of the actual and expected local frequency/active power and voltage/reactive power neighborhood tracking errors. To mitigate the negative impact of attack, a self-belief value, as an indication of the probability of presence of attacks on neighbors of an agent, is presented for each DER by utilizing KL-based detectors. The self-belief value is a measure of trustworthiness of the agent's own outgoing information and is transmitted to neighboring DERs. Moreover, the trustworthiness of the incoming information from neighboring DERs is estimated using a trust factor. Trust for individual DERs is developed based on the relative entropy between DER own information and its neighbor's information on the communication graph. The attack mitigation algorithm utilizes self-belief and trust values to modify distributed control protocols.

The rest of paper is organized as follows: Section II discusses the preliminaries of graph theory. In Section III, the conventional distributed secondary control of AC microgrids is reviewed. Section IV discusses the attack modeling and detection mechanism. In Section V, the cyber-secure attack mitigation mechanism is proposed. The proposed attack detection and mitigation techniques are verified in Section VI. Section VII concludes the paper.

II. Preliminaries of Graph Theory

The communication network of a microgrid can be modeled by a graph. DERs are considered as the nodes of the communication graph and the communication links are considered as the edges. A graph is usually expressed as $\mathcal{G}=(\mathcal{V},\mathcal{E},\mathcal{A})$ with a nonempty finite set of N nodes $\mathcal{V}=\{v_1,v_2,\ldots,v_N\}$, a set of edges or arcs $\mathcal{E}\subset\mathcal{V}\times\mathcal{V}$, and the associated adjacency matrix $\mathcal{A}=[a_{ij}]\in\mathbb{R}^{N\times N}$. a_{ij} is the weight of edge (v_j,v_i), and $a_{ij}>0$ if $(v_j,v_i)\in\mathcal{E}$, otherwise $a_{ij}=0$. The set of neighbors of node i is denoted as $N_i=\{j\,|\,(v_j,v_i)\in\mathcal{E}\}$. The in-degree matrix is defined as $D=\mathrm{diag}\{d_i\}\in\mathbb{R}^{N\times N}$ with $d_i=\sum_{j\in N_i}a_{ij}$. The Laplacian matrix is defined as $L=D-\mathcal{A}$ [37].

Assumption 1. The communication graph $\mathcal{G}$ has a spanning tree.

III. Conventional Distributed Secondary Control

In the microgrid hierarchical control structure, the primary control level maintains the voltage and frequency stability of the microgrid. The secondary control level restores the microgrid voltage and frequency to their nominal values. DERs are integrated to the rest of microgrid through Voltage Source Inverters (VSI). Depending on the control objectives, DERs can be of two main types, namely grid forming and grid following. Grid forming DERs utilize a Voltage Controlled VSI (VCVSI) and have the capability of dictating microgrid frequency and voltage. On the other hand, grid following DERs utilize a Current Controlled VSI (CCVSI) and follow the microgrid frequency and voltage while supplying a specific amount of active and reactive power based on external setpoints [10].

The primary control is locally implemented at grid forming DERs by the droop technique. This technique prescribes a relation between the frequency, ω_i, and the active power, and between the voltage magnitude, $v_{o,magi}$, and the reactive power. The frequency and voltage droop characteristics are

$$\begin{cases}\omega_i=\omega_{ni}-m_{Pi}P_i\\ v_{o,magi}=V_{ni}-n_{Qi}Q_i\end{cases},\tag{1}$$

where ω_{ni} and V_{ni} are the primary frequency and voltage control references and m_{Pi} and n_{Qi} are the active and reactive power droop coefficients, respectively. Conventionally, the active power droop coefficients are proportionally selected based on the apparent power rating of DERs. However, the reactive power droop coefficients are proportionally selected based on the maximum reactive power which is calculated using a minimum allowable power factor and apparent power rating of DER [2]. The apparent power rating is related to thermal rating of DER equipment (e.g., power electronics switches).

The objective of distributed secondary control is to mitigate the microgrid frequency and voltage deviations from their nominal values which are caused by primary control. Distributed secondary control utilizes distributed control protocols implemented on individual DERs that can communicate with each other through a distributed communication network and share their local information with neighboring DERs.

Problem 1: The distributed secondary control chooses ω_{ni} and V_{ni} in (1) such that the operating frequency and terminal voltage magnitude of each DER synchronize to the reference frequency and voltage, ω_{ref} and v_{ref}, i.e.,

$$\begin{cases}\lim\limits_{t\to\infty}\left\|\omega_i(t)-\omega_{ref}\right\|=0\\ \lim\limits_{t\to\infty}\left\|v_{o,magi}(t)-v_{ref}\right\|=0\end{cases}\quad\forall i\in N.\tag{2}$$

Moreover, the secondary control should guarantee the allocation of active and reactive power of DERs based on the droop coefficients [7]-[11] as

$$m_{Pi}P_i=m_{Pj}P_j,\tag{3}$$

$$n_{Qi}Q_i=n_{Qj}Q_j,\tag{4}$$

where $P_{\max i}$ / $Q_{\max i}$ and $P_{\max j}$ / $Q_{\max j}$ are the active and reactive power ratings of i-th and j-th DER, respectively.

The secondary control of a microgrid including N DERs is described as the synchronization problem for the following first-order multi-agent system to adjust the primary control inputs

$$\left\{\dot{\omega}_{ni}=v_{\omega i},\quad \dot{V}_{ni}=v_{vi},\quad i=1,\ldots,N,\right.\tag{5}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

where $v_{\omega i}$ and v_{vi} are the distributed secondary frequency and voltage control (DSFC and DSVC) protocols that are chosen based on the local information of each DER and neighboring DERs' information and can be written as [10]

$$v_{\omega i} = -c_\omega \delta_{\omega i}, \tag{6}$$

$$v_{vi} = -c_v \delta_{vi}, \tag{7}$$

where c_ω and c_v are the control gains; $\delta_{\omega i}$ and δ_{vi} are the local frequency and voltage neighborhood tracking errors that can be written as

$$\begin{aligned}\delta_{\omega i} = &\sum_{j\in N_i} a_{ij}(\omega_i - \omega_j) + g_i(\omega_i - \omega_{ref}) \\ &+ \sum_{j\in N_i} a_{ij}(m_{Pi}P_i - m_{Pj}P_j),\end{aligned} \tag{8}$$

$$\begin{aligned}\delta_{vi} = &\sum_{j\in N_i} a_{ij}(v_{o,magi} - v_{o,magj}) + g_i(v_{o,magi} - v_{ref}) \\ &+ \sum_{j\in N_i} a_{ij}(n_{Qi}Q_i - n_{Qj}Q_j),\end{aligned} \tag{9}$$

The pinning gain g_i is assumed nonzero for only one DER.

Remark 1. Note that there always exists a low-level communication noise in the network of DERs. Therefore, in the presence of the communication noise, one can write the auxiliary controls $v_{\omega i}$ and v_{vi} of *i*-th DER in (6) and (7) as

$$\begin{cases}\zeta_{\omega i} = v_{\omega i} + \eta_{\omega i} \\ \zeta_{vi} = v_{vi} + \eta_{vi}\end{cases}, \tag{10}$$

where $\eta_{\omega i} \sim \mathcal{N}(0, \Sigma_{\omega_i})$ and $\eta_{vi} \sim \mathcal{N}(0, \Sigma_{v_i})$, respectively, denote the aggregate Gaussian noise affecting the incoming neighbors' frequency and voltage to *i*-th DER. In general, the noise associated with electronic devices at the receiver end lies under the category of thermal noise and statistically modeled as Gaussian, thus we assumed communication noise to be Gaussian and it is a standard assumption in the literature [12]. In noisy scenarios, the synchronization problem for microgrid frequency and voltage as defined in Problem 1 changes to the mean square synchronization problem and becomes

$$\begin{cases}\lim\limits_{t\to\infty} \mathbb{E}\left\|\omega_i(t) - \omega_{ref}(t)\right\|^2 = 0 \\ \lim\limits_{t\to\infty} \mathbb{E}\left\|v_{o,magi}(t) - v_{ref}(t)\right\|^2 = 0\end{cases} \quad \forall i \in N. \tag{11}$$

IV. Attack Modeling and Detection Mechanism

This section presents attack modelling and detection mechanism for the distributed secondary control of microgrid.

Definition 1. (Compromised DER). A DER that is directly under attack is called a compromised DER.

Definition 2. (Intact DER). A DER that is not compromised or not under direct attack is called an intact DER.

A. Attack Modeling

For the direct attack on controller, one can model the DER's frequency as

$$\omega_i^{cr} = \omega_i + \gamma_i \omega_i^a, \tag{12}$$

with ω_i^a as the injected attacker's input into the controller of *i*-th DER and ω_i^{cr} denotes the corrupted DER frequency with scalar γ_i equal to 1 in the presence of attack. Similarly, for the attack on the communication channel between two DERs, one can model the received corrupted frequency signal from *j*-th DER as

$$\omega_j^{cr} = \omega_j + \gamma_j \omega_j^a, \tag{13}$$

where ω_j^a represents the injected attacker's input into the communication channel between two DERs and ω_i^{cr} denotes the corrupted DER frequency of neighbor *j* received at *i*-th DER with scalar γ_i equal to 1 in the presence of attack.

Remark 2. This subsection discusses the attack model in terms of DER's frequency which affects the auxiliary control $v_{\omega i}$ in (6). Moreover, the rest of the paper considers frequency-based attacks and presents attack detection and mitigation mechanisms. Without loss of generality, the same approach holds true for attack modelling, detection and mitigation mechanisms for voltage-based attacks.

Remark 3. Attack models in (12)-(13) represent frequency manipulation attacks on controllers. Due to the extensive deployment of communication and control technologies and the presence of Intelligent Electronic Devices (IEDs), the microgrid control system is highly vulnerable to cyber-attacks. In Fig. 1, an *attack tree* for FDI threat analysis is provided to illustrate the attack path. As seen, the FDI attack can tamper with either the sensors (e.g., Phasor Measurement Units (PMUs)) or actuators (control and decision-making units). Such attacks can be launched by injecting counterfeit attack signals into sensors of DER measurement units or directly by injecting a disturbance into the control units and even hijacking the entire controller. More specifically, FDI attacks on DERs can endanger microgrid voltage and frequency stability, slow down the DER control system responses, or overload DERs.

The existing firewall/intrusion detection systems (IDSs) monitor and analyze information flow in the network and detect if there exists considerable change in the information flow. However, there is no single IDS that is able to detect all different attack types [38]. Moreover, the IDSs' effectiveness highly depends on their parameters. So, if the IDS parameters are not fine-tuned, the possibility of not detecting attacks increases [38]. On the other hand, IDSs do not block the corrupted information and cannot mitigate attacks. Therefore, it is of vital importance to design a resilient control protocol for

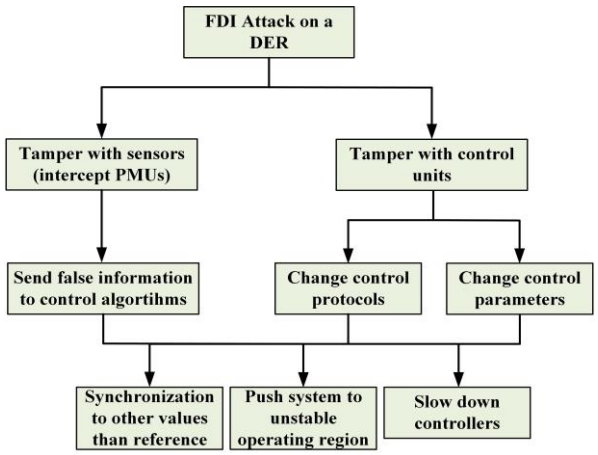


Fig. 1. FDI attack tree for microgrid control system.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

microgrids that can mitigate attacks and ensure an acceptable level of functionality for microgrid despite attacks.

B. Attack Detection Mechanism

This subsection presents a relative entropy-based attack detection approach for the distributed secondary control of microgrid. More specifically, KL divergence, a non-negative measure of the relative entropy between two probability distributions is employed to measure the discrepancy between them.

Definition 3. (KL divergence) [39]-[40] Let X and Z be two random sequences with probability density function P_X and P_Z, respectively. The KL divergence measure between P_X and P_Z in continuous-time is defined as

$$D_{KL}(X \| Z) = \int P_X(\theta) \log\left(\frac{P_X(\theta)}{P_Z(\theta)}\right) d\theta \ , \tag{14}$$

with the following properties:

1. $D_{KL}(P_X \| P_z) \geq 0$,
2. $D_{KL}(P_X \| P_z) = 0$ if and only if, $P_X = P_z$.

If the sequences X and Z are Gaussian distributed, then the KL divergence in (14) can be simplified in the terms of mean and covariance of sequences as [39]

$$\begin{aligned} D_{KL}(X \| Z) = \frac{1}{2}\left(\log\frac{|\Sigma_Z|}{|\Sigma_X|} - n + tr(\Sigma_Z^{-1}\Sigma_X) \right), \\ + \frac{1}{2}(\mu_Z - \mu_X)^T \Sigma_Z^{-1}(\mu_Z - \mu_X) \end{aligned} \tag{15}$$

where μ_X and Σ_X denote the mean and covariance of sequence X, and μ_Z and Σ_Z denote the mean and covariance of sequence Z. Moreover, n denotes the dimension of the sequences.

For the design of an attack detector, we first rewrite the frequency auxiliary control $\zeta_{\omega i}$ in (10) with statistical properties and then present an attack detection mechanism based on the KL divergence measure for distributed secondary control of AC microgrids. We show that in the presence of an attack, one can identify different sophisticated attacks based on the change in the statistical properties of the auxiliary control variables. In the absence of attack, since we consider the Gaussian noise in the communication channel, then the auxiliary control $\zeta_{\omega i}$ in (10) can be written as

$$\zeta_{\omega i} = -c_\omega \delta_{\omega i} + \eta_{\omega i} , \tag{16}$$

where $\eta_{\omega i}$ denotes the aggregate Gaussian noise affecting the incoming neighbors' information given by

$$\eta_{\omega i} = \sum_{j \in N_i} a_{ij} \eta_{\omega ij} \sim \mathcal{N}(0, \Sigma_{\omega_i}) . \tag{17}$$

Due to presence of noise, the statistical properties of the auxiliary control $\zeta_{\omega i}$ in (10) becomes

$$\zeta_{\omega i} \sim \mathcal{N}(0, \Sigma_{\omega_i}) , \tag{18}$$

and it represents the nominal behavior of the DSFC.

In the presence of attacks, using (10), the auxiliary control $\zeta_{\omega i}^a$ becomes

$$\zeta_{\omega i}^a = -c_\omega \delta_{\omega i}^{cr} + \eta_{\omega i} , \tag{19}$$

with the corrupted local neighborhood tracking error $\delta_{\omega i}^{cr} = \delta_{\omega i} + f_i$ where

$$f_i = [(\sum_{j \in N_i} a_{ij} + g_i)\omega_i^a - \sum_{j \in N_i} a_{ij}\omega_j^a] \tag{20}$$

denotes the overall deviation in the local neighborhood tracking error due to the attacks on controller/communication channel in the network. Note that in presence of attacks, one can observe the corrupted frequency of DERs and based on corrupted frequency, one has the corrupted auxiliary control $\zeta_{\omega i}^a$. The overall attacker's input f_i is neither measurable nor required to be known. The statistical properties of corrupted control protocol changes due to the effect of attacks. Now, from (19), one has the following statistical properties

$$\zeta_{\omega i}^a \sim \mathcal{N}(\mu_{f_i}, \Sigma_{f_i} + \Sigma_{\omega_i}) , \tag{21}$$

where μ_{f_i} and Σ_{f_i} are mean and covariance of the injected overall attack signal f_i, respectively. Since both $\zeta_{\omega i}^a$ and $\zeta_{\omega i}$ have normal Gaussian distributions, according to (15) the KL divergence $D_{KL}(\zeta_{\omega i}^a \| \zeta_{\omega i})$ between control sequences $\zeta_{\omega i}^a$ and $\zeta_{\omega i}$ becomes

$$\begin{aligned} D_{KL}(\zeta_{\omega i}^a \| \zeta_{\omega i}) = \frac{1}{2}\left(\log\frac{|\Sigma_{\zeta_{\omega i}}|}{|\Sigma_{\zeta_{\omega i}^a}|} - 1 + tr(\Sigma_{\zeta_{\omega i}}^{-1}\Sigma_{\zeta_{\omega i}^a}) \right), \\ + \frac{1}{2}(\mu_{\zeta_{\omega i}} - \mu_{\zeta_{\omega i}^a})^T \Sigma_{\zeta_{\omega i}}^{-1}(\mu_{\zeta_{\omega i}} - \mu_{\zeta_{\omega i}^a}) \end{aligned} \tag{22}$$

where $\mu_{\zeta_{\omega i}}$ and $\Sigma_{\zeta_{\omega i}}$ denote the mean and covariance of $\zeta_{\omega i}$ and $\mu_{\zeta_{\omega i}^a}$ and $\Sigma_{\zeta_{\omega i}^a}$ denote the mean and covariance of $\zeta_{\omega i}^a$.

We define the average of KL divergence over a window T as

$$\Omega_i = \frac{1}{T}\int_k^{k+T-1} D_{KL}(\zeta_{\omega i}^a \| \zeta_{\omega i}) d\tau \tag{23}$$

to detect the change due to the adversarial input. Now, in the following theorem, we show that the effect of attacks in the secondary distributed control of the microgrid can be detected based on the discrepancy of the control sequences $\zeta_{\omega i}^a$ and $\zeta_{\omega i}$.

Theorem 1. Consider the distributed auxiliary control $\zeta_{\omega i}$ in (16) under attacks. Then, a) Ω_i defined in (23) becomes zero, if there is no attack on DERs. b) Ω_i defined in (23) is greater than a design threshold γ_i, if the microgrid secondary control is under attack.

Proof. In the absence of attacks, the statistical properties of sequences $\zeta_{\omega i}^a$ and $\zeta_{\omega i}$, respectively, in (18) and (21) are the same because μ_{f_i} and Σ_{f_i} become zero as $f_i = 0$. Therefore, the KL divergence $D_{KL}(\zeta_{\omega i}^a \| \zeta_{\omega i})$ in (22) becomes zero based on (15) which yields Ω_i in (23) to be zero. This complete the proof of part (a).

For the proof of Part (b), using (18)-(21) in (22), the KL divergence between $\zeta_{\omega i}^a$ and $\zeta_{\omega i}$ becomes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

$$D_{KL}(\zeta^{a}_{\omega i} \,\|\, \zeta_{\omega i}) = \frac{1}{2}(\log \frac{\left|\Sigma_{\omega_i}\right|}{\left|\Sigma_{f_i}+\Sigma_{\omega_i}\right|} + tr(\Sigma^{-1}_{\omega_i}\Sigma_{f_i}) + \mu^{T}_{f_i}\Sigma^{-1}_{\omega_i}\mu_{f_i}) . \tag{24}$$

Then, using (23), one has

$$\Omega_i = \frac{1}{T}\int_{k}^{k+T-1}(\frac{1}{2}\log \frac{\left|\Sigma_{\omega_i}\right|}{\left|\Sigma_{f_i}+\Sigma_{\omega_i}\right|} + tr(\Sigma^{-1}_{\omega_i}\Sigma_{f_i}) + \mu^{T}_{f_i}\Sigma^{-1}_{\omega_i}\mu_{f_i}))d\tau > \gamma_i , \tag{25}$$

where T and γ_i denote the sliding window size and the predefined positive design threshold, respectively. This completes the proof. ■

Based on the presented Theorem 1, effect of attacks on the distributed secondary control of microgrids can be detected using the predefined design threshold γ_i. Attack detection in (25) uses the idea of average over a fixed length moving window to avoid false detection. If there is a short-period anomaly rather than attack (such as disturbance or packet dropout), it vanishes in a few time steps and such anomalies are not detected as attacks.

V. Resilient Distributed Control Mechanism

This section presents a resilient distributed control mechanism for distributed secondary control of microgrids based on the proposed attack detection algorithm in the previous section. To this end, first, we introduce the notion of self and external-belief of DERs about trustworthiness of their own information and their neighbor's information, respectively. Then the presented beliefs are incorporated in the distributed secondary control protocols.

A. Belief of DERs About Their Own Observed Frequency

To measure the level of trustworthiness of each DER about its own observed frequency, which depends on the proximity to the source of the attack in the network, a self-belief is presented. In the presence of the adversary, a DER reduces its level of trustworthiness about its own observed frequency and transmits its self-belief to its immediate neighbors which prevent the propagation of attack in the microgrid.

Using the $D_{KL}(\zeta^{a}_{\omega i} \,\|\, \zeta_{\omega i})$ from Theorem 1, self-belief of *i*-th DER about its own observed frequency is defined as

$$I^{Bel}_{i}(t) = \kappa_1 \int_{0}^{t} e^{\kappa_1(\tau - t)}\psi_i(\tau)d\tau , \tag{26}$$

where $0 \le I^{Bel}_{i}(t) \le 1$ with

$$\psi_i(t) = \frac{\Delta_1}{\Delta_1 + D_{KL}(\zeta^{a}_{\omega i} \,\|\, \zeta_{\omega i})} , \tag{27}$$

where Δ_1 represents the threshold to account for the channel fading and other uncertainties and $0 < \kappa_1 < 1$ denotes the discount factor. Equation (26) can be implemented by the following differential equation

$$\dot{I}^{Bel}_{i}(t) + \kappa_1 I^{Bel}_{i}(t) = \kappa_1 \psi_i(t) . \tag{28}$$

Based on Theorem 1, in the presence of attacks, $D_{KL}(\zeta^{a}_{\omega i} \,\|\, \zeta_{\omega i}) >> \Delta_1$, which makes the self-belief of the DER $\psi_i(t)$ close to zero and, consequently, the value of $I^{Bel}_{i}(t)$ becomes close to zero. On the other hand, based on Theorem 1, in the absence of attack $D_{KL}(\zeta^{a}_{\omega i} \,\|\, \zeta_{\omega i})$ tends to zero, which makes $\psi_i(t)$ close to one and, consequently, $I^{Bel}_{i}(t)$ becomes close to one.

If a DER is under direct attack, its self-belief tends to zero according to (26). The DER transmits its self-belief value to the neighboring DERs. Using the received self-belief values, neighboring DERs ignore the information received from the attacked DER which prevents the attack propagation. Note that the discount factor in (26) evaluates the importance of current information with regards to past information. The discount factor ensures that if an attacker removes the effect of attack in a while, or if a short-period adversarial effect exists rather than attack (such as packet dropout), then the belief of the DER will be recovered, as it mainly depends on the current information.

B. Belief of DERs About Their Neighbor's Observed Frequency

To evaluate the level of confidence of a DER on its neighbor's observed frequency, we introduce the notion of external-belief or trust. If the self-belief value of a DER is low, it forms beliefs on its neighboring DER's information (either intact or compromised) and updates its external-belief which depends on the beliefs on each of its neighbors using only local information. Therefore, the DERs can identify the compromised neighbor and discard its information in their control protocol. In the worst-case scenario, a compromised DER always transmits the self-belief value of 1 to its neighbors to deceive them. Based on the external-belief a DER can identify the corrupted neighbors and discards their information.

Using the KL divergence between exchanged information of the *i*-th DER and its neighbor, one can define the $\Upsilon_{ij}(t)$ as

$$\Upsilon_{ij}(t) = \kappa_2 \int_{0}^{t} e^{\kappa_2(\tau - t)}\chi_{ij}(\tau)d\tau , \tag{29}$$

where $0 \le \Upsilon_{ij}(t) \le 1$ and

$$\chi_{ij}(t) = \frac{\Delta_2}{\Delta_2 + D_{KL}(\omega_i \,\|\, m_i)} \quad \forall j \in N_i , \tag{30}$$

with $m_i = (1/\left|N_i\right|)\sum_{j\in N_i}\omega_j$; $\Delta_2 > 0$ represent the threshold to account for the channel fading and other uncertainties; $0 < \kappa_2 < 1$ denotes the discount factor. For the neighboring DER under direct attack, the KL divergence $D_{KL}(\omega_i \,\|\, m_i)$ becomes high which makes $\chi_{ij}(t)$ close to zero. Consequently, this makes the value of $\Upsilon_{ij}(t)$ close to zero. On the other hand, if the incoming information from neighboring DER is intact, then $D_{KL}(\omega_i \,\|\, m_i)$ becomes close to zero which makes $\chi_{ij}(t)$ close to one. Equation (29) can be implemented using the following differential equation

$$\dot{\Upsilon}_{ij}(t) + \kappa_2 \Upsilon_{ij}(t) = \kappa_2 \chi_{ij}(t) . \tag{31}$$

Now, we define the external-belief value of a DER on its neighbors as

$$E^{Bel}_{ij}(t) = \min(I^{Bel}_{i}(t), \Upsilon_{ij}(t)) , \tag{32}$$

with $0 \le E^{Bel}_{ij}(t) \le 1$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

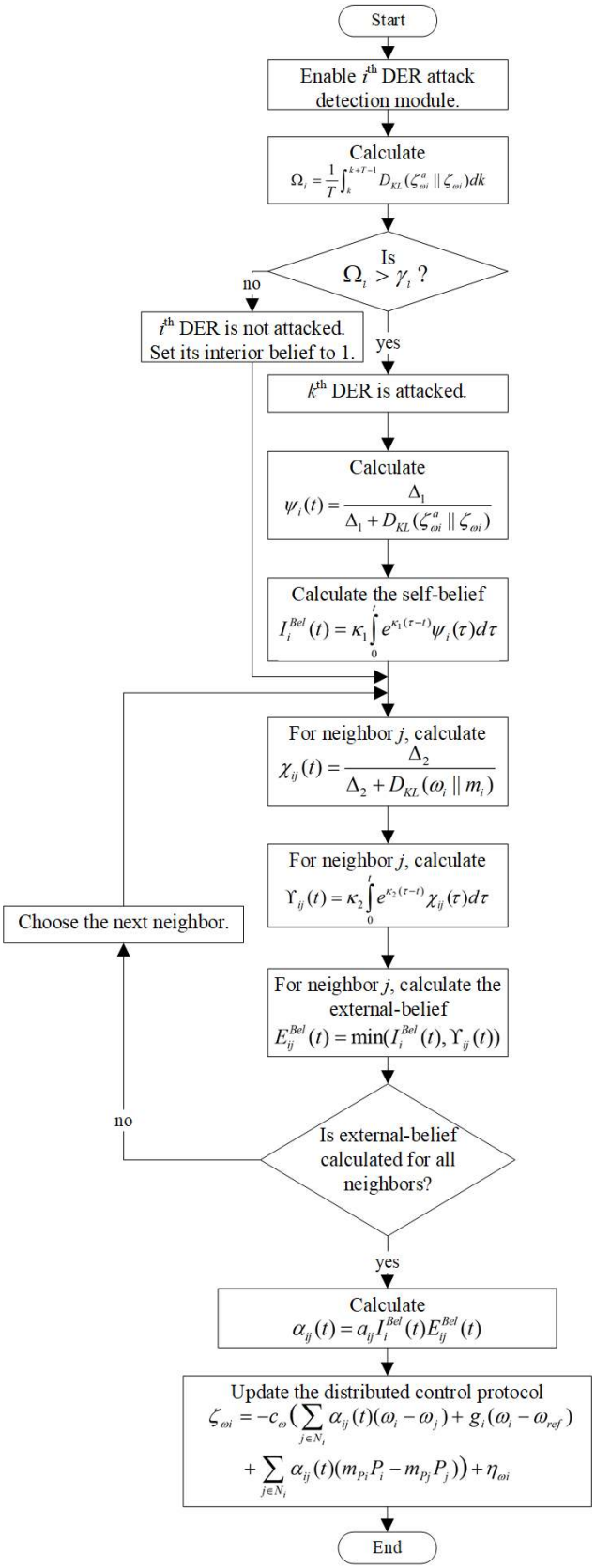


Fig. 2. The flowchart of proposed attack detection and mitigation approach.

Note also that the discount factor in (26) and (29) determines how much we value the current experience with regards to past experiences. It also guarantees that if the attack is not persistent and disappears after a while, or if a short-period adversary rather than attack (such as disturbance or packet dropout) causes, the belief will be recovered, as it mainly depends on the current circumstances.

C. The Mitigation Mechanism Using Self and External-belief values

This subsection presents a resilient or cyber-secure auxiliary control protocol for secondary control of microgrid. We employ the entropy-based self and external-belief values in the mitigation algorithm (See Fig. 2). More specifically, both self and external-belief values in (26) and (32) are incorporated into the frequency based auxiliary control in (10) and the resilient form is presented as

$$\zeta_{\omega i} = -c_\omega\Big(\sum_{j\in N_i} \alpha_{ij}(t)(\omega_i - \omega_j) + g_i(\omega_i - \omega_{ref}) + \sum_{j\in N_i} \alpha_{ij}(t)(m_{Pi}P_i - m_{Pj}P_j)\Big) + \eta_{\omega i}, \quad (33)$$

where

$$\alpha_{ij}(t) = a_{ij} I_i^{Bel}(t) E_{ij}^{Bel}(t) \quad (34)$$

incorporates the self and external-belief discussed in the previous subsection. The following theorem solves Problem 1 using proposed resilient auxiliary control protocol in (33) for intact DERs in the presence of attack.

Assumption 2 (*m-local connectivity).* If at most m neighbors of each intact DER is under attack, at least $(m+1)$ neighbors of each intact DER are intact [41].

Remark 4. Assumption 2 is a common assumption in the distributed control literature [29]-[30], [41]. This assumption provides a minimum requirement for any distributed system to ensure consensus in the presence of attack.

Theorem 2. Consider the resilient DSFC in (33). Let Assumptions 1 and 2 be satisfied. Then, the frequency of the intact DERs synchronizes to the desired nominal frequency in mean square sense, despite the m compromised DERs.

Proof. The resilient frequency based secondary control in (33) can be rewritten as

$$\zeta_{\omega i} = -c_\omega\Big(\sum_{j\in N_i} \alpha_{ij}(t)(\omega_i - \omega_j) + g_i(\omega_i - \omega_{ref}) + \sum_{j\in N_i} \alpha_{ij}(t)(m_{Pi}P_i - m_{Pj}P_j)\Big) + \eta_{\omega i}, \quad (35)$$

where the weight $\alpha_{ij}(t)$ defined in (34) combines the self-belief of agent i and its external belief on agent j. The global form of the (35) becomes

$$\zeta_\omega = -c_\omega((L(t)+G)(\omega - \bar{\omega}_{ref}) + L(t)\bar{P}) + \eta_\omega, \quad (36)$$

where $\omega = [\omega_1, \ldots, \omega_N]^T$, $\omega_{ref} = 1_N \otimes \bar{\omega}_{ref}$, $\eta_\omega = [\eta_{\omega 1}, \ldots, \eta_{\omega N}]^T$, $\bar{P} = [m_{P1}P_1, \ldots, m_{PN}P_N]^T$ and $\zeta_\omega = [\zeta_{\omega 1}, \ldots, \zeta_{\omega N}]^T$. Moreover, $L(t) \in \mathbb{R}^{N\times N}$ and $G \in \mathbb{R}^{N\times N}$ denote the graph Laplacian matrix and the diagonal gain matrix, with diagonal entries equal to the pinning gains g_i, respectively.

According to Assumption 2, the total number of the compromised agents is less than half of the network connectivity, i.e., $2m+1$. Therefore, even if m neighbors of an intact DER are attacked and collude to transmit the same value to mislead the intact DER, there still exists m+1 intact

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

neighbors that transmit the actual values which differ from the compromised ones. Moreover, since m+1 intact DER's neighbors are intact, it can update its external belief and isolate the compromised neighbors. As shown in [41], the resulting graph after isolating the compromised DERs in the entire network remains connected to the intact DERs. Therefore, there exists a spanning tree in the graph associated with all intact DERs. On the other hand, it is shown in [42]-[43], that distributed agents reach mean square consensus in the presence of Gaussian noise if the graph contains spanning tree. Thus, resilient DSFC in (33) intact DERs synchronize to the nominal frequency or the leader's state. This completes the proof. ■

Remark 5. Note that even in the presence of replay attacks where the attacker replicates all the statistical characteristics of previous control signals for the DER, intact DERs lose their trust on the compromised DER's due to the divergence term in in calculating the external-belief in (30) and reject the corrupted information in their control protocol.

Remark 6. Although not considered in this paper, the proposed cyber-secure distributed secondary control can be effectively integrated into the event-triggered based distributed controls (e.g., [20]) to increase the resilience of control system with respect to both FDI and DoS attacks.

VI. Case Studies

A. Case A: Simulation results for IEEE 34-bus feeder

The microgrid test system is illustrated in Fig. 3. The IEEE 34 bus test feeder is utilized as the back bone of microgrid with six DERs integrated to different locations. This microgrid system is simulated in MATLAB/Simulink. The specification of lines is provided in [43]. A balanced feeder model by averaging the line parameters is utilized in the test system. Tables I and II summarize the specifications of the loads and DERs, respectively. The nominal frequency and line-to-line voltage are set to 60 Hz and 24.9 kV, respectively. DERs are connected to the feeder through six Y-Y, 480 V/24.9 kV, 400 kVA transformers with the series impedance of 0.03 + j 0.12 pu. The communication graph of distributed secondary control system is depicted in Fig. 4. Only DER 1 knows the frequency and voltage reference values with the pinning gain $g_1 = 1$. The control gains c_ω and c_v in (6) and (7) are set to 40. We assume zero-mean Gaussian communication noise with following statistical properties $\mathcal{N}(0, 0.01)$. Two different cases are considered to evaluate the presented results for attack detection and mitigation in the distributed secondary control of microgrids. *Case A.1* analyzes the results for DSFC and *Case A.2* presents the results for DSVC in the presence of attacks in the microgrid.

Case A.1.1 (effect of attack on the conventional DSFC): In this case, we consider the attack on DER 6 based on (12). *A*t $t = 0$, the microgrid is islanded from the main grid. From $t = 0$ to $t = 0.6$ s only the primary control is applied. The primary control takes action to provide frequency stability in the islanded

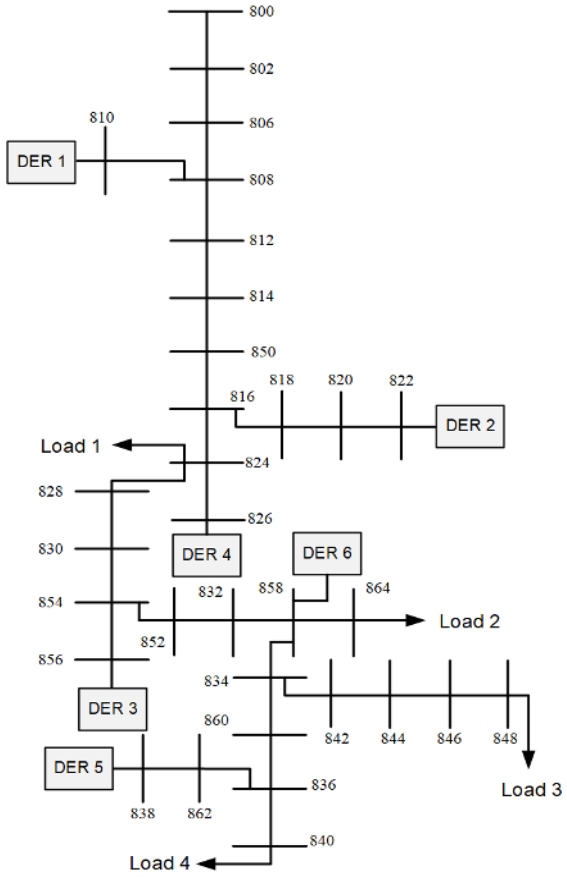


Fig. 3. Single line diagram of the microgrid test system in Case A.

TABLE I. Specification of Loads in Case A

Load 1		Load 2		Load 3		Load 4	
R	***X***	***R***	***X***	***R***	***X***	***R***	***X***
1.5 Ω	1 Ω	0.5 Ω	0.5 Ω	1 Ω	1 Ω	0.8 Ω	0.8 Ω

TABLE II. Specification of DERs in Case A

DER	1, 2, 5, 6	3, 4
m_P	5.64×10^{-5}	7.5×10^{-5}
n_Q	5.2×10^{-4}	6×10^{-4}
R_c	0.03 Ω	0.03 Ω
L_c	0.35 mH	0.35 mH
R_f	0.1 Ω	0.1 Ω
L_f	1.35 mH	1.35 mH
C_f	50 µF	50 µF
K_{PV}	0.1	0.05
K_{IV}	420	390
K_{PC}	15	10.5
K_{IC}	20000	16000

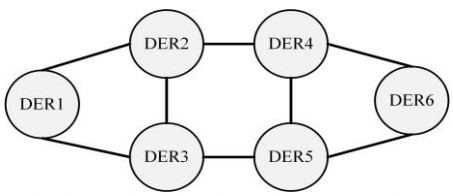


Fig. 4. Communication graph of the microgrid test system in Case A.

Case A.1.1 (effect of attack on the conventional DSFC): In this case, we consider the attack on DER 6 based on (12). *A*t $t = 0$, the microgrid is islanded from the main grid. From $t = 0$ to $t = 0.6$ s only the primary control is applied. The primary control takes action to provide frequency stability in the islanded

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

microgrid. However, the primary control only maintains frequency in stable ranges and cannot maintain frequency at exactly 60 Hz. Then, the secondary distributed frequency control is applied at $t = 0.6$ s to restore the microgrid frequency to 60 Hz. However, the attacker hijacks the DSFC of DER 6 and replaces the actual frequency with 60.2 Hz. Fig. 5(a) and Fig. 5(b) show that the conventional DSFC protocol leads to the loss of desired consensus. The frequency of each DER deviates from the desired frequency of 60 Hz and shows oscillatory behavior. In the presence of attack, the behavior of the compromised DER 6 is directly affected by the attack signal and its corrupted frequency is observed by reachable intact DERs which are affected by it and they also show oscillatory behaviors as shown in Fig. 5(a). Fig. 6 clearly shows that the relative entropy of compromised and reachable DERs diverge and go beyond the predefined design threshold which is assumed to be $\gamma_i = 5 \quad \forall i$ in the presence of attack. The relative entropy of compromised DER is relatively much higher than the intact DERs and designed detector can easily detect the effect of attack.

Case A.1.2 (*attack detection and mitigation*): Similar to *Case A.1.1*, at $t = 0$, the microgrid is islanded from the main grid. From $t = 0$ to $t = 0.6$ s only primary control is applied. Then, the secondary distributed frequency control is applied at $t = 0.6$ s to restore the microgrid frequency to 60 Hz. However, the attacker hijacks the DSFC of DER 6 and replaces the actual frequency with 60.2 Hz at $t = 0.6$ s and then, the designed attack detection and mitigation mechanism is applied at $t = 0.7$ s. As shown in Fig. 7(a) and Fig. 7(b), frequency of intact DERs restores to 60 Hz after applying the attack mitigation mechanism at $t = 0.7$ s. Active power of all DERs are also retrieved back as in intact mode. After applying the resilient DSFC in (33), intact DERs discard the frequency value received from corrupted DER and the mean and variance of their local frequency neighborhood tracking error distribution remain close to the normal case. Therefore, based on (22), the relative entropy for intact DERs remains close to zero but it keeps growing for the compromised DER 6 due to deviation in mean and variance of the corrupted frequency signal from the nominal one as shown in Fig. 8(a). According to (26)-(27), self-belief of a DER depends on its relative entropy and one can see in Fig. 8(b) that self-belief for all DERs becomes one except for the compromised DER 6, which indicates that all the DERs are confident about their frequencies, except for the compromised one. The self-belief of a DER measures the level of trustworthiness about its observed frequency, which is updated in each iteration and recursively used in resilient DSFC in (33) for mitigation of the attack. Based on the presented resilient DSFC, intact DERs do not incorporate the corrupted frequency from DER 6 and achieve the desired synchronization as shown in Fig. 7(a).

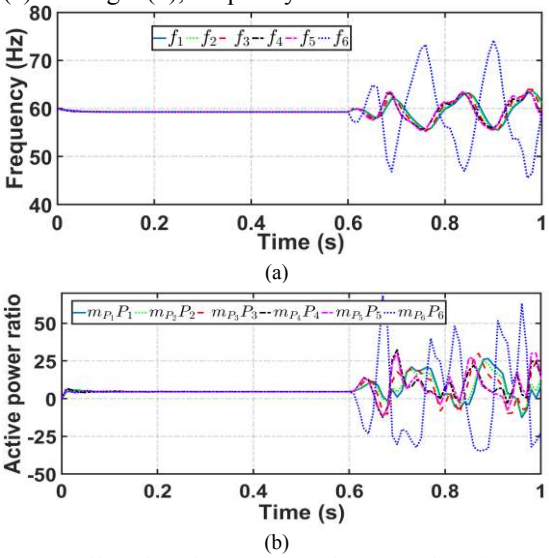


Fig. 5. Case A: Effect of attack on DSFC: (a) frequency; (b) active power ratio.

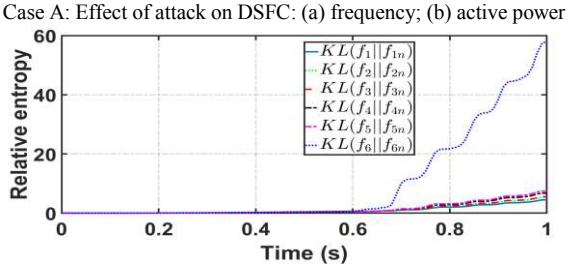


Fig. 6. Case A: Relative entropy based on frequency of DERs.

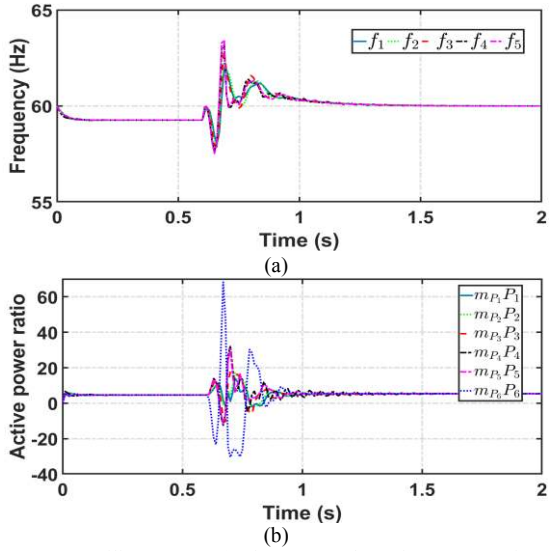


Fig. 7. Case A: Resilient DSFC: (a) frequency; (b) active power ratio.

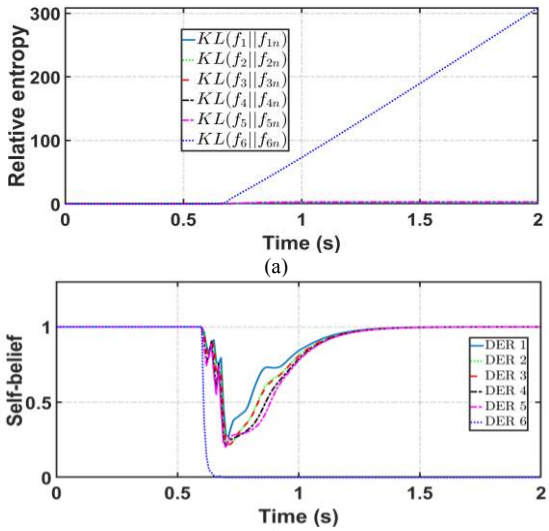
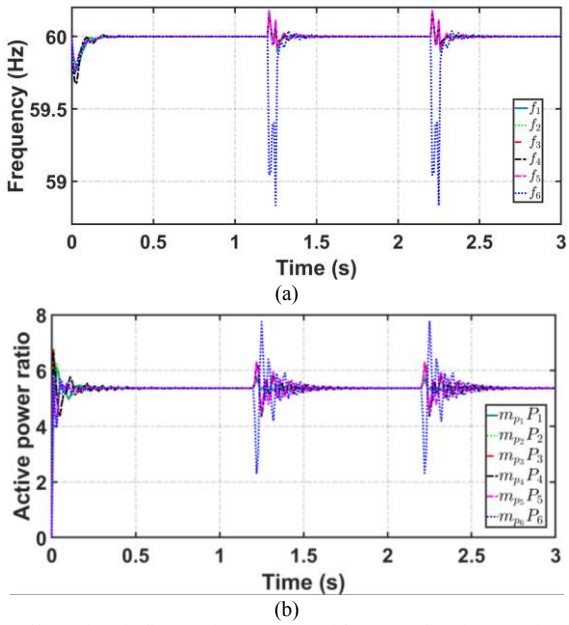


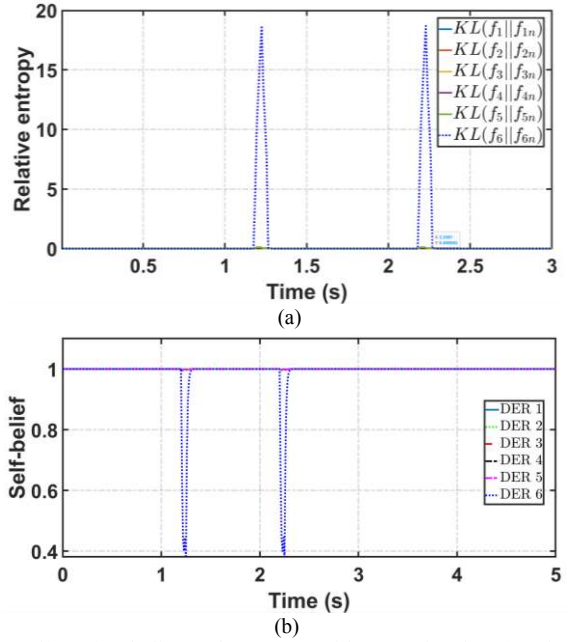
Fig. 8. Case A: Resilient DSFC: (a) relative entropy; (b) self-believes of DERs.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid



(a) (b)

Fig. 9. Effect of periodic attack on DSFC with 0.05 s duration: (a) frequency; (b) active power ratio.



(a) (b)

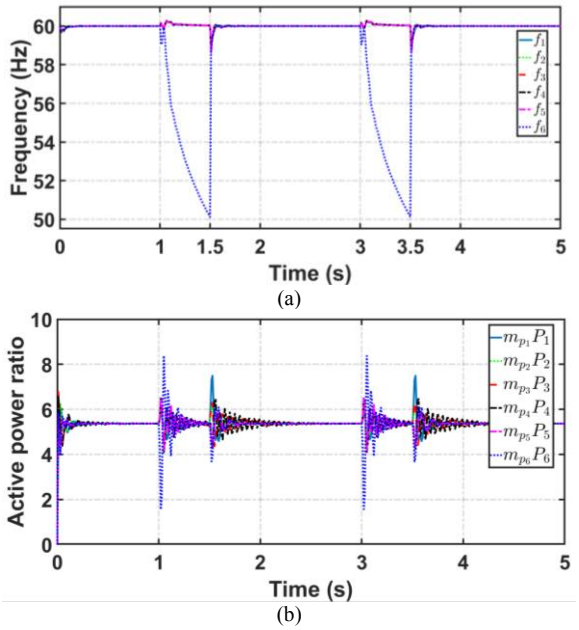
Fig. 10. Effect of periodic attack on DSFC with 0.05 s duration: (a) relative entropy; (b) self-believes of DERs.

Case A.1.3 (*attack detection and mitigation for periodic adversaries*): In this subsection, the effectiveness of the presented attack detection and mitigation algorithm is validated for periodic attacks. The secondary distributed frequency control is applied at t = 0 s which synchronizes the frequency of the microgrid to 60 Hz. Then, the attacker hijacks the DSFC of DER 6 and replaces the actual frequency with 60.2 Hz at t = 1.2 s and t = 2.2 s. In the following, the simulation results are provided for two different attack durations. First, it is assumed that when the attack is applied at t = 1.2 s and t = 2.2 s, it is only effective for 0.05 s. Fig. 9 shows the DER frequencies and active power ratios. As seen in Fig. 9, due to the short duration of attack, its impact is minimal; DER frequencies slightly deviate from 60 Hz.

Based on (22), the relative entropy for intact DERs remains close to zero, but it keeps growing for the compromised DER 6 when the attack is effective due to deviation in mean and variance of the corrupted frequency signal from the nominal one as shown in Fig. 10(a). According to (26)-(27), the self-belief of a DER depends on its relative entropy; one can see in Fig. 10(b) that self-belief values during the attack period are one for all DERs except for the compromised DER 6, which indicates that all the DERs are confident about their exchanged frequencies, except for the compromised one. As expected, for the time interval that the attacker turns off its attack signal, DER frequencies and active power ratios are restored to their intact values before the attack is applied.

In the second simulation scenario, it is assumed that when the attack is applied at t = 1 s and t = 3 s, it is effective for 0.5 s. Fig. 11 shows the DER frequencies and active power ratios. As seen in Fig. 11, after the attack is applied, DER frequencies deviate from 60 Hz and active power ratios experience noticeable oscillations. The relative entropy for intact DERs remains close to zero, but it keeps growing for the compromised DER 6 during durations of attack as shown in Fig. 12(a). As seen in Fig. 12(b), self-belief during attack periods becomes one for all DERs except for the compromised DER 6. The attack mitigation scheme restores DER frequencies to 60 Hz and active power ratios to a common value. For the time interval that the attacker turns off its attack signal, DER frequencies and active power ratios are restored to their intact values before the attack is applied.

Case A.2.1 (*effect of attack on the conventional DSVC*): In this case, we consider the attack on DER 6 based on (12). From t = 0 to t = 0.65 s only primary control is applied and then the attacker hijacks the DSVC of DER 6 and replaces the actual voltage with 482 V at t = 0.65 s. In the presence of attack, the conventional DSVC leads to the loss of desired consensus as



(a) (b)

Fig. 11. Effect of periodic attack on DSFC with 0.5 s duration: (a) frequency; (b) active power ratio.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

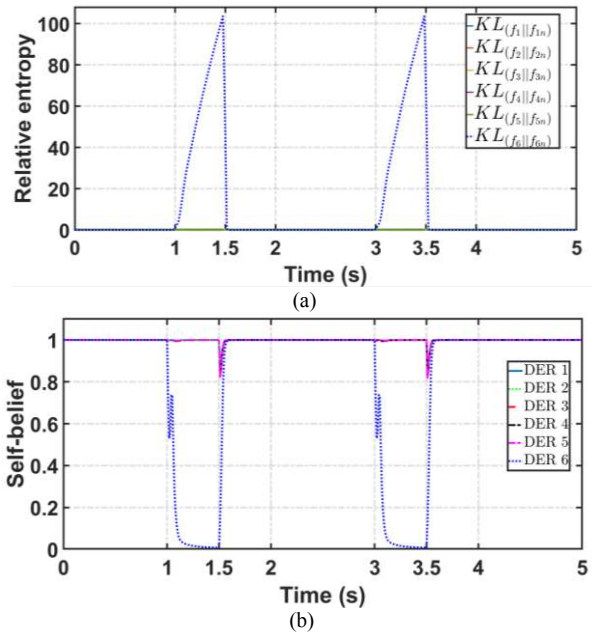


Fig. 12. Effect of periodic attack on DSFC with 0.5 s duration: (a) relative entropy; (b) self-believes of DERs.

shown in Fig. 13(a) and Fig. 13(b). Voltage and reactive power ratio for each DER deviate from the desired consensus and show oscillatory response. The corrupted voltage magnitude of DER 6 is directly observed by reachable intact DERs which are affected by it. The reachable neighboring DERs also show oscillatory behaviors in their operating voltage and reactive power as shown in Fig. 13(a). This makes the relative entropy of compromised and reachable DERs diverge and go beyond the predefined design threshold of $\gamma_i = 5 \quad \forall i$ in the presence of attack as shown in Fig. 14.

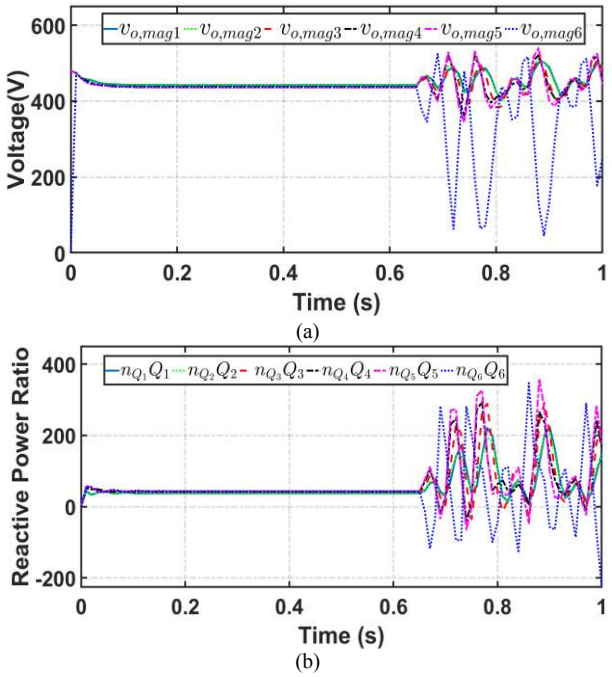


Fig. 13. Case A: Effect of attack on DER 2 in DSVC: (a) voltage (V): (b) reactive power ratio.

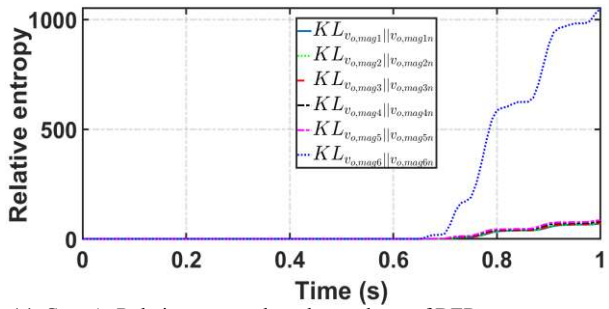


Fig. 14. Case A: Relative entropy based on voltage of DERs.

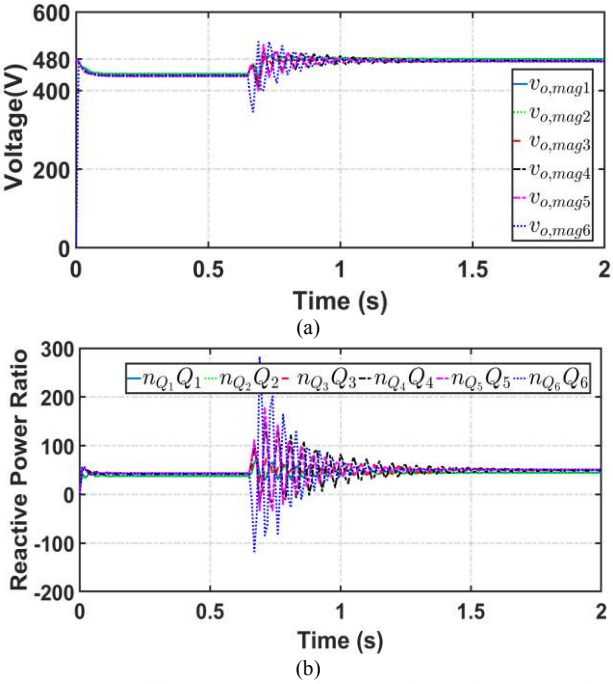


Fig. 15. Case A: Resilient DSVC: (a) voltage (V); (b) reactive power ratio.

Case A.2.2 (attack detection and mitigation on DSVC): In this case, we consider the attack on DER 6. From $t = 0$ to $t = 0.65$ s only primary control is applied and then the attacker hijacks the DSVC of DER 6 and replaces the actual voltage with 482 V at $t = 0.65$ s. As shown in Fig. 15(a) and Fig. 15(b), voltage of all DERs except the hijacked one synchronize to 480 V after applying the mitigation mechanism at $t = 0.7$ s. The reactive power of DERs are also shared based on their ratings. Fig. 16(a) shows that the relative entropy for intact DERs remains close to zero, but it keeps growing for the compromised DER 6 due to deviation of the corrupted voltage from the nominal one, and, consequently, as shown in Fig. 16(b), self-belief for all DERs becomes one except for the compromised DER 6.

B. *Case B: Simulation results for an Islanded Microgrid with 20 DERs*

Case B verifies the validity of proposed control techniques on a 60 Hz and 480 V microgrid test system with 20 DERs. The single-line diagram of this microgrid test system is illustrated in Fig. 17. This test system is simulated in MATLAB/Simulink. The specifications of DERs are listed in Table III. Lines and loads specifications are shown in Tables IV. The communication network graph is depicted in Fig. 18. The frequency reference value is shared with DER1 with the pinning

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

gain $g_1 = 1$. ω_{ref} is set to 2π×60 rad/s. The control gains c_ω is set to 40. We assume zero-mean Gaussian communication noise with following statistical properties $\mathcal{N}(0, 0.01)$. This system is used to validate the proposed attack detection and mitigation schemes considering the DSFC.

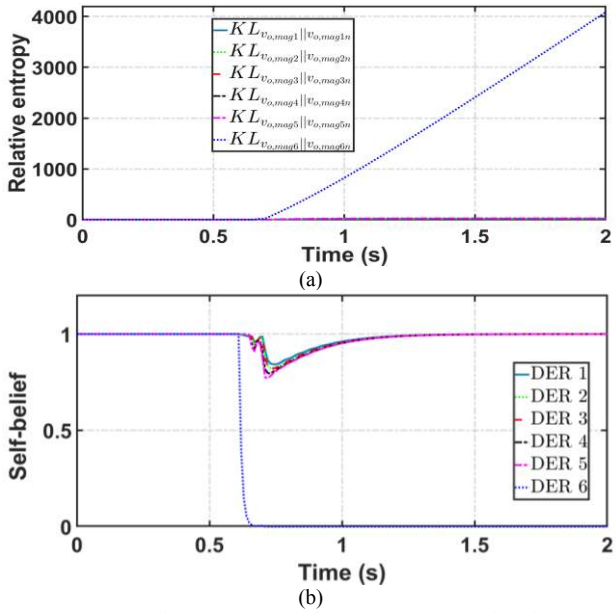


Fig. 16. Case A: Resilient DSVC: (a) relative entropy; (b) self-belief of DERs.

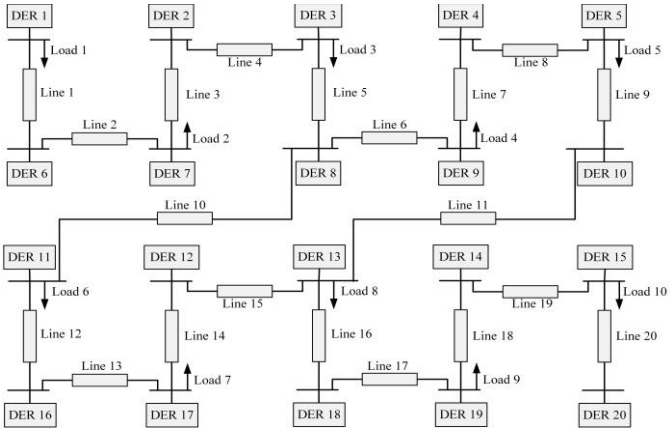


Fig. 17. Microgrid testbed with 20 DERs.

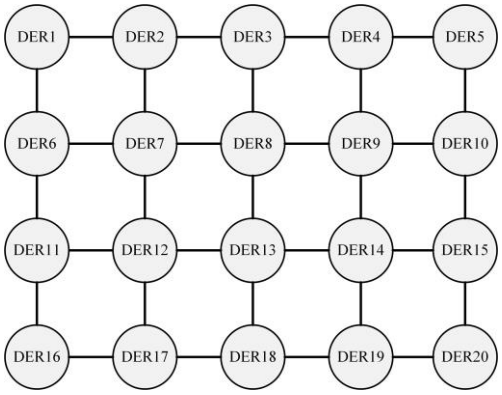


Fig. 18. Communication graph of the microgrid testbed in Case B.

TABLE III. SPECIFICATION OF DERS IN CASE B

DER 1, 2, 3, 4, 5, 11, 12, 13, 14, and 15		DER 6, 7, 8, 9, 10, 16, 17, 18, 19 and 20	
m_P	9.4×10^{-5}	m_P	12.5×10^{-5}
n_Q	1.3×10^{-3}	n_Q	1.5×10^{-3}
R_c	30 mΩ	R_c	30 mΩ
L_c	350 μH	L_c	350 μH
R_f	100 mΩ	R_f	100 mΩ
L_f	1350 μH	L_f	1350 μH
C_f	50 μF	C_f	50 μF
K_{PV}	0.1	K_{PV}	0.05
K_{IV}	420	K_{IV}	390
K_{PC}	15	K_{PC}	10.5
K_{IC}	20000	K_{IC}	16000

TABLE IV. SPECIFICATION OF LINES AND LOADS IN CASE B

Line 1, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 18, 19		Line 2, 5, 8, 11, 14, 17, 20	
R	0.23 Ω	R	0.35 Ω
X	0.1 Ω	X	0.58 Ω
Load 1, 3, 5, 6, 9		Load 2, 4, 6, 8, 10	
R	2 Ω	R	2 Ω
X	1 Ω	X	0.5 Ω

Case B.1 (effect of attack on the conventional DSFC): We consider the attack on DER 20. At t = 0, the microgrid is islanded from the main grid. From t = 0 to t = 0.7 s only primary control is applied. The primary control takes action to provide frequency stability in the islanded microgrid. However, primary control only maintains frequency in stable ranges and cannot maintain frequency at exactly 60 Hz. Then, the secondary distributed frequency control is applied at t = 0.7 s to restore microgrid frequency to 60 Hz. However, the attacker hijacks the DSFC of DER 20 and replaces the actual frequency with 60.2 Hz. Fig. 19(a) and Fig. 19(b) show that the conventional DSFC protocol leads to the loss of the desired consensus. The frequency of each DER deviates from the desired frequency of 60 Hz and shows oscillatory behavior. In the presence of attack, the behavior of the compromised DER 20 is directly affected by the attack signal and its corrupted frequency is shared with neighboring DERs. This causes an oscillatory behavior in the neighboring DERs as shown in Fig. 19(a). Fig. 20 shows that the relative entropy of compromised and neighboring DERs diverge due to deviation in their behavior from the nominal one and go beyond predefined design threshold which is assumed to be $\gamma_i = 5 \quad \forall i$.

Case B.2 (attack detection and mitigation): Similar to *Case B.1*, at t = 0, the microgrid is islanded from the main grid. From t = 0 to t = 0.7 s only primary control is applied. Then, the secondary distributed frequency control is applied at t = 0.7 s. The attacker hijacks the DSFC of DER 20 and replaces the actual frequency with 60.2 Hz at t = 0.7 s and then, the designed attack detection and mitigation mechanism is applied at t = 0.75 s. As shown in Fig. 21(a) and Fig. 21(b), frequency of intact DERs restores to 60 Hz after applying the attack mitigation mechanism at t = 0.75 s. Active power of all DERs are also retrieved back as in intact mode. After applying resilient DSFC, intact DERs discard locally observed frequency of corrupted

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

DER. Therefore, the relative entropy for intact DERs remains close to zero but it keeps growing for the compromised DER 20 as shown in Fig. 22(a). Fig. 22(b) shows that self-belief for all DERs becomes one except the compromised DER 20.

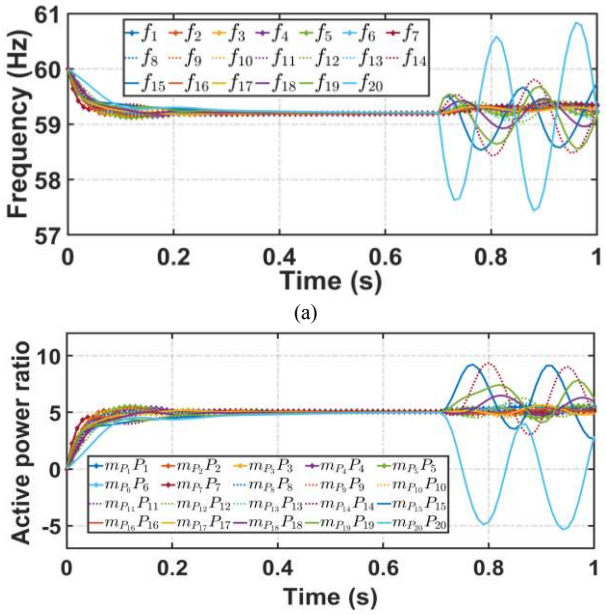


Fig. 19. Case B: Effect of attack on DSFC: (a) frequency; (b) active power ratio.

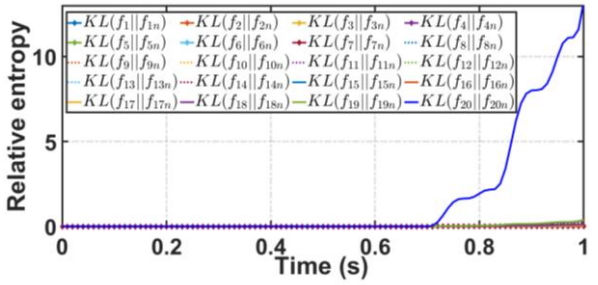


Fig. 20. Case B: Relative entropy based on frequency of DERs.

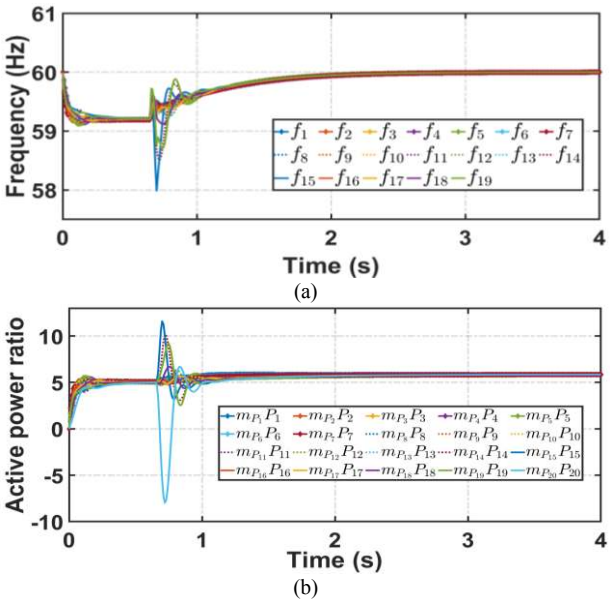


Fig. 21. Case B: Resilient DSFC: (a) frequency; (b) active power ratio.

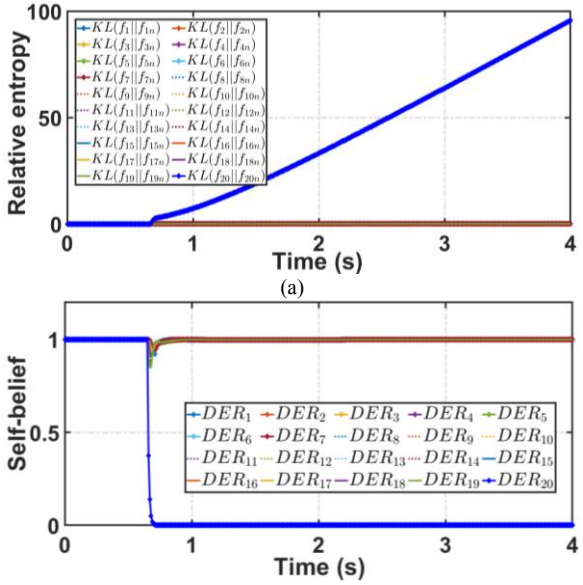


Fig. 22. Case B: Resilient DSFC: (a) relative entropy; (b) self-belief of DERs.

C. Case C: Experimental verification of proposed techniques using a hardware-in-the-loop testing setup

To experimentally validate the performance of proposed attack detection and mitigation techniques, a hardware-in-the-loop (HIL) laboratory testbed is developed using Opal-RT as a real-time digital simulator and Raspberry Pi modules. A microgrid testbed including four DERs is simulated in Opal-RT. The microgrid single line diagram is shown in . The specifications of DERs, loads, and lines are summarized in Table V. It is assumed that DERs communicate to each other through the communication graph network in Fig. 23. The nominal operating voltage and frequency of the microgrid test system are 480 V and 60 Hz, respectively. The frequency reference value is shared with DER1 with the pinning gain $g_1 = 1$. ω_{ref} is set to $2\pi\times60$ rad/s. The control gains c_ω is set to 40. We assume zero-mean Gaussian communication noise with following statistical properties $\mathcal{N}(0, 0.01)$.

As seen in Fig. 23, four Raspberry Pi modules are utilized in the HIL testing. Each Raspberry Pi module hosts the cyber-secure DSFC protocol for a DER. Raspberry Pi modules communicate to each other through a distributed communication network. The HIL setup, including Opal-RT, Raspberry Pi modules, Gigabit ethernet switch, and host computer, is shown in Fig. 24. The microgrid electric circuit, including DERs, loads, lines, and primary controllers, are modelled in RT-LAB. The DER local measurements including the voltage, frequency, and active/reactive power measurements are sent to the corresponding Raspberry Pi module through User Datagram Protocol (UDP). Each Raspberry Pi module runs three processes in parallel. These processes include receiving real-time DER measurements and sending secondary control references to DERs, communicating to the neighboring DER Raspberry Pi modules, and running the secondary control protocol and attack detection and mitigation techniques.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

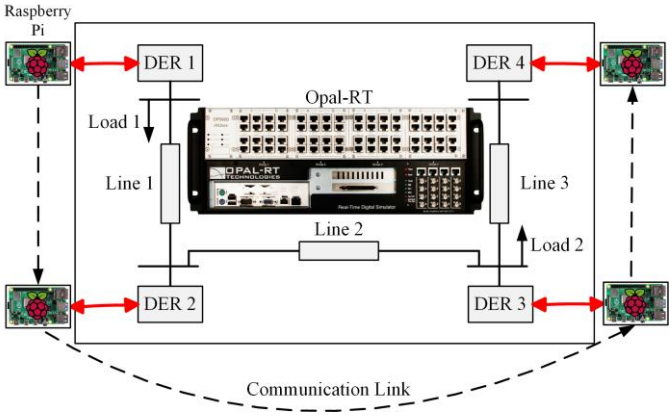


Fig. 23. Microgrid test system for HIL testing.

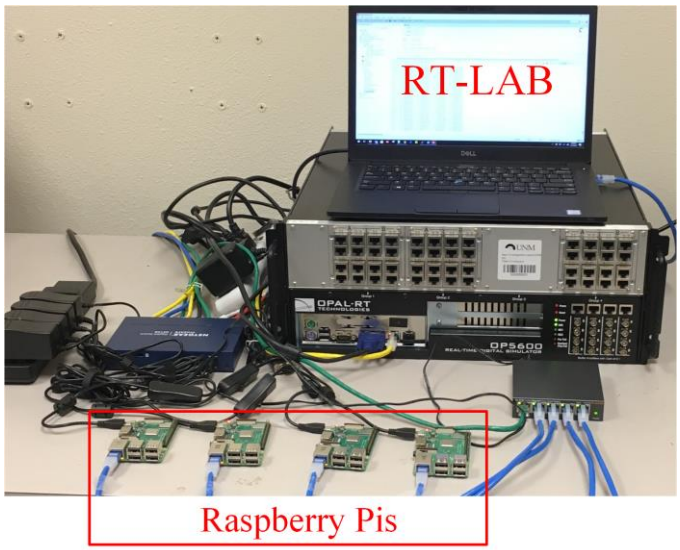


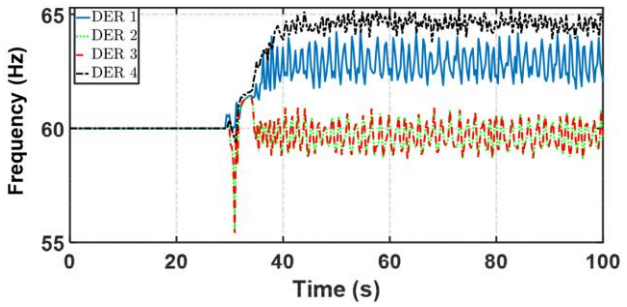
Fig. 24. HIL Setup.

Case C.1 (effect of attack on the conventional DSFC): We consider the attack on DER 2. At $t = 0$, the microgrid is islanded from the main grid. From $t = 0$ to $t = 30$ s only primary control is applied. Then, the secondary distributed frequency control is applied at $t = 30$ s to restore microgrid frequency to 60 Hz. However, the attacker hijacks the DSFC of DER 2 and replaces the actual frequency with 66 Hz. Fig. 25(a) and Fig. 25(b) show that the conventional DSFC protocol leads to the loss of the desired consensus. The frequency of each DER deviates from the desired frequency of 60 Hz and shows oscillatory behavior. In the presence of attack, the behavior of the compromised DER 2 is directly affected by the attack signal and its corrupted frequency is shared with neighboring DERs. This causes an oscillatory behavior in the neighboring DERs. Fig. 26 shows that the relative entropy of compromised and neighboring DERs diverge due to deviation in their behavior from the nominal one.

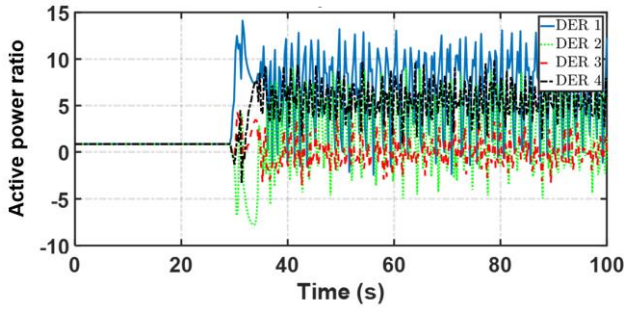
Case C.2 (attack detection and mitigation): At $t = 0$, the microgrid is islanded from the main grid. From $t = 0$ to $t = 30$ s only primary control is applied. Then, the secondary distributed frequency control is applied at t = 30 s. The attacker hijacks the DSFC of DER 2 and replaces the actual frequency with 66 Hz at $t = 30$ s and then, the designed attack detection and mitigation mechanism is applied at the same time. As shown in Fig. 27(a) and Fig. 27(b), frequency of intact DERs restores to 60 Hz after applying the attack mitigation mechanism. Active power of all DERs are also retrieved back as in intact mode.

TABLE V
SPECIFICATIONS OF THE MICROGRID TEST SYSTEM

DGs	DG 1 & 2				DG 3 & 4	
	m_P	4×10^{-5}			m_P	6×10^{-5}
	n_Q	1.3×10^{-3}			n_Q	1.5×10^{-3}
	R_c	0.03 Ω			R_c	0.03 Ω
	L_c	0.35 mH			L_c	0.35 mH
	R_f	0.1 Ω			R_f	0.1 Ω
	L_f	1.35 mH			L_f	1.35 mH
	C_f	50 µF			C_f	50 µF
	K_{PV}	0.1			K_{PV}	0.05
	K_{IV}	420			K_{IV}	390
	K_{PC}	15			K_{PC}	10.5
	K_{IC}	20000			K_{IC}	16000
Lines	Line 1		Line 2		Line 3	
	R_{l1}	0.23 Ω	R_{l2}	0.35 Ω	R_{l3}	0.23 Ω
	L_{l1}	318 µH	L_{l2}	1847 µH	L_{l3}	318 µH
Loads	Load 1			Load 2		
	P_{L1} (per phase)	12 kW		P_{L2} (per phase)	15.3 kW	
	Q_{L1} (per phase)	12 kVAr		Q_{L2} (per phase)	7.6 kVAr	



(a)



(b)

Fig. 25. Case C: Effect of attack on DSFC: (a) frequency; (b) active power ratio.

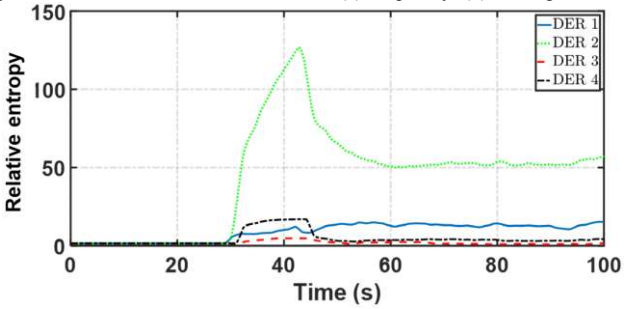


Fig. 26. Case C: Relative entropy based on frequency of DERs.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2019.2958014, IEEE Transactions on Smart Grid

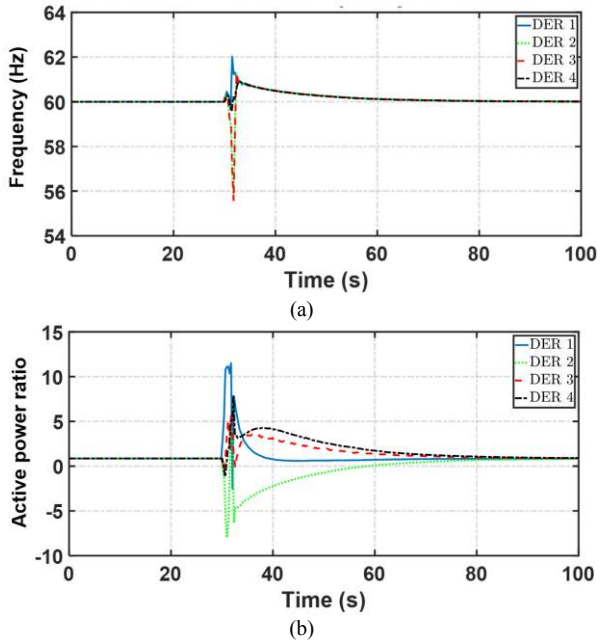


Fig. 27. Case C: Resilient DSFC: (a) frequency; (b) active power ratio.

VII. Conclusion

This paper addresses the effects of data manipulation attacks on distributed secondary frequency and voltage control in AC microgrids. An information-theoretic approach is employed for design of detection and mitigation mechanism. Each DER detects the misbehavior of its neighbors on the distributed communication network and, consequently, calculates a belief related to the trustworthiness of the received information. It is shown that using the proposed cyber-secure approach, a DER can distinguish data manipulation attacks from legitimate events and only discards the information received from a neighbor if it is compromised. The proposed approach is ensured to work under a mild communication graph connectivity.

References

[1] D. T. Ton and M. A. Smith, "The U.S. Department of Energy's Microgrid Initiative", *Elseiveir, The Electricity Journal,* vol. 25, pp. 84-94, Oct. 2012.

[2] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Trans. Smart Grid,* vol. 3, pp. 1963-1976, Dec. 2012.

[3] Z. Li, C. Zang, P. Zeng, H. Yu, and S. Li, "Fully distributed hierarchical control of parallel grid-supporting inverters in islanded AC microgrids," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 679-690, Feb. 2018.

[4] J. Schiffer, T. Seel, J. Raisch, and T. Sezi, "Voltage stability and reactive power sharing in inverter-based microgrids with consensus based distributed voltage control," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 1, pp. 96-109, Jan. 2016.

[5] M.Yazdanian and A. Mehrizi-Sani, "Distributed control techniques in microgrids," *IEEE Trans. Smart Grid,* vol. 5, no. 6, pp. 2901-2909, Nov. 2014.

[6] A. Bidram, A. Davoudi, F. L. Lewis, and J. M. Guerrero, "Distributed cooperative control of microgrids using feedback linearization," *IEEE Trans. Power Syst.,* vol. 28, no. 3, pp. 3462-3470, Aug. 2013.

[7] A. Bidram, F. L. Lewis, and A. Davoudi, "Distributed control systems for small-scale power networks: Using multiagent cooperative control theory," *IEEE Control Systems Magazine,* vol. 34, no. 6, pp. 56-77, Nov. 2014.

[8] J. Duan, C. Wang, H. Xu, W. Liu, J. C. Peng, and H. Jiang, "Distributed control of inverter-interfaced microgrids with bounded transient line currents," *IEEE Trans. Ind. Informat.,* vol. 14, no. 5, pp. 2052-2061, May 2018.

[9] San Diego Gas & Electric Company, "Smart grid architecutre demonstrations program – EPIC-1, Project 1 report," Electric Power Investment Charge (EPIC), Dec. 2017.

[10] A. Bidram, A. Davoudi, and F. L. Lewis, "A Multiobjective distributed control framework for islanded AC microgrids," *IEEE Trans. Ind. Informat.,* vol. 10, no. 3, pp. 1785-1798, May 2014.

[11] A. Bidram, A. Davoudi, F. L. Lewis, and Z. Qu, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Generation, Transmission, & Distribution,* vol. 7, no. 8, pp. 822-831, Aug. 2013.

[12] N. M. Dehkordi, H. R. Baghaee, N. Sadati and J. M. Guerrero, "Distributed noise-resilient secondary voltage and frequency control for islanded microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3780-3790, July 2019.

[13] J. Duan, C. Wang, H. Xu, W. Liu, Y. Xu, J. C. Peng, and H. Jiang, "Distributed control of inverter-interfaced microgrids based on consensus algorithm with improved transient performance," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1303-1312, Mar. 2019.

[14] D. Jin, Z. Li, C. Hannon, C. Chen, J. Wang, M. Shahidehpour, and C. W. Lee, "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Trans. Smart Grid,* vol. 8, no. 5, pp. 2494-2504, Sept. 2017.

[15] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239-2248, Sept. 2017.

[16] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. 44th Annu. Conf. Inf. Sci. Syst. (CISS)*, 2010, pp. 1-6.

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

[18] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.

[19] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702-4711, Sept. 2018.

[20] W. Meng, X. Wang and S. Liu, "Distributed load sharing of an inverter-based microgrid with reduced communication," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1354-1364, Mar. 2018.

[21] B. Schafer, D. Witthaut, M. Timme, and V. Latora, "Dynamically induced cascading failures in power grids" *Nature Communications*, vol. 9, Article Number 1975, pp. 1-13, 2018.

[22] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Realtime detection of false data injection in smart grid networks: An adaptive cusum method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532-543, June 2016.

[23] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370-379, Dec. 2014.

[24] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216-1227, May 2014.

[25] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396-1407, July 2014.

[26] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612-621, Mar. 2014.

[27] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[28] X. Wang, X. Luo, Y. Zhang, and X. Guan, "Detection and isolation of false data injection attacks in smart grids via nonlinear internal observer," vol. 6, no. 4, pp. 6498–6512, Aug. 2019.

[29] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90-104, Jan. 2012.

[30] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715-2729, Nov. 2013.

[31] L. Y. Lu, H. J. Liu, and H. Zhu, "Distributed secondary control for isolated microgrids under malicious attacks," in *Proc. North American Power Symposium (NAPS)*, Denver, CO, USA, 2016, pp. 1-6.

[32] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693-2703, Oct. 2017.

[33] S. Saha, T. K. Roy, M. A. Mahmud, M. E. Haque, S. N. Islam, "Sensor fault and cyber attack resilient operation of DC microgrids," *Int. J. Electr. Power Energy Syst*. vol. 99, pp. 540-554, 2018.

[34] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of DC microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 1083-1085, Jan. 2019.

[35] T. R. B. Kushal, K. Lai, and M. S. Illindala, "Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system," *IEEE Trans. Smart Grid,* vol. 10, no. 5, pp. 4741-4750, Sept. 2019.

[36] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid,* vol. 9, no. 6, pp. 6731-6741, Nov. 2018.

[37] Z. Qu, *Cooperative control of dynamical systems: Applications to autonomous vehicles*. New York: Springer-Verlag, 2009.

[38] M. Zhou, Y. Wang, A. K. Srivastava, Y. Wu, and P. Banerjee, "Ensemble-based algorithm for synchrophasor data anomaly detection," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2979-2988, May 2019.

[39] M. Basseville, and I. V. Nikiforov, *Detection of Abrupt Changes: Theory and Application*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.

[40] S. Kullback, and R. A. Leibler, "On information and sufficiency", *The annals of mathematical statistics*, vol. 22, no. 1, pp.79-86, 1951.

[41] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun*., vol. 31, no. 4, pp. 766–781, 2013.

[42] F. Sun, Z. H. Guan, L. Ding, and Y.W. Wang, "Mean square average-consensus for multi-agent systems with measurement noise and time delay," *International Journal of System and Science*, vol. 44, no. 6, pp. 995-1005, 2013.

[43] T. Li, and J. F. Zhang, "Consensus conditions of multi-agent systems with time-varying topologies and stochastic communication noises," *IEEE Trans. Autom. Control,* vol. 55, no. 9, pp. 2043-2057, 2010.

[44] N. Mwakabuta and A. Sekar, "Comparative study of the IEEE 34 node test feeder under practical simplifications," in *Proc. 39th North American Power Symposium*, 2007, pp. 484-491.

Aquib Mustafa (S'17) received the B. Tech. degree from the AMU, Aligarh, India, in 2013, and the Master's degree from the Indian Institute of Technology Kanpur, Kanpur, India, in 2016. He is currently pursuing the Ph.D. degree in the Department of Mechanical Engineering, Michigan State University, East Lansing, USA. His primary research interests include resilient control, multi-agent systems, and sensor networks.

Binod Poudel (S'13) received the B.E. degree from the Institute of Engineering, Tribhuvan University, Nepal, the M.S. degree in electrical engineering from the South Dakota State University, Brookings, SD, USA, in 2009 and 2014, respectively. He is currently pursuing PhD degree in electrical engineering from University of New Mexico. His research interests include microgrid, cyber security of power system, voltage control, power system protection.

Ali Bidram (S'12-M'17) is currently an Assistant Professor in the Electrical and Computer Engineering Department, University of New Mexico, Albuquerque, NM, USA. He has received his B.Sc. and M.Sc. from Isfahan University of Technology, Iran, in 2008 and 2010, and Ph.D. from the University of Texas at Arlington, USA, in 2014. Before joining University of New Mexico, he worked with Quanta Technology, LLC, and was involved in a wide range of projects in electric power industry. He is an Associate Editor for the IEEE Transactions on Industry Applications. His area of expertise lies within control and coordination of energy assets in power electronics-intensive energy distribution grids. Such research efforts are culminated in a book, several journal papers in top publication venues and articles in peer-reviewed conference proceedings, and technical reports.

Hamidreza Modares (M'15, SM'18) received the B.Sc. degree from Tehran University, Tehran, Iran, in 2004, the M.Sc. degree from the Shahrood University of Technology, Shahrood, Iran, in 2006, and the Ph.D. degree from the University of Texas at Arlington (UTA), Arlington, TX, USA, in 2015. From 2006 to 2009, he was with the Shahrood University of Technology as a Senior Lecturer. From 2015 to 2016, he was a Faculty Research Associate with UTA. From 2016 to 2018, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, USA.

He is currently an Assistant Professor with the Department of Mechanical Engineering, Michigan State University, East Lansing, USA. He has authored several journal and conference papers on the design of optimal controllers using reinforcement learning. His current research interests include cyber-physical systems, machine learning, distributed control, robotics, and renewable energy microgrids.

Dr. Modares was a recipient of the Best Paper Award from the 2015 IEEE International Symposium on Resilient Control Systems, the Stelmakh Outstanding Student Research Award from the Department of Electrical Engineering, UTA, in 2015, and the Summer Dissertation Fellowship from UTA, in 2015. He is an Associate Editor of the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS.