Resilient and Cybersecure Distributed Control of Inverter-Based Islanded Microgrids

Bidram, Ali; Poudel, Binod; Damodaran, Lakshmisree; Fierro, Rafael; Guerrero, Josep M.

Published in:
IEEE Transactions on Industrial Informatics

DOI (link to publication from Publisher):
10.1109/TII.2019.2941748

Publication date:
2020

Document Version
Accepted author manuscript, peer reviewed version

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

Resilient and Cybersecure Distributed Control of Inverter-based Islanded Microgrids

Ali Bidram, *Member, IEEE,* Binod Poudel, *Student Member, IEEE,* Lakshmisree Damodaran, Rafael Fierro, *Senior Member, IEEE,* and Josep M. Guerrero, *Fellow, IEEE*

***Abstract*—This paper addresses the security of distributed secondary control of inverter-based Distributed Energy Resources (DERs) in microgrids. The proposed cyber-secure scheme utilizes the Weighted Mean Subsequence Reduced (WMSR) algorithm at each DER to discard the corrupted information received from neighboring DERs. This algorithm requires the connectivity of underlying communication graph to be above a specific threshold. To cope with this requirement, a methodology is proposed such that each DER is able to virtually change the quality of communication links connected to that DER to enhance the connectivity of communication graph. Two islanded microgrid test systems are simulated to validate the effectiveness of proposed cyber-secure secondary control.**

***Index Terms*—Cyber-attacks, distributed control, microgrids, secondary control, WMSR algorithm.**

I. Introduction

MICROGRIDs are controllable power systems that are able to supply their local loads through the available Distributed Energy Resources (DERs) [1]. DERs can be of electric machine type like synchronous generators or inverter-based type to facilitate the integration of emerging resources such as fuel-cells, battery energy storage systems, and solar energy. The unique feature of microgrids is their ability to operate autonomously after preplanned and/or unplanned islanding. Microgrids are equipped with a hierarchical control structure, including primary, secondary, and tertiary controls, to support the reliable operation in both grid-connected and islanded modes [2]-[3]. This paper considers the secondary control level.

Conventionally, secondary control level is implemented through a centralized control structure in which all DERs communicate and share their local information with a central controller. Centralized secondary control has a reliability bottle neck related to the single point of failure at the central controller. More recently, distributed secondary control has gained much attention because of increased flexibility, reliability, and scalability [4]-[13]. In this paper, distributed secondary control is of concern.

This material is based upon work supported by the National Science Foundation EPSCoR Program under Award #OIA-1757207.

Ali Bidram, Binod Poudel, Lakshmisree Damodaran, and Rafael Fierro are with the Department of Electrical and Computer Engineering, the University of New Mexico, Albuquerque, NM, (e-mail: {bidram, binodpoudel309, lakshmid, rfierro}@unm.edu). J. M. Guerrero is with the Department of Energy Technology, Aalborg University, 9220 Aalborg East, Denmark (Tel: +45 2037 8262; Fax: +45 9815 1411; e-mail: joz@et.aau.dk). J. M. Guerrero was funded by a Villum Investigator grant (no. 25920) from The Villum Fonden.

Microgrids hugely utilize information and communication technologies which in turn expose them to cyber-threats. In [14], cyber security of microgrids is proposed as one of the concepts that should be considered for an outlook of higher resilience. In a microgrid control system, both control and communication entities can be potential targets for cyber-threats (See Fig. 1) [15]-[22]. False data injection (FDI) attacks target the sensors and control and decision-making units which in turn corrupt the data transferred through the communication links and impact the microgrid data integrity [23]. Denial-of-Service (DoS) attacks endanger the availability of communication system services [24]. This paper focus is on FDI attacks targeting the control and decision-making units of DERs. FDI attacks can endanger microgrid voltage and frequency stability which in turn (i) cause cascading failures and power outage for microgrid customers [25], (ii) slow down the DER control system responses, (iii) make DERs synchronize to values other than actual voltage and frequency reference values, and (iv) overload DERs or violate the microgrid equipment thermal limits.

The majority of the research performed in the power grids cyber-security is on the cyber-attack detection [15]-[21]. In [13], the cyber-attack mitigation of AC microgrids is addressed which only focuses on frequency restoration and does not address the microgrid voltage and DERs' active/reactive power control. In [15], a cyberattack mitigation scheme is proposed for the reliable operation of voltage control protocols in an AC microgrid. In [16], a methodology is presented for discarding the information of attacked agents in the control protocols which needs a communication graph with high connectivity.

This paper proposes a secure intrusion mitigation approach for microgrid distributed control system that uses the Weighted Mean Subsequence Reduced (WMSR) technique. The proposed secondary control is inspired by the WMSR-based mitigation technique proposed in [15], [26]. The WMSR is a systematic technique to discard the information shared by non-cooperative attacked agents in a multi-agent network. The WMSR technique requires the communication graph to meet a minimum connectivity criterion for providing consensus among agents in the presence of cyber-attacks. To achieve the connectivity requirement, this paper introduces the concept of virtual communication graph in which the communication links' qualities are calculated based on DER's relative power angles. To this end, an exponential-based function is selected to define the quality of communication links based on the DER power angles which controls the flow of information and can stop the information flow if the power angle of

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

neighboring DERs significantly diverge from each other. A control protocol is proposed to tune up the quality of communication links to ensure that the communication graph's algebraic connectivity is above a specific cyber-secure threshold. Once the cyber-secure threshold is satisfied the WMSR technique is applied to restore frequency and voltage of microgrid to the nominal values.

This paper makes the following contributions:

- The concept of time-varying communication graphs is utilized to improve the microgrid resilience with respect to cyberthreats.
- Cyber-secure control protocols are proposed for the reliable operation of frequency/active power and voltage/reactive power control of DERs in an islanded microgrid which enhance the connectivity of communication graph and effectively discard the corrupted information distributed by attacked DERs.

The rest of paper is organized as follows: Preliminaries of graph theory are provided in Section II. The DER model, primary control, and secondary control of microgrids are discussed in Section III. The cyber-secure distributed secondary control is presented in Section IV. Section V discusses the communication and control requirements to implement the proposed cyber-secure distributed control system. The validity of the proposed secondary control protocols is verified in Section VI. A conclusion is provided in Section VII.

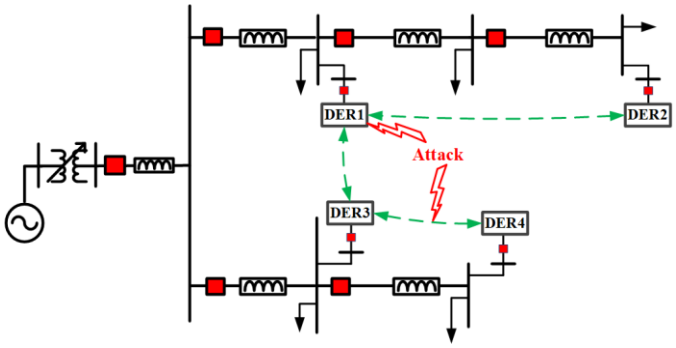


Fig. 1. Cyber-attacks on DERs or communication links in microgrid distributed control system.

II. Preliminaries on Graph Theory

The microgrid communication network can be modeled by a communication graph. A graph $\mathcal{G}=(\mathcal{V},\mathcal{E},\mathcal{A})$ includes a set of N nodes $\mathcal{V}=\{v_1,v_2,\ldots,v_N\}$ and a set of edges $\mathcal{E}\subset\mathcal{V}\times\mathcal{V}$. The nodes and edges of a communication graph are shown in Fig. 2. In a microgrid system, DERs denote graph nodes and communication links denote graph edges. A graph is represented by an adjacency matrix $\mathcal{A}=[a_{ij}]\in\mathbb{R}^{N\times N}$ to describe the connectivity of nodes. An edge from node j to node i, denoted by (v_j,v_i), indicates the information flow from node j to node i. 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 neighbors of node i in a set is described as $N_i=\{j\,|\,(v_j,v_i)\in\mathcal{E}\}$. The Laplacian matrix is defined as $L=D-\mathcal{A}$, where the in-degree matrix, $D=\mathrm{diag}\{d_i\}\in\mathbb{R}^{N\times N}$, elements are defined as $d_i=\sum_{j\in N_i}a_{ij}$ [27].

III. Microgrid Primary and Secondary Control

In this section, first, an inverter-based DER dynamical model is presented. Then, microgrid primary control level is discussed. Finally, the centralized and distributed secondary control levels are elaborated.

A. Dynamic Model of an Inverter-based DER

An inverter-based DER includes the Voltage Source Inverter (VSI) and the internal power, voltage, and current controllers to regulate the DER terminal voltage and operating frequency. The internal voltage and current control loops control the terminal voltage of DER to match it with the reference provided by power controller. The detailed description of these internal control loops is provided in [6].

This paper models DERs in *d-q* (direct-quadrature) reference frame [6]. In the reference-frame theory, the *d-q* reference frame of *i*-th DER is rotating with the angular speed of ω_i. This angular speed corresponds to the DER operating frequency. It is assumed that microgrid and one of the DERs are formulated in the common reference frame with the angular speed of ω_{com}. The power angle (or reference frame angle) δ_i denotes the angle difference between *i*-th DER and common reference frames satisfying

$$\dot{\delta}_i=\omega_i-\omega_{com}. \tag{1}$$

In practice, each DER power angle can be measured using a Phasor Measurement Units (PMU) [28] which utilizes an internal Phase-Locked Loop (PLL) system [29]. The power angle δ_i and its relationship to *d-q* reference frame is shown in Fig. 3. Inverter-based DERs in an AC microgrid are shown in Fig. 4.

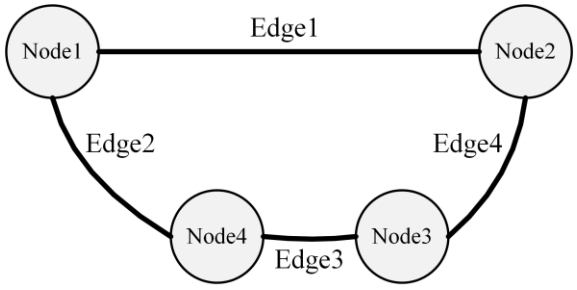


Fig. 2. A sample communication graph with nodes and edges.

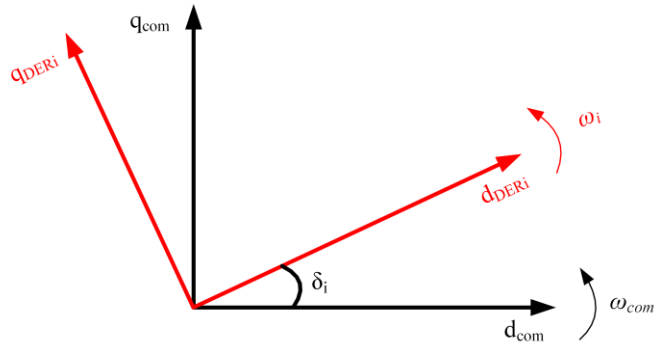


Fig. 3. The power angle δ_i and its relationship to d-q reference frame.

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

B. Primary Control Level

The primary control level is a local DER control. It conventionally employs the droop techniques to regulate the DER frequency through the active power and DER voltage magnitude through reactive power. The frequency and voltage droop techniques are

$$\begin{cases} \omega_i = \omega_{ni} - m_{Pi} P_i \\ v_{o,magi} = V_{ni} - n_{Qi} Q_i \end{cases}, \quad (2)$$

where P_i and Q_i are the output active and reactive power of DER; ω_{ni} and V_{ni} are the frequency and voltage droop references; m_{Pi} and n_{Qi} denote the P_i and Q_i droop coefficients, respectively. $v_{o,magi}$ is the output voltage magnitude of DER [2]. The droop coefficients are proportionally calculated based on the active/reactive power ratings of DERs to ensure that the DERs' active/reactive powers are assigned accordingly, i.e.,

$$\begin{cases} \dfrac{P_j}{P_i} = \dfrac{P_{\max j}}{P_{\max i}} = \dfrac{m_{Pi}}{m_{Pj}} \\ \dfrac{Q_j}{Q_i} = \dfrac{Q_{\max j}}{Q_{\max i}} = \dfrac{n_{Qi}}{n_{Qj}} \end{cases}, \quad (3)$$

where $P_{\max i}/Q_{\max i}$ and $P_{\max j}/Q_{\max j}$ are the active/reactive power ratings of i-th and j-th DER, respectively. Since frequency is a global variable, DERs' active powers are allocated based on DER ratings using the droop technique in (2). On the other hand, since voltage is not a global variable in the microgrid (i.e. each bus has a different voltage magnitude.), allocation of reactive powers based on DER ratings depends on the microgrid circuit topology and loading condition.

C. Secondary Control

The secondary control is to restore the operating frequency and terminal voltage magnitude of DERs to the reference frequency and voltage, i.e., $\omega_i \to \omega_{ref}$ and $v_{o,magi} \to V_{ref}$. ω_{ref} is set to $2\pi \times f_{nom}$, where f_{nom} is the nominal frequency of microgrid. For secondary voltage control, v_{ref} is chosen such that the voltage magnitude of a critical bus of microgrid synchronizes to microgrid nominal voltage v_{nom}. The microgrid critical buses host the critical loads and infrastructure which require to operate at the microgrid nominal voltage. To this end, v_{ref} is calculated as

$$v_{ref} = k_p (v_{nom} - v_{c,mag}) + k_i \int (v_{nom} - v_{c,mag}) dt, \quad (4)$$

where $v_{c,mag}$ denotes the critical bus voltage magnitude; k_p and k_i denote the proportional and integral PI controller parameters.

Secondary control level tunes DER primary control inputs, i.e., ω_{ni} and V_{ni} in (2). Secondary control must ensure that DERs' active/reactive powers are allocated based on a pattern similar to primary control [7]-[12].

The conventional secondary control utilizes a central control which communicates to DER primary controls using a centralized communication structure. The central control is exposed to the single point of failure which endangers the reliability of secondary control. Alternatively, distributed secondary control has been proposed in the literature which utilizes distributed control protocols implemented on all DERs. DERs can communicate with each other through a distributed communication network and share their local information with neighboring DERs to reach a consensus on the operating frequency and voltage of microgrid [5]-[12].

The distributed 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:

$$\begin{cases} \dot{\omega}_{ni} = v_{\omega i} \\ \dot{V}_{ni} = v_{vi} \end{cases} \quad i = 1, \ldots, N, \quad (5)$$

where $v_{\omega i}$ and v_{vi} are the distributed control protocols formulated using the local information of each DER and its neighbors' information and can be written as [11]

$$v_{\omega i} = -c_\omega \Big(\sum_{j \in N_i} a_{ij} (\omega_i - \omega_j) + g_i (\omega_i - \omega_{ref}) + \sum_{j \in N_i} a_{ij} (m_{Pi} P_i - m_{Pj} P_j) \Big), \quad (6)$$

$$v_{vi} = -c_v \Big(\sum_{j \in N_i} a_{ij} (v_{o,magi} - v_{o,magj}) + g_i (v_{o,magi} - v_{ref}) + \sum_{j \in N_i} a_{ij} (n_{Qi} Q_i - n_{Qj} Q_j) \Big), \quad (7)$$

where c_ω and c_v are the frequency and voltage control gains, respectively. The pinning gain $g_i \geq 0$ is nonzero for only one DER.

IV. Cyber-secure Microgrid Distributed Control

This section formulates the proposed cyber-secure distributed secondary control based on WMSR technique.

A. Cyber-threat Analysis

In a microgrid system, both control and communication entities can be potential targets for cyber-threats. FDI attacks target the sensors and control and decision-making units which in turn corrupt the data transferred through the communication links and impact the microgrid data integrity. On the other hand, DoS attacks target the communication links and tamper the transfer of data. If a communication link is subjected to a DoS attack, the performance of distributed secondary control is not affected as long as the underlying communication graph is strongly connected. In a strongly connected graph, there is a path for the flow information between any two distinct DERs. This paper focus is on FDI attacks targeting the sensors and control and decision-making units of DERs. Due to the extensive deployment of communication and control technologies and the presence of Intelligent Electronic Devices (IEDs), microgrid control system is *vulnerable* to cyber-threats. For example, FDI attacks can simply gain access to the PMUs, IEDs, or DER control and decision-making units through the communication ports and tamper the algorithms and functionalities of these devices to cause a major catastrophe in microgrid.

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

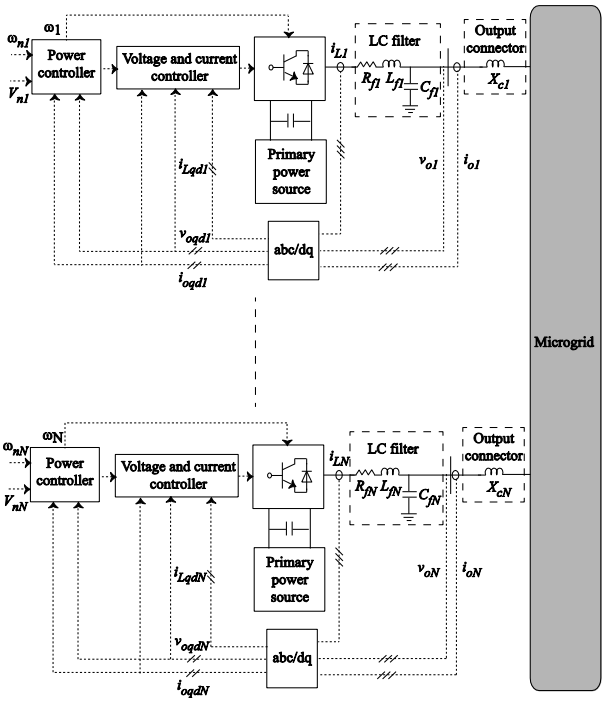


Fig. 4. Inverter-based DERs in an islanded microgrid.

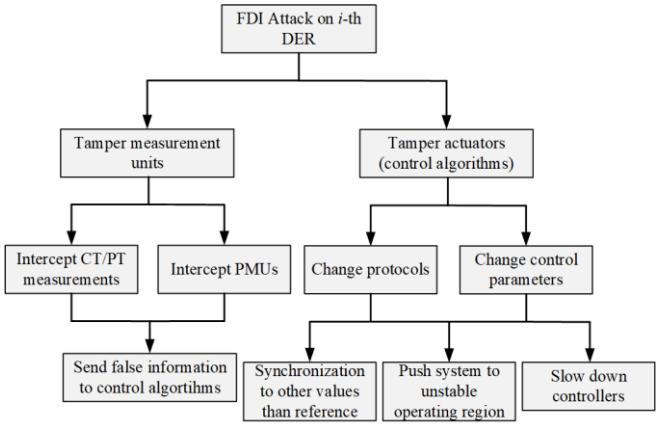


Fig. 5. Attack tree for FDI threat analysis.

A DER is healthy (cooperative) if it successfully runs the distributed control protocols in (6) and (7), and shares its actual measurements with the neighboring DERs. On the other hand, a corrupted (non-cooperative) DER is exposed to an FDI attack where the attacker takes control of DER sensors and control unit. In Fig. 5, an *attack tree* for FDI threat analysis is provided. As seen, the FDI attack can tamper either the DER sensors (measurement units) or actuators (control and decision-making unit). The measurement units include the local CT and PT or PMUs. The attacker can gain access to these measurement units and send false data to DER internal control and decision-making unit. On the other hand, an attacker can directly tamper the control and decision-making unit on each DER to change control protocols or control parameters. More specifically, FDI attacks on DERs can endanger the operation of distributed secondary control and have the following *impacts* on the microgrid operation,

- endangering microgrid voltage and frequency stability which in turn causes power outage for microgrid customers,
- slowing down the DER control system responses,
- making DERs synchronize to values other than actual voltage and frequency reference values,
- overloading DERs and violating the microgrid equipment thermal limits.

B. Virtual Time-Varying Communication Graph

Conventionally, microgrid distributed control utilizes a fixed adjacency matrix, $\mathcal{A}=[a_{ij}]\in\mathbb{R}^{N\times N}$, i.e., the communication link qualities are time-invariant values. This paper proposes to adopt a virtual communication graph in which the communication link qualities, a_{ij}, are virtually and locally calculated by each DER. Each DER determines the quality of communication links connected to that DER (See Fig. 6). To this end, an exponential-based Communication Link Quality (CLQ) function [26] is implemented at each DER. The CLQ function provides each DER with a set of weighting factors to apply to the data that DER transmits through the distributed communication network. This paper proposes the following CLQ function based on the DER power angles, δ_i, as

$$a_{ij}=\begin{cases} a_{\max} & \left|\delta_i-\delta_j\right|<R_1 \\ 0 & \left|\delta_i-\delta_j\right|\geq R_2 \\ a_{\max}\times\exp\left(\dfrac{-\gamma\left(\left|\delta_i-\delta_j\right|-R_1\right)}{R_2-R_1}\right) & \text{otherwise,} \end{cases} \quad (8)$$

where R_1 and R_2 describe the relative power angle thresholds acting as measures to reflect the health of microgrid control system. If DERs' power angles are relatively close to each other, microgrid operates in a healthy condition in terms of frequency stability. Therefore, this threshold is set as a relatively small value. If power angle difference between two neighboring DERs is less than R_1, the communication link between them virtually adopts a maximum value of $a_{\max}$. Depending on the communication graph topology, $a_{\max}$ is selected based on the criteria explained in Section IV.C. As the power angle of communicating DERs diverge, the microgrid stability is at a higher risk. The CLQ function exponentially decreases communication link quality until the difference between the power angles is more than R_2 and the communication link quality is forced to zero, i.e. the flow of information between two DERs is prevented. R_2 should be chosen large enough to reflect the risk of microgrid frequency instability when the power angles of two neighboring DERs are diverging. γ is a CLQ design parameter to tune the smoothness and shape of function. The relationship between γ and CLQ function smoothness is shown in Fig. 7.

C. Cyber-secure Microgrid Distributed Control Using WMSR Technique

In a multi-agent system, the WMSR algorithm objective is to enhance the security of system with respect to cyber-threats by discarding the information from attacked agents in a systematic manner [30]-[31]. The communication graph must meet a specific connectivity criterion to ensure the reliable

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

operation of distributed control system. Theorem 1 discusses this connectivity requirement for WMSR technique.

Definition 1 [26]: A communication graph is called *r*-robust if for any of two disconnected subsets, at least one subset is *r*-reachable. A subset is *r*-reachable if for at least one DER, the number of communication links leaving the subset from that DER is larger than *r*.

Theorem 1 [30]: A microgrid with N DERs and a communication graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$ is considered. Assuming n_{NC} non-cooperative attacked DERs, WMSR technique provides asymptotic consensus for DERs if the communication graph is $(2n_{NC}+1)$-robust.

To implement WMSR technique, each DER performs the following stages at each time step:

Stage 1: At each DER, a list of angular speeds and voltage magnitudes from the neighboring DERs, i.e., ω_j and $v_{o,magj}$, $j\in N_i$, is created. This list is sorted based on ω_j and $v_{o,magj}$ values.

Stage 2: ω_j and $v_{o,magj}$ of neighboring DERs are compared with DER's ω_i and $v_{o,magi}$ to update the distributed frequency and voltage control protocols as follows:

- For *angular frequencies*, if there are n_{NC} or more larger ω_j values, the n_{NC} largest ω_j values are discarded from the distributed control protocol in (6). If there are fewer than n_{NC} larger ω_j values, all of them are removed from (6). For smaller ω_j values, the same process is utilized to discard the neighboring ω_j values. After the removal process is done, the distributed frequency control protocol in (6) is updated as

$$v_{\omega i}=-c_{\omega}\Big(\sum_{j\in R_{\omega i}}a_{ij}(\omega_i-\omega_j)+g_i(\omega_i-\omega_{ref})+\sum_{j\in R_{\omega i}}a_{ij}(m_{Pi}P_i-m_{Pj}P_j)\Big), \tag{9}$$

where $R_{\omega i}$ describes the updated neighboring set in distributed frequency control protocol for *i*-th DER.

- For *voltage magnitudes*, if there are n_{NC} or more larger $v_{o,magj}$ values, the n_{NC} largest $v_{o,magj}$ values are discarded from the distributed control protocol in (7). If there are fewer than n_{NC} larger $v_{o,magj}$ values, all of them are removed from (7). For smaller $v_{o,magj}$ values, the same process is utilized to discard the neighboring $v_{o,magj}$ values. After the removal process is done, the distributed voltage control protocol in (7) is updated as

$$v_{vi}=-c_v\Big(\sum_{j\in R_{vi}}a_{ij}(v_{o,magi}-v_{o,magj})+g_i(v_{o,magi}-v_{ref})+\sum_{j\in R_{vi}}a_{ij}(n_{Qi}Q_i-n_{Qj}Q_j)\Big), \tag{10}$$

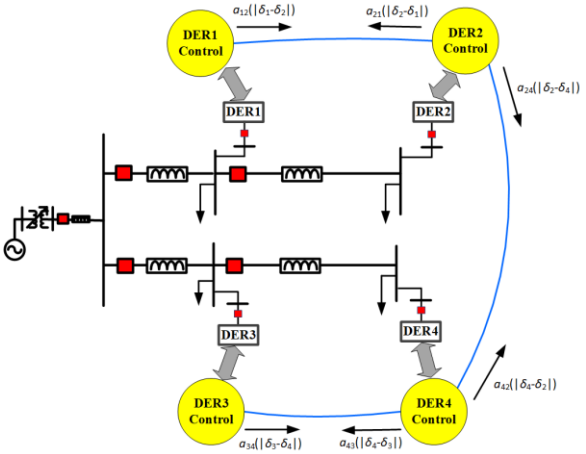


Fig. 6. Virtual communication graph imposed by DERs.

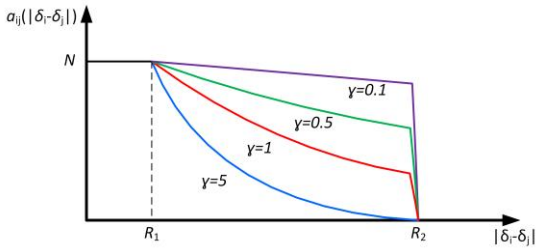


Fig. 7. CLQ function for different values of γ.

where R_{vi} describes the updated neighboring set in distributed voltage control protocol for *i*-th DER.

As stated in Theorem 1, WMSR technique ensures frequency and voltage restoration if the communication graph of microgrid control system is $(2n_{NC}+1)$-robust. According to [32], finding the *r*-robustness of a graph is a co-NP complete problem. This significantly increases the computational burden of distributed control system in microgrids with large number of DERs. Theorem 2 presents an alternative metric that lower-bounds the *r*-robustness metric.

Theorem 2 [26]: For a communication graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$, $\left\lceil\frac{\lambda_2}{2}\right\rceil$ lower-bounds the level of *r*-robustness, *r*. λ_2 denotes the algebraic connectivity of communication graph $\mathcal{G}$.

From Theorems 1 and 2, the WMSR technique can provide frequency and voltage restoration if

$$\lambda_2>4n_{NC}. \tag{11}$$

Equation (11) is a cyber-secure threshold to guarantee WMSR technique effectiveness in the presence of n_{NC} attacked DERs. To this end, $a_{\max}$ in (8) is selected such that the algebraic connectivity of the communication graph assuming all links adopting the fixed weight of $a_{\max}$ is greater than $4n_{NC}$. Moreover, since the virtual communication graph link quality values are a function of DER power angles, the following control protocol is used to satisfy (11) before the WMSR technique is applied

$$v_{\omega i}=c_{\lambda_2}\frac{\partial\lambda_2}{\partial\delta_i}, \tag{12}$$

where is c_{λ_2} control parameter, $v_{\omega i}$ is the auxiliary frequency control variable in (5) , and δ_i is the power angle of *i*-th DER.

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

It should be noted that (12) should be fast enough to force the algebraic connectivity of virtual communication graph above the cyber-secure threshold in (11) in a few cycles. Doing so, the microgrid can recover to normal operation after the attack is detected. The control parameter c_{λ_2} is the key parameter to tune the response speed of (12). As c_{λ_2} is set to larger values, the response speed of control protocol in (12) increases accordingly.

The algebraic connectivity is a function of Laplacian matrix *L*. According to [33], the derivative of algebraic connectivity with respect to Laplacian matrix is

$$\frac{\partial \lambda_2(L)}{\partial L} = \frac{\mathbf{v}_2 \mathbf{v}_2^T}{\mathbf{v}_2^T \mathbf{v}_2}, \tag{13}$$

where $\mathbf{v}_2$ is eigen vector related to λ_2. L is a function of the power angle of DERs according to (8). Using the chain rule, the control protocol in (12) can be written as [26]

$$v_{\omega i} = c_{\lambda_2} \text{Trace}\left\{ \left[\frac{\mathbf{v}_2 \mathbf{v}_2^T}{\mathbf{v}_2^T \mathbf{v}_2} \right]^T \left[\frac{\partial L}{\partial \delta_i} \right] \right\}. \tag{14}$$

Remark 1. Equations (12) or (14) ensure that the DER power angles are pushed toward a more stable operating region which in turn increases the communication links' qualities and the algebraic connectivity of communication graph. It is proven in [26] that (12) or (14) increase the algebraic connectivity of communication graph to reach the cyber-secure threshold in (11) in definite time.

This paper proposes the following algorithm for the secondary control of microgrids in the presence of cyber-attacked DERs. In this algorithm (Algorithm 1), each DER estimates the communication graph algebraic connectivity and compares it with $\eta \times 4n_{NC}$, where η is a factor to provide enough margin for algebraic connectivity to remain above the cyber-secure threshold in (11). If the algebraic connectivity is less than $\eta \times 4n_{NC}$, the control protocol in (14) is applied until the algebraic connectivity is greater than $\eta \times 4n_{NC}$. If the algebraic connectivity is greater than or equal to $\eta \times 4n_{NC}$, the WMSR technique is utilized to update the distributed secondary control protocols in (6) and (7) by discarding the information of corrupted DERs over time. The proposed cyber-secure distributed secondary control is shown in Fig. 8.

Algorithm 1: Cyber-secure distributed secondary control

for t = 0,*T*,2*T*,… **do**
  if $\lambda_2 < \eta \times 4n_{NC}$ **then**
    update $v_{\omega i}$ in (5) using (14),
    force v_{vi} in (5) to zero.
  else
    use WMSR algorithm,
    update $v_{\omega i}$ in (5) using (9),
    update v_{vi} in (5) using (10).
  end if
end for

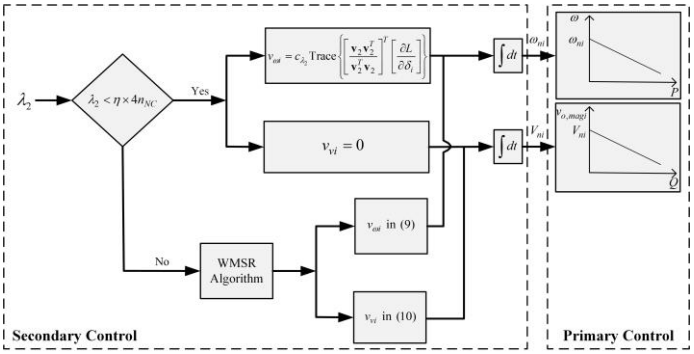


Fig. 8. Cyber-secure distributed secondary control at each DER.

D. Distributed Estimation of Algebraic Connectivity

The proposed methodology requires each DER to know algebraic connectivity of the overall communication graph to switch between the control protocol in (14) and WMSR algorithm. One approach could be to utilize a central coordinator that oversees the communication graph, calculates the algebraic connectivity, and shares it with all DERs. However, the presence of a central coordinator exposes the secondary control to the single-point-of failure issue. To incorporate a fully distributed control platform and avoid the requirement of any central coordinator, this paper utilizes a two-layer distributed algebraic connectivity estimation approach [34] which is elaborated as follows. The algebraic connectivity can be estimated locally at *i*-th DER using

$$\lambda_{2,i}(kT_s) = \frac{\hat{\mathbf{v}}_{2,i}((k+1)T_s)}{\left|\hat{\mathbf{v}}_{2,i}(kT_s)\right|} \left\| \gamma^{-1} \hat{W}_i(kT_s) \right\|, \tag{15}$$

where $\hat{\mathbf{v}}_{2,i}$, the estimated *i*-th element of $\mathbf{v}_2$, is updated with sampling period of T_s using the outer-layer observer

$$\hat{\mathbf{v}}_{2,i}((k+1)T_s) = \frac{1}{\left\| \gamma^{-1} \hat{W}_i(kT_s) \right\|} \left[\sum_{j \in N_i} a_{ij}(kT_s) \hat{\mathbf{v}}_{2,j}(kT_s) - \hat{\gamma}_{1,i}(kT_s) \hat{W}_i^T(kT_s) \mathbf{1}_N \right], \tag{16}$$

where $\hat{W}_i$ denotes the outer layer observer tuning variable; $\mathbf{1}_N$ is the vector of one with N elements; $\gamma = \text{diag}\left[\hat{\gamma}_1\right]$ with $\hat{\gamma}_1$ defined as the estimated first left eigenvector of adjacency matrix; $\hat{\gamma}_{1,i}$ denotes the *i*-th element of $\hat{\gamma}_1$. The inner-layer consists of two observers that update $\hat{W}_i$ and $\hat{\gamma}_1$ estimations with the sampling period of $T_s^* < T_s$. $\hat{W}_i$ is updated at each DER using

$$\hat{W}_i\,(kT_s + (l+1)T_s^*) = \sum_{j \in N_i} a_{ij}(kT_s + lT_s^*) \hat{W}_j\,(kT_s + lT_s^*), \tag{17}$$

$\hat{\gamma}_1$ is updated at each DER using

$$\hat{\gamma}_1\,(kT_s + (l+1)T_s^*) = \sum_{j \in N_i} a_{ij}(kT_s + lT_s^*) \hat{\gamma}_1\,(kT_s + lT_s^*), \tag{18}$$

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

V. Control and Communication Infrastructure Requirements to Impalement the Proposed Distributed Secondary Control

The proposed distributed secondary control consists of control and communication layers. To facilitate the practical implementation of microgrid distributed control system, some technical factors and requirements should be taken into consideration on both control and communication infrastructure.

A. Control Infrastructure Requirements

The control infrastructure includes the local sensors and decision-making units located on individual DERs. The distributed control protocols for each DER can be implemented on the existing micro-processor of VSIs with a software update to pre-existing codes and do not impose heavy processing burden. As mentioned earlier, this paper focuses on the FDI attacks on the individual DER decision-making units. The proposed cyber-secure distributed control can be implemented by creating two software modules on the internal processor of VSIs. These software modules are to estimate the algebraic connectivity of the communication graph and implement the cyber-secure distributed control algorithm shown in Fig. 8.

B. Communication Infrastructure Requirements

In this section, the communication infrastructure requirements from standard, protocol, and technology points of view are taken into consideration.

The communication system standard should account for the interoperability requirement. This requirement ensures that IEDs, e.g., inverters and control equipment, from different manufactures that support different communication protocols can be easily integrated into the rest of communication system. The IEC 61850 standard [35] is an industry-approved option to promote the interoperability of IEDs in microgrid distributed control system. The interoperability feature of IEC 61850 standard facilitates the seamless data transfer among microgrid control, monitoring, and protection systems [36]. The information flow among DERs can be in the format of GOOSE messages to transfer DER local measurements like voltage, frequency, and active/reactive power over the distributed communication network. Each DER acts as a publisher while the neighboring DERs on the communication network act as subscribers.

The TCP/IP based communication protocol is a suitable option for the implementation of microgrid distributed control system. This protocol is provided with sufficient bandwidth and high availability which help with the timely network awareness. Due to the unpredictable performance and slow-start nature of TCP protocol, one can argue that it is not a suitable option for reliable monitoring and control applications. On the other hand, UDP based protocol is associated with less latency and a more reliable operation which is a critical factor for the microgrid control system.

The microgrid control system can adopt wired, wireless, or hybrid technologies. The wired technologies like fiber optics have higher capacity but they are costlier to implement specially in larger scale microgrids. Fiber optics technology can support data transfer rate up to several Giga bits per second. The wireless technologies like high frequency radio benefit from the lower installation costs, flexible configuration and fast deployment. However, they suffer from the lower data transfer rates compared to wired technologies. Moreover, they are more prone to cyber-attacks.

VI. Simulation Results

A. Case A: Model Verification for Islanded IEEE 34 Bus Test Feeder with 6 DERs

Case A verifies the validity of proposed control techniques on the IEEE 34 bus test feeder. In Fig. 9, the single-line diagram of IEEE 34 bus test feeder with six integrated DERs is illustrated. This test system is simulated in MATLAB/Simulink. The original IEEE 34 bus feeder is transformed to a balanced feeder by averaging the line parameters. The specification of lines is provided in [37]. The specifications of DERs and loads are provided in Table I and II, respectively. The microgrid is operating at the frequency of 60 Hz. The nominal line-to-line voltage is 24.9 kV. DERs are integrated to the feeder through a wye-wye transformer, with 480 V/24.9 kV voltage ratings, and 400 kVA power rating. The series impedance of each transformer is 0.03 + j 0.12 pu. The microgrid critical bus is Bus 824 at which Load 1 is connected.

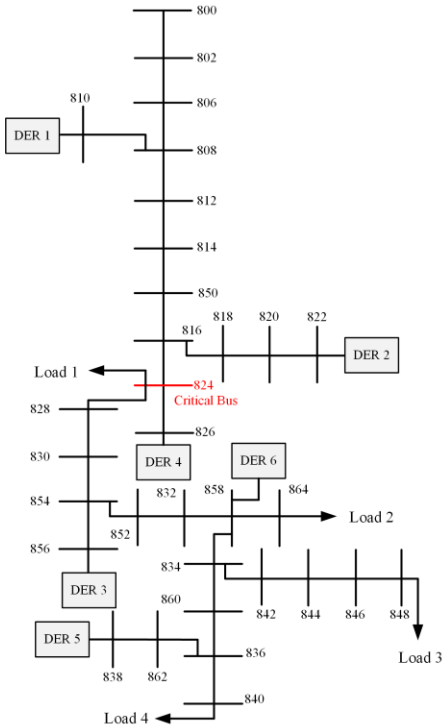


Fig. 9. Islanded IEEE 34 bus feeder.

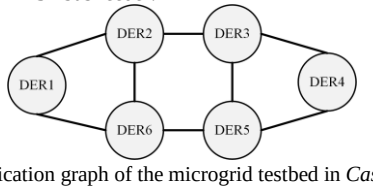


Fig. 10. Communication graph of the microgrid testbed in *Case A*.

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

TABLE I. SPECIFICATION OF DERS IN CASE A

DER 1, 2, 5 and 6		DER 3 and 4	
m_P	5.64×10^{-5} Hz/W	m_P	7.5×10^{-5} Hz/W
n_Q	5.2×10^{-4} V/Var	n_Q	6×10^{-4} V/Var
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

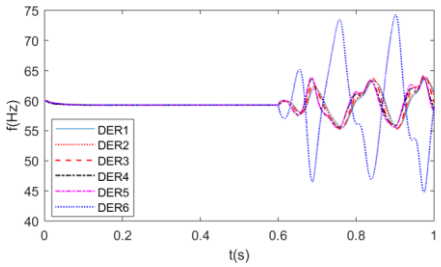
TABLE II. SPECIFICATION OF LOADS IN CASE A

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

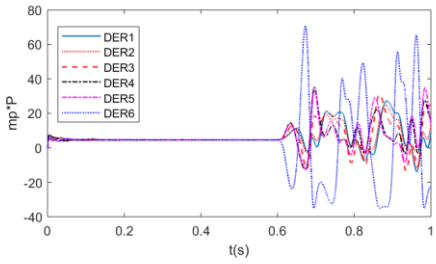
The communication network graph is depicted in Fig. 10. This communication graph illustrates the DERs as the control nodes and communication links which can either utilize wired/wireless technologies. The frequency and voltage reference values are shared with DER1 with the pinning gain $g_1 = 1$. ω_{ref} is set to $2\pi\times60$ rad/sec. v_{ref} is calculated using (4) with k_p and k_i parameters set to 0.01 and 10, respectively. v_{nom} is set to 1 pu. The control gains c_ω and c_v in (9) and (10) are set to 40. The parameters of CLQ function in (8) are as follows: R_1 is set to $\pi/50$; R_2 is set to $\pi/2$; γ is set to 5; $a_{\max}$ is set to 4. T_s in (16) is set to 0.001 s and T_s^* in (17) and (18) is set to 0.0001 s. To better show the impact of cyber-attacks on the secondary control of microgrid and verify the validity of proposed cyber-secure distributed secondary control, two case studies, namely *Case A.1* and *Case A.2* are performed which are elaborated as follows. In both cases the distributed secondary frequency and voltage control protocols are applied simultaneously.

Case A.1: This test case investigates the impact of an attacked DER on the secondary control of microgrid. The FDI attack takes control of DER6 and shares the constant frequency of 60.2 Hz and constant voltage of 482V with its neighbors, i.e., DER1 and DER5. Assuming that the communication network adopts a TCP/IP based protocol, the FDI attack can take control of DER6 control and decision-making unit through the available communication ports. The impact of attack on the operation of conventional distributed secondary frequency control in (6) is shown in Fig. 11(a) and Fig. 11(b). These figures show the frequency of DERs and their active power ratios (i.e., $m_{Pi}P_i$) before and after applying the conventional distributed frequency control. Microgrid islanding occurs at $t = 0$. Conventional secondary frequency control takes action at $t = 0.6$ s. As seen, the conventional distributed frequency control fails to restore the frequency of microgrid to 60 Hz and the frequency stability in the microgrid is lost. The impact of attack on the operation of conventional distributed secondary voltage control in (7) is shown in Fig. 12(a) and Fig. 12(b). These figures show the voltage magnitude of critical bus of microgrid (Bus 824) and DERs' reactive power ratios ($n_{Qi}Q_i$) before and after the conventional distributed secondary voltage control is applied. Microgrid islanding occurs at $t = 0$. Conventional secondary voltage control takes action at $t = 0.6$ s. As seen, the conventional distributed voltage control fails to restore the voltage magnitude of critical bus of microgrid and voltage stability of microgrid is lost.

Case A.2: This test case verifies the validity of the proposed cyber-secure distributed secondary control. Microgrid islanding occurs at $t = 0$. Conventional secondary frequency and voltage control take action at $t = 0.6$ s. The cyber-secure distributed frequency and voltage control act at $t = 0.65$ s. From $t = 0.6$ s to $t = 0.65$ s, the conventional secondary control is impacted by the attacked DER6 which in turn affects the voltage and frequency restoration of microgrid. The microgrid frequency and DERs' active power ratios are shown in Fig. 13(a) and Fig. 13 (b), respectively. The critical bus voltage magnitude and DERs' reactive power ratios are shown in Fig. 14(a) and Fig. 14(b), respectively. As seen in Fig. 13(a) and Fig. 13 (b), after the cyber-secure frequency control is applied, the frequency and active power ratio ($m_{Pi}P_i$) of DERs synchronize to a common value. The DER frequencies are restored to 60 Hz. Additionally, the active power of DERs are allocated based on their active power ratings. As seen in Fig. 14(a) and Fig. 14(b), after the cyber-secure voltage control is applied, the critical bus voltage magnitude is restored to 1 pu, and reactive power ratio ($n_{Pi}Q_i$) of DERs converge back to the values they had before the secondary control took action. The power angles of DERs and communication graph algebraic connectivity are shown in Fig. 15(a) and Fig. 15(b), respectively. As shown, after the conventional distributed control takes action, the power angles start to drift apart from each other due to the presence of false information that attacked DER shares with its neighbors. This results in the drop of algebraic connectivity of graph below the cyber-secure threshold. However, the cyber-secure distributed secondary control utilizes the control protocol in (14) to push back the algebraic connectivity above the cyber-secure threshold with a safety factor of $\eta = 1.025$. The cyber secure threshold in this case study is equal to 4.1.



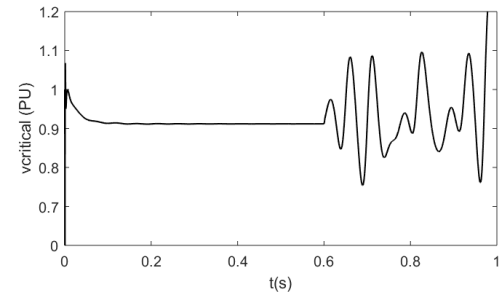
(a)



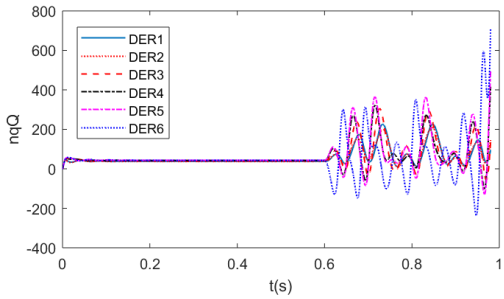
(b)

Fig. 11. Cyber-attack impact on conventional distributed secondary frequency control in *Case A*: (a) DER frequencies; (b) DER active power ratios ($m_{Pi}P_i$).

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

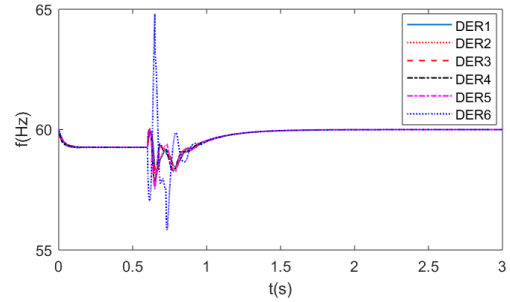


(a)

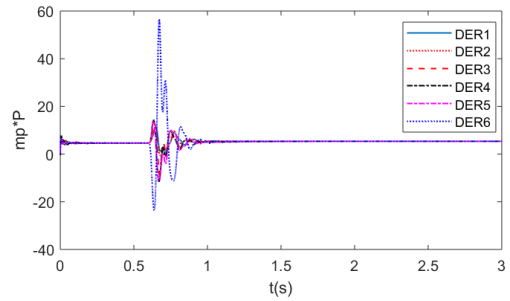


(b)

Fig. 12. Cyber-attack impact on conventional distributed secondary voltage control in *Case A*: (a) critical bus voltage; (b) DER reactive power ratios ($n_{Qi}Q_i$).



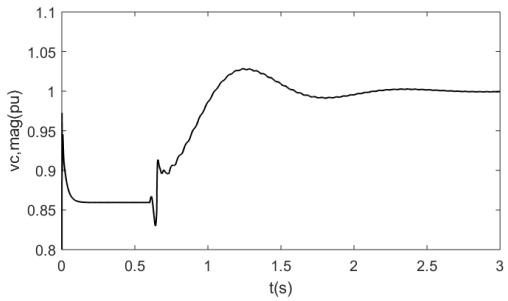
(a)



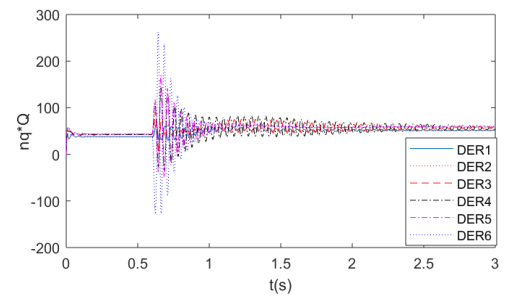
(b)

Fig. 13. Cyber-secure distributed secondary frequency control under attack in *Case A*: (a) DER frequencies; (b) DER active power ratios ($m_{Pi}P_i$).

The impact of control parameter c_{λ_2} on the response speed of (12) is studied through simulating the proposed cyber-secure distributed secondary control with two different values of c_{λ_2}. The algebraic connectivity of communication graph after the control protocol in (12) is applied is shown in Fig. 16. The control parameter c_{λ_2} is set to 1 and 10 in Fig. 16(a) and Fig. 16(b), respectively. As seen, with a larger value of c_{λ_2}, the algebraic connectivity reaches the cyber-secure threshold faster.

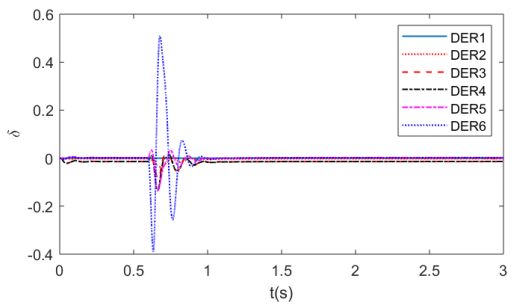


(a)

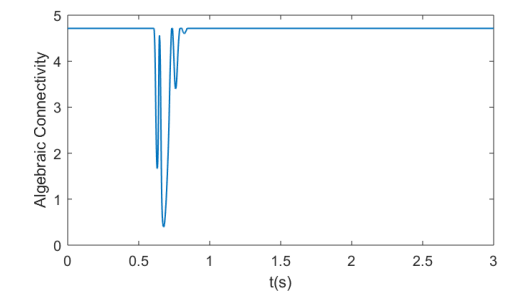


(b)

Fig. 14. Cyber-secure distributed secondary voltage control under attack in *Case A*: (a) critical bus voltage; (b) DER reactive power ratios ($n_{Qi}Q_i$).



(a)



(b)

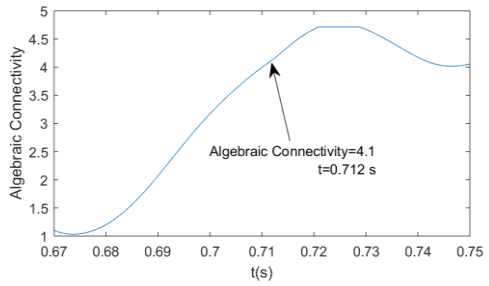
Fig. 15. *Case A* with cyber-secure distributed secondary control: (a) DER power angles; (b) algebraic connectivity of communication graph.

To highlight the impact of proposed cyber-secure distributed control on the resilience of microgrid, a resilience index (RI) is adopted from [14] which is defined as

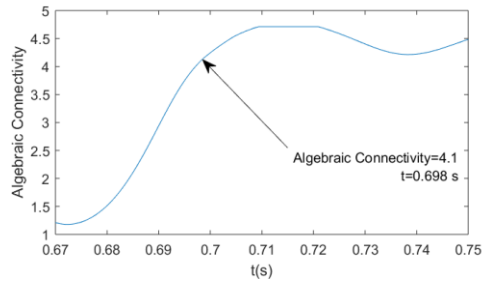
$$RI = 1 - \frac{PF_{\text{before}} - PF_{\text{after}}}{PF_{\text{before}}}, \tag{19}$$

where PF_{before} and PF_{after} denote the values of a performance function (PF) before and after applying the FDI attack, respectively. The performance index reflects system performance in terms of frequency and voltage restoration capability. The performance function for the distributed frequency control is defined as

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics



(a)



(b)

Fig. 16. Impact c_{λ_2} of on the response speed of (12): (a) c_{λ_2} =1; (b) c_{λ_2} =10.

$$PF = 1 - \frac{1}{T}\int_0^T \left(\left|\frac{f - f_{nom}}{f_{nom}}\right|\right)dt \,. \tag{20}$$

The performance function for the distributed voltage control is defined as

$$PF = 1 - \frac{1}{T}\int_0^T \left(\left|\frac{v_{c,mag} - v_{nom}}{v_{nom}}\right|\right)dt \,. \tag{21}$$

Table III summarizes the calculated RI and PFs before and after applying the cyber-attack for two different cases. In the first case, the conventional distributed secondary control is utilized. The second case uses the proposed cyber-secure approach. In all cases, it is assumed that microgrid is islanded at t = 0, and the secondary control acts at t = 0.6 s. The resilience index is calculated for the time interval t=[0.6s, 3s]. As seen, the proposed cyber-secure approach significantly helps with the improvement of RI.

TABLE III. IMPACT OF PROPOSED CYBER-SECURE APPROACH ON RI

	Distributed Frequency Control		Distributed Voltage Control	
	Conventional	Cyber-secure	Conventional	Cyber-secure
PF_{before}	0.9982	0.9982	0.9295	0.9295
PF_{after}	0.1479	0.9967	0.0833	0.9295
RI	0.1481	0.9984	0.0896	1

B. *Case B: Model Verification 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 IV. Lines and loads specifications are shown in Tables V. The microgrid critical bus is highlighted in Fig. 17 at where Load 6 is connected. The communication network graph is depicted in Fig. 18. The frequency and voltage reference values are shared with DER1 with the pinning gain g_1 = 1. ω_{ref} is set to 2π×60 rad/s. v_{ref} is calculated using (4) with k_p and k_i parameters set to 4 and 40, respectively. v_{nom} is set to 1 pu. The control gains c_ω and c_v in (9) and (10) are set to 40. The parameters of CLQ function in (8) are as follows: R_1 is set to π/50; R_2 is set to π/2; γ is set to 10; $a_{\max}$ is set to 40. T_s in (16) is set to 0.001 s and T_s^* in (17) and (18) is set to 0.0001 s.

The FDI attack takes control of DER20 decision-making unit and shares the constant frequency of 60.2 Hz and constant voltage of 482V with its neighbors, i.e., DER 15 and DER 19. It is assumed that microgrid islanding occurs at t = 0; conventional secondary frequency and voltage control acts at t = 0.6 s; the cyber-secure distributed frequency and voltage control act at t = 0.62 s. From t = 0.6 s to t = 0.62 s, the conventional secondary control is impacted by the attacked DER20 which in turn affects the voltage and frequency restoration of microgrid. The microgrid frequency and DERs' active power ratios are shown in Fig. 19(a) and Fig. 19(b), respectively. The critical bus voltage magnitude and DERs' reactive power ratios are shown in Fig. 20(a) and Fig. 20(b), respectively. As seen in Fig. 19(a) and Fig. 19(b), after the cyber-secure frequency control is applied, the frequency and active power ratio ($m_{Pi}P_i$) of DERs converge back to a common value. The DER frequencies are restored to 60 Hz. Additionally, the active power of DERs are allocated based on their active power ratings. As seen in Fig. 20(a) and Fig. 20(b), after the cyber-secure voltage control is applied, the critical bus voltage magnitude is restored to 1 pu, and reactive power ratio ($n_{Pi}Q_i$) of DERs converge back to the values they had before the secondary control took action.

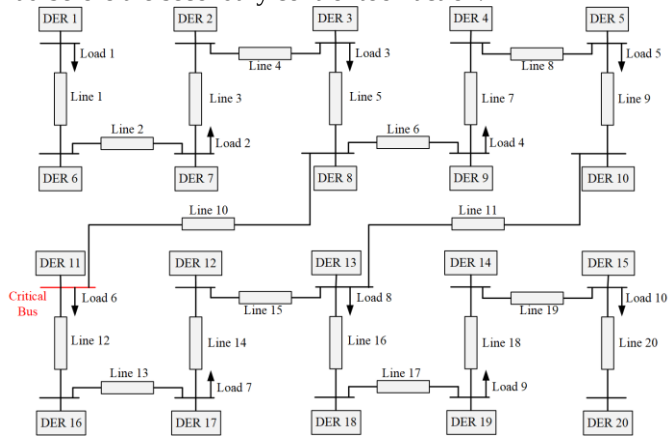


Fig. 17. Microgrid testbed with 20 DERs.

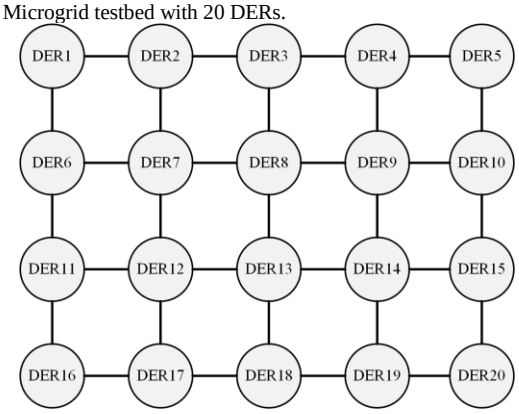


Fig. 18. Communication graph of the microgrid testbed in *Case B*.

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

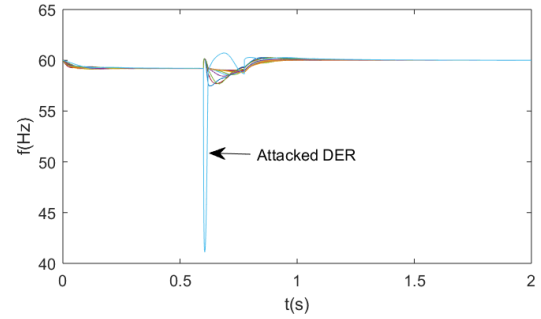
The DERs' power angles and communication graph algebraic connectivity are shown in Fig. 21(a) and Fig. 21(b), respectively. As seen, after the conventional distributed control takes action, the power angles start to drift apart from each other due to the presence of false information that attacked DER shares with its neighbors. This results in the drop of algebraic connectivity of graph below the cyber-secure threshold. However, the cyber-secure distributed secondary control utilizes the control protocol in (14) to push back the algebraic connectivity above the cyber-secure threshold with a safety factor of $\eta = 1.025$. The cyber secure threshold in this case study is equal to 4.1.

TABLE IV. SPECIFICATION OF DERS IN CASE B

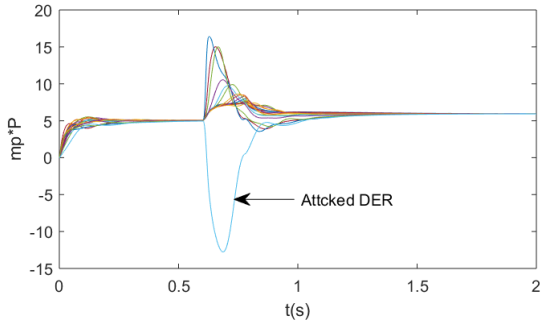
DER 1, 2, 3, 4, 5, 11, 12, 13, 14, and 15		DER 6, 7, 8, 9, 10, 16, 17, 18, 19 and 20	
m_P	9.4×10^{-5}	m_P	12.5×10^{-5}
n_Q	1.3×10^{-3}	n_Q	1.5×10^{-3}
R_c	30 mΩ	R_c	30 mΩ
L_c	350 μH	L_c	350 μH
R_f	100 mΩ	R_f	100 mΩ
L_f	1350 μH	L_f	1350 μH
C_f	50 μF	C_f	50 μF
K_{PV}	0.1	K_{PV}	0.05
K_{IV}	420	K_{IV}	390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

TABLE V. 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

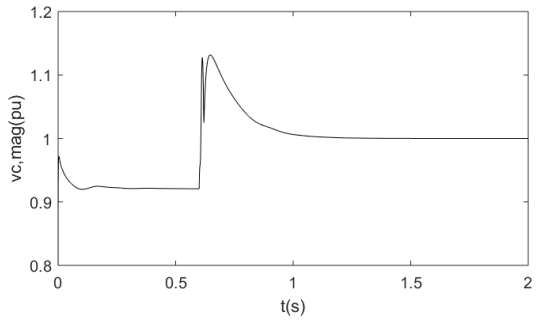


(a)

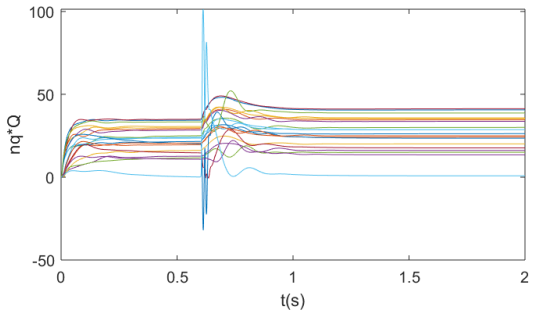


(b)

Fig. 19. Cyber-secure distributed secondary frequency control under attack in *Case B*: (a) DER frequencies; (b) DER active power ratios ($m_{Pi}P_i$).

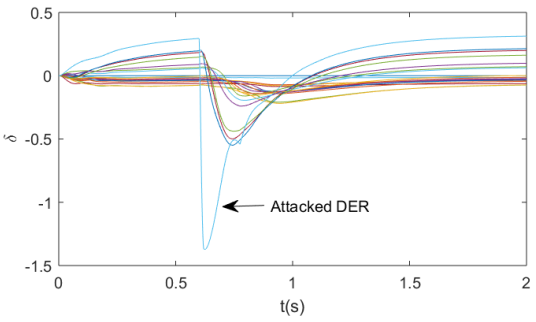


(a)

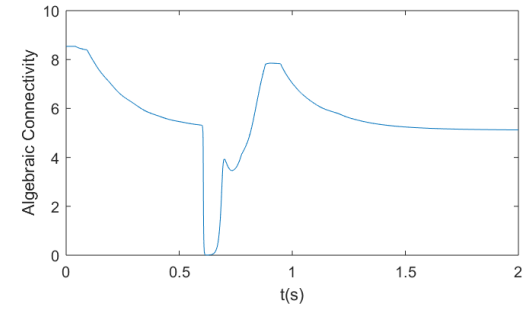


(b)

Fig. 20. Cyber-secure distributed secondary voltage control under attack in *Case B*: (a) critical bus voltage; (b) DER reactive power ratios ($n_{Qi}Q_i$).



(a)



(b)

Fig. 21. *Case B* with cyber-secure distributed secondary control: (a) DER power angles; (b) algebraic connectivity of communication graph.

VII. CONCLUSION

In this paper, a cyber-secure distributed secondary control for AC microgrids is proposed which utilizes WMSR technique. The proposed control uses a time-varying virtual communication graph. Each DER uses its own power angle and the power angle of its neighboring DER to calculate the communication link quality between them. A control protocol is proposed to tune up the quality of communication links such that the algebraic connectivity of communication graph is above a cyber-secure threshold to satisfy the effectiveness of

WMSR technique in the presence of attacked DERs. Two microgrid testbeds are simulated in MATLAB/Simulink to verify the validity of proposed cybersecure control approach.

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] Q. Shafiee, V. Nasirian, J. C. Vasquez, J. M. Guerrero, and A. Davoudi, "A multi-functional fully distributed control framework for AC microgrids," *IEEE Trans. Smart Grid*, vol. 9, pp. 3247-3258, July 2018.

[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] X. Lu, J. Lai, X. Yu, Y. Wang, and J. M. Guerrero, "Distributed coordination of islanded microgrid clusters using a two-layer intermittent communication network," *IEEE Trans. Ind. Informat.*, vol. 28, no. 3, pp. 3956-3969, Sept. 2018.

[8] L. Ding, Q. Han, L. Y. Wang, and E. Sindi, "Distributed cooperative optimal control of DC microgrids with communication delays," *IEEE Trans. Ind. Informat.*, to be published, DOI: 10.1109/TII.2018.2799239.

[9] M. Chen, X. Xiao, and J. M. Guerrero, "Secondary restoration control of islanded microgrids with a decentralized event-triggered strategy," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3870-3880, Sept. 2018.

[10] X. Lu, J. Lai, X. Yu, Y. Wang, and J. M. Guerrero "Distributed coordination of islanded microgrid clusters using a two-layer intermittent communication network," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3956-3969, Sept. 2018.

[11] 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.

[12] X. Lu, X. Yu, J. Lai, J. M. Guerrero, and H. Zhou, "Distributed secondary voltage and frequency control for islanded microgrids with uncertain communication links," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 448-460, April 2017.

[13] 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.

[14] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked microgrids for enhancing the power system resileince," vol. 105, no. 7, pp. 1289-1310, July 2017.

[15] A. Bidram, L. Damodaran, and R. Fierro, "Cybersecure distributed voltag control of AC microgrids," in *Proc. 55th Industrial and Commercial Power Systems Technical Conference*, 2019, pp. 1-6.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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, March 2014.

[23] 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.

[24] 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.

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

[26] K. Saulnier, D. Saldana, A. Prorok, G. J. Pappas, and V. Kumar, "Resileint flocking for mobile robot teams," *IEEE Robotics and Automation letters*, vol. 2, no. 2, pp. 1039-1046, Apr. 2017.

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

[28] M. Farajollahi, A. Shahsavari, E. M. Stewaty, and H. Mohsenian-rad, "Locating the source of events in power distribution systems using micro-PMU data," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6343-6354, May 2018.

[29] F. Hans, W. Schumacher, and L. Harnefors, "Small-signal modeling of three-phase synchronous refrence frame phase-locked loops," *IEEE Trans. Power Electron.*, vol. 33, no. 7, pp. 5556-5560, July 2018.

[30] H. Zhang and S. Sundaram, "Robustness of information diffusion algorithms to locally bounded adversaries," in *IEEE Proc. Amer. Controls Conf.*, 2012, pp. 5855-5861.

[31] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 766-781, Apr. 2013.

[32] H. Zhang, E. Fata, and S. Sundaram, "Robustness of complex networks: Reaching consensus despite adversaries," CoRR, vol. abs/1203.6119, 2012, 35 pages.

[33] E. Stump, A. Jadbabaie, and V. Kumar, "Connectivity management in mobile robot teams," in *Proc. IEEE Int. Conf. Robot. Autom.*, May 2008, pp. 1525-1530.

[34] C. Li and Z. Qu, "Distributed estimation of algebriac connectivity of directed networks," *Systems & Control Letters*, vol. 62, pp. 517-524, 2013.

[35] C. Brunner, "IEC 61850 for power system communication," in *Proc. IEEE/PES T&D Conf. Expo.*, Apr. 2008, vol. 2, pp. 1–6.

[36] Q. Yang, J. A. Barria, and T. C. Green, "Communication infrastructures for distributed control of power distribution networks," *IEEE Trans. Ind. Informat.*, vol. 7, pp. 316-327, May. 2011.

[37] 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.

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.

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/TII.2019.2941748, IEEE Transactions on Industrial Informatics

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.

Lakshmisree Damodaran is a PhD student at the Department of Electrical and Computer Engineering at University of New Mexico. She completed her Bachelors in Electronics and Communication Engineering at Amrita University and obtained her masters from UNM. Her PhD Emphasis is Systems and Controls. Her Research interests are Resiliency in Heterogeneous Robotic Networking systems, Machine Learning Applications in Robotics.

Rafael Fierro (S'95-M'98-SM'13) is a Professor of the Department of Electrical and Computer Engineering, the University of New Mexico where he has been since 2007. He received an MSc. degree in control engineering from the University of Bradford, England and a Ph.D. degree in electrical engineering from the University of Texas at Arlington. His current research interests include cyber-physical systems; coordination and planning in heterogeneous multi-agent systems; and hybrid control and switched systems. The National Science Foundation (NSF), US Department of Defense (DOD), Department of Energy (DOE), and Sandia National Laboratories have funded his research. He directs the AFRL-UNM Agile Manufacturing Center and the Multi-Agent, Robotics, and Heterogeneous Systems (MARHES) Laboratory. Dr. Fierro was the recipient of a Fulbright Scholarship, National Science Foundation CAREER Award, and the 2008 International Society of Automation (ISA) Transactions Best Paper Award. He is an associate editor for the IEEE Transactions on Automation Science and Engineering.

Josep M. Guerrero (S'01-M'04-SM'08-FM'15) received the B.S. degree in telecommunications engineering, the M.S. degree in electronics engineering, and the Ph.D. degree in power electronics from the Technical University of Catalonia, Barcelona, in 1997, 2000 and 2003, respectively. Since 2011, he has been a Full Professor with the Department of Energy Technology, Aalborg University, Denmark, where he is responsible for the Microgrid Research Program (www.microgrids.et.aau.dk). From 2014 he is chair Professor in Shandong University; from 2015 he is a distinguished guest Professor in Hunan University; and from 2016 he is a visiting professor fellow at Aston University, UK, and a guest Professor at the Nanjing University of Posts and Telecommunications. From 2019, he became a Villum Investigator by The Villum Fonden, which supports the Centre for Research on Microgrids (CROM) at Aalborg University, being Prof. Guerrero the founder and Director of the same centre.

His research interests is oriented to different microgrid aspects, including power electronics, distributed energy-storage systems, hierarchical and cooperative control, energy management systems, smart metering and the internet of things for AC/DC microgrid clusters and islanded minigrids. Specially focused on maritime microgrids for electrical ships, vessels, ferries and seaports. Prof. Guerrero is an Associate Editor for a number of IEEE TRANSACTIONS. He has published more than 500 journal papers in the fields of microgrids and renewable energy systems, which are cited more than 40,000 times. He received the best paper award of the IEEE Transactions on Energy Conversion for the period 2014-2015, and the best paper prize of IEEE-PES in 2015. As well, he received the best paper award of the Journal of Power Electronics in 2016. During six consecutive years, from 2014 to 2019, he was awarded by Clarivate Analytics (former Thomson Reuters) as Highly Cited Researcher. In 2015, he was elevated as IEEE Fellow for his contributions on "distributed power systems and microgrids."