Distributed Secondary Control for Isolated Microgrids under Malicious Attacks

Lin-Yu Lu*†, Hao Jan Liu† and Hao Zhu†

*Department of Electrical Engineering, National Tsing Hua University, Hsinchu, Taiwan
†Department of Electrical & Computer Engineering, University of Illinois, Urbana, IL, USA

***Abstract*—High penetration of distributed generation units in microgrids has caused severe frequency stability challenges. Coordinated secondary control can resolve this problem by judiciously dispatching active power resources using the communication infrastructure that supports the microgrid operations. In this paper, a distributed secondary control design for isolated microgrids is developed, and the effects of malicious attacks on the communication links are also investigated. The proposed design architecture consists of the local droop control in the primary level and a distributed dual-ascent based update in the secondary level. The objective of the latter is to achieve proportional power sharing while maintaining the system nominal frequency. Two types of malicious attacks on the distributed secondary control, namely, the link and node attacks, are investigated. To mitigate these attacks, detection and localization strategies are developed by checking the values of the dual-ascent update iterates. Numerical simulations on an isolated microgrid have been performed to demonstrate the effectiveness of the proposed control design and countermeasures against malicious attacks.**

***Index Terms*—Microgrid, Frequency Stability, Droop Control, Distributed Control, Cyber-Security, Malicious Attack.**

I. Introduction

As the penetration of renewable energy sources increases in microgrids (MGs), coordination of these mostly power-electronics interfaced resources becomes crucial to achieving system frequency stability [1]. Conventionally, the coordination of distributed energy resources (DERs) interface converters (DICs) follows from the power-frequency (P-f) droop control [2]. This class of control design is motivated by the swing equation dynamics of synchronous generators and can attain autonomous power sharing among DICs. However, the P-f droop control can not guarantee zero frequency deviation from the nominal grid frequency under varying operating points. Albeit this issue could be solved by appending a local frequency restoration mechanism, the power sharing relations would be violated accordingly [2]. Thus, new (de-)centralized control schemes are required for achieving these two goals simultaneously.

Recently, the hierarchical control of isolated MGs has become a standard operational paradigm [3], [4]. The droop control along with inner-loop voltage and current control at the primary control level is responsible for stabilizing the system frequency and voltage while providing power sharing capability. At the secondary control level, the system-wide information from all DICs is taken into account to minimize the steady-state mismatch. Traditional secondary control follows from a centralized communication architecture to manage system-wide resources. To reduce the communication cost and enhance DICs' plug-n-play ability, recent work has developed several distributed secondary control designs by utilizing the communications among neighboring DICs [5]–[7]. Although a distributed control design with DIC-to-DIC communication can indeed improve the system robustness to localized faults and communication failures, it also makes the microgrid infrastructure more prone to malicious cyber-attacks. Several recent efforts aim to investigate the cyber-physical security issues in monitoring transmission networks; see e.g., [8]–[10]. In addition to considering power system monitoring, a few papers have addressed the vulnerability of grid control systems by accounting for the cyber-physical coupling [11]–[13]. In the context of isolated MGs, the cyber-physical vulnerability of distributed frequency control design is of particular interest due to the low system inertia.

In our proposed design, the DICs are governed by P-f droop control in the primary level. As for the secondary level, we formulate the steady-state frequency mismatch minimization problem as a consensus optimization one. Assuming the communication graph among DICs is undirected and connected, we adopt the dual-ascent algorithm for the secondary problem which leads to a distributed control design. To adapt to the system dynamics that couples the DICs with the power network, we advocate modifying the dual-ascent updates originally derived for the steady-state objective to an online feedback-based design that incorporates the instantaneous power measurements. We show that the proposed control is able to obtain accurate power sharing while maintaining zero frequency deviation under appropriate control parameter choices. To study the impacts of cyber-attacks on the proposed distributed control design, we introduce attack models with either link-based or node-based adversary inputs. Compared with previous work in linear consensus algorithms under malicious attacks [14], [15], which requires system-wide information, we propose effective attack detection and localization strategies using only localized neighborhood information. Isolation of the malicious link or node can be determined by a centralized MG energy management system. Numerical tests on a DIC-based MG are performed using

This material is based upon work supported by the Department of Energy under Award Number DE-OE000078. Contact authors. Emails: {lyl,haoliu6,haozhu}@illinois.edu.

MATLAB® Simulink® to validate the proposed secondary control along with our countermeasure designs.

The remainder of this paper is organized as follows. Section II presents the droop control basics for isolated MGs while formulating the steady-state problem at the secondary control level. Section III develops the distributed frequency control design by adopting the dual-ascent updates for the steady-state problem. Attack models are introduced and the countermeasures are offered in Section IV. Section V presents the numerical results to validate our analytical claims.

II. P-f Droop Control in Isolated MicroGrids

We consider an isolated microgrid with $\mathcal{N}_B$ buses, where the subset of buses $\mathcal{N} := \{1, \cdots n\}$ is installed with DICs and the rest are load buses. Per bus-i, let the bus voltage magnitude and phase angle be denoted by V_i and θ_i, respectively. Let P_i represent the active power injection while P_i^* the active power rating of DIC-i.

For this isolated microgrid, we assume that all possible load variations can be supported by DICs without violating any limitation of the ratings. This assumption can be guaranteed in the planning phase of deploying microgrids. Thus, with the capability to support all loads, the operational objectives of a secondary active power control in microgrids are two-fold:

(i) Zero frequency deviation from a nominal frequency under steady-state.

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

$$\frac{P_1}{P_1^*} = \frac{P_2}{P_2^*} = \cdots \frac{P_n}{P_n^*}. \tag{1}$$

A class of DIC control, namely the power-frequency droop control, has been proposed to achieve these objectives [2]. This control design is motivated by mimicking the dynamical swing equation of a synchronous generator with zero machine inertia. Defining the frequency deviation $\omega_i := (\dot{\theta}_i - \omega_b)$ per DIC-i, it satisfies that

$$D_i \omega_i = P_i^* - P_i - p_i \tag{2}$$

where $\dot{\theta}_i = d\theta_i/dt$ and ω_b are the frequency of DIC-i and the nominal frequency set-point, respectively. The droop coefficient D_i is designed in accordance with the DIC rating. To this end, we set an uniform D_i/P_i* among DICs. Compared to conventional P-f droop control, an additional control input p_i is introduced in (2). Considering P_i^* and D_i are fixed parameters based on the size of DIC-i, one can only change the operating set-points of DIC-i by judiciously choosing p_i. To understand the systemwide operation characteristics of P-f droop controlled DICs, the following remark defines the shared system frequency to which the network converges.

Remark 2.1: The joint behavior of all DIC frequencies follows the *Center-Of-Mass* frequency

$$\omega_c = \frac{\sum_{i=1}^n D_i \omega_i}{\sum_{i=1}^n D_i} = \frac{\sum_{i=1}^n (P_i^* - P_i - p_i)}{\sum_{i=1}^n D_i}. \tag{3}$$

This remark directly relates the power balance to the system frequency in isolated microgrids, which is independent of state and can be determined directly from the power injections [16]. Furthermore, due to the proximity among DICs in a typical microgrid, all DICs should always converge to ω_c under steady-state. Albeit the individual bus frequency ω_i could be different under transient state, it is sufficient to only consider the slow dynamics of secondary control while neglecting the fast internal ones. Thus, we assume:

Assumption 2.1: All DICs share the same system frequency, i.e., $\omega_i = \omega_c, \forall i$, and converge to ω_c once the load condition and control inputs are settled.

For a given secondary control design under the steady-state, the objectives of controlling p_i are equivalent to the following two measures:

(i) Summing (2) over all DICs, which categorizes the frequency deviation:

$$n\omega_c = \sum\nolimits_{i=1}^n \frac{(P_i^* - P_i)}{D_i} - \sum\nolimits_{i=1}^n \frac{p_i}{D_i}. \tag{4}$$

By setting the right-hand-side of (4) to zero, a systemwise zero frequency deviation can be achieved.

(ii) Dividing (2) by P_i^*, which manifests the power sharing ratio P_i/P_i^*:

$$\frac{P_i}{P_i^*} = 1 - \frac{D_i}{P_i^*}\frac{p_i}{D_i} - \frac{D_i}{P_i^*}\omega_c. \tag{5}$$

Fixing $p_i/D_i = p_j/D_j, \forall i, j$ guarantees power sharing among DICs since $\frac{D_i}{P_i^*}, \forall i$ is the same by design.

Zero frequency deviation is achieved by ensuring $\omega_c = 0$. Thus, upon combining (2) and (3) and concatenating all scalar variables into vector form, the secondary control problem can be cast as a *consensus optimization* one, as given by

$$\begin{aligned} &\min_{\boldsymbol{p}} \ \frac{1}{2}\|(\boldsymbol{P}^* - \boldsymbol{P} - \boldsymbol{p})\|_{\boldsymbol{D}^{-1}}^2 \\ &\text{subject to } \frac{p_i}{D_i} = \frac{p_j}{D_j}, \ \forall i, j \end{aligned} \tag{6}$$

where $\boldsymbol{D} := \text{diag}\{D_i\}$ 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 program and can be solved using off-the-shelf convex solvers. Yet, the difficulty in solving (6) lies in the fact that active power injection $\boldsymbol{P}$ is dynamical and dependent on $\boldsymbol{p}$ because of power network coupling. Also, it is challenging to analytically determine the relation between these two vectors without modeling the microgrid network. In the following section, we propose to tackle this problem by adopting a feedback approach to account for system dynamics and to solve it in a distributed fashion.

III. Distributed Secondary Control Design

This section introduces our proposed distributed secondary control framework. We first neglect the internal dynamics coupling between $\boldsymbol{P}$ and $\boldsymbol{p}$, and thus the objective in (6) is fully separable. Furthermore, considering the communication network among the set of DICs as an undirected and connected graph $\mathcal{G} = (V, E)$, one can solve the consensus optimization problem (6) in a fully distributed fashion.

A. Update Design

For notational convenience, we define optimization variable $x_i = p_i/D_i$ and input variable $c_i = (P_i^* - P_i)/D_i$ where P_i is locally measurable. We denote the set of DICs connected to DIC-i as $\mathcal{N}_i := \{j|(i,j) \in E\}$. Hence, (6) can be reformulated as

$$\min_{\boldsymbol{x}} \sum\nolimits_{i=1}^{n} \frac{D_i}{2}(c_i - x_i)^2, \quad \text{subject to } x_i = x_j, \forall j \in \mathcal{N}_i \quad (7)$$

where the equality constraints in (6) is equivalent to the ones in (7) under a connected graph $\mathcal{G}$. Introducing Lagrangian multipliers $\tilde{\boldsymbol{\mu}} := \{\tilde{\mu}_{ij}\}_{\forall i, j \in \mathcal{N}_i} := \frac{1}{2}\boldsymbol{\mu}$ for the equality constraints in (7), we obtain the following Lagrangian function:

$$\mathcal{L}(\boldsymbol{x}, \tilde{\boldsymbol{\mu}}) = \sum_{i=1}^{n} \left[\frac{D_i}{2}(c_i - x_i)^2 + \sum_{j \in \mathcal{N}_i} \tilde{\mu}_{ij}(x_i - x_j) \right]. \quad (8)$$

Based on the Lagrangian function $\mathcal{L}(\boldsymbol{x}, \tilde{\boldsymbol{\mu}})$, we adopt the dual-ascent algorithm which works by cyclically minimizing the primal variable $\boldsymbol{x}$ and performing gradient ascent-based update on the dual variable $\tilde{\boldsymbol{\mu}}$. Its $(k+1)$-st iteration for DIC-i with stepsize $\epsilon > 0$ involves the following two steps [17]:

$$x_i^{k+1} = -D_i^{-1} \sum\nolimits_{j \in \mathcal{N}_i} \mu_{ij}^k + c_i^k \quad (9a)$$

$$\mu_{ij}^{k+1} = \mu_{ij}^k + \epsilon(x_i^{k+1} - x_j^{k+1}), \ \forall j \in \mathcal{N}_i \quad (9b)$$

where $\mu_{ij}^k = (\tilde{\mu}_{ij}^k - \tilde{\mu}_{ji}^k) = 2\tilde{\mu}_{ij}^k$ by initializing $\tilde{\boldsymbol{\mu}}^0 = \mathbf{0}$. The droop controller takes in x_i^{k+1} and updates according to (2). Compared with conventional static optimization problems, c_i^k serves as a feedback control signal to account for the power network coupling between $\boldsymbol{P}$ and $\boldsymbol{p}$. Thanks to the communication network, each DIC-i is able to exchange the primary variable x_i, which means the proposed secondary control (9) is fully distributed.

Remark 3.1: Since $\boldsymbol{\mu}^0 = \mathbf{0}$, we sum (9a) over all DICs

$$\sum\nolimits_{i=1}^{n} D_i(c_i^k - x_i^{k+1}) = \sum\nolimits_{i=1}^{n} \sum\nolimits_{j \in \mathcal{N}_i} \mu_{ij}^k = 0. \quad (10)$$

Thus, ω_c at $(k+1)$-st is

$$\omega_c^{k+1} = \frac{\sum_{i=1}^{n} D_i(c_i^{k+1} - c_i^k)}{\sum_{i=1}^{n} D_i}. \quad (11)$$

Interestingly, any power imbalance is compensated after one iteration of the proposed update design (9). Assuming constant loading, $\omega_c^k = 0$ is assured for $k \geq 2$. Thus, any changes in $\boldsymbol{p}$ has no effect on steady-state frequency ω_c^k .

B. Convergence Analysis

Performance analysis of the design is pursued assuming the microgrid to be without any load disturbance, which leads to $\sum_{i=1}^{n} P_i$ remain constant within the time period of interest. Carrying out the stability analysis for the proposed control, we define a vector $\boldsymbol{\lambda^k}$,i.e., $\lambda_i^k := \sum_{j \in \mathcal{N}_i} \mu_{ij}^k$, and $\boldsymbol{\omega}^k := (\boldsymbol{c}^k - \boldsymbol{x}^k)$ as the frequency deviations at time instant k. The update rules in (9) are

$$\boldsymbol{x}^{k+1} = (-\epsilon \boldsymbol{D}^{-1}\boldsymbol{L} + \boldsymbol{I}_n)\boldsymbol{x}^k - \boldsymbol{D}^{-1}\boldsymbol{\lambda}^{k-1} + \boldsymbol{\omega}^k, \quad (12a)$$

$$\boldsymbol{\lambda}^{k+1} = \boldsymbol{\lambda}^k + \epsilon \boldsymbol{L}\boldsymbol{x}^{k+1} \quad (12b)$$

where $\boldsymbol{L}$ and $\boldsymbol{I}_n$ are the Laplacian of graph $\mathcal{G}$ and an $n \times n$ identity matrix, respectively. Let $\boldsymbol{z}^k = \boldsymbol{x}^k - \boldsymbol{x}^{k-1}$ represent the iterative changes in $\boldsymbol{x}$, and (12) becomes

$$\begin{bmatrix} \boldsymbol{x}^{k+1} \\ \boldsymbol{z}^{k+1} \end{bmatrix} = \begin{bmatrix} -\epsilon \boldsymbol{D}^{-1}\boldsymbol{L} + \boldsymbol{I}_n & \boldsymbol{I}_n \\ -\epsilon \boldsymbol{D}^{-1}\boldsymbol{L} & \boldsymbol{I}_n \end{bmatrix} \begin{bmatrix} \boldsymbol{x}^k \\ \boldsymbol{z}^k \end{bmatrix} + \begin{bmatrix} \boldsymbol{\omega}^k - \boldsymbol{\omega}^{k-1} \\ \boldsymbol{\omega}^k - \boldsymbol{\omega}^{k-1} \end{bmatrix}. \quad (13)$$

Defining $\boldsymbol{x}^k = (\boldsymbol{x}_A^k + \boldsymbol{x}_\omega^k)$ and $\boldsymbol{z}^k = (\boldsymbol{z}_A^k + \boldsymbol{z}_\omega^k)$, we have

$$\begin{bmatrix} \boldsymbol{x}_A^{k+1} \\ \boldsymbol{z}_A^{k+1} \end{bmatrix} = \begin{bmatrix} -\epsilon \boldsymbol{D}^{-1}\boldsymbol{L} + \boldsymbol{I}_n & \boldsymbol{I}_n \\ -\epsilon \boldsymbol{D}^{-1}\boldsymbol{L} & \boldsymbol{I}_n \end{bmatrix} \begin{bmatrix} \boldsymbol{x}_A^k + \boldsymbol{x}_\omega^k \\ \boldsymbol{z}_A^k + \boldsymbol{z}_\omega^k \end{bmatrix}, \quad (14a)$$

$$\begin{bmatrix} \boldsymbol{x}_\omega^{k+1} \\ \boldsymbol{z}_\omega^{k+1} \end{bmatrix} = \begin{bmatrix} \boldsymbol{\omega}^k - \boldsymbol{\omega}^{k-1} \\ \boldsymbol{\omega}^k - \boldsymbol{\omega}^{k-1} \end{bmatrix}. \quad (14b)$$

For $k \geq 2$, note that (14b) always converges to $\omega_i^k = \omega_c^k = 0, \forall i$ according to Assumption 2.1 and Remark 3.1. Therefore, it is sufficient to analyze the stability of the proposed secondary control by considering the state-transition matrix of (14a)

$$\boldsymbol{A} = \begin{bmatrix} -\epsilon \boldsymbol{D}^{-1}\boldsymbol{L} + \boldsymbol{I}_n & \boldsymbol{I}_n \\ -\epsilon \boldsymbol{D}^{-1}\boldsymbol{L} & \boldsymbol{I}_n \end{bmatrix}. \quad (15)$$

Let $\mathcal{W} = \{W_1, \cdots W_n\} \in \mathbb{R}^n$ be the set of eigenvalues for the underlying graph Laplacian $\boldsymbol{L}$ with a property of $\{0 = W_1 < W_2 \leq W_3 \leq \cdots W_n\}$ [18], and similarly for $\boldsymbol{D}^{-1}\boldsymbol{L}$ with $\mathcal{U} = \{U_1, \cdots U_n\}$. Specifically, calculating $\mathcal{U}$ is equivalent to finding the eigenvalues of $\boldsymbol{D}^{-\frac{1}{2}}\boldsymbol{L}\boldsymbol{D}^{-\frac{1}{2}}$. Since $\boldsymbol{L} \succeq 0$ and $\boldsymbol{D} \succ 0$, definiteness of $\boldsymbol{D}^{-1}\boldsymbol{L}$ for some nonzero vector $\boldsymbol{v} \in \mathbb{R}^n$ is

$$\boldsymbol{v}^T \boldsymbol{D}^{-\frac{1}{2}} \boldsymbol{L} \boldsymbol{D}^{-\frac{1}{2}} \boldsymbol{v} = (\boldsymbol{D}^{-\frac{1}{2}}\boldsymbol{v})^T \boldsymbol{L} (\boldsymbol{D}^{-\frac{1}{2}}\boldsymbol{v}) \succeq 0. \quad (16)$$

Hence, the set of eigenvalues for matrix $\boldsymbol{A}$ is a function of $\mathcal{U} \in \mathbb{R}^n$

$$\lambda_{\boldsymbol{A}} = \left\{ \frac{1}{2}\left[(2 - \epsilon U) \pm \sqrt{\epsilon^2 U^2 - 4\epsilon U}\right] : U \in \mathcal{U} \right\}. \quad (17)$$

The stablity conditions for (15) can be guaranteed by selecting a proper stepsize $\epsilon > 0$ to ensure all the eigenvalues of matrix $\boldsymbol{A}$ to be within the unit circle. As the null-space of $\boldsymbol{L}$ lies in $\boldsymbol{L}\mathbf{1}_n = \mathbf{0}$, the average consensus solution for (15) is $\boldsymbol{x} = X\mathbf{1}_n$ for some $X \in \mathbb{R}$ and $\boldsymbol{z} = \mathbf{0}$ [18]. Notice that (11) already guarantees $\omega_c^k = 0$ for $k \geq 2$, $\sum_{i=1}^{n}(c_i^k - x_i^k) = n\omega_c^k = 0$ holds. To sum up, we have $(c_i - x_i) = 0, \forall i$ and $\boldsymbol{c} = \boldsymbol{x} = X\mathbf{1}_n$ because of the consensus algorithm. Consequently, the two operational objectives in (4) and (5) are achieved.

IV. Attack Models and Countermeasures

In this section, the attack models against the proposed distributed control are introduced, and the ensuing attack detection and localization strategies are proposed. We consider malicious communication signal inputs with constant value $\boldsymbol{u}$, which attend to alter the microgrid operating points.

A. Link Attack

We first study the link attack scenario, where the malicious inputs are applied only to the information sent to specific neighbor of the attacked node. Let u_{ij} be the malicious input received by node-i from link-$(i,j) \in E$, the update (9b) becomes

$$\mu_{ij}^{k+1} = \mu_{ij}^{k} + \epsilon[x_i^{k+1} - (x_j^{k+1} + u_{ij})]. \tag{18}$$

Combining (9a) and (18) into the compact form, we have

$$\begin{bmatrix} \boldsymbol{x}^{k+1} \\ \boldsymbol{z}^{k+1} \end{bmatrix} = \boldsymbol{A} \begin{bmatrix} \boldsymbol{x}^{k} \\ \boldsymbol{z}^{k} \end{bmatrix} + \begin{bmatrix} -\epsilon\bar{\boldsymbol{L}} \\ -\epsilon\bar{\boldsymbol{L}} \end{bmatrix} \begin{bmatrix} \boldsymbol{u}_l \\ \boldsymbol{u}_l \end{bmatrix} \tag{19}$$

where $\bar{\boldsymbol{L}}$ indicates the specific malicious links for $\boldsymbol{u}_l$. Accordingly, it is clear that the closed-loop system can not converge to an average consensus solution. Therefore, the information from neighbor nodes can be leveraged for the attack detection/localization purposes.

B. Node Attack

Under the node attack scenario, the malicious inputs are applied to the information sent to attacked node's neighbors, as well as the attacked node itself. By denoting u_i as the malicious input at node-i, the update (9b) becomes

$$\mu_{ij}^{k+1} = \mu_{ij}^{k} + \epsilon[(x_i^{k+1} + u_i) - (x_j^{k+1} + u_j)]. \tag{20}$$

Similar to the link attack scenario, the compact form becomes

$$\begin{bmatrix} \boldsymbol{x}^{k+1} \\ \boldsymbol{z}^{k+1} \end{bmatrix} = \boldsymbol{A} \begin{bmatrix} \boldsymbol{x}^{k} + \boldsymbol{u} \\ \boldsymbol{z}^{k} \end{bmatrix}. \tag{21}$$

For some $\hat{X} \in \mathbb{R}$, the closed-loop system under the node attack scenario converges to a different inaccurate solution with $(\boldsymbol{x} + \boldsymbol{u}) = \hat{X}\mathbf{1}_n$. Compared to a link attack scenario, the neighbors' information is not indicative in this case as each node will eventually achieve consensus. Fortunately, the dual variable μ_{ij}^k keeps the memory of initial disturbances introduced by malicious inputs, and thus can be employed for attack localization.

C. Detection/Localization Strategies

Based on the aforementioned observations, the following remarks are made for DIC-i under malicious attacks:

- Both link and node attacks: $(c_i^k - x_i^k) = \omega_i^k \neq 0$.
- Link attack: $(c_i^k - (x_j^k + u_{ij}))$ provides the measure of u_{ij}.
- Node attack: μ_{ij}^k tends to be larger compared with other dual variable associated with non-malicious nodes when node-j is compromised.

Accordingly, the following three different types of indices are proposed:

$$\begin{cases} E_i^k = \|c_i^k - x_i^k\| \\ E_{ij}^k = \|c_i^k - x_j^k\| \quad , \; j \in \mathcal{N}_i. \\ F_{ij}^k = \|\mu_{ij}^k\| \end{cases} \tag{22}$$

All the indices in (22) of node-i can be determined locally based on direct neighboring information. For a given threshold E_T for both E_i^k and E_{ij}^k, Fig. 1 illustrates the flowchart of the proposed attack detection and localization strategies, which can be descried as the followings:

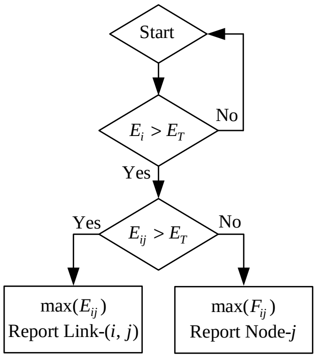

Fig. 1. Flowchart for attack detection and localization strategies.

- $E_i^k > E_T$ indicates a non-zero frequency deviation. Thus, the existence of malicious input should be localized and isolated. This task is then passed to the next two stages.
- $\max(E_{ij}^k) > E_T$ implies that the attack signal is either from link-(i,j) or propagates from node-j. After this event lasting for a pre-defined time period, node-i reports link-(i,j) as a malicious link to the microgrid control center.
- $\max(E_{ij}^k) < E_T$ indicates a node-based attack. Node-j from $\max(F_{ij}^k)$ is reported as a malicious node to the control center.

Based on the tolerable frequency deviation, E_T can be determined as both E_i^k and E_{ij}^k provide the measure of bus frequencies. The microgrid control center then makes decisions based on the information sent from DICs, and performs the following isolation strategies: (i) switch attacked node-j to the local primary control under a node attack event; (ii) stop node-i from utilizing the information on the malicious link-(i,j) under a link attack scenario.

V. Numerical Simulations

Control block diagrams of individual DIC-i are shown in Fig. 2, which consist of both the primary droop control and distributed secondary control levels and the attack detection/localization mechanisms. The local control in primary level works with a sampling rate of 20kHz for 10kHz PWM implementation, while the distributed control updates at a much slower rate of a 5Hz due to limited communication bandwidth. Fig. 3 depicts the system configuration of the underlying microgrid where DIC-1 is connected to both DIC-2 and DIC-3, and thus receives information from both neighbors. For ease of observation, we set the ratings of these DICs to be the same as 2kW. The simulations are performed using MATLAB$^{\circledR}$ Simulink$^{\circledR}$.

A. Case I: Load Variations

We increase the system loading from half to full at $t = 10$. The resulting DIC active power injections and bus frequencies are shown in Fig. 4. Within a few seconds, the secondary

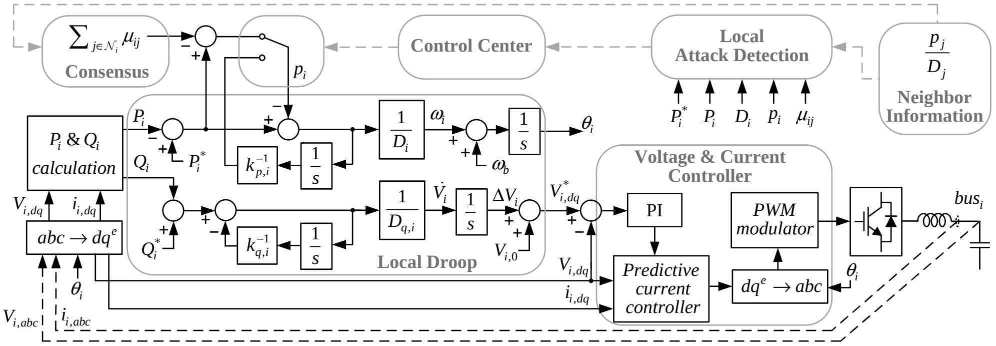

Fig. 2. Proposed control diagrams for individual DIC i.

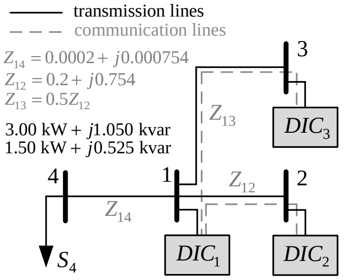

Fig. 3. One-line diagram of the 4-bus/3-DIC microgrid.

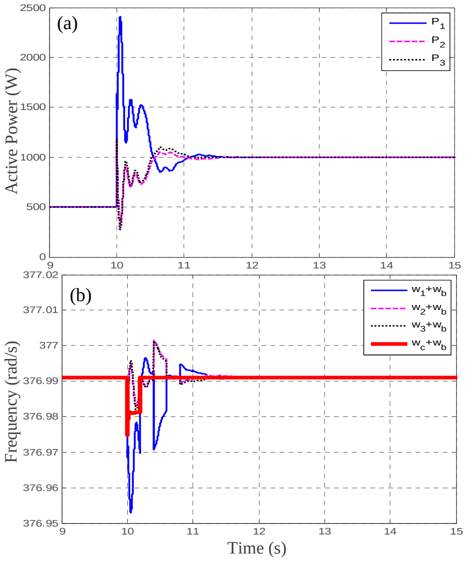

Fig. 4. Case I: DICs' (a) active power outputs; (b) droop frequencies.

control is able to achieve a zero frequency deviation and accurate power sharing under such a severe disturbance. Notice that ω_c^k in Fig. 4(b) remains at zero for $k \geq 2$ and $w_i^k \to w_c^k, k \to \infty$. This corroborates our earlier Assumption 2.1 and Remark 3.1. Therefore, as long as the detection time window is sufficient, the detection and localization mechanisms should not be affected.

B. Case II: Link Attack

An attack signal, 20% of the steady-state x_1, is introduced at $t = 10$ to link-(1,3) and received by DIC-1. The resulting plots of DIC output responses are shown in Fig. 5 while Fig. 6 depicts the detection indices of DIC-1. Clearly, the system does not converge as the bus frequencies in Fig. 5(b) indicates the existence of an attacker. In addition, Fig. 6 shows that there is a significant difference between E_{12}^k and E_{13}^k. Thus, for a given appropriate threshold E_T and a 10-second detection time window, the malicious link is confirmed to be link-(1,3) and reported to the control center based on the strategies in Fig. 1. Because there is only one link connected to DIC-3, the control center at $t = 20$ disables its communication and only allows it to update based on the primary droop control. Accordingly, Fig. 5(a) shows that the active power injections of DIC-1 and DIC-2 reach a new consensus after $t = 20$ while DIC-3 no longer participates in the operation of power sharing. Thus, the frequency is back to nominal at $t = 20$ after isolation of malicious link as shown in Fig. 5(b).

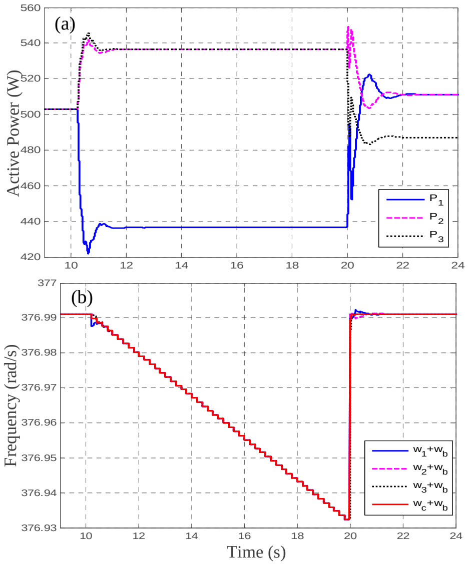

Fig. 5. Case II: DICs' (a) active power outputs; (b) droop frequencies.

C. Case III: Node Attack

For a similar setting as in case II, a node attack signal with the same level is inserted to DIC-3 at $t = 10$. The resulting plots of DIC output responses, detection indices E_{ij}^k and F_{ij}^k are illustrated in Fig. 7, Fig. 8 and Fig. 9, respectively. Under

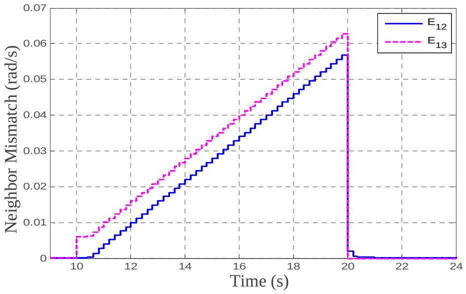

Fig. 6. Case II: Neighbor mismatches E_{ij} computed at DIC-1.

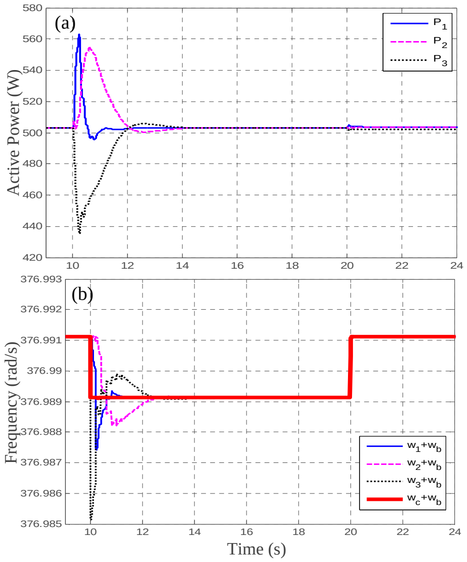

Fig. 7. Case III: DICs' (a) active power outputs; (b) droop frequencies.

this attack scenario, albeit ω_i^k and thereby E_i^k indicates the attack being identified, there is no difference among E_{ij}^k of DIC-1 as an inaccurate consensus is achieved. Fortunately, μ_{ij}^k has the memory of initial attack impacts as illustrated in Fig. 9. By comparing F_{12} and F_{13} of DIC-1, one can localize the attack at $t = 20$ and report to control center. Similarly to case II, DIC-3 is switched back to local droop control, a slight deviation in power sharing and a zero system frequency deviation are observed in Fig. 7(a) and Fig. 7(b) after $t = 20$, respectively. For future research directions, we plan to incorporate the secondary voltage and reactive power control designs and to investigate the cyber-security aspects of inverter control in isolated microgrids.

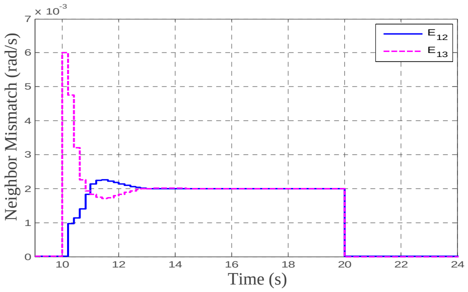

Fig. 8. Case III: Neighbor mismatches E_{ij} computed at DIC-1.

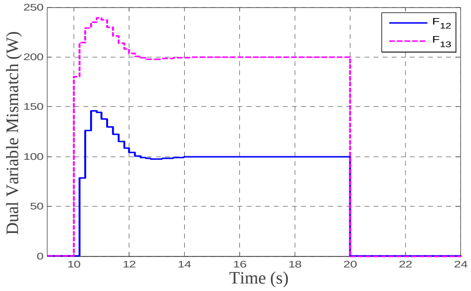

Fig. 9. Case III: μ-based detection indices F_{ij} computed at DIC-1.

References

[1] IEEE-PES Task Force on Microgrid Control, "Trends in microgrid control," *IEEE Trans. Smart Grid*, vol. 5, pp. 1905–1919, Jul. 2014.

[2] 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, pp. 136–143, Jan 1993.

[3] J. Guerrero, J. Vasquez, J. Matas, L. de Vicuña, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids – general approach toward standardization," *IEEE Trans. Ind. Electron.*, vol. 58, pp. 158–172, Jan 2011.

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

[5] F. Dörfler, J. Simpson-Porco, and F. Bullo, "Breaking the hierarchy: Distributed control & economic optimality in microgrids," *IEEE Trans. Control Netw. Syst.*, vol. PP, no. 99, pp. 1–1, 2015.

[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, pp. 2243–2256, Nov 2014.

[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, pp. 1717–1735, Sept 2015.

[8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, pp. 645–658, Dec 2011.

[9] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, pp. 210–224, Jan 2012.

[10] 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.

[11] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, pp. 580–591, March 2014.

[12] P. Srikantha and D. Kundur, "A der attack-mitigation differential game for smart grid security analysis," *IEEE Trans. Smart Grid*, vol. 7, pp. 1476–1485, May 2016.

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

[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, pp. 1495–1508, July 2011.

[15] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, pp. 90–104, Jan 2012.

[16] 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, pp. 4310–4319, Nov. 2013.

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

[18] R. Olfati-Saber, J. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, pp. 215–233, Jan. 2007.