Intrusion Detection in Distributed Frequency Control of Isolated Microgrids

Lin-Yu Lu, *Member, IEEE*, Hao Jan Liu, *Member, IEEE*, Hao Zhu, *Member, IEEE*, and Chia-Chi Chu, *Senior Member, IEEE*

***Abstract*—This paper presents a framework for distributed frequency control and intrusion detection in isolated microgrids (MGs). First, a distributed secondary control for isolated MGs, consisting of the local droop control at the primary level and a distributed node-to-node update at the secondary level, is proposed for achieving a proportional power sharing while maintaining the nominal system frequency. By casting it as a consensus optimization problem, we adopt the partial primal–dual algorithm for a totally distributed update requiring only neighboring information exchange. Attack models as well as countermeasures for malicious attacks on the communication network are also investigated. Two types of malicious attacks on the communication network, including link and node attacks, are studied. Model-based anomaly detection and localization strategies are developed by exploring the dual variable-related metrics. Numerical experiments have been performed to demonstrate the effectiveness of the proposed control and countermeasure metrics.**

***Index Terms*—Microgrid, distributed droop control, partial primal-dual algorithm, malicious attack, cyber-security.**

I. Introduction

As THE penetration of renewable energy sources increases in microgrids (MGs), coordinating these mostly power electronics-interfaced resources raises major concerns over the frequency stability problem [1]. Hierarchical control of distributed energy resources (DERs) interface converters (DICs) has recently become a standard operational paradigm for isolated microgrids [2], [3]. At the primary control level, a conventional power-frequency (P-ω) droop control assisted by the faster inner-loop controls can help to reduce the frequency and/or voltage mismatch error while providing power sharing capability [4]. Meanwhile, at the secondary control level, the grid-wide information regarding the status of all DICs can be further used to minimize the mismatch error attained by a local control in a centralized fashion.

The traditional centralized paradigm of the secondary control falls short of achieving scalability and flexibility goals of MG operations. To reduce the communication overhead and enhance DICs' plug-and-play ability, the distributed architecture has been advocated recently [5]–[10]. Under a connected communication network, the proportional power sharing objective is equivalent to having pair-wise consensus between any two neighbouring nodes. Hence, the distributed control problem becomes to minimize the frequency mismatch under linear consensus constraints. Nonetheless, these steady-state objectives do not necessarily guarantee the stability of resultant online control updates [5]–[7], [9]. In [5], the first-order consensus-based updates have been proposed and its stability is analyzed for the linearized system around a preferred equilibrium point. Convergence of the consensus-based updates is guaranteed by the time-scale separation assumption in [6]. A ratio consensus algorithm is developed in [7] to account for lower and upper limits of DER outputs. More recently, the per-node balance mode and the network balance mode of optimal distributed frequency control of multi-area power system with operational constraints, including the regulation capacity of individual control area and the power limits on tie-lines, have been comprehensively investigated [11], [12]. In [10], the distributed enforcement of phase-cohesiveness for frequency control is investigated by tracking a slowly-varying reference that is set sufficiently close to its actual active power of reference of each DIC. This control mechanism would ensure that the system remains stable at all times and the actual active power injections track the slowly-varying reference. In [13], the gather-and-broadcast control architecture, which is a continuous-time feedback control version of the dual decomposition optimization method, was proposed for the frequency control in power systems.

Meanwhile, a communication-based distributed frequency control framework also exposes the microgrid assets to potential malicious cyber attacks. In general, attack detection for distributed consensus algorithms under false-data injecting attacks has been considered in [14]–[16]. This type of attack is also related to the so-called Byzantine consensus, a fairly popular research topic in distributed computing. The goal of the Byzantine consensus algorithm is to find a near optimal

Manuscript received February 19, 2018; revised July 1, 2018, October 8, 2018, and January 13, 2019; accepted March 5, 2019. Date of publication March 21, 2019; date of current version October 30, 2019. This work was supported in part by the Department of Energy, USA, under Award DE-OE000078, in part by the U.S. National Science Foundation under Award ECCS-1802319, and in part by the Ministry of Science and Technology, Taiwan, under Grant MOST 105-2917-I-007-006, Grant MOST 105-2221-E-007-074, Grant MOST 105-3113-E-002-013, Grant MOST 106-2221-E-007-067, and Grant MOST 107-2221-E-007-094. Paper no. TSG-00271-2018. *(Corresponding author: Chia-Chi Chu.)*

L.-Y. Lu is with the Motor Drive Solution BU, Delta Electronics, Taoyuan 33068, Taiwan (e-mail: steven.lu@deltaww.com).

C.-C. Chu is with the Department of Electrical Engineering, National Tsing Hua University, Hsinchu 30013, Taiwan (e-mail: ccchu@ee.nthu.edu.edu.tw).

H. J. Liu is with the Amazon Web Services, Urbana, IL 61801 USA (e-mail: maxliu@amazon.com).

H. Zhu is with the Department of Electrical and Computer Engineering, University of Texas at Austin, Austin, TX 78712 USA (e-mail: haozhu@utexas.edu).

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

Digital Object Identifier 10.1109/TSG.2019.2906573

solution for an optimization problem despite the presence of malicious agents [17]–[20]. However, in practice, this approach has significant drawbacks: i) online implementations are infeasible as diminishing step-sizes fail to incorporate the most up-to-date system operating conditions; and ii) most system operators are more concerned about determining the *identity* of a malicious agent as settling with a near optimal solution with unidentified attackers presents a notable security threat within a cyber communication network. Thus, it is extremely important to distinguish malicious agents and isolate them within control frameworks. The concern about false-data injection attacks has increasingly challenged the power grid infrastructures along with more smart grid deployments, see, e.g., [21]–[27] and references therein, particularly for distributed power system state estimation in [22], [24]. Earlier work has considered the impacts of cyber attacks on grid monitoring or its control operations, but mostly for wide-area transmission systems. More recently, the vulnerability of consensus-based distributed energy scheduling algorithm to data integrity attacks was addressed in [28]–[31]. For example, a neighborhood-watch-based distributed energy management algorithm was proposed in [28] to guarantee the accurate control computation in solving the economic dispatch problem in the presence of compromised generation units. A reputation-based neighborhood-watch mechanism was introduced to detect the false information and achieve optimal operating point in the presence of misbehaving controllers [29]. Since there exist fewer resources for cyber defense and less inertia for frequency stability in isolated microgrids, it is of higher interest to investigate the cyber-security problems therein [30]–[32]. The false data injection attack against distributed load sharing in the microgrid was studied in [31]. Nevertheless, only the stable region under such attack was investigated and no countermeasure was provided. In [30], an attack-resilient distributed synchronization of inverter-based networked AC microgrids was addressed. However, the control algorithm requires an additional confidence index exchanged between DICs and also equips DICs with the ability to disconnect their neighbors based on information from the proposed observers. None of the aforementioned approaches has considered distributed control settings for isolated microgrids, where physical grid measurements and optimization-related variables can provide additional information for attack detection.

The main contributions of this paper are two-fold. First, the full MG network dynamics, including power flow dynamics and droop controlled DICs, are considered. The problem of minimizing the frequency error and ensuring a proportional power sharing operation simultaneously is formulated as a consensus optimization problem. Assuming connected communication graph among DICs, we adopt the partial primal-dual (PPD) algorithm to solve the steady-state problem in closed-form. Interestingly, parts of the proposed update rules boil down to network power flow dynamics and thus are seamlessly implemented by the physical system itself. Hence, the proposed control design only requires the exchange of a few variables, while its stability follows directly from the PPD algorithm. Distinct from most of the previous work, the proposed control design can guarantee the MG stability through the selection of optimization step-size. Secondly, the PPD-based design with localized dual variable information can be further utilized to improve the capability to attack detection. Earlier attack detection work for general distributed consensus methods typically requires system-wide information collection and accordingly has a very high computational burden [14], [15]. To overcome these limitations, we have developed the metrics for detection and identification by using local physical measurements and neighbouring dual variable information. The centralized energy management system (EMS) collects all this information to decide the attack scenarios, as motivated by standards on cyber networks for integrating DER into power systems [33]–[35], and also by practical work studying cybersecurity framework in supervisory control and data acquisition systems (SCADA) of modern power systems [36], [37]. Different layers of protection schemes for managing cyber/physical security have been considered to evaluate intrusion probability for preventing possible cyber attacks. Accordingly, the proposed implementation is very scalable. Compared with previous work where the cyber-security of the MG has not been addressed [5], [7], [8], [10], [38], we have provided analytical understanding and mitigation strategies for cyber intrusions.

The remainder of this paper is organized as follows. Section II introduces the microgrid network model and the droop control design for isolated MGs. The steady-state problem at the secondary control level is then formulated. Section III develops the distributed frequency control design based on the PPD algorithm. Attack models against the proposed control architecture are introduced, and the countermeasures are offered in Section IV. Section V presents the numerical results, which are acquired under the real-time simulation environment. Finally, conclusions and future work are made in Section VI.

II. Problem Formulations

We consider an isolated MG with m buses, where buses in $\mathcal{N} = \{1, \dots n\}$ are installed with DICs and the rest in $\mathcal{N}_L = \{n+1, \dots m\}$ are load buses. Per bus-i, the voltage magnitude and phase angle are denoted by V_i and θ_i respectively. Let P_i represent the active power injection of DIC-i, P_i^M the active power rating of DIC-i, and $\omega_i = (\dot{\theta}_i - \omega_b)$ the frequency deviation with ω_b being the nominal frequency set-point.

To facilitate theoretical developments of the proposed consensus droop control, the following assumptions are made:

(A1) The power lines are relatively short and thus lossless.

(A2) Each bus voltage magnitude V_i is regulated to stay constant.

(A3) All potential load variations can be fully supported by DICs without violating their active power rating limits.

(A4) Under the time-scale of frequency control, each load's output stays constant and is independent of frequency.

Assumption (A1) commonly holds for typical MGs. Constant voltage magnitude in (A2) can be ensured through the fast inner-loop voltage control design of DICs [39] and the voltage magnitude at all nodes can be assumed to be fixed [5], [7], [10]. (A3) can be guaranteed through system

planning at the MG deployment stage [38, Remark 1]. The assumption in (A4) is needed for developing and analyzing the proposed distributed frequency control algorithm by using the Kron reduction technique to simplify theoretical developments of the proposed intrusion detection methods. Although various network-preserving MG models have been considered in order to preserve the sparsity of the power grid and to characterize frequency dependency of load behaviors [6], [7], [40], these extensions will be explored in future work. Motivated by [40], it is potentially feasible to generalize the proposed PPD-based control design to include frequency dependent loads. Note that these assumptions have been made to facilitate the development of the proposed distributed frequency control algorithm. Nonetheless, the effectiveness of this algorithm will be demonstrated in Section V.

A. P-ω Droop Control

The operational objectives of a secondary active power control in MGs are two-fold:

(i) Zero frequency deviation from a nominal frequency under the steady-state (synchronization) such that

$$\omega_1 = \omega_2 = \cdots = \omega_n = 0. \tag{1}$$

(ii) Autonomous active power sharing among all DICs. Specifically, DICs share the total loads according to their nominal ratings such that

$$\frac{P_1}{P_1^M} = \frac{P_2}{P_2^M} = \cdots = \frac{P_n}{P_n^M}. \tag{2}$$

The power-frequency droop control has already been proposed to achieve these objectives [4]. This control design is motivated by mimicking the swing equation of a synchronous generator with zero machine inertia. It satisfies that

$$D_i\omega_i = P_i^M - P_i - p_i, \forall i \in \mathcal{N}. \tag{3}$$

The choice of droop coefficient D_i is determined in accordance with the DIC rating to maintain the uniform ratio of D_i/P_i^M across the network [7]. As detailed soon, a uniform droop-rating ratio is key to ensuring fair load sharing among DICs. In addition to the primary P-ω droop control, the control input p_i is included in (3) to set the reference power output for DIC-i. Since P_i^M and D_i are fixed parameters based on the size of DIC-i, one can only change the operating setpoints by judiciously choosing p_i. Under (A2), the model (3) holds because of the decoupled dynamics between frequency and voltage control. Accordingly, the frequency will be controlled by adjusting the active power only assuming voltage magnitudes stay constant [5], [7], [10].

B. MG Dynamics

Based on (A1), we separate the bus injection P_i into branch flows, as given by

$$P_i = \sum\nolimits_{j=1}^{m} f_{ij} = \sum\nolimits_{j=1}^{m} \frac{V_i V_j \sin\big(\theta_i - \theta_j\big)}{X_{ij}} \tag{4}$$

where f_{ij} denotes the line power flow from node-i to node-j in the MG and X_{ij} is the line reactance between these two nodes. Under the lossless assumption, $f_{ji} = -f_{ij}$ always holds. Under (A1), the angular difference across any power line is relatively small. Thus, the dynamics of the branch flow between bus-i and bus-j can be characterized by

$$\dot{f}_{ij} = B_{ij}\big(\omega_i - \omega_j\big) \tag{5}$$

where $B_{ij} = V_i V_j X_{ij} \cos(\theta_i^0 - \theta_j^0)/X_{ij}$ is a constant with θ_i^0 being the nominal phase angle at node-i. Interestingly, it turns out that by specially designing our ensuing distributed control, the update rules would include the network dynamics of (5) which is seamlessly implemented by its physical system.

C. Equilibrium Points of Droop Controlled DICs

By concatenating all scalar variables into the vector form, the desired equilibrium point fulfilling operational objectives of the droop control can be characterized as follows:

Proposition 1: Under the frequency-droop control rule (3), an equilibrium point $(\boldsymbol{\omega}^*, \boldsymbol{P}^*, \boldsymbol{p}^*)$ that fulfils objectives (1) and (2) must also satisfy

$$D_i^{-1}\big(P_i^M - P_i^* - p_i^*\big) = 0, \ \forall i \in \mathcal{N}, \tag{6a}$$

$$\frac{p_i^*}{D_i} = \frac{p_j^*}{D_j}, \ \forall i, j \in \mathcal{N}. \tag{6b}$$

This proposition is based on the synchronization of all DICs at the equilibrium point. By considering (5) at the equilibrium point, we have

$$\dot{f}_{ij}^* = B_{ij}\Big(\omega_i^* - \omega_j^*\Big) = 0, \forall i, j \in \mathcal{N} \cup \mathcal{N}_L.$$

This implies that a system-wise synchronization frequency is attained, i.e., $\omega_i^* = \omega_j^*, \forall i, j \in \mathcal{N}$. In addition, fulfilling (1) requires each $\omega_i^* = 0$. Thus, by substituting $\omega_i^* = 0, \forall i \in \mathcal{N}$ into (3), we obtain (6a). For (6b), we divide both side of (3) by P_i^M, as given by

$$\frac{P_i^*}{P_i^M} = 1 - \frac{D_i}{P_i^M}\frac{p_i^*}{D_i} - \frac{D_i}{P_i^M}\ \omega_i^*, \forall i \in \mathcal{N}.$$

Since the uniform setting of D_i/P_i^M, the proportional power sharing among DICs is equivalent to (6b).

D. Formulations by Consensus Optimization

Based on (6a) and (6b), the secondary control problem can be cast as a *consensus optimization* one:

$$\begin{aligned} \min_{\boldsymbol{p}} \ & \big\|\boldsymbol{P}^M - \boldsymbol{P} - \boldsymbol{p}\big\|_{\boldsymbol{D}^{-1}}^2 \\ \text{s.t.} \ & \frac{p_i}{D_i} = \frac{p_j}{D_j}, \ \forall i, j \in \mathcal{N} \end{aligned} \tag{7}$$

where $\boldsymbol{D} = \text{diag}(D_1, \ldots, D_n)$ is an $n \times n$ diagonal matrix and the weighted norm $\|\boldsymbol{v}\|_{\boldsymbol{D}}^2 = \boldsymbol{v}^T\boldsymbol{D}\boldsymbol{v}$. This is a quadratic optimization problem with equality constraints and thus can be solved using off-the-shelf convex solvers. Yet, the difficulty in solving (7) lies in that active power injection $\boldsymbol{P}$ is dynamical and dependent on the power network coupling. In our previous work [9], this issue is tackled by adopting a feedback approach to account for system dynamics. Nevertheless, since (5) provides a good approximation of network dynamics of MGs, we will propose a distributed frequency control

algorithm that can also consider the dynamics of active power injection $\boldsymbol{P}$.

To this end, each bus of the MG is connected to a DIC with the resultant network described by (3) and (4). Under the assumptions (A1)–(A4), we adopt the *Kron reduction* technique to obtain an equivalent reduced network. By eliminating all load buses and redistributing their corresponding loadings to buses in the subset $\mathcal{N}$ [41], the network is reduced to only containing n DIC buses. Such network contains one DIC at each bus, and all the branch flows of it can be well defined based on the frequency outputs of DICs. Under this equivalent network, by concatenating the reduced branch flows $\hat{\boldsymbol{f}} := \{\hat{f}_{ij}\}_{\forall i,j\in\mathcal{N}}$ and denoting the redistributed load $\boldsymbol{P}^L := \{P_i^L\}_{i\in\mathcal{N}}$, we have

$$\boldsymbol{P} = \boldsymbol{P}^L + \hat{\boldsymbol{H}}\hat{\boldsymbol{f}} \tag{8}$$

where the constant graph-based matrix $\hat{\boldsymbol{H}}$ is derived from (4) [42]. According to (A4), $\boldsymbol{P}^L$ is a constant vector and independent of frequency. Thus, given the equivalent network, the optimization problem (7) becomes

$$\begin{aligned} \min_{\hat{\boldsymbol{f}},\boldsymbol{p}} \ & \left\|\boldsymbol{P}^M - \left(\boldsymbol{P}^L + \hat{\boldsymbol{H}}\hat{\boldsymbol{f}}\right) - \boldsymbol{p}\right\|_{\boldsymbol{D}^{-1}}^2 \\ \text{s.t.} \ & \frac{p_i}{D_i} = \frac{p_j}{D_j}, \ \forall i,j \in \mathcal{N}. \end{aligned} \tag{9}$$

Worthy of noticing, under (A3), the active power rating limits of DICs are not violated. This gives the necessary and sufficient conditions for the existence of a power flow solution for the problem (9). As detailed soon, including $\hat{\boldsymbol{f}}$ as the optimization variable would seamlessly incorporate network power flow dynamics into the control update design.

III. Distributed Frequency Control

The DICs in the equivalent network naturally form an undirected and connected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Without loss of generality, we assume that the communication links among DICs corresponds to $\mathcal{G}$. This assumption is only used for notational simplicity. It turns out that as long as the communication network is fully connected, the proposed frequency control framework can attain the centralized performance in (7). For convenience, we define the optimization variable $x_i = p_i/D_i$ and the input variable $c_i(P_i) = (P_i^M - P_i)/D_i$. Note that P_i is locally measurable for DIC-i. $c_i(P_i)$ can also be expressed in terms of the branch flow vector $\hat{\boldsymbol{f}}$, as given by

$$c_i\left(\hat{\boldsymbol{f}}\right) = D_i^{-1}\left[P_i^M - \left(P_i^L + \sum\nolimits_{j=1}^n \hat{f}_{ij}\right)\right]. \tag{10}$$

By defining the neighbouring set of DICs connected to DIC-i as $\mathcal{N}_i := \{j|(i,j) \in \mathcal{E}\}$, we rewrite (9) as

$$\begin{aligned} \min_{\hat{\boldsymbol{f}},\boldsymbol{x}} \ & \sum\nolimits_{i=1}^n D_i(c_i - x_i)^2 \\ \text{s.t.} \ & x_i = x_j = 0, \forall i \in \mathcal{N}, \forall j \in \mathcal{N}_i \end{aligned} \tag{11}$$

where the equality constraints in (9) is equivalent to the ones in (11) under a connected graph $\mathcal{G}$.

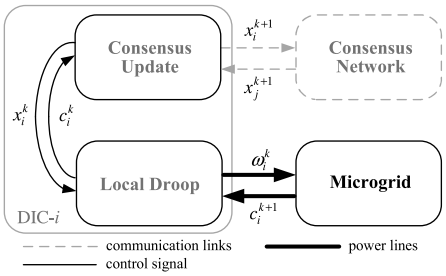


Fig. 1. Operation of DIC-i and its interaction with the MG and the consensus network under the proposed PDD-based consensus droop control.

A. Control Variables Updating

Introducing Lagrangian multipliers $\boldsymbol{\mu} = \{\mu_{ij}\}_{\forall i\in\mathcal{N},\forall j\in\mathcal{N}_i}$ for equality constraints in (11), we form the following Lagrangian function:

$$\mathcal{L}\left(\hat{\boldsymbol{f}}, \boldsymbol{x}, \boldsymbol{\mu}\right) = \sum_{i=1}^n \left[D_i(c_i - x_i)^2 + \sum_{j\in\mathcal{N}_i} \mu_{ij}\left(x_i - x_j\right)\right]. \tag{12}$$

Based on (12), we can adopt the PPD algorithm, which works by cyclically *partially* minimizing the primal variable $(\hat{\boldsymbol{f}}, \boldsymbol{x})$ and performing gradient ascent-based update on the dual variable $\boldsymbol{\mu}$ [43]. In order to reduce the communication cost, the proposed design keeps each dual variable μ_{ij} as local information for DIC-i. As to preserving the symmetric property of $\mu_{ij} = -\mu_{ji}$, where link-(i,j) associated dual variables μ_{ij} and μ_{ji} are updated by DIC-i and DIC-j separately, the dual variables $\boldsymbol{\mu}$ are simply initialized as $\boldsymbol{0}$. Thus, the PPD algorithm of (11) at DIC-i can be written as follows:

$$\dot{\hat{f}}_{ij} = \hat{B}_{ij}\left(\omega_i - \omega_j\right), \ \forall j \in \mathcal{N}_i, \tag{13a}$$

$$\boldsymbol{x} = \arg\min_{\boldsymbol{x}} \mathcal{L}\left(\hat{\boldsymbol{f}}, \boldsymbol{x}, \boldsymbol{\mu}\right), \tag{13b}$$

$$\dot{\mu}_{ij} = \rho\left(x_i - x_j\right), \ \forall j \in \mathcal{N}_i \tag{13c}$$

where $\hat{B}_{ij}$ is defined by (5) under the reduced network, and ρ is a positive step-size. Under this special step-size choice in (13a), it is equivalent to the branch flow dynamics in (5) for the reduced network using the mapping (8). Hence, the update in (13a) is naturally implemented by the active power flow coupling of the MG network in which varying power network topologies are accounted for. For the other two updates in (13), digital control implementations will convert them into the discrete-time counterpart. Thus, the control updates at $(k+1)$-st iteration for DIC-i with the step-size $\epsilon > 0$ are given by the following two steps [44]:

$$x_i^{k+1} = -D_i^{-1}\left(\sum\nolimits_{j\in\mathcal{N}_i} \mu_{ij}^k\right) + c_i^k, \tag{14a}$$

$$\mu_{ij}^{k+1} = \mu_{ij}^k + \epsilon\left(x_i^{k+1} - x_j^{k+1}\right), \ \forall j \in \mathcal{N}_i. \tag{14b}$$

We refer readers to Appendix A for detailed derivations of (14). In summary, under a proper step-size ϵ, the proposed control updates in (14) would achieve both control objectives (1) and (2) while accounting for the network power flow constraints. This leads to the following proposition.

Proposition 2: Given a proper step-size $\epsilon > 0$, the proposed control updates in (14) converges to an equilibrium point $(\hat{\boldsymbol{f}}^*, \boldsymbol{x}^*, \boldsymbol{\mu}^*)$ where $(\hat{\boldsymbol{f}}^*, \boldsymbol{x}^*)$ is the optimum of problem (11).

This proposition comes from the optimization problem (11), which is a linear quadratic one with a strongly convex objective function. Moreover, the *Slater condition* can be guaranteed by (A3). Hence, the strong duality property holds. Under a proper step-size choice of ϵ, the PPD algorithm (14) would converge linearly to $(\hat{\boldsymbol{f}}^*, \boldsymbol{x}^*, \boldsymbol{\mu}^*)$ which is indeed the optimum of (11) because of zero duality gap [43], [45]. Notice that $\hat{\boldsymbol{f}}$ directly corresponds to the bus injections P_i in (3) through the linear mapping (8). Now since the DICs' output frequencies are implemented as $\boldsymbol{\omega}^k = (\boldsymbol{c}^k - \boldsymbol{x}^k)$ according to (3), which in terms relates $(\hat{\boldsymbol{f}}^*, \boldsymbol{x}^*)$ to $(\boldsymbol{\omega}^*, \boldsymbol{P}^*, \boldsymbol{p}^*)$, the optimum in Proposition 2 indeed corresponds to the equilibrium point in Proposition 1.

Under a connected communication network, the operation of DIC-i at iteration k for the proposed distributed control can be illustrated in Fig. 1. Given the local dual variable $\{\mu_{ij}^k\}_{\forall j \in \mathcal{N}_j}$, the consensus update unit takes in the current local measurement c_i^k from the local droop controller and updates its primal variable x_i^{k+1} as (14a), which is then broadcast to the neighbouring DICs. Next, after receiving $\{x_j^{k+1}\}_{\forall j \in \mathcal{N}_i}$ via communication links from the neighbouring DICs, we update $\{\mu_{ij}\}_{\forall j \in \mathcal{N}_j}$ according to (14b). Meanwhile, the local droop unit adjusts its output frequency ω_i^k based on (3). The MG reacts to the variations in frequencies of DICs and reaches a new power flow dispatch according to (13a). This result in the updated measurement c_i^{k+1} which is used for the next iteration. Thanks to the communication network, each DIC can obtain neighbours' information and the proposed secondary control (14) is fully distributed. Thus, this distributed control is scalable and flexible with respect to the size of the network.

Remark 1 (Limited Communication): The performance of the distributed control design relies on the quality of bus-to-bus communication links, which we have assumed to be perfect thus far. Nonetheless, random link failures and messaging delays could arise due to either network congestion, or poor signal-to-noise ratios in some wireless environments. Additionally, denial of service attacks can also be thought of as limited communication connectivity. Thus, it is useful to investigate how the control scheme would work under imperfect communication. Informally speaking, considering the communication delay is bounded which can be guaranteed under modern communication infrastructure [46], and the time-varying communication graph $\mathcal{G}$ is connected on average [47], [48], it is possible to select a small enough stepsize ϵ to guarantee stability. Prior work has offered some analysis for algorithms under these conditions (see, e.g., [49], [50]). More recently, the stability analysis of the closed-loop system with dynamic communication topology and delays has been investigated by exploring the strict Lyapunov function under the framework of linear matrix inequailitied (LMI) [51]. The effect of clock mismatches on the stability and active power sharing was also studied in [52]. By following these recent studies, a rigorous proof of convergence properties under these conditions is an important future direction of this work.

B. Choice of the Step-Size

Albeit the convergence of the proposed control algorithm (14) can always be guaranteed, its implementation in MG control requires the proper design of update step-size ϵ. To this end, the notion of the Center-of-Mass (COM) frequency will be introduced.

Remark 2 (Center-of-Mass Frequency): The joint behavior of all DIC frequencies follows the *center-of-mass* (COM) frequency

$$\omega_c = \frac{\sum_{i=1}^n D_i \omega_i}{\sum_{i=1}^n D_i} = \frac{\sum_{i=1}^n \left(P_i^M - P_i - p_i\right)}{\sum_{i=1}^n D_i}. \tag{15}$$

This COM frequemcy directly relates the power balance to the system frequency in isolated MGs, which is independent of state and can be determined directly from power injections [53]. By integrating (14a) and (14b) into each DIC, ω_c can also be characterised as follows.

Remark 3 (Characteristics of ω_c): Initializing $\boldsymbol{\mu}^0 = \mathbf{0}$, we sum (14a) over all DICs

$$\sum\nolimits_{i=1}^n D_i \left(c_i^k - x_i^{k+1}\right) = \sum\nolimits_{i=1}^n \sum\nolimits_{j \in \mathcal{N}_i} \mu_{ij}^k = 0. \tag{16}$$

This leads to the following two observations:

1) The first updates of all x_i take the mismatch between power outputs of DICs as the initial condition, i.e.,
$$\sum\nolimits_{i=1}^n D_i x_i^1 = \sum\nolimits_{i=1}^n D_i c_i^0. \tag{17}$$
2) Substituting x_i^{k+1} in (16) into (15), ω_c at $(k+1)$-st is
$$\omega_c^{k+1} = \frac{\sum_{i=1}^n \left[D_i \left(c_i^{k+1} - c_i^k\right) + \sum_{j \in \mathcal{N}_i} \mu_{ij}^k\right]}{\sum_{i=1}^n D_i}. \tag{18}$$

Interestingly, any power imbalance is compensated after one iteration of the proposed update design (14). Under (A4) of a constant loading, we have the following equality: $\sum_{i=1}^n P_i = \sum_{i=1}^n D_i c_i^k$ Thus, $\omega_c^k = 0$ is assured for $k \geq 2$, and hence any changes in $\boldsymbol{p}$ has no effect on steady-state frequency ω_c^k.

To analyze these effects in the step-size design, we define a vector $\boldsymbol{\lambda}^k := \{\lambda_i^k\}_{\forall i \in \mathcal{N}}$ where $\lambda_i^k := \sum_{j \in \mathcal{N}_i} \mu_{ij}^k$, the updates in (14a) and (14b) become

$$\boldsymbol{x}^{k+1} = \left(-\epsilon \boldsymbol{D}^{-1}\boldsymbol{L} + \boldsymbol{I}_n\right)\boldsymbol{x}^k - \boldsymbol{D}^{-1}\boldsymbol{\lambda}^{k-1} + \left(\boldsymbol{c}^k - \boldsymbol{x}^k\right), \tag{19a}$$

$$\boldsymbol{\lambda}^{k+1} = \boldsymbol{\lambda}^k + \epsilon \boldsymbol{L}\boldsymbol{x}^{k+1} \tag{19b}$$

where $\boldsymbol{L}$ and $\boldsymbol{I}_n$ are the Laplacian of graph $\mathcal{G}$ and an $n \times n$ identity matrix, respectively. By substituting $\boldsymbol{\lambda}^k$ in (19b) into (19a), we have

$$\boldsymbol{x}^{k+1} = \boldsymbol{W}\boldsymbol{x}^k + \left(\boldsymbol{c}^k - \boldsymbol{c}^{k-1}\right) \tag{20}$$

where $\boldsymbol{W} = (-\epsilon \boldsymbol{D}^{-1}\boldsymbol{L} + \boldsymbol{I}_n)$. The linear dynamical system in (20) can be viewed as a consensus iteration of $\boldsymbol{x}^k$ with a disturbance depended on $(\boldsymbol{c}^k - \boldsymbol{c}^{k-1})$, which can be examined by the following weighted sum:

$$\mathbf{1}_n^T \boldsymbol{D}\left(\boldsymbol{c}^k - \boldsymbol{c}^{k-1}\right) = \sum\nolimits_{i=1}^n \left(P_i^k - P_i^{k-1}\right) \tag{21}$$

where $\mathbf{1}_n$ denotes the n-vector with all coefficients one. Based on (21), the disturbance is actually bounded by the total

load variations. Accordingly, selecting the step-size ϵ properly ensures matrix $\boldsymbol{W}$ to have all but one of the eigenvalues strictly within the unit circle. Therefore, the iterate $\boldsymbol{x}^{k+1}$ under the update in (20) would converge to the average consensus vector $\bar{\boldsymbol{x}}$ [54]. Detailed derivations for the convergence analysis are given in Appendix B.

IV. Attack Models and Countermeasures

Two attack models against the proposed distributed droop control are introduced in this section. The ensuing attack detection and localization strategies will also been examined. Such strategies are anomaly tests based on examining the secondary control objectives (1) and (2) under the steady-state.

We will consider constant malicious communication signal inputs which attempt to alter the MG operating points to be the worst-case attack scenario. As explained later, such attack can effectively drive the frequency deviation ω_i everywhere away from zero, which is of extremely high stability concerns. Regarding the attack strategy other than constant signals, it is possible to improve its design assuming the attacker had the full knowledge of the communication network as well as the detection mechanism. This scenario is, nonetheless, less likely from the practical standpoint. This is because almost all recent cyber attacks that have been deployed to the energy sector are agnostic to the system information; see, e.g., [55]. With the growing interest in MG cybersecurity research, studying these interactions between the design of attack strategies and counter-measure algorithms is an important direction for our future work.

Based on the complexity of the malicious inputs, the attack models are categorized into link and node attack scenarios, which both may further be extended to individual and coordinated cases. As the malicious inputs are implemented to alter the operation of consensus iterations, the formulation in (20) is adopted to constitute the basis for developing the ensuing attack models.

A. Link Attack

We first study the link attack scenario, where the malicious inputs are applied only to the information sent to specific neighbours of the attacked DICs. Given the undirected communication link-$(i,j) \in \mathcal{E}$, we define the attack signal ℓ_{ij} as the malicious input sent from DIC-j to DIC-i. Under this situation, the update equation of per DIC-$i \in \mathcal{N}$, can be re-written as:

$$\mu_{ij}^{k+1} = \mu_{ij}^{k} + \epsilon\Big[x_i^{k+1} - \Big(x_j^{k+1} + \ell_{ij}\Big)\Big],\ \forall j \in \mathcal{N}_i. \quad (22)$$

Reformulate (14a) and (22) into the compact form, (20) will be modified as

$$\boldsymbol{x}^{k+1} = \boldsymbol{W}\boldsymbol{x}^{k} + \epsilon \boldsymbol{D}^{-1}\tilde{\boldsymbol{L}}\boldsymbol{\ell} + \Big(\boldsymbol{c}^{k} - \boldsymbol{c}^{k-1}\Big) \quad (23)$$

where $\boldsymbol{\ell} = \{\ell_{ij}\}_{\forall i \in \mathcal{N}, j \in \mathcal{N}_i}$, and $\tilde{\boldsymbol{L}}$ specifies the malicious link indices of $\boldsymbol{\ell}$. Accordingly, $\boldsymbol{\lambda}$, the sum of dual variables, is manipulated by the malicious inputs. Thus, the change of the COM frequency ω_c^k will be modified as follows:

$$\omega_c^k - \omega_c^{k-1} = \frac{\mathbf{1}_n^T\big(\boldsymbol{\lambda}^{k-1} - \boldsymbol{\lambda}^{k-2}\big)}{\mathbf{1}_n^T\boldsymbol{D}\mathbf{1}_n} = \frac{-\epsilon\mathbf{1}_n^T\tilde{\boldsymbol{L}}\boldsymbol{\ell}}{\mathbf{1}_n^T\boldsymbol{D}\mathbf{1}_n}. \quad (24)$$

Interestingly, one may observe the structure of (24) and alter the frequency by coordinating the link attack inputs. This would lead to the following two cases:

1) Individual link attack: Malicious inputs ℓ_{ij}'s are appended to the information sent from DIC-j individually, resulting in $(\omega_c^k - \omega_c^{k-1}) \neq 0$ and $\omega_c^k \neq 0$.
2) Coordinated link attack: Multiple malicious inputs are deliberately deployed such that $(\omega_c^k - \omega_c^{k-1}) = 0$ and thus $\omega_c^k = 0$.

Note that these link-based attack input vectors will not lie in the null space of $\boldsymbol{L}$ in $\boldsymbol{W}$. In fact, the cases where $\tilde{\boldsymbol{L}}\boldsymbol{\ell}$ lies in the null space of $\boldsymbol{L}$ should be categorized into node attacks which is analyzed in Section IV-B. The system (23) can not reach the consensus among $\boldsymbol{x}$ in both the individual and coordinated cases. Albeit the system frequency behaves differently in these scenarios, the objective of power sharing can not be achieved in both cases. This would potentially lead to the violation of DIC ratings and thus damage the equipment. It is then imperative to identify the malicious links and isolate them from the network. To this end, we check the values of the dual variables which provide essential information on cyber-physical interactions. Because of not achieving a consensus, the dual variables of the proposed algorithm would keep integrating, i.e.,

$$\Big(\mu_{ij}^{k+1} - \mu_{ij}^{k}\Big) \neq 0, \forall i \in \mathcal{N}, \forall j \in \mathcal{N}_i. \quad (25)$$

Therefore, we can detect such attack by checking the convergence of the dual variables.

B. Node Attack

Under the node attack scenario, the malicious inputs are applied to the information sent to attacked nodes' neighbours, as well as the attacked nodes themselves. By denoting u_i as the malicious input at DIC-$i \in \mathcal{N}$, the update (14b) becomes

$$\mu_{ij}^{k+1} = \mu_{ij}^{k} + \epsilon\Big[\Big(x_i^{k+1} + u_i\Big) - \Big(x_j^{k+1} + u_j\Big)\Big],\ \forall j \in \mathcal{N}_i. \quad (26)$$

Reformulate (14a) and (26) into the compact form, we have

$$\boldsymbol{x}^{k+1} = \boldsymbol{W}\Big(\boldsymbol{x}^{k} + \boldsymbol{u}\Big) + \Big(\boldsymbol{c}^{k} - \boldsymbol{c}^{k-1}\Big). \quad (27)$$

Different from the link attack scenario, $(\boldsymbol{x}+\boldsymbol{u})$ lies in the null space of $\boldsymbol{L}$, the consensus is therefore achieved and the disturbance $(\boldsymbol{c}^k - \boldsymbol{c}^{k-1})$ diminishes. However, instead of reaching the true consensus vector $\bar{\boldsymbol{x}}$, a false consensus vector is attained from (27) and is dictated by $\boldsymbol{u}$. Recall that the proportional power sharing can always be achieved whenever $p_i/D_i, \forall i \in \mathcal{N}$ coincides across the network. Therefore, the steady-state DIC power output P_i is not affected by the node-based malicious attack. As to the frequency deviation, similar to the link attack scenario, we can examine the COM frequency ω_c^k as

$$\omega_c^k = \frac{\mathbf{1}_n^T\boldsymbol{D}\big[\boldsymbol{c}^k - \big(\boldsymbol{x}^k + \boldsymbol{u}\big)\big]}{\mathbf{1}_n^T\boldsymbol{D}\mathbf{1}_n} = \frac{-\mathbf{1}_n^T\boldsymbol{D}\boldsymbol{u}}{\mathbf{1}_n^T\boldsymbol{D}\mathbf{1}_n} \quad (28)$$

which leads to the following two different cases depending on the malicious signal $\boldsymbol{u}$:

1) Individual node attack: The attack input is implemented individually and results in a deviated system frequency, i.e., $\omega_c^k \neq 0$.

2) Coordinated node attack: Multiple attack inputs are purposely implanted such that $\omega_c^k = 0$.

The consensus among DICs can be achieved in both cases; hence, there is no dynamic changes that can be utilized as malicious detection/localization index in the system. Fortunately, the information from the inherent dual variable characteristics contains cognizance regarding such attack. In fact, once the consensus is achieved, the summations of the dual variables for normal DIC-i and attacked DIC-j can be determined as

$$\lambda_i^k = D_i\ \omega_c^k, \tag{29a}$$

$$\lambda_j^k = D_j\Big(\omega_c^k + u_j\Big) \tag{29b}$$

which implies anomaly arising among the dual variables that can be utilized to detect the attack event. Assuming $\{\lambda_j^k, D_j\}_{\forall j\in\mathcal{N}_i}$ is known at DIC-i, it is plausible to localized the node attack by comparing these values. Nonetheless, this would result in a higher communication cost due to exchanging these additional variables, and might even further jeopardize the control performance against the threat of malicious attacks.

Remark 4 (Malicious Local Measurements and Noisy Communication Channels): Albeit c_i^k at each DIC-i is the local feedback control signal, it may potentially be maliciously manipulated under the node attack scenario. As shown in Fig. 1, the value of c_i^k could be falsified while sending to the consensus updates unit. However, (14a) implies that appending constant offset to c_i^k has an equivalent effect of altering x_i^{k+1}. Consequently, the attack on c_i^k can be generalized to the aforementioned node attack model. As for the noisy communication channels, since a detection time window has been deployed to avoid misjudging normal load/generation disturbance, it can rule out the possibility of random perturbations or temporary bad data. If the data corruption environment lasts for a longer period of time, it may be equivalent ot have the communication links experience certain data corruption. Under this scenario, our countermeasure design could effectively isolate the source of corruption, as for malicious scenario. It is also true that with sufficient connectivity of the consensus network, one would be able identify and possibly correct the corrupted data [56]. Such operations are however beyond the scope of this work.

C. Detection/Localization Strategies

Although attack detection is possible based on characteristics of dual variables μ_{ij}^k as shown in (25) and (29), locating the attack sources is crucial for restoring MG to normal operations. To achieve this goal, let e_{ij} represent either the attack input on direct link-(i,j) or from neighbouring DIC-j, while $\forall m \in \mathcal{N}_i,\ m \neq j$ be the index of all other normal neighbouring nodes. The attack models in (22) and (26) can then be generalized as:

$$\mu_{ij}^{k+1} - \mu_{ij}^k = \epsilon\Big(x_i^{k+1} - x_j^{k+1}\Big) - \epsilon e_{ij}, \tag{30a}$$

$$\mu_{im}^{k+1} - \mu_{im}^k = \epsilon\Big(x_i^{k+1} - x_m^{k+1}\Big),\ \forall m \in \mathcal{N}_i,\ m \neq j. \tag{30b}$$

Algorithm 1 Attack Detection/Localization for DIC-i

Input: $\{\mu_{ij}^{k+1}, \mu_{ij}^k\}_{\forall j\in\mathcal{N}_i}$
Require: DIC-i has at least 2 neighbours
for $j \in \mathcal{N}_i$ **do**
  Compute $F_{ij}^k = |\mu_{ij}^k|$ and $\Delta_{ij}^k = |\mu_{ij}^{k+1} - \mu_{ij}^k|$;
  if $\max(F_{ij}^k) > 0$ *for a given time window* τ **then**
    if $\Delta_{ij}^k > 0$ **then**
      Link-(i,j) is recognized as malicious;
    else
      DIC-j is recognized as malicious;
Report events to the EMS of the MG.

Based on the proposed updates in (14), the effects of malicious input e_{ij} propagate to neighbouring nodes through the broadcast of x_i^k in a average consensus manner [57]. Therefore, it is expected that the mismatch term (30a) would dominate the one in (30b) due to the extra term ϵe_{ij} for link (i,j).

As to the node attack case, the consensus can be achieved and $(\mu_{ij}^{k+1} - \mu_{ij}^k)$ eventually diminishes. Note that during normal operation at no attack, we have $x_i^k = x_j^k,\ \forall j \in \mathcal{N}_i$ and $\boldsymbol{\mu}^k = \mathbf{0}$ with $\boldsymbol{\mu}^0 = \mathbf{0}$ properly initialized. Suppose the attack start at $t = k$, and the first two iterations upon the insertion of malicious input can be found as:

$$\begin{aligned}
\mu_{ij}^{k+1} &= -\epsilon\ e_{ij},\\
\mu_{im}^{k+1} &= 0,\\
\mu_{ij}^{k+2} &= \epsilon\Big[x_i^{k+2} - \Big(x_j^{k+2} + e_{ij}\Big)\Big] - \epsilon\ e_{ij}\\
\mu_{im}^{k+2} &= \epsilon\Big(x_i^{k+2} - x_m^{k+2}\Big).
\end{aligned}$$

Since the update of dual variable μ_{ij} in (14b) can also be viewed as an integration over $(x_i - x_j)$, which is the deviation in consensus, one can expect $|\mu_{ij}^k| > |\mu_{im}^k|$ as $k \to \infty$ due to a larger initial condition on ϵe_{ij}.

Thanks to the information from dual variables μ_{ij}^k, the following conclusions can be made for DIC-i within a given detection time window while experiencing an attack from either its direct link-$(i,j) \in \mathcal{E}$ or neighbouring DIC-$j \in \mathcal{N}_i$:

1) $\mu_{ij}^k \neq 0$ under either malicious signals of ℓ_{ij} or u_j according to (25) and (29). Also, $|\mu_{ij}^k|$ is larger compared to neighbouring ones associated with non-malicious inputs.
2) μ_{ij}^k diverges under the malicious signal ℓ_{ij} whereas μ_{ij}^k converge to a fixed point for a given node attack scenario.

According to these facts, the following detection indices for each DIC-i are introduced:

$$F_{ij}^k = |\mu_{ij}^k|,\ \text{and}\ \Delta_{ij}^k = |\mu_{ij}^{k+1} - \mu_{ij}^k| \tag{31}$$

which both can be obtained locally based on neighbouring information. Note that when $\max(F_{ij}^k) = 0$ for $j \in \mathcal{N}_i$, there is no anomaly in the system. Given these indices, the overall malicious attack detection and localization strategies are tabulated in Algorithm 1. To perform appropriate attack isolation actions, the report events are sent to the EMS.

D. Decision Making in EMS

In our proposed cyber-security framework, the task of isolating the malicious node or link from the consensus algorithm is handled by a centralized agent such as the EMS, which is an essential component in typical MG frameworks. Different from the communication links between DICs, which are implemented based on high interoperability and low cost principles, the links between the EMS and DICs, though at very low bandwidth/rate needs, should be regulated to be highly reliable for security and even privacy purposes [33]–[35]. Accordingly, they are implemented with different protocols or even separately from the one deployed among the DICs. Such implementation principle is also suggested by several works in the area of cybersecurity framework specifically for electrical grid systems [36], [37], which concluded that domain-specific cyberframework with multiple levels can better ensure the security of cyber-based control systems for power grids. Thus, based on the report events from all DICs through cyber layer different from the one among DICs, the centralized EMS can make reliable decision regarding the operations of distributed DICs.

In the present context, we assume that the attack inputs in the MG are sparse and do not exceed the theoretical bound under which the detection and localization strategies are no longer feasible. Under this assumption, the attack isolation strategies involve the following two stages: (i) identify the source of link or node attack; (ii) isolate the malicious link or node from the consensus network. Motivated by the work of [57], the mechanism behind the former stage adopts the characteristics of information propagation in typical consensus networks. Thus, once the malicious source is pinpointed, the attack isolation intelligence would either command to exclude attacked nodes from the consensus network under a node attack scenario, or remove the malicious links from the communication graph under a link attack scenario. Under either case, the reconfiguration of consensus network would be carried out if the communication graph is no longer connected after the attack isolation where both communication and power networks may have different topologies. Notice that the DICs being removed from the consensus network only turn back to local primary control mode, which still provide load sharing capability based on static droop settings. In summary, the decision making process tabulated in Algorithm 2 is capable of isolating malicious attacks. Worth to notice, although the attacked DIC would possibly send false report to the EMS, the decision making mechanism should be able to rule it out by comparing it with the reports from the attacked node's neighbors. The theoretical bound of false reports that maintains the EMS to function properly is indeed an interesting topic and would be a focus of our future study.

Algorithm 2 Decision Making in the EMS

Input: Events reported from all DICs
Require: Reports from all DICs received
for $i \in \mathcal{N}$ and $\mathcal{N}_i \geq 2$ **do**
  Link attack events:
  if *DIC-i reports link-*(i,j) *as malicious* **then**
    Examine the flag raised by DIC-*j*;
    if *DIC-j also indicates link-*(i,j) *as malicious* **then**
      Remove link-(i,j) from consensus network;
  Node attack events:
  if *DIC-i reports DIC-j as malicious* **then**
    Examine DIC-$m, \forall m \in \mathcal{N}_j$;
    if *DIC-*$m, \forall m \in \mathcal{N}_j$ *reports DIC-j as malicious* **then**
      Isolate DIC-*j* from the consensus network;
Reconfigure the consensus network in case of disconnected graph after the isolation action.

V. Simulation Verifications

The control block diagram of individual DIC-*i* is depicted in Fig. 2. The control architecture consists of both the primary droop control and distributed secondary frequency control levels. The local *P*-ω droop control in the primary level works with a sampling rate of 20kHz, while the distributed frequency control updates at a much slower rate of 10Hz due to limited communication infrastructure in practical implementations. Numerical tests of the 14-bus/6-DIC MG, as shown in Fig. 3 [6], are conducted to demonstrate the validity of the propose control. Physical details of the MG including pulse width modulation emulation are included in the tests and implemented in the real-time simulation environment Opal-RT. We fix the ratings of these DICs to be the same as 2kW while the droop gain is set uniformly as $5 \times 10^4 \mathrm{W} \cdot \mathrm{s} \cdot \mathrm{rad}^{-1}$. Three scenarios are studied as follows.

A. Case I: Convergence Analysis

1) Case I-A (Load Variations): A load variation from 50% to 100% of their ratings is implemented at $t = 35$. Such changes may represent a typical sudden increase in power demand. The resulting DIC active power injections and bus frequencies are shown in Fig. 4. Under this severe disturbance, the proposed distributed secondary control is still capable of achieving a zero system frequency deviation while maintaining proportional power sharing within a few seconds (80 iterations). Based on the amount of time to attain convergence which depends on system configuration, communication rate, and step-size choice, we design the attack detection time window τ to be slightly longer than this value. Fig. 4(b) also plots the COM frequency ω_c^k. Clearly, $\omega_c^k = 0, \forall k \geq 2$, and $\omega_i^k \to \omega_c^k$ as $k \to \infty$. This validates our claim in Remark 3.

2) Case I-B (Choice of the Step-Size): Given the system information, to ensure the eigenvalues of $\boldsymbol{W}$ within the unit circle, we calculate the step-size $\epsilon \leq 2 \times 10^4$ which guarantees the system stability. In this case, we set $\epsilon = 1 \times 10^4$ for $t < 35$ and change to $\epsilon = 2.1 \times 10^4$ at $t = 35$ for which the step-size stability criterion is violated. Fig. 5 plots the resultant active power outputs of DICs. Albeit the DICs operate in the steady-state during the first few seconds after the transition of step-size, they would eventually start to oscillate and diverge from their nominal states. This results in potential severe inverter rating violations. Hence, results in Section III-B are helpful in selecting ϵ if the full network information is available.

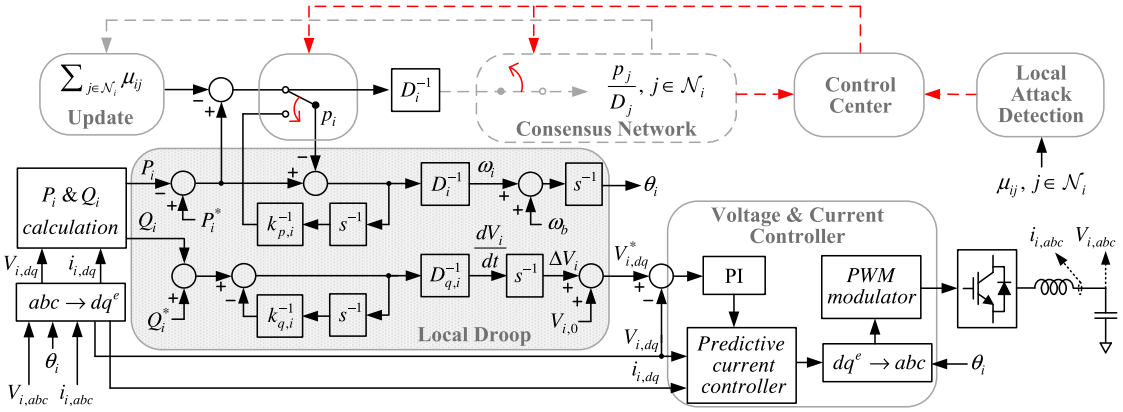


Fig. 2. Proposed control diagrams for individual DIC-*i*.

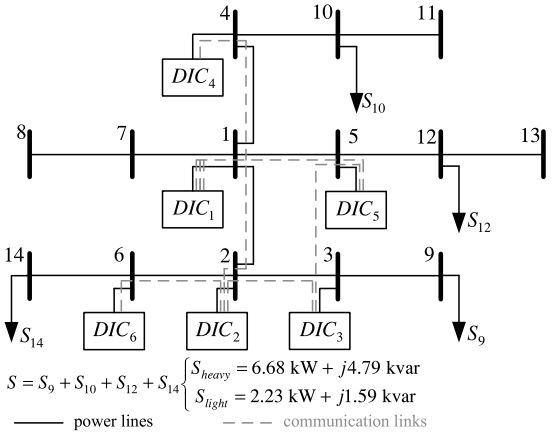


Fig. 3. One-line diagram of the 14-bus/6-DIC microgrid.

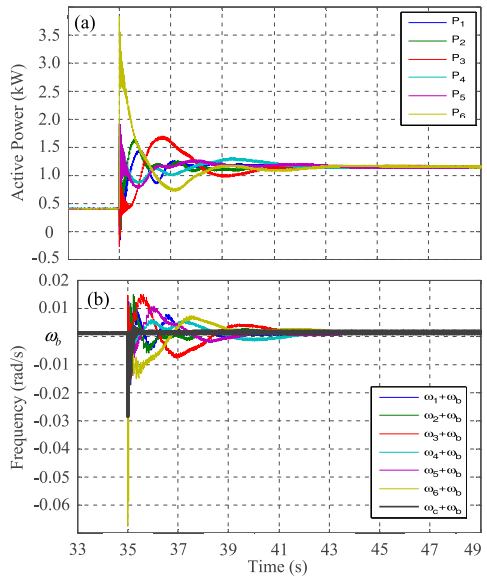


Fig. 4. Case I-A: DICs' (a) active power outputs; (b) droop frequencies.

B. Case II: Link Attack

Both the individual link attack and the coordinated link attack are considered.

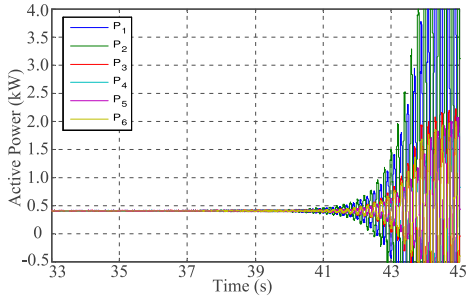


Fig. 5. Case I-A: DICs' active power outputs.

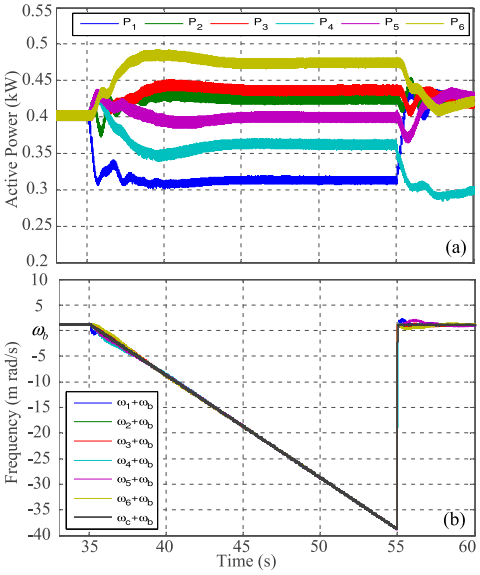


Fig. 6. Case I-A: DICs' (a) active power outputs; (b) droop frequencies.

1) Case II-A (Individual Link Attack): An attack signal, 20% of the steady-state x_1, is introduced at $t = 35$ to link-(1,4) and received by DIC-1. The resultant plot of all DICs responses is shown in Fig. 6. Clearly, due to this individual link attack, the COM frequency ω_c^k diverges as derived in (24). In addition, the power sharing is deteriorated since the consensus can no longer be attained. To validate our proposed detection indices, we plot $\{F_{1j}^k\}_{\forall j \in \mathcal{N}_1}$ in Fig. 7, which attests our claim

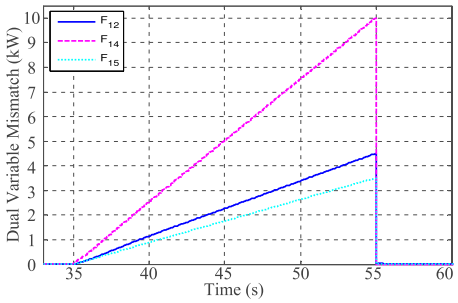


Fig. 7. Case I-A: Detection indices F_{ij}^k of DIC-1.

in Section IV-A that a dual variable associated with the malicious link would always be greater than the ones without the malicious attacks, i.e., F_{14}^k exhibits the largest detection index during the detection time window. According to Algorithm 1, one can then localize the malicious link-(1,4) based on the fact that F_{14}^k being the largest. For a 20-second detection time window, the malicious link-(1,4) is flagged and reported to the EMS. Since DIC-4 only has one link, the control center corresponding to Algorithm 2 disables DIC-4's communication and commands it to operate in primary droop mode at $t = 55$, which leads to no participation of power sharing operation from DIC-4 as depicted in Fig. 6(a). After eliminating malicious link-(1,4), the active power injections of all DICs except for DIC-4 reach a new consensus, and the steady-state system frequency is zero after $t = 55$.

2) Case II-B (Coordinated Link Attack): Under a more complex attack scenario, two malicious inputs received by DIC-1 and DIC-2 are simultaneously appended at $t = 35$ to link-(1,4) and link-(2,6), respectively. These two inputs which have opposite signs are both 20% of the steady-state x_1 in their magnitudes. Fig. 8 depicts the responses of all DICs. Under this attack, the COM frequency ω_c^k in (24) would remain at zero regardless of the coordinated attack inputs while the proportional power sharing no longer holds. Conventionally, such attack would be challenging to identify since ω_c^k stays at its optimal value throughout the process as shown in Fig. 8(b). Thanks to the information obtained from the dual variables, the detection indices of DIC-1 and DIC-2 are computed and plotted in Fig. 9. Similar results to the aforementioned individual link attack scenario, the malicious links are localized by the largest F_{14}^k and F_{26}^k of DIC-1 and DIC-2, respectively. Under a 20-second detection time window, malicious link-(1,4) and link-(2,6) are reported to the EMS. Since both DIC-4 and DIC-6 have only one neighbour, they are therefore removed from the consensus network after $t = 55$ and thus operate in primary droop mode. Fig. 8(a) then depicts the recovery of a proportional power sharing operation among all DICs except for the DIC-4 and DIC-6.

C. Case III: Node Attack

Similar to the previous case, both the individual node attack and the coordinated node attack are studied.

1) Case III-A (Individual Node Attack): With a similar setting to case II-A, a node attack signal with the same level is inserted to DIC-4 at $t = 35$, resulting a false received

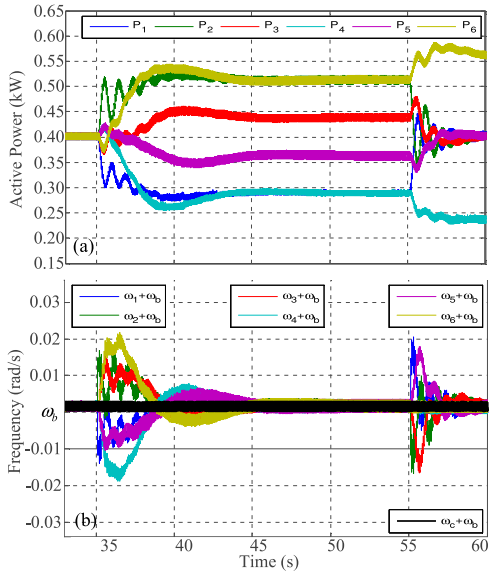


Fig. 8. Case I-B: DICs' (a) active power outputs; (b) droop frequencies.

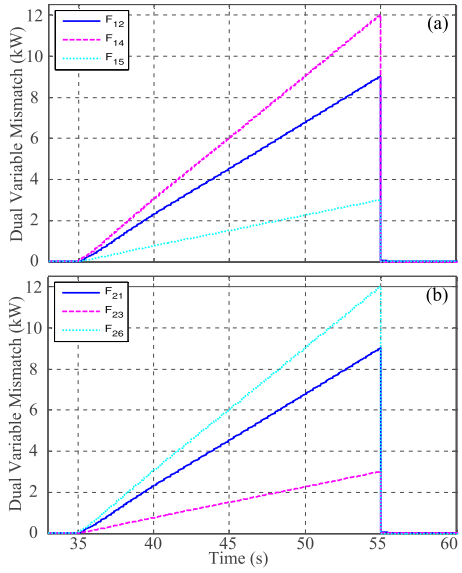


Fig. 9. Case I-B: Detection indices: (a) F_{ij}^k of DIC-1; (b) F_{ij}^k of DIC-2.

information at DIC-1. The consequent plots of DIC output responses and detection indices F_{ij}^k are illustrated in Fig. 10 and Fig. 11, respectively. Under this attack scenario, as $(\boldsymbol{x}^k + \boldsymbol{u})$ lies in the null space of $\boldsymbol{L}$, the COM frequency ω_c^k in (28) would depend on $\boldsymbol{u}$ and become non-zero while maintaining a proportional power sharing operation as shown in Fig. 10. This corroborates our attack analysis in Section IV-B. To isolate the attacked DIC-4, Algorithms 1 and 2 are executed. Accordingly, the EMS receives the flag reported by DIC-1 regarding the largest detection index of F_{14}^k, and therefore commands DIC-4 to switch to primary droop control mode at $t = 55$. After isolating malicious signals, similar results to earlier link attack scenarios can be observed in Fig. 10(a), where the nominal frequency is restored with a proper power sharing operation among all DICs except for DIC-4.

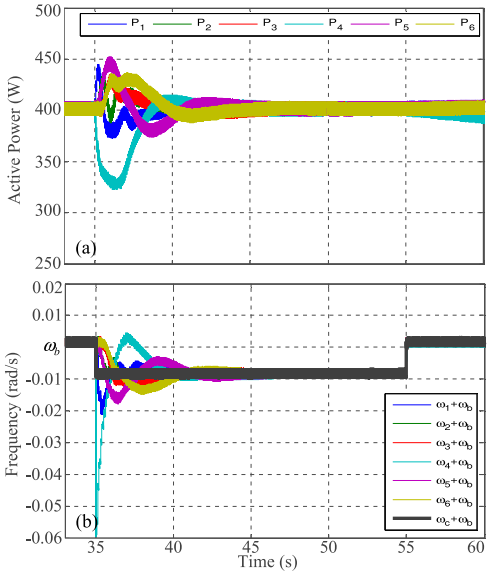


Fig. 10. Case II-A: DICs' (a) active power outputs; (b) droop frequencies.

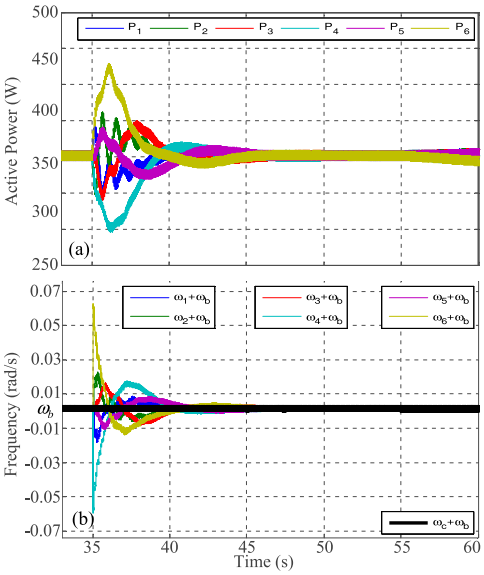


Fig. 12. Case II-B: DICs' (a) active power outputs; (b) droop frequencies.

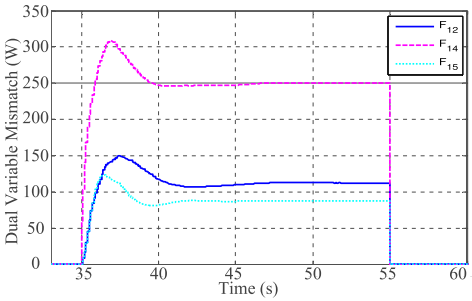


Fig. 11. Case II-A: Detection indices F_{ij}^k of DIC-1.

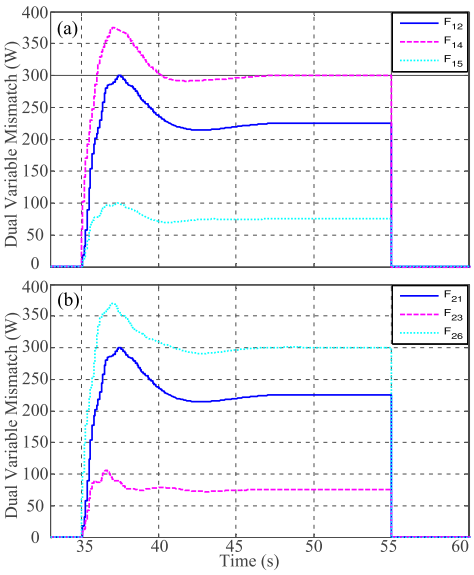


Fig. 13. Case II-B: Detection indices: (a) F_{ij}^k of DIC-1; (b) F_{ij}^k of DIC-2.

2) Case III-B (Coordinated Node Attack): To validate our proposed detection and isolation strategies under a coordinated node attack scenarios, we introduce malicious inputs which are simultaneously appended to DIC-4 and DIC-6 at $t = 35$. These inputs are with the same magnitude as 20% of the steady-state value of x_1 but opposite in their signs. Fig. 12 plots the resultant output response of DICs. As mentioned in Section IV-B, such attack scenario would not deviate the COM frequency ω_c^k away from its optimal value and deteriorate the power sharing scheme. As shown in Fig. 12, albeit the transient of $\omega_i^k, \forall i \in \mathcal{N}$ is disturbed by the coordinated node attack, the overall system would eventually settle back to the pre-attack conditions. Thanks to the information from the dual variables, the detection indices of DIC-1 and DIC-2 shown in Fig. 13 are used to localize these two attacks through the largest F_{14}^k and F_{26}^k. For a 20-second detection time window, both DIC-4 and DIC-6 are flagged and reported to EMS which commands the removal of DIC-4 and DIC-6 from the consensus network at $t = 55$. After the isolation of malicious inputs, a slight change of power sharing operation is illustrated in Fig. 12(a) due to switching of local droop control mode in DIC-4 and DIC-6. To sum up, the aforementioned test case II and III manifest the effectiveness of our proposed strategies in terms of detecting and isolating malicious link and node attacks.

VI. Conclusion

This paper develops a distributed secondary frequency control for DICs in isolated microgrids. The proposed control design consists of a local droop control in the primary level and a distributed PPD based algorithm in the secondary level. Albeit the network power flow constraints are not modelled in our optimization problem, the control updates by design seamlessly incorporate the dynamics of power flow. In addition, the convergence proof along with the stepsize choice for such control design are offered. Accordingly, the proportional power sharing would be guaranteed with a zero system frequency deviation. To consider the cyber-security aspects of control design, malicious attack models are investigated along with detection and localization strategies. Numerical tests

implemented in the real-time simulator demonstrate the effectiveness of the proposed control design in terms of achieving the objectives. Furthermore, the proposed dual variable-based detection indices provide sufficient information to locate and isolate the malicious link or node. For future work, we plan to extend our study to include limited communication scenarios with possible signal delay or loss of neighbors, complex attack schemes, e.g., time-varying attack signals, statistical studies of microgrid frequency deviation for better detection threshold design and to incorporate the distributed secondary voltage control design into the current framework.

APPENDIX A
DERIVATION OF UPDATE DESIGN (14)

Based on the Lagrangian $\mathcal{L}(\hat{\boldsymbol{f}}, \boldsymbol{x}, \boldsymbol{\mu})$ in (12), the derivation for the partial primal-dual (PPD) algorithm can be separated into two parts.

A. $\hat{f}_{ij}$-Update

According to (10), $\partial c_i(\hat{\boldsymbol{f}})/\partial \hat{f}_{ij} = -D_i^{-1}$, and the gradient of $\mathcal{L}$ with respect to the primal variable $\hat{f}_{ij}$ by chain rule is

$$\frac{\partial \mathcal{L}(\hat{\boldsymbol{f}}, \boldsymbol{x}, \boldsymbol{\mu})}{\partial \hat{f}_{ij}} = \big[-(c_i - x_i) + \big(c_j - x_j\big)\big]. \tag{32}$$

Setting a step-size of $\hat{B}_{ij}$ for this gradient decent direction would directly lead to (13a). In addition, since the droop controller is implemented as $\omega_i = (c_i - x_i)$ governed by (3), substituting ω_i into (32) gives

$$\dot{\hat{f}}_{ij} = \hat{B}_{ij}\big(\omega_i - \omega_j\big).$$

This can be exactly transformed to (5) based on the linear mapping of (8). Thus, the dynamics-based update (13a) would account for the network power flow constraints.

B. x-Update and μ-Update

The gradient of $\mathcal{L}$ with respect to the primal optimization variable x_i is

$$\frac{\partial \mathcal{L}\big(\hat{\boldsymbol{f}}, \boldsymbol{x}, \boldsymbol{\mu}\big)}{\partial x_i} = \left[-2D_i(c_i - x_i) + \sum_{j \in \mathcal{N}_i} \big(\mu_{ij} - \mu_{ji}\big)\right]. \tag{33}$$

Since $\mu_{ij} = -\mu_{ji}$ always holds by initializing $\boldsymbol{\mu}^0 = \mathbf{0}$, setting (33) to zero results in (14a). This update directly minimizes the dual function rather than following the primal gradient algorithm with respect to x_i. Thus, the so-termed *partial* primal-dual algorithm is adopted.

For the dual variable $\boldsymbol{\mu}$, the gradient of μ_{ij} is

$$\frac{\partial \mathcal{L}\big(\hat{\boldsymbol{f}}, \boldsymbol{x}, \boldsymbol{\mu}\big)}{\partial \mu_{ij}} = \big(x_i - x_j\big). \tag{34}$$

Given the step-size ϵ and the gradient ascent direction of (34), this boils down to the dual-ascent-based update in (14b), and thus completes the derivation.

APPENDIX B
CONVERGENCE OF CONSENSUS ITERATIONS (20)

Assume a proper step-size ϵ is chosen such that the iteration matrix $\boldsymbol{W}$ in (20) is stable. The work in [54] with slight modifications leads to

$$\lim_{k \to \infty} \boldsymbol{W}^k = \frac{\mathbf{1}_n \mathbf{1}_n^T}{\mathbf{1}_n^T \boldsymbol{D} \mathbf{1}_n} \boldsymbol{D}. \tag{35}$$

This differs from [54] because of the weighting matrix $\boldsymbol{D}^{-1}$ in $\boldsymbol{W}$. Since the disturbance $(\boldsymbol{c}^k - \boldsymbol{c}^{k-1})$ in (20) is bounded and assumed diminishing, the consensus iteration of (35) becomes

$$\lim_{k \to \infty} \boldsymbol{x}^k = \lim_{k \to \infty} \boldsymbol{W}^k \boldsymbol{x}^1 = \frac{\mathbf{1}_n \mathbf{1}_n^T}{\mathbf{1}_n^T \boldsymbol{D} \mathbf{1}_n} \boldsymbol{D} \boldsymbol{x}^1. \tag{36}$$

According to (17), it suggests that the initial condition for x_i takes the form of

$$\frac{\sum_{i=1}^n D_i x_i^1}{\sum_{i=1}^n D_i} = \mathbf{1}_n^T \frac{\boldsymbol{D}\boldsymbol{x}^1}{\mathbf{1}_n^T \boldsymbol{D} \mathbf{1}_n}. \tag{37}$$

Thus, the average consensus $\bar{\boldsymbol{x}}$ is given by

$$\bar{\boldsymbol{x}} = \mathbf{1}_n^T \frac{\boldsymbol{D}\boldsymbol{x}^1}{\mathbf{1}_n^T \boldsymbol{D} \mathbf{1}_n} \mathbf{1}_n = \frac{\mathbf{1}_n \mathbf{1}_n^T}{\mathbf{1}_n^T \boldsymbol{D} \mathbf{1}_n} \boldsymbol{D} \boldsymbol{x}^1 \tag{38}$$

which is the same as the steady-state value of $\boldsymbol{x}^k$ shown in (36).

REFERENCES

[1] D. E. Olivares, "Trends in microgrid control," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1905–1919, Jul. 2014.

[2] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuña, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—General approach toward standardization," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan. 2011.

[3] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1963–1976, Dec. 2012.

[4] M. C. Chandorkar, D. M. Divan, and R. Adapa, "Control of parallel connected inverters in standalone AC supply systems," *IEEE Trans. Ind. Appl.*, vol. 29, no. 1, pp. 136–143, Jan./Feb. 1993.

[5] J. W. Simpson-Porco, F. Dörfler, and F. Bullo, "Synchronization and power sharing for droop-controlled inverters in islanded microgrids," *Automatica*, vol. 49, no. 9, pp. 2603–2611, Sep. 2013.

[6] L.-Y. Lu and C.-C. Chu, "Consensus-based droop control synthesis for multiple DICs in isolated micro-grids," *IEEE Trans. Power Syst.*, vol. 30, no. 5, pp. 2243–2256, Sep. 2015.

[7] S. T. Cady, A. D. Domínguez-García, and C. N. Hadjicostis, "A distributed generation control architecture for islanded AC microgrids," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 5, pp. 1717–1735, Sep. 2015.

[8] G. Hug, S. Kar, and C. Wu, "Consensus + innovations approach for distributed multiagent coordination in a microgrid," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1893–1903, Jul. 2015.

[9] L.-Y. Lu, H. J. Liu, and H. Zhu, "Distributed secondary control for isolated microgrids under malicious attacks," in *Proc. IEEE NAPS*, Sep. 2016, pp. 1–6.

[10] M. Zholbaryssov and A. D. Domínguez-García, "Distributed enforcement of phase-cohesiveness for frequency control of islanded inverter-based microgrids," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 868–878, Sep. 2018.

[11] Z. Wang, F. Liu, S. H. Low, C. Zhao, and S. Mei, "Distributed frequency control with operational constraints, part I: Per-node power balance," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 40–52, Jan. 2019.

[12] Z. Wang, F. Liu, S. H. Low, C. Zhao, and S. Mei, "Distributed frequency control with operational constraints, part II: Network power balance," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 53–64, Jan. 2019.

[13] F. Dörfler and S. Grammatico, "Gather-and-broadcast frequency control in power systems," *Automatica*, vol. 79, pp. 296–305, May 2017.

[14] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.

[15] 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.

[16] H. J. Leblanc, H. Zhang, S. Sundaram, and X. Koutsoukos, "Consensus of multi-agent networks in the presence of adversaries using only local information," in *Proc. Int. Conf. High Confidence Netw. Syst. (HiCoNS)*, 2012, pp. 1–10.

[17] L. Tseng and N. H. Vaidya, "Fault-tolerant consensus in directed graphs," in *Proc. ACM Symp. Princ. Distrib. Comput. (PODC)*, 2015, pp. 451–460. [Online]. Available: http://doi.acm.org/10.1145/2767386.2767399

[18] B. Kailkhura, V. S. S. Nadendla, and P. K. Varshney, "Distributed inference in the presence of eavesdroppers: A survey," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 40–46, Jun. 2015.

[19] L. Su and N. Vaidya, "Multi-agent optimization in the presence of Byzantine adversaries: Fundamental limits," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2016, pp. 7183–7188.

[20] L. Su and N. H. Vaidya, "Fault-tolerant multi-agent optimization: Optimal iterative distributed algorithms," in *Proc. ACM Symp. Princ. Distrib. Comput. (PODC)*, 2016, pp. 425–434. [Online]. Available: http://doi.acm.org/10.1145/2933057.2933105

[21] 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.

[22] O. Vukovìc and G. Dàn, "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1500–1508, Jul. 2014.

[23] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[24] S. Nabavi and A. Chakrabortty, "An intrusion-resilient distributed optimization algorithm for modal estimation in power systems," in *Proc. IEEE CDC*, 2015, pp. 39–44.

[25] A. Teixeira, K. Paridari, H. Sandberg, and K. H. Johansson, "Voltage control for interconnected microgrids under adversarial actions," in *Proc. IEEE ETFA*, Sep. 2015, pp. 1–8.

[26] X. Liu *et al.*, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580, Mar. 2017.

[27] A. Farraj, E. Hammad, and D. Kundur, "A distributed control paradigm for smart grid to address attacks on data integrity and availability," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 70–81, Mar. 2018.

[28] W. Zeng, Y. Zhang, and M.-Y. Chow, "Resilient distributed energy management subject to unexpected misbehaving generation units," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 208–216, Feb. 2017.

[29] J. Duan and M.-Y. Chow, "A resilient consensus-based distributed energy management algorithm against data integrity attacks," *IEEE Trans. Smart Grid*, to be published.

[30] 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.

[31] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in an inverter-based microgrid," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1543–1551, Feb. 2019.

[32] T. R. Nudell, S. Nabavi, and A. Chakrabortty, "A real-time attack localization algorithm for large power system networks using graph-theoretic techniques," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2551–2559, Sep. 2015.

[33] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power Systems Interfaces*, IEEE Standard 1547, 2018.

[34] *IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected With Electric Power Systems*, IEEE Standard 1547.3-2007, 2007.

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

[36] T. Cruz *et al.*, "A cybersecurity detection framework for supervisory control and data acquisition systems," *IEEE Trans. Ind. Informat.*, vol. 12, no. 6, pp. 2236–2246, Dec. 2016.

[37] C.-S. Cho, W.-H. Chung, and S.-Y. Kuo, "Cyberphysical security and dependability analysis of digital control systems in nuclear power plants," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 3, pp. 356–369, Mar. 2016.

[38] X. Wu, C. Shen, and R. Iravani, "A distributed, cooperative frequency and voltage control for microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2764–2776, Jul. 2018.

[39] J. Schiffer *et al.*, "A survey on modeling of microgrids—From fundamental physics to phasors and voltage sources," *Automatica*, vol. 74, pp. 135–150, Dec. 2016.

[40] C. Zhao, U. Topcu, N. Li, and S. Low, "Design and stability of load-side primary frequency control in power systems," *IEEE Trans. Autom. Control*, vol. 59, no. 5, pp. 1177–1189, May 2014.

[41] F. Dörfler and F. Bullo, "Kron reduction of graphs with applications to electrical networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 60, no. 1, pp. 150–163, Jan. 2013.

[42] H. J. Liu, W. Shi, and H. Zhu, "Decentralized dynamic optimization for power network voltage control," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 3, no. 3, pp. 568–579, Sep. 2017.

[43] N. Li, C. Zhao, and L. Chen, "Connecting automatic generation control and economic dispatch from an optimization view," *IEEE Trans. Control Netw. Syst.*, vol. 3, no. 3, pp. 254–264, Sep. 2016.

[44] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge Univ. Press, 2004.

[45] Z.-Q. Luo and P. Tseng, "On the convergence rate of dual ascent methods for linearly constrained convex minimization," *Math. Oper. Res.*, vol. 18, no. 4, pp. 846–867, Nov. 1993. doi: 10.1287/moor.18.4.846.

[46] Z. Fan *et al.*, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 21–38, 1st Quart., 2013.

[47] A. Nedić and A. Ozdaglar, "Convergence rate for consensus with delays," *J. Glob. Optim.*, vol. 47, no. 3, pp. 437–456, Jul. 2010. [Online]. Available: https://doi.org/10.1007/s10898-008-9370-2

[48] A. Nedić, A. Olshevsky, and W. Shi, "Achieving geometric convergence for distributed optimization over time-varying graphs," *SIAM J. Optim.*, vol. 27, no. 4, pp. 2597–2633, Jan. 2017.

[49] F. Iutzeler, P. Bianchi, P. Ciblat, and W. Hachem, "Asynchronous distributed optimization using a randomized alternating direction method of multipliers," in *Proc. IEEE CDC*, 2013, pp. 3671–3676.

[50] P. Bianchi, W. Hachem, and F. Iutzeler, "A stochastic primal-dual algorithm for distributed asynchronous composite optimization," in *Proc. IEEE Glob. Conf. Signal Inf. Process. (GlobalSip)*, Dec. 2014, pp. 732–736.

[51] J. Schiffer, F. Dörfler, and E. Fridman, "Robustness of distributed averaging control in power systems: Time delays & dynamic communication topology," *Automatica*, vol. 80, pp. 261–271, Jun. 2017.

[52] R. R. Kolluri *et al.*, "Stability and active power sharing in droop controlled inverter interfaced microgrids: Effect of clock mismatches," *Automatica*, vol. 93, pp. 469–475, Jul. 2018.

[53] N. Ainsworth and S. Grijalva, "A structure-preserving model and sufficient condition for frequency synchronization of lossless droop inverter-based AC networks," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4310–4319, Nov. 2013.

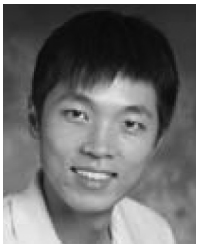
[54] L. Xiao and S. Boyd, "Fast linear iterations for distributed averaging," *Syst. Control Lett.*, vol. 53, no. 1, pp. 65–78, 2004.

[55] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[56] A. G. Phadke and J. S. Thorp, *Synchronized Phasor Measurements and Their Applications* (Power Electronics and Power Systems), 2nd ed. New York, NY, USA: Springer Int., 2017.

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

Lin-Yu Lu (M'17) received the B.S., M.S., and Ph.D. degrees in electrical engineering from National Tsing Hua University, Hsinchu, Taiwan, in 2009, 2011, and 2017, respectively. He is currently a Principal Engineer of Motor Drive Solution BU with Delta Electronics, Taoyuan, Taiwan. He had been a Visiting Scholar with Bigwood Systems, Inc., Ithaca, NY, USA, and the Department of Electrical and Computer Engineering, University of Illinois at Urbana–Champaign, IL, USA. His research interests include micro-grid control, cyber-security in micro-grids, and related power electronics applications.



Hao Jan (Max) Liu (M'17) received the B.S. degree in electrical and computer engineering from the Missouri University of Science and Technology, USA, in 2011 and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Illinois at Urbana–Champaign, USA, in 2013 and 2017, respectively. He is currently an Electrical Engineer Subject Matter Expert of power systems with Amazon Web Services. His research interests include the intersection of power systems, control, optimization, and machine learning. He was a recipient of the National Science Foundation East Asia and Pacific Summer Institutes Fellowship in 2015, the Second Best Paper Award at the 2016 *North American Power Symposium*, the Siebel Scholar Award in 2017, and the Siebel Energy Institute Seed Grand in 2018.

Hao Zhu (M'12) received the B.E. degree in electrical engineering from Tsinghua University, China, in 2006 and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Minnesota, USA, in 2009 and 2012, respectively. She is currently an Assistant Professor of electrical and computer engineering with the University of Texas at Austin, USA. She was a Post-Doctoral Researcher with the University of Illinois at Urbana–Champaign, USA, from 2012 to 2013 and an Assistant Professor of ECE from 2014 to 2017. Her research focus is on the algorithmic approaches for problems related to monitoring, optimization, and statistical learning in power systems. She was a recipient of the NSF CAREER Award in 2017, the Siebel Energy Institute Seed Grant, and the U.S. AFRL Summer Faculty Fellowship in 2016. She is also the Faculty Advisor and/or co-authored two best papers at the past North American Power Symposium, and currently a member of IEEE SPS SPTM Technical Committee.

Chia-Chi Chu (M'96–SM'15) received the B.S. and M.S. degrees in electrical engineering from National Taiwan University, Taipei, Taiwan, and the Ph.D. degree in electrical engineering from Cornell University, Ithaca, NY, USA, in 1996.

From 1995 to 1996, he was a member of the Technical Staff with Avant! Corporation, Fremont, CA, USA. From 1996 to 2006, he was a Faculty Member of electrical engineering with Chang Gung University, Taoyuan, Taiwan. He was a Visiting Scholar with the University of California at Berkeley, Berkeley, CA, USA, in 1999 and the University of Sydney, Sydney, NSW, Australia, in 2014. Since 2006, he has been a Faculty Member of electrical engineering with National Tsing Hua University, Hsinchu, Taiwan, where he is currently a Professor. His current research interests include power system stability and micro-grid control. He was a recipient of the Young Author Award from the IEEE Control of Oscillations and Chaos Conference in 1997 and the IEEE 8th International Conference on Power Electronics and Drive Systems in 2009. He is currently a Reviewer for several journal and conference publications, including IEEE TRANSACTIONS and conferences. He was a Guest Editor of the Special Issue on Complex Network Theory for Modern Smart Grid Applications of the IEEE JOURNAL OF EMERGING AND SELECTED TOPICS ON CIRCUITS AND SYSTEMS. From 2015 to 2017, he was the Chair of the Power and Energy Circuits and Systems Technical Committee of the IEEE Circuits and Systems Society.