A Distributed Strategy for Electricity Distribution Network Control in the face of DER Compromises

Devendra Shelar, Jairo Giraldo and Saurabh Amin

***Abstract*— We focus on the question of distributed control of electricity distribution networks in the face of security attacks to Distributed Energy Resources (DERs). Our attack model includes strategic manipulation of DER set-points by an external hacker to induce a sudden compromise of a subset of DERs connected to the network. We approach the distributed control design problem in two stages. In the first stage, we model the attacker-defender interaction as a Stackelberg game. The attacker (leader) disconnects a subset of DERs by sending them wrong set-point signals. The distribution utility (follower) response includes Volt-VAR control of non-compromised DERs and load control. The objective of the attacker (resp. defender) is to maximize (resp. minimize) the weighted sum of the total cost due to loss of frequency regulation and the cost due to loss of voltage regulation. In the second stage, we propose a distributed control (defender response) strategy for each local controller such that, if sudden supply-demand mismatch is detected (for example, due to DER compromises), the local controllers automatically respond based on their respective observations of local fluctuations in voltage and frequency. This strategy aims to achieve diversification of DER functions in the sense that each uncompromised DER node either contributes to voltage regulation (by contributing reactive power) or to frequency regulation (by contributing active power). We illustrate the effectiveness of this control strategy on a benchmark network.**

I. Introduction

Distributed energy resources (DERs) are fast becoming an integral part of electric distribution networks [1], [2], [3]. Classically, each DER was viewed as a single energy source (or negative load), and the main expectation was that the DERs contribute by way of active power production. Consequently, the first standards of DER integration (e.g., IEEE 1547) required that the DERs be simply disconnected during disturbances. However, with increasing penetration of DERs (e.g., photovoltaics and small-scale wind farms) in distribution networks, the operators are increasing their expectations from DERs. In nominal conditions, energy harvesting still remains the main objective. However, during contingency conditions, the DER inverters can be required to serve as *ancillary services*. In particular, the inverters can help maintain power factor and provide VAR support [3], [4]. Thus, network operators can benefit by coordinated control of DER inverters, where an almost instantaneous change of inverter set-points can provide ancillary services in a timely manner, thus reducing the need of controlling more expensive equipment such as capacitor banks or other voltage regulating devices.

This paper is motivated by two interrelated questions:

(i) How to exploit inverter capabilities such as control of reactive (kVAR) and active power (kW), to improve frequency and voltage regulation?

(ii) How to ensure that the distribution networks are able to operate securely in the face of deliberate or inadvertent modification to the data used by the DER controllers for local control strategies, or manipulation of the set-points sent by the control center to DERs?

To address these questions, we build on the hierarchical control architecture that defines the interactions between the control center and the DER controllers [5].[1] Under our assumptions, this interaction is enabled by a communication network. The primary control is locally implemented by each DER, and it is not considered further in this paper. In our problem formulation, the main control capabilities of interest are secondary and tertiary DER control.

For the purpose of secondary control, we assume that each DER controller executes local or distributed control actions to respond to the voltage and frequency deviations. For the purpose of tertiary control, we assume that the control center periodically communicates set-points to individual DERs based on the solution of an optimal power flow problem [6]. This communication is prone to adversarial manipulation.

Specifically, motivated by the recently published threat scenarios [7], our threat model considers strategic manipulation of optimal set-points that are sent from the control center to individual DER controllers; see Fig. 1. Such an attack would disrupt a subset of DERs, creating a sudden supply-demand mismatch. *Our objective is to design a distributed control strategy that aims to control the non-compromised DERs (and controllable loads, if available) toward maintaining both frequency and voltage regulation, starting from the time of attack until the time the bulk generator takes to restore adequate supply.*

Our main contributions are as follows: We model the attacker-defender interaction as a Stackelberg game model, where the attacker (leader) manipulates the set-points of a subset of DERs with the goal of inducing loss of frequency regulation and loss of voltage regulation (§III). The defender (follower) response includes the control of non-compromised DERs and controllable loads in a distributed manner. In Sec. IV, for the case of linear power flows, we compute the optimal defender response (Prop. 2), and present a greedy algorithm Algorithm 1 to compute the optimal solution of the Stackelberg game.

D. Shelar and S. Amin are with department of Civil and Environmental Engineering (CEE), Massachusetts Institute of Technology, MA, USA. Their work was supported by EPRI grant for "Modeling the Impact of ICT Failures on the Resilience of Electric Distribution Systems" contract ID: 10000621, and the NSF project "CPS: Frontiers: Collaborative Research: Foundations Of Resilient CybEr-physical Systems (FORCES)" (award number: CNS-1239054). Jairo Giraldo is with the Department of Electrical and Electronic Engineering, Universidad de los Andes, Colombia. His work was supported by Colciencias scholarship for doctoral studies 567. Emails: {shelard,amins}@mit.edu,ja.giraldo908@uniandes.edu.co

[1] A local sub-station can also mediate the control center to DER interactions.

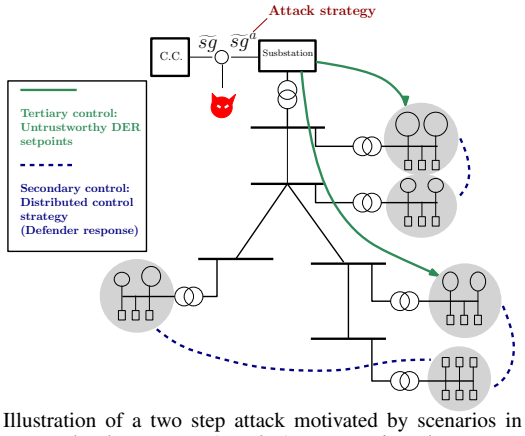

Fig. 1: Illustration of a two step attack motivated by scenarios in [7]. In the first stage, the threat agent (attacker) compromises the communication between the control center (or DER SCADA) and the substation, and introduces incorrect set-points. In the second stage, the substation selectively disconnects a number of DER nodes.

We present a distributed control strategy (see §V) which imposes that if each DER has the knowledge of the local voltage and frequency conditions, and also knows the *location of the worst-affected node*, then it should either contribute toward reducing frequency deviation from the grid frequency or contribute toward maintaining voltage regulation. Specifically, we show that there exists a *critical node* on the distribution network corresponding to the worst-affected node, which partitions the DERs into two disjoint subsets: All non-compromised nodes upstream (resp. downstream) of this critical node relative to the worst-affected node contribute toward reducing the frequency deviation (resp. maintaining voltage regulation) [2].

Finally, we compare by way of simulations on a 14-node test network (§VI) the performance of the aforementioned distributed control strategy (§V) against the centralized optimal defender response strategy (§IV).

II. Network Model

We summarize the network model of radial electric distribution systems [3], [8], and [9], . Consider a tree network of nodes and distribution lines $\mathcal{G} = (\mathcal{N} \cup \{0\}, \mathcal{E})$, where $\mathcal{N}$ denotes the set of all nodes except the substation (labeled as node 0), and let $N := |\mathcal{N}|$. Let $V_i \in \mathbb{C}$ denote the complex voltage at node i, and $\nu_i = |V_i|^2$ denote the square of the voltage magnitude. Let $I_j \in \mathbb{C}$ denote the current flowing from node i to node j on line $(i,j) \in \mathcal{E}$. The square of the magnitude of the current is denoted by $\ell_j = |I_j|^2$. A distribution line $(i,j) \in \mathcal{E}$ (also denoted by $i \to j$) has a complex impedance $z_j = r_j + \mathbf{j}x_j$, where $r_j > 0$ and $x_j > 0$ denote the resistance and inductance of the line (i,j), respectively, and $\mathbf{j} = \sqrt{-1}$.

For voltage regulation under *nominal* (no attack) conditions we require that:

$$\forall \quad i \in \mathcal{N}, \quad \underline{\nu}_i \le \nu_i \le \overline{\nu}_i, \tag{1}$$

where $\underline{\nu}_i = |\underline{V}_i|^2$ and $\overline{\nu}_i = |\overline{V}_i|^2$ are the *soft* lower and upper bounds on voltage quality at node i. Additionally, voltage magnitudes under *all* conditions satisfy the following *hard* safety bounds:

$$\forall \quad i \in \mathcal{N}, \quad \underline{\mu} \le \nu_i \le \overline{\mu}, \tag{2}$$

where $0 < \underline{\mu} < \min_{i\in\mathcal{N}} \underline{\nu}_i \le \max_{i\in\mathcal{N}} \overline{\nu}_i < \overline{\mu}$.

1) Bulk Generator Model: Assume that the substation node is connected to only one bulk generator, i.e., the bulk generator node is also a substation node. The voltage magnitude of this node $|V_0|$ is assumed to be constant and identical to that of bulk generator node, and let $|V_0| = 1$. Let $S_0(t)$ denote the complex power inflow from the bulk generator into the DN at time t; S_0^{nom} the complex power flowing into the substation node during *nominal* (no attack) conditions.

The bulk generator has a rotational inertia constant $\mathrm{M} = 2\pi J$, where J is its moment of inertia. It delivers AC power at frequency of $f_0(t)$ (in Hz), at time t. At node 0, we can model the frequency response of the network in terms of the mismatch between the active power generated by a synchronous generator and the active power delivered to the network. The dynamical equation governing the generator model is as follows:

$$\mathrm{M}\dot{f}_0 + \mathrm{D}f_0 = P_{m,0}(t) - P_{e,0}(t), \tag{3}$$

where M, D are the inertia and damping coefficients of the synchronous generator, $P_{m,0}(t)$ and $P_{e,0}(t) = \mathbf{Re}(S_0(t))$ denote the mechanical and electrical power at the generator [5]. At equilibrium $P_{m,0}(t) = P_{e,0}(t)$. Sudden changes in the loads or in the DERs' generation induces changes in $P_{e,0}$, causing changes in frequency, i.e., the frequency of the bulk generator deviates from its *nominal* frequency f_{nom}. We would like to compute $\Delta f_{0,max} := \min_t f_0(t) - f_{nom}$, which is the maximum deviation in the frequency of the bulk generator.

We assume that the mechanical power $P_{m,0}(t)$ is controlled by a Proportional-Integral (PI) controller with coefficients $\mathrm{K_P}$ and $\mathrm{K_I}$ [10].

Rewriting the terms in (3) as change from their respective nominal values, $P_{e,0}(t) = \mathbf{Re}(S_0^{\text{nom}}) + \Delta P_{e,0}(t)$, $f_0(t) = f_{nom} + \Delta f_0(t)$, applying a Laplace transform to (3), and under the assumption that the DER/load responses are fast (i.e., assuming that $\Delta P_{e,0}(s) = \Delta P_{e,0}/s$ is a step function), we obtain:

$$\Delta f_0(s) = \frac{-\Delta P_{e,0}/\mathrm{M}}{s^2 + (D + \mathrm{K_P})\mathrm{s}/\mathrm{M} + \mathrm{K_I}/\mathrm{M}}. \tag{4}$$

Using an appropriate change of variables, $\omega_n := \sqrt{\mathrm{K_I}/\mathrm{M}}$, $\xi := (D+\mathrm{K_P})/2\mathrm{M}\omega_\mathrm{n}$, one can obtain the second-order linear model [11]. Furthermore, the maximum frequency deviation can be computed as:

$$\Delta f_{0,max} = -H^{BG}\Delta P_{e,0} = -H^{BG}\mathbf{Re}(S_0 - S_0^{\text{nom}}). \tag{5}$$

where

$$H^{BG} = \frac{\omega_n}{\mathrm{K_I}} \exp\left(-\frac{\xi}{\sqrt{1-\xi^2}} \tan^{-1}\left(\frac{\sqrt{1-\xi^2}}{\xi}\right)\right).$$

For the frequency regulation under *nominal* conditions we require that:

$$\Delta\underline{f}_{th} \le \Delta f_{0,max} \le \Delta\overline{f}_{th}, \tag{6}$$

where $\Delta\underline{f}_{th}$ and $\Delta\overline{f}_{th}$ are the *soft* lower and upper bounds on the maximum frequency deviation of the bulk generator. Additionally, for the safety of the bulk generator, its maximum frequency deviation must satisfy the following safety bounds under *all* conditions:

$$\Delta\underline{f}_0 \le \Delta f_{0,max} \le \Delta\overline{f}_0, \tag{7}$$

[2] We assume that the communication between individual DERs is not compromised by the adversary. We plan to relax this assumption in our future work.

where $\Delta\underline{f}_0 < \Delta\underline{f}_{th} \leq \Delta\overline{f}_{th} < \Delta\overline{f}_0$. The bulk generator will be tripped off (disconnected from the DN) if these constraints are not met.

2) Load and DER Model: We refer to our working paper [12] for details on the load and DER[3] models. We assume constant power load model. Let $sc_i \in \mathbb{C}$ denote the power consumed at node i which is constrained as follows:

$$sc_i \leq \mathrm{sc}_i^{\mathrm{nom}}, \tag{8}$$

where $\mathrm{sc}_i^{\mathrm{nom}} \in \mathbb{C}$ denotes the *nominal* power demand.

Let sg_i denote the power generated by DER i; sg_i^{nom} the *nominal* power generated by DER i; $\overline{sg}_i$ the apparent power capability of its inverter; $\mathrm{sp}_i = \mathbf{Re}(\mathrm{sp}_i) + \mathbf{j}\mathbf{Im}(\mathrm{sp}_i)$ the set-point of DER i, where $\mathbf{Re}(\mathrm{sp}_i)$ and $\mathbf{Im}(\mathrm{sp}_i)$ are its real and reactive components. The power generated at each node is constrained as follows:

$$\forall \quad i \in \mathcal{N}, \quad sg_i \leq \mathrm{sp}_i \in \mathcal{S}_i, \tag{9}$$

where $\mathcal{S}_i \coloneqq \{\mathrm{sp}_i \in \mathbb{C} \quad | \quad \mathbf{Re}(\mathrm{sp}_i) \geq 0 \text{ and } |\mathrm{sp}_i| \leq \overline{sg}_i\}$. Let $\mathcal{S} \coloneqq \prod_{i\in\mathcal{N}} \mathcal{S}_i$ denote the set of configurable set-points; see [3], [4]. If a node i has no DER connected to it, then $sg_i = 0 + 0\mathbf{j}$.

The frequency and voltage evolution for inverter-based DERs can also be described by a droop control model that allows each DER to track its desired DER set-point [13]. However, due to the high inertia of the bulk generator, its frequency dominates all the frequency changes in the network [14]. Therefore, in this paper, we assume that the frequency of all nodes rapidly synchronize with the main grid frequency.

In addition to (6)-(7), the maximum frequency deviation of the network must lie within the permissible range for the DERs to keep operating.

$$\Delta\underline{f}_{der} \leq \Delta f_{0,max} \leq \Delta\overline{f}_{der}, \tag{10}$$

where $\Delta\underline{f}_{der}$, $\Delta\overline{f}_{der}$ are the minimum and maximum frequency deviations for which the DERs can stay connected to the network. The range of allowable frequency deviations for the DERs is a subset of the allowable frequency deviation range for the bulk generator, i.e., $[\Delta\underline{f}_{der}, \Delta\overline{f}_{der}] \subset [\Delta\underline{f}_0, \Delta\overline{f}_0]$. As a result, if the frequency deviations go beyond the allowable frequency range for the DERs, more DERs may disconnect leading to network-wide failures [15]. We assume $[\Delta\underline{f}_{th}, \Delta\overline{f}_{th}] \subset [\Delta\underline{f}_{der}, \Delta\overline{f}_{der}]$.

Several works have addressed the problem of combining the OPF with the dynamic behaviour of the system [16], [17]. However, these works mainly focus on the frequency regulation assuming lines having positive inductance, but no resistance (i.e. the $\mathbf{r}/\mathbf{x}$ ratio ≈ 0). In this work, we consider simultaneous voltage and frequency regulation under a wide range of DER failure and attack scenarios using a distributed DER control strategy (§V), although we only consider a static network model.

3) Power Flow Equations: The 3-phase balanced nonlinear power flow (NPF) on line $(i,j) \in \mathcal{E}$ is given by [8]:

$$S_j = \textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + sc_j - sg_j + z_j\ell_j \tag{11a}$$

$$\nu_j = \nu_i - 2\mathbf{Re}(\bar{z}_j S_j) + |z_j|^2\ell_j \tag{11b}$$

$$\ell_j = \frac{|S_j|^2}{\nu_i} \tag{11c}$$

$$S_0 = \textstyle\sum_{k:(0,k)\in\mathcal{E}} S_k, \tag{11d}$$

[3]We call the complete DER-inverter assembly as a DER node.

where $S_j = P_j + \mathbf{j}Q_j$ denotes the complex power flowing from node i to node j on line $(i,j) \in \mathcal{E}$, and $\bar{z}$ is the complex conjugate of z; (11a) and (11d) are the power conservation equations; (11b) relates the voltage drop and the power flows; and (11c) is the current-voltage-power relationship.

For the NPF model (11), we define a state as follows:

$$\mathrm{x} \coloneqq \left[\nu, \ell, sc, sg, S, S_0, \Delta f_{0,max}\right],$$

where $\mathrm{x} \in \mathbb{R}_+^{2N} \times \mathbb{C}^{3N+1} \times \mathbb{R}$, ν, ℓ, sc, sg, and S are row vectors of appropriate dimensions, and $\Delta f_{0,max}$ is a scalar. Let $\mathcal{F}$ denote the set of all states x that satisfy (5), (8), (9) and the NPF model (11), and define the set of all states with *no reverse power flows* as follows:

$$\mathcal{X} \coloneqq \{\mathrm{x} \in \mathcal{F} | S \geq 0\}.$$

The linear power flow (LPF) approximation of (11) is:

$$\widehat{S}_j = \textstyle\sum_{k:(j,k)\in\mathcal{E}} \widehat{S}_k + sc_j - sg_j \tag{12a}$$

$$\widehat{\nu}_j = \widehat{\nu}_i - 2\mathbf{Re}(\bar{z}_j\widehat{S}_j) \tag{12b}$$

$$\widehat{\ell}_j = \frac{|\widehat{S}_j|^2}{\widehat{\nu}_i} \tag{12c}$$

$$S_0 = \textstyle\sum_{k:(0,k)\in\mathcal{E}} S_k \tag{12d}$$

where $\hat{\mathrm{x}} \coloneqq [\widehat{\nu}, \widehat{\ell}, sc, sg, \widehat{S}, \widehat{S}_0, \Delta\widehat{f}_{0,max}]$ is a state of the LPF model, and analogous to the NPF model, define the set of LPF states $\hat{\mathrm{x}}$ with no reverse power flows as $\widehat{\mathcal{X}}$. Note that, although equation (12c) is non-linear, it can be invoked after all the voltages and power flows are calculated using linear equations (12a)-(12b).

Notation and definitions: All vectors are row vectors, unless otherwise stated. For two vectors c and d, $c \odot d$ denotes their Hadamard product. For complex numbers $e, f \in \mathbb{C}$, $e \cdot f$ denotes their dot product, i.e., $e \cdot f = \mathbf{Re}(\bar{e}f)$, where $\bar{e}$ is the complex conjugate of e, and $\angle e \coloneqq \arctan\frac{\mathbf{Im}(e)}{\mathbf{Re}(e)}$ denotes the angle made by the vector e with the real axis. Following [18], for any given node $i \in \mathcal{N}$, let $\mathcal{P}_i$ be the path from the root node to node i. We say that node j is an *ancestor* of node k ($j \prec k$), or equivalently, k is a successor of j *iff* $\mathcal{P}_j \subset \mathcal{P}_k$. We define the *relative ordering* $\preceq_i$, with respect to a "pivot" node i as follows:

- j *precedes* k ($j \preceq_i k$) *iff* $\mathcal{P}_i \cap \mathcal{P}_j \subseteq \mathcal{P}_i \cap \mathcal{P}_k$.
- j *strictly precedes* k ($j \prec_i k$) *iff* $\mathcal{P}_i \cap \mathcal{P}_j \subset \mathcal{P}_i \cap \mathcal{P}_k$.
- j is at the *same precedence level* as k ($j =_i k$) *iff* $\mathcal{P}_i \cap \mathcal{P}_j = \mathcal{P}_i \cap \mathcal{P}_k$.

We define the common path impedance between any two nodes $i, j \in \mathcal{N}$ as the sum of impedances of the lines in the intersection of paths $\mathcal{P}_i$ and $\mathcal{P}_j$, i.e., $Z_{ij} \coloneqq \sum_{k\in\mathcal{P}_i\cap\mathcal{P}_j} z_k$, and denote the resistive (real) and inductive (imaginary) components of Z_{ij} by R_{ij} and X_{ij}, respectively.

We make the following assumptions throughout the paper:

$(\mathbf{A0})_0$ Voltage and Frequency quality: In no attack (nominal) conditions, both $\mathcal{X}$ and $\widehat{\mathcal{X}}$ satisfy the voltage quality bounds (1) as well as the frequency quality bounds (6).

$(\mathbf{A0})_1$ Safety: Safety bounds (2) and (7) are always satisfied, i.e., $\forall\ (\psi,\phi) \in \Psi \times \Phi$, $\forall\ \mathrm{x}(\psi,\phi) \in \mathcal{X}$, $\underline{\mu}\mathbf{1}_N \leq \nu \leq \overline{\mu}\mathbf{1}_N$, and $\Delta\underline{f}_0 \leq \Delta f_{0,max} \leq \Delta\overline{f}_0$.

$(\mathbf{A0})_2$ No reverse power flows: Power flows from the substation node towards the downstream nodes, i.e., $\widehat{S} \geq 0$. This implies that $\forall\ \hat{\mathrm{x}} \in \widehat{\mathcal{X}}$, $\widehat{\nu} \leq \nu_0\mathbf{1}_N$; similarly, for NPF model. We will denote assumptions $(\mathbf{A0})_0$-$(\mathbf{A0})_2$ by **(A0)** .

III. Modeling and Problem Formulation

A. Two-Stage Stackelberg Game

We consider a 2-stage sequential game between an attacker and a defender, where the attacker's objective is to compromise DERs, and induce loss of voltage regulation (LOVR) and frequency regulation (LOFR).

- **Stage 1:** The attacker chooses a subset of DERs, and compromises them by manipulating their set-points according to a strategy $\psi := [\mathrm{sp}^{\mathrm{a}}, \delta] \in \Psi_M$;
- **Stage 2:** The defender responds by choosing the set-points of the uncompromised DERs, and impose load control at one or more nodes according to a strategy $\phi := [\mathrm{sp}^{\mathrm{d}}, \gamma] \in \Phi(\psi)$.

In this Stackelberg game, Ψ_M denotes the set of attacker strategies in Stage 1; and $\Phi(\psi)$ denotes the set of defender actions in Stage 2. Formally, the attacker-defender [AD] game is defined as follows:

$$[\mathrm{AD}] \quad \mathcal{L} \;:=\; \max_{\psi\in\Psi_M} \min_{\phi\in\Phi(\psi)} \mathrm{L}(\mathrm{x}(\psi,\phi)) \tag{13}$$

$$\text{s.t. } \mathrm{x}(\psi,\phi) \in \mathcal{X} \tag{14a}$$

$$sc(\psi,\phi) = \gamma \odot \mathrm{sc}^{\mathrm{nom}} \tag{14b}$$

$$sg(\psi,\phi) = \delta \odot \mathrm{sp}^{\mathrm{a}} + (\mathbf{1}_N - \delta) \odot \mathrm{sp}^{\mathrm{d}} \tag{14c}$$

$$\Delta f_{0,max}(\psi,\phi) = -H^{BG}\mathbf{Re}(S_0(\psi,\phi) - S_0^{\mathrm{nom}}), \tag{14d}$$

where (14b) specifies that the *actual power consumed* at node i is equal to the nominal power demand scaled by the defender's corresponding load control parameter $\gamma_i \in [\underline{\gamma}_i, 1]$.

The constraint (14c) models the net effect of the attacker choice $(\mathrm{sp}_i^{\mathrm{a}}, \delta_i)$ in Stage 1, and the defender choice $\mathrm{sp}_i^{\mathrm{d}}$ in Stage 2 on the *actual power generated* at node i. Thus, (14c) is the *adversary model* of [AD] game: the DER i is compromised *if and only if* it was targeted by the attacker ($\delta_i = 1$). Specifically, if i is compromised, $\mathrm{sp}_i = \mathrm{sp}_i^{\mathrm{a}}$, where $\mathrm{sp}_i^{\mathrm{a}} \in \mathcal{S}_i$ is the false set-point chosen by the attacker (different from the nominal set-point). The set-points of non-compromised DERs are governed by the defender, i.e., if DER i is not compromised ($\delta_i = 0$), then $\mathrm{sp}_i = \mathrm{sp}_i^{\mathrm{d}}$. Note that our adversary model assumes that the DER power output, sg, quickly attain the set-points specified by (14c), i.e., the model does not consider dynamic set-point tracking.

The constraint (14d) models the maximum frequency deviation due to the sudden active power imbalance.

The loss function in [AD] is defined as follows:

$$\mathrm{L}(\mathrm{x}(\psi,\phi)) \;:=\; \mathrm{L}_{\mathrm{VR}}(\mathrm{x}) + \mathrm{L}_{\mathrm{FR}}(\mathrm{x}), \tag{15}$$

where L_{VR} denotes the cost due to loss of voltage regulation; and L_{FR} the cost due to loss of frequency regulation. These costs are defined as follows:

$$\mathrm{L}_{\mathrm{VR}}(\mathrm{x}) \;:=\; ||W \odot (\underline{\nu} - \nu)_+||_\infty \tag{16a}$$

$$\mathrm{L}_{\mathrm{FR}}(\mathrm{x}) \;:=\; C(\Delta\underline{f}_{th} - \Delta f_{0,max})_+, \tag{16b}$$

where $W \in \mathbb{R}^N_+$, and $C \in \mathbb{R}_+$. Here, W_i is the weight assigned to violation of voltage bound, and L_{VR} is the maximum over all nodes the weighted non-negative difference between the lower bound $\underline{\nu}_i$ and nodal voltage square ν_i; C is the cost of unit frequency deviation, $\Delta\underline{f}_{th}$ is the lower threshold bound with which we will compare the system frequency deviation, and $\Delta f_{0,max}$ is the maximum frequency deviation attained as a result of the sudden supply-demand mismatch.

Note that, this is a bilevel optimization formulation in which the inner decision variables are continuous variables whereas the outer decision variables are mixed-integer variables. In our attack model, the attacker can reduce the active and reactive power, which leads to reduction in frequency and voltage. So, we compare the frequency and the voltages with only the lower bounds and not the upper bounds, in the objective function.

We now describe each stage in more detail:

1) Stage 1 [Attack]: Let $\Psi_M := \mathcal{S} \times \mathcal{D}$ denote the set of attacker actions, where

$$\mathcal{D} \;:=\; \{\delta \in \{0,1\}^{\mathcal{N}} \quad | \quad ||\delta||_0 \le M\}, \tag{17}$$

and $M \le |\mathcal{N}|$ is the maximum number of DERs that the attacker can compromise. It is reasonable to assume that the number of compromised DERs is bounded by M, as this limits the resources available to the attacker and/or the scope of actions that the attacker can take over a single substation.

The DER set-points introduced by the attacker are denoted by sp^{a}. We further introduce a vector $\delta \in \{0,1\}^N$. The vector δ denotes the state of the DERs. If DER node i is compromised, then $\delta_i = 1$ and $\mathrm{sp}_i = \mathrm{sp}_i^{\mathrm{a}}$. If the DER node is not compromised, then $\delta_i = 0$. We denote the complete attacker strategy by $\psi = [\mathrm{sp}^{\mathrm{a}}, \delta]$.

The objective of the attacker is to impose an attack strategy $\psi \in \Psi$ to violate the frequency constraint (6) and voltage constraint (1) at one or more nodes, and to induce the defender to respond by satisfying only partial demand at a subset of nodes (although the cost of load control is not included in the loss function).

2) Stage 2 [Defender Response]: Let $\underline{\gamma}_i \ge 0$ denote the minimum permissible fraction of load control at node i, and define the set of Stage 3 defender actions as:

$$\Phi(\psi) := \mathcal{S} \times \Gamma,$$

where $\Gamma := \prod_{i\in\mathcal{N}}[\underline{\gamma}_i, 1]$. The defender chooses new set-points $\mathrm{sp}_i^{\mathrm{d}}$ for the non-compromised DERs, and load control parameters γ_i to reduce the loss L. The defender action is modeled as a vector $\phi := [\mathrm{sp}^{\mathrm{d}}, \gamma] \in \Phi(\psi)$, where sp^{d} (resp. γ) denotes the vector of $\mathrm{sp}_i^{\mathrm{d}}$ (resp. γ_i).

Since we do not consider any penalty for load control during contingency, it is trivial to see that the optimal load control paramater γ^* attains the minimum possible value $\underline{\gamma}$.

IV. Sequential Game With Linear Power Flow

Now, consider the following simplified and approximate version of the sequential game [AD]:

$$\widehat{[\mathrm{AD}]} \quad \widehat{\mathcal{L}} \;:=\; \max_{\psi\in\Psi} \min_{\phi\in\Phi} \mathrm{L}(\hat{\mathrm{x}}(\psi,\phi))$$

$$\text{s.t. } \hat{\mathrm{x}}(\psi,\phi) \in \widehat{\mathcal{X}}, (14b), (14c), (14d)$$

where the NPF equations (11) are replaced by the LPF equations (12). In this section, we first compute the optimal attacker set-points and defender set-points (§IV-A), and then present a greedy algorithm to come up with the optimal solution for $\widehat{[\mathrm{AD}]}$ (§IV-B).

Following the computational approach in the literature to solve (bilevel) interdiction problems [19], [20], we define the master-problem $[\mathrm{AD}]^{\mathrm{a}}$ (resp. sub-problem $[\mathrm{AD}]^{\mathrm{d}}$) for fixed $\phi \in \Phi$ (resp. fixed $\psi \in \Psi$):

$$[\mathrm{AD}]^{\mathrm{a}} \quad \psi^*(\phi) \in \mathrm{argmax}_{\psi\in\Psi} \quad \mathrm{L}(\mathrm{x}(\psi,\phi)) \quad \text{s.t.} \quad (14),$$

$$[\mathrm{AD}]^{\mathrm{d}} \quad \phi^*(\psi) \in \mathrm{argmin}_{\phi\in\Phi} \quad \mathrm{L}(\mathrm{x}(\psi,\phi)) \quad \text{s.t.} \quad (14).$$

Similarly, define master- and sub- problems $\widehat{[\mathrm{AD}]}^{\mathrm{a}}$ $(\hat{\psi}^*(\phi))$ and $\widehat{[\mathrm{AD}]}^{\mathrm{d}}$ $(\hat{\phi}^*(\psi))$ for the variant $\widehat{[\mathrm{AD}]}$.

Proposition 1. *Let (ψ^*, ϕ^*) and $(\widehat{\psi}^*, \widehat{\phi}^*)$ be the optimal solutions to* [AD] *and* $[\widehat{\text{AD}}]$ *with the corresponding optimal losses $\mathcal{L}$ and $\widehat{\mathcal{L}}$, respectively. Then, $\mathcal{L} \geq \widehat{\mathcal{L}}$.*

Proof. We first prove a preliminary result relating $\mathrm{x}(\psi, \phi)$ and $\widehat{\mathrm{x}}(\psi, \phi)$.

Lemma 1. *For a fixed strategy profile (ψ, ϕ),*

$$S \geq \widehat{S}, \quad \nu \leq \widehat{\nu}, \quad \Delta f_{0,max} \geq \Delta \widehat{f}_{0,max} \tag{18}$$

Hence,

$$\left.\begin{aligned} \mathrm{L_{VR}}(\mathrm{x}) \geq \mathrm{L_{VR}}(\widehat{\mathrm{x}}) \\ \mathrm{L_{FR}}(\mathrm{x}) \geq \mathrm{L_{FR}}(\widehat{\mathrm{x}}) \end{aligned}\right\} \implies \mathrm{L}(\mathrm{x}) \geq \mathrm{L}(\widehat{\mathrm{x}}). \tag{19}$$

Proof. The relationships $S \geq \widehat{S}$ and $\nu \leq \widehat{\nu}$ is already proved in [21]. Since, $S \geq \widehat{S}$ implies $\mathbf{Re}(S) \geq \mathbf{Re}(\widehat{S})$, from (14d) we get, $\Delta f_{0,max} \geq \Delta \widehat{f}_{0,max}$. ■

From Lemma 1, we get,

$$\begin{aligned} \mathcal{L} &= \mathrm{L}(\mathrm{x}(\psi^*, \phi^*(\psi^*))) \\ &\geq \mathrm{L}(\mathrm{x}(\widehat{\psi}^*, \phi^*(\widehat{\psi}^*))) && \text{(by optimality of } \psi^*) \\ &\geq \mathrm{L}(\widehat{\mathrm{x}}(\widehat{\psi}^*, \phi^*(\widehat{\psi}^*))) && \text{(by Lemma 1)} \\ &\geq \mathrm{L}(\widehat{\mathrm{x}}(\widehat{\psi}^*, \widehat{\phi}^*(\widehat{\psi}^*))) && \text{(by optimality of } \widehat{\phi}^*) \\ &= \widehat{\mathcal{L}}. \end{aligned}$$

■

Lemma 1 implies that if there is a successful attack strategy for $[\widehat{\text{AD}}]$, then there also exists a successful attack strategy for [AD]. However, the converse need not be true.

A. Optimal attacker and defender set-points

The following theorem proven in [12] provides the optimal attacker set-points:

Theorem 1 (Optimal attacker set-points)**.** *The optimal attacker DER set-points $\widehat{\mathrm{sp}}^{\mathrm{a}}$ to the problem $[\widehat{\text{AD}}]$ are given as:*

$$\widehat{\mathrm{sp}}^{\mathrm{a}}_i = 0 - \boldsymbol{j}\overline{sg}_i \tag{20}$$

Proof. Similar to the proof of Thm. 1 in [12]. ■

Thanks to the Thm. 1, the loss function $\mathrm{L}(\widehat{\mathrm{x}}(\psi, \phi))$ can be written as $\mathrm{L}(\widehat{\mathrm{x}}(\delta, \phi))$, as the optimal attacker preferred setpoints are already known.

Now, consider the following definition:

Definition 1. *Let $\mathcal{S}^+ := \{s \in \mathcal{S} \mid s \geq 0\}$. For a given attacker strategy $\psi \in \Psi$, if there exists a node that has the least voltage among all nodes regardless of the defender response, then it is called as the* worst-affected *node, i.e.,*

$$\forall\, \mathrm{sp}^{\mathrm{d}} \in \mathcal{S}^+ : \widehat{\mathrm{x}}(\psi, [\mathrm{sp}^{\mathrm{d}}, \underline{\gamma}]) \in \widehat{\mathcal{X}},\ t(\psi) = \operatorname*{argmax}_{i \in \mathcal{N}} (\underline{\nu}_i - \widehat{\nu}_i).$$

In this section, we compute the optimal defender setpoints under the following assumptions:

(A1) For a fixed $\psi \in \Psi$, *worst-affected* node $t(\psi)$ exists.

(A2) For a given $\psi \in \Psi$, under optimal defender response, the loss of voltage regulation and the loss of frequency regulation are both positive, i.e., $\mathrm{L_{VR}}(\widehat{\mathrm{x}}(\psi, \widehat{\phi}^*(\psi))) > 0$ and $\mathrm{L_{FR}}(\widehat{\mathrm{x}}(\psi, \widehat{\phi}^*(\psi))) > 0$.

Similar to the intuition presented in [12] the optimal attacker strategy in $[\widehat{\text{AD}}]$ is to impose clustered DER compromises on a target pivot node, so that that pivot node has the least voltage (A1). Further, as we see in Prop. 2, there is a trade-off for the defender between $\mathrm{L_{VR}}$ and $\mathrm{L_{FR}}$. If the defender minimizes only $\mathrm{L_{VR}}$, then the frequency deviations will be too high, and other DERs may disconnect. On the other hand, if he minimizes only $\mathrm{L_{FR}}$, then the voltage quality at all nodes will suffer. Hence, assumption (A2).

The following proposition computes the optimal defender DER set-points under the knowledge of *worst-affected* node.

Proposition 2 (Optimal Defender Set-points)**.** *Assume (A1) and (A2). For a fixed $\psi \in \Psi$, let t be the* worst-affected *node under (A1). Let $\widehat{\mathrm{sp}}^c$ denote the optimal defender set-point under the centralized control strategy. Then*

$$\forall\, i \in \mathcal{N}, \quad |\widehat{\mathrm{sp}}^c_i| = \overline{sg}_i \text{ and } \angle \widehat{\mathrm{sp}}^c_i = \angle \lambda_{it}, \tag{21}$$

where $\lambda_{it} = CH^{BG} + 2W_t Z_{it}$.

Proof. Under (A1) and (A2), it can be checked that the loss function L can be written as:

$$\begin{aligned} &\mathrm{L}(\widehat{\mathrm{x}}(\psi, \widehat{\phi}^*)) \\ &= W_t(\underline{\nu}_t - \widehat{\nu}_t) + C(\Delta \underline{f}_{th} - \Delta \widehat{f}_{0,max}) \\ &= \text{const.} + \textstyle\sum_{i \in \mathcal{N}} -CH^{BG}\mathbf{Re}(\widehat{\mathrm{sp}}^c_i) - 2W_t\mathbf{Re}(\bar{Z}_{it}\widehat{\mathrm{sp}}^c_i) \\ &= \text{const.} - \textstyle\sum_{i \in \mathcal{N}} \lambda_{it} \cdot \widehat{\mathrm{sp}}^c_i \\ &= \text{const.} - \textstyle\sum_{i \in \mathcal{N}} |\lambda_{it}||\widehat{\mathrm{sp}}^c_i| \cos(\angle \lambda_{it} - \angle \widehat{\mathrm{sp}}^c_i) \end{aligned}$$

It can be checked that[4] L is minimized when $|\widehat{\mathrm{sp}}^c_i| = \overline{sg}_i$, and $\angle \widehat{\mathrm{sp}}^c_i = \angle \lambda_{it}$. ■

B. Greedy Algorithm to solve $[\widehat{\text{AD}}]$

We now present a greedy algorithm to solve for $[\widehat{\text{AD}}]$.

Under (A1), we know that for the optimal attacker strategy $\widehat{\psi}^*$, some node is the worst-affected node. Consider node t as a candidate worst-affected node, which we call a pivot node. Assuming that pivot node t is a worst-affected node for some attacker strategy, we compute the attacker strategy ψ that will maximize $\mathrm{L}^t := W_t(\underline{\nu}_t - \widehat{\nu}_t) + CH^{BG}(\Delta \underline{f}_{th} - \Delta \widehat{f}_{0,max})$. For pivot node t, we know the optimal defender set-points by Prop. 2. We also know the optimal attacker set-points, thanks to Thm. 1. Hence, the DER set-points sp^{d} are fixed by (14c). Furthermore, since $\gamma = \underline{\gamma}$, the defender strategy $\phi = [\mathrm{sp}^{\mathrm{d}}, \underline{\gamma}]$ is fixed. Hence, the problem $[\widehat{\text{AD}}]$ becomes an integer optimization problem over δ. To solve this, we present a greedy algorithm to compute the optimal attack vector δ for the pivot node t.

Let $\Delta_i(\mathrm{L}^t)$ (resp. $\Delta_\delta(\mathrm{L}^t)$) be the change in loss function at node t caused due to compromise of DER at node j (resp. compromise of DERs due to attack vector δ). The following Lemma computes $\Delta_i(\mathrm{L}^t)$ and $\Delta_\delta(\mathrm{L}^t)$.

Lemma 2. *Assume (A1) and (A2). For a fixed $\psi \in \Psi$, let t be the* worst-affected *node under (A1). Let $\widehat{\mathrm{sp}}^{\mathrm{a}}$ (resp. $\widehat{\mathrm{sp}}^c$) denote the optimal attacker (resp. defender) set-points as computed in Thm. 1 (resp. Prop. 2). Further, let $\mathrm{L}^t := W_t(\underline{\nu}_t - \widehat{\nu}_t) + CH^{BG}(\Delta \underline{f}_{th} - \Delta \widehat{f}_{0,max})$. Then,*

$$\Delta_i(\mathrm{L}^t) = \lambda_{it} \cdot (\widehat{\mathrm{sp}}^{\mathrm{a}}_i - \widehat{\mathrm{sp}}^c_i) \tag{22}$$

$$\Delta_\delta(\mathrm{L}^t) = \textstyle\sum_{i:\delta_i = 1} \Delta_i(\mathrm{L}^t) \tag{23}$$

Proof. As seen in Prop. 2, the individual contribution of DER i when t is the worst-affected node is equal to $\lambda_{it} \cdot \widehat{\mathrm{sp}}^{\mathrm{d}}_i$.

[4] If $a, b \in \mathbb{C}$, then $\mathbf{Re}(\bar{a}b)$ is the dot product of complex numbers a and b, and is maximized when $|a|$ and $|b|$ are maximized, and $\angle a = \angle b$.

Since, the set-point changes from $\widehat{\mathrm{sp}}_i^{\mathrm{d}}$ to $\widehat{\mathrm{sp}}_i^{\mathrm{a}}$, the change in the loss L^t is $\lambda_{it} \cdot (\widehat{\mathrm{sp}}_i^{\mathrm{a}} - \widehat{\mathrm{sp}}_i^{c})$. (23) follows because L^t is a linear function of $\widehat{\mathrm{sp}}^{\mathrm{d}}$. ■

The following greedy algorithm can be used to find δ that generate the worst impact.

Algorithm 1 Solution to $\widehat{[\mathrm{AD}]}$ under **(A1)**, **(A2)**

$(\widehat{\psi}^*, \widehat{\phi}^*, \widehat{\mathcal{L}}^*) \leftarrow$ SOLVE($\widehat{[\mathrm{AD}]}$)
procedure SOLVE($\widehat{[\mathrm{AD}]}$)
  for $i \in \mathcal{N}$ **do**
    $(\psi^i, \phi^i, \mathcal{L}^i) \leftarrow$ OPTIMALATTACKFORPIVOTNODE(i)
  end for
  Compute worst-affected node as $t \leftarrow \mathrm{argmax}_{i \in \mathcal{N}} \mathcal{L}^i$
  return $\psi^t, \phi^t, \mathcal{L}^t$
end procedure
procedure OPTIMALATTACKFORPIVOTNODE(t)
  Compute $\widehat{\mathrm{sp}}^{\mathrm{d}}$ as in Prop. 2 and $\widehat{\mathrm{sp}}^{\mathrm{a}}$ as in Thm. 1
  Sort nodes in $\mathcal{N}$ in decreasing order of their $\Delta_j(\widehat{\nu}_t, f)$ (computed using Lemma 2), and choose the top M DERs
  Compute $\delta^t \in \mathcal{D}$ such that if a node i is chosen, $\delta_i^t = 1$
  return $\psi^t \leftarrow [\widehat{\mathrm{sp}}^{\mathrm{a}}, \delta^t]$, $\phi^t \leftarrow [\widehat{\mathrm{sp}}^{\mathrm{d}}, \underline{\gamma}]$, $\mathcal{L}^t \leftarrow \mathrm{L}(\widehat{\mathrm{x}}(\psi^t, \phi^t))$
end procedure

V. A DISTRIBUTED CONTROL STRATEGY

A. Proposed Design

Under nominal conditions, the defender is able to remotely configure optimal DER set-points by solving the OPF problem. However, under our adversarial model, during a contingency, the DER controllers can no longer rely on the set-points received from the control center as they can also be compromised by the adversary. Thus, our goal is to establish a distributed control strategy to enable the non-compromised DERs to reduce defender loss (i.e., improve voltage and frequency regulation). We make the following assumption for simplicity.

(A3) The DN has identical $\mathbf{r}/\mathbf{x}$ ratio, or equivalently, $\forall\ (i,j) \in \mathcal{E}, \angle z_j = \angle z_u = $ constant, where z_u denotes the impedance per unit length of the lines.

Within a DN, it is reasonable to assume that the lines are made of same type of conductor, and hence, regardless of the line's length or its cross-sectional area, its $\mathbf{r}/\mathbf{x}$ ratio is constant **(A3)**.

Now, we present a distributed control strategy in which we impose that each non-compromised DER should either contribute to the voltage or frequency regulation (but not both).

Definition 2. 1) *First the node controllers detect an attack due to sudden drop in local voltage and frequency, and they set the load control parameter to the minimum load control parameter* $\underline{\gamma}$.
2) *Second, the DERs communicate with other nodes to estimate the identity of the* worst-affected *node in terms of the voltage violation, i.e. the DERs determine the node* $t = \mathrm{argmax}_{i \in \mathcal{N}} W_i(\underline{\nu}_i - \nu_i)$.
3) *For every node* $i \in \mathcal{N}$*, the DER controller of* $i-th$ *DER has a precomputed partition of the nodes* $\mathcal{N}_t^f$ *and* $\mathcal{N}_t^v$*, such that* $\mathcal{N}_t^f \cap \mathcal{N}_t^v = \emptyset$ *and* $\mathcal{N}_t^f \cup \mathcal{N}_t^v = \mathcal{N}$.
4) *Finally, each DER configures a new DER set-point such that if* $i \in \mathcal{N}_t^f$*, the* $i-th$ *DER controller contributes to only frequency regulation, otherwise it contributes to only voltage regulation.*

In order to compute the *worst-affected node*, we assume a fairly simple communication protocol for the secondary distributed control strategy. We assume that the communication topology is similar to the physical network topology. Every DER controller has the current best knowledge of the node with the least voltage. Initially, every DER just stores its own identity and corresponding nodal voltage value. In every iteration, each DER controller sends updates to its neighbors about the current minimum ν_i value and the corresponding node i. Then, the DER controller compares its current best knowledge with the information it receives from its neighbors, computes the new minimum ν_j value and determines the corresponding node j. And, so on and so forth. It can be shown that this process converges in at most $D+1$ iterations, where D is the diameter of network $\mathcal{G}$. For a more detailed discussion of such protocols, we refer the reader to [22], [23].

The advantage of the proposed design is that during an attack scenario (or more broadly under a range of contingency situations), the DER controllers need not rely upon the possibly compromised control center set-points. Moreover, since the DERs use the distributed control strategy only to communicate with their neighboring DER controllers (and not with every other DER controller), the communication requirements are relatively less stringent.

The following proposition computes the optimal defender set-points for non-compromised DERs should they contribute to either only frequency regulation or only voltage regulation.

Proposition 3. *Assume* **(A1)**, **(A2)**, **(A3)**. *Let* $\widehat{\mathrm{sp}}^d$ *denote the optimal defender set-points under the distributed control strategy as in Definition 2. Consider fixed* $\psi \in \Psi$. *For a node* $i \in \mathcal{N}$*, assume fixed* $\widehat{\mathrm{sp}}_{-i}^{\mathrm{d}} \in \mathcal{S}_{-i}$*, where* $\widehat{\mathrm{sp}}_{-i}^{\mathrm{d}}$ *denotes the vector of all defender set-points except for node* i. *Furthermore, let* $\phi = [\widehat{\mathrm{sp}}^{\mathrm{d}}, \underline{\gamma}]$. *Then,*

1) $\forall\ i \in \mathcal{N}_t^f$, $\widehat{\mathrm{sp}}_i^{\mathrm{f}} \in \mathrm{argmin}_{\widehat{\mathrm{sp}}_i^{\mathrm{d}} \in \mathcal{S}_i} \mathrm{L}_{\mathrm{FR}}(\widehat{\mathrm{x}}(\psi, \phi))$, *where*
$$|\widehat{\mathrm{sp}}_i^{\mathrm{f}}| = \overline{sg}_i, \text{ and } \angle \widehat{\mathrm{sp}}_i^{\mathrm{f}} = 0 \tag{24}$$
2) $\forall\ i \in \mathcal{N}_t^v$, $\widehat{\mathrm{sp}}_i^{\mathrm{v}} \in \mathrm{argmin}_{\widehat{\mathrm{sp}}_i^{\mathrm{d}} \in \mathcal{S}_i} \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\psi, \phi))$, *where*
$$|\widehat{\mathrm{sp}}_i^{\mathrm{v}}| = \overline{sg}_i, \text{ and } \angle \widehat{\mathrm{sp}}_i^{\mathrm{v}} = \angle z_u \tag{25}$$

Proof. If node $i \in \mathcal{N}$ contributes to only frequency regulation, then L_{FR} can be written as:
$$\mathrm{L}_{\mathrm{FR}}(\widehat{\mathrm{x}}) = -H^{BG}\mathbf{Re}(\widehat{\mathrm{sp}}_i^d) + \text{const.}$$
Hence, L_{FR} is a decreasing function of $\mathbf{Re}(\widehat{\mathrm{sp}}_i^{\mathrm{d}})$, and will be minimized when $\mathbf{Re}(\widehat{\mathrm{sp}}_i^d) = \overline{sg}_i$. However, $\widehat{\mathrm{sp}}_i^d \in \mathcal{S}_i$ implies that $\mathbf{Im}(\widehat{\mathrm{sp}}_i^d) = 0$.

If node $i \in \mathcal{N}$ contributes to only voltage regulation, then L_{VR} can be written as:
$$\mathrm{L}_{\mathrm{FR}}(\widehat{\mathrm{x}}) = -2W_t Z_{it} \cdot \widehat{\mathrm{sp}}_i^d + \text{const.}$$
Under identical $\mathbf{r}/\mathbf{x}$ ratio, $\angle Z_{it} = \angle z_u$. The rest of the proof follows similarly to the proof of Prop. 2. ■

Theorem 2. *Assume* **(A1)**, **(A2)**, **(A3)**. *For a fixed* $\psi \in \Psi$, *let* t *be the worst-affected node. Let* $\mathcal{N}_t^f, \mathcal{N}_t^v$ *form a disjoint partition of* $\mathcal{N}_{NC}$ *(the set of non-compromised DERs), such that for all* $j \in \mathcal{N}_t^f$ *(resp. for all* $k \in \mathcal{N}_t^v$*),* $\widehat{\mathrm{sp}}_j^d = \widehat{\mathrm{sp}}_j^{\mathrm{f}}$ *(resp.*

$\widehat{\mathrm{sp}}_k^d = \widehat{\mathrm{sp}}_k^{\mathrm{v}}$*) is as specified by (24) (resp. (25)). Then*

$$\begin{aligned} j \in \mathcal{N}_t^f \quad &\Longrightarrow \quad 0 \quad \leq \angle\lambda_{jt} \quad \leq \frac{\angle z_u}{2} \\ k \in \mathcal{N}_t^v \quad &\Longrightarrow \quad \frac{\angle z_u}{2} \quad < \angle\lambda_{kt} \quad \leq \angle z_u \end{aligned}$$

Proof. Under **(A1)** and **(A2)**, it can be checked that the loss function L can be written as:

$$\begin{aligned} \mathrm{L}(\widehat{\mathrm{x}}(\psi,\phi)) &= W_t(\underline{\nu}_t - \widehat{\nu}_t) + C(\Delta\underline{f}_{th} - \Delta\widehat{f}_{0,max}) \\ &= \text{const.} + \textstyle\sum_{i\in\mathcal{N}} -\lambda_{it}\cdot \mathrm{sp}_i, \end{aligned}$$

where $\lambda_{it} = CH^{BG} + 2W_tZ_{it}$.

Under **(A1)**, **(A2)**, **(A3)**, let $\widehat{\mathrm{sp}}_i^{\mathrm{f}}$ and $\widehat{\mathrm{sp}}_i^{\mathrm{v}}$ be the defender set-points as in (24) and (25), respectively. Let the change in the value of the loss function, holding all else the same, if the $j-$th DER is used for frequency regulation (resp. voltage regulation) be denoted by $\Delta_{jt}^f(\mathrm{L})$ (resp. $\Delta_{jt}^v(\mathrm{L})$). Then the difference in these two changes, holding all else equal, is given by

$$\begin{aligned} \Delta_{jt}^f(\mathrm{L}) - \Delta_{jt}^v(\mathrm{L}) &= \lambda_{jt}\cdot\widehat{\mathrm{sp}}_j^{\mathrm{f}} - \lambda_{jt}\cdot\widehat{\mathrm{sp}}_j^{\mathrm{v}} \\ &= |\lambda_{jt}|\overline{sg}_j(\cos(\angle z_u - \angle\lambda_{jt}) - \cos\angle\lambda) \\ &= 2|\lambda_{jt}|\overline{sg}_j \sin\frac{z_u}{2}\sin(\angle\lambda_{jt} - \frac{\angle z_u}{2}) \end{aligned}$$

Clearly, $\Delta_{jt}^f(\mathrm{L}) > \Delta_{jt}^v(\mathrm{L}) \iff \angle\lambda_{jt} < \frac{\angle z_u}{2}$.

Now, $\cot\angle\lambda_{it} = \frac{CH^{BG}+2W_tR_{it}}{2W_tX_{it}} = \frac{CH^{BG}}{2W_tX_{it}} + \frac{1}{z_u}$, which decreases when X_{it} increases, or equivalently, $\angle\lambda_{it}$ increases when Z_{it} increases. Now, Z_{it} is minimum (resp. maximum) when $i = 0$ (resp. $i = t$). Hence, $\angle\lambda_{it}$ is minimum (resp. maximum) when $i = 0$ (resp. $i = t$). If $\angle\lambda_{0t} \leq \frac{\angle z_u}{2} < \angle\lambda_{tt}$, then there must exist a node $t_c \in \mathcal{P}_t$ where $\angle\lambda_{it}$ changes from less than $\frac{\angle z_u}{2}$ to greater than $\frac{\angle z_u}{2}$. This node t_c is the critical node which gives us the partition $\mathcal{N}_t^f = \{i \in \mathcal{N} : i \prec_t t_c\}$ and $\mathcal{N}_t^v = \{i \in \mathcal{N} : t_c \preceq_t i\}$. Note that $\forall\, i \in \mathcal{N}_t^f,\ \angle\lambda_{it} < \angle\lambda_{t_ct}$ and $\forall\, i \in \mathcal{N}_t^v,\ \angle\lambda_{it} \geq \angle\lambda_{t_ct}$.

Finally, if $\forall\ j \in \mathcal{N},\ \angle\lambda_{jt} < \frac{\angle z_u}{2}$, then $\mathcal{N}_t^f = \mathcal{N}$ and $\mathcal{N}_t^v = \emptyset$. If $\forall\ j \in \mathcal{N},\ \angle\lambda_{jt} > \frac{\angle z_u}{2}$, then $\mathcal{N}_t^v = \mathcal{N}$ and $\mathcal{N}_t^f = \emptyset$. ■

As per the existing IEEE 1547 DER interconnection guidelines, if the voltages fall below $\underline{\nu}$, then the DERs should disconnect from the network. Let us denote these defender DER setpoints by $\widehat{\mathrm{sp}}^{\mathrm{d}} = \mathbf{0}$. Let $\widehat{\phi}^0 := [\mathbf{0}, \underline{\gamma}]$ be the defender *"Disconnect-DERs"* strategy when $\widehat{\mathrm{sp}}^{\mathrm{d}} = \mathbf{0}$. Furthermore, let $(\widehat{\psi}^*, \widehat{\phi}^*)$ be the optimal solution to $[\widehat{\mathrm{AD}}]$. Let $\widehat{\phi}^c$ (resp. $\widehat{\phi}^d$) be the defender strategies when defender set-points are as specified by the centralized (resp. distributed) strategy. Also, let $\widehat{\mathcal{L}}$, $\widehat{\mathcal{L}}_d$, and $\widehat{\mathcal{L}}_0$ be the optimal losses corresponding to the strategy profiles $(\widehat{\psi}^*, \widehat{\phi}^c)$, $(\widehat{\psi}^*, \widehat{\phi}^d)$, and $(\widehat{\psi}^*, \widehat{\phi}^0)$, respectively. The following proposition compares the performance of distributed control strategy with that of centralized control strategy relative to the *Disconnect-DERs* strategy.

Proposition 4.

$$\frac{\widehat{\mathcal{L}}_d - \widehat{\mathcal{L}}_0}{\widehat{\mathcal{L}}_c - \widehat{\mathcal{L}}_0} \geq \cos\left(\frac{\angle z_u}{2}\right), \tag{26}$$

where z_u is the impedance per unit length.

Proof. Under the distributed control strategy, node i contributes to either frequency regulation or voltage regulation, depending upon which contribution is larger, i.e., $\lambda_{it}.\widehat{\mathrm{sp}}_i^c = \max(\lambda_{it}.\widehat{\mathrm{sp}}_i^{\mathrm{f}}, \lambda_{it}.\widehat{\mathrm{sp}}_i^{\mathrm{v}})$. Now, node $i \in \mathcal{N}_t^f$ if

$$\begin{aligned} \lambda_{it}\cdot\widehat{\mathrm{sp}}_i^{\mathrm{f}} \quad &\geq \quad \lambda_{it}\cdot\widehat{\mathrm{sp}}_i^{\mathrm{v}} \\ \Longleftarrow |\lambda_{it}|\overline{sg}_i\cos(\angle\lambda_{it}) \quad &\geq \quad |\lambda_{it}|\overline{sg}_i\cos(\angle z_u - \angle\lambda_{it}) \\ \Longleftarrow \cos(\angle\lambda_{it}) \quad &\geq \quad \cos(\angle z_u - \angle\lambda_{it}) \end{aligned}$$

Also, if $\cos(\angle\lambda_{it}) \geq \cos(\angle z_u - \angle\lambda_{it})$, then $\cos(\angle\lambda_{it}) \geq \max(\cos(\angle\lambda_{it}), \cos(\angle z_u - \angle\lambda_{it})) \geq \cos(\frac{\angle z_u}{2})$. Hence,

$$\begin{aligned} &\widehat{\mathcal{L}}_d - \widehat{\mathcal{L}}_0 \\ &= \textstyle\sum_{i\in\mathcal{N}} \max(\lambda_{it}\cdot\widehat{\mathrm{sp}}_i^{\mathrm{f}}, \lambda_{it}\cdot\widehat{\mathrm{sp}}_i^{\mathrm{v}}) \\ &= \textstyle\sum_{i\in\mathcal{N}} |\lambda_{it}|\overline{sg}_i \max(\cos(\angle\lambda_{it}), \cos(\angle z_u - \angle\lambda_{it})) \\ &\geq \textstyle\sum_{i\in\mathcal{N}} |\lambda_{it}|\overline{sg}_i \cos(\frac{\angle z_u}{2}) \\ &= \cos(\tfrac{\angle z_u}{2}) \textstyle\sum_{i\in\mathcal{N}} \lambda_{it}\cdot\widehat{\mathrm{sp}}_i^c = \cos(\tfrac{\angle z_u}{2})(\widehat{\mathcal{L}}_c - \widehat{\mathcal{L}}_0). \end{aligned}$$

■

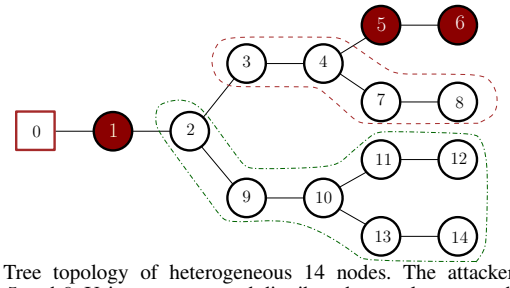

Fig. 2: Tree topology of heterogeneous 14 nodes. The attacker selects nodes $1, 5$ and 6. Using our proposed distributed control strategy, the DERs cooperatively react to the attacker's strategy: nodes $2, 9, 10, 11, 12, 13, 14$ contribute toward reducing frequency deviation, whereas, nodes $3, 4, 7, 8$ contribute toward maintaining voltage regulation.

VI. Case Study

We present a simple case study to illustrate the main aspects of our distributed control approach. We consider the 14 node radial network illustrated in Figure 2. Each node represent a DER connected to loads. The DERs are heterogeneous (please refer to caption of Fig. 2). We assume that the DER units closer to the substation are owned by the utility, and these units possess larger power injection capacities. On the other hand, downstream DERs (e.g., rooftop PVs) are smaller in their capacities, and are owned by users. As we have shown in §IV, attacks on the downstream nodes cause larger voltage deviations, while attacks to the larger generators primarily impact the frequency deviations, independent of their location.

The test circuit is homogeneous, i.e., all the lines and loads have similar physical properties. The impedance per unit length for all lines is $z_u = 0.1{+}0.3\mathbf{j}\ \Omega/km$, and nominal power demand is $\mathrm{sc}_i^{\mathrm{nom}} = 25\ kW + \mathbf{j}7.5\ kvar$. DERs supply 50% of the total demand. The maximum apparent power that generator i can produce is $\overline{sg}_i = 20.7\ kVA$ for i=1,2; $14.6\ kVA$ for i=3,4,9,10; and $11.8\ kVA$ otherwise. The voltage at each node is constrained to be within 0.95 and 1.05 $p.u$. Frequency should be maintained above 59.7 Hz (assuming nominal frequency to be 60 Hz) to avoid the LAARS (Load Acting As Resource) tripping. The bulk generator parameters are $\mathrm{M} = 5\ s$, $\mathrm{D} = 5x10^{-4}\ Hz/kW$, $\mathrm{K_P} = 5.1$, $\mathrm{K_I} = 2$ s. $C = 1000$ and $\forall\ i \in \mathcal{N},\ W_i = 70$, where C and W are the weights for LOFR and LOVR, respectively.

An attacker compromises the set point information delivered by the control center after 1000 s, and simultaneously

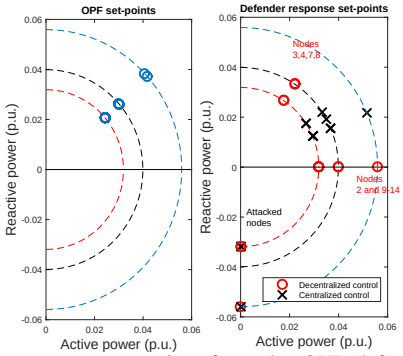

Fig. 3: Apparent power set points from the OPF (left) and after the attack (right). According to the proposed distributed control strategy, each DER either contributes to voltage regulation or toward reducing frequency deviation.

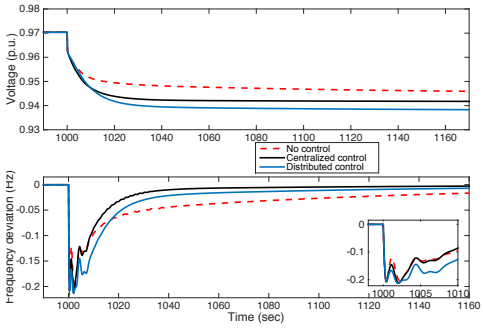

Fig. 4: Dynamic response of the voltage in node 6 and the bulk generator frequency. An attack occurs at $t = 2000$ s.

modifies the setpoints to DERs attached to nodes $1, 5$ and 6. The attack causes a frequency and voltage deviation that activates the contingency response. Note that $C > W$, i.e., frequency regulation is a priority. Using the exchange of information between DERs about the node voltages described in section IV, the *worst-affected* node t is determined to be node 6. Also, we find the critical node $t_c = 3$, which results in the partition of non-compromised nodes as shown in figure 2. As a consequence, nodes $3, 4, 7, 8$ start contributing to voltage regulation, and $2, 9, 10, 11, 12, 13, 14$ to frequency regulation, as depicted in Figures 2 and 3. Further, $\cos \frac{\angle z_u}{2} = 0.937$. Hence, Prop. 4 implies that the distributed control strategy performs at least as good as 86.7% compared to the centralized control strategy.

The minimum voltage level and the grid frequency dynamics are illustrated in Fig. 4 for the case without a defense action, i.e., maintaining the nominal set points, and with the defender response. Note that frequency deviation is rapidly driven to zero using the centralized and distributed strategies. However, due to the trade-off between frequency and voltage regulation, the voltage levels are lower than without any defense action. Depending on the system operator requirements, the selection of C and W will determine the priority to voltage or to frequency regulation. Figures 3 and 4 compare the performance of centralized and distributed control strategies. Clearly, the solution obtained with the centralized strategy performs better than the distributed one, but it requires the central control to process all the information from the entire network. However, the new set-points may also been compromised. On the other hand, using the proposed distributed method results in a simple solution where each node only needs to decide to contribute to frequency or to voltage regulation based on knowing the worst node location, which is found using a local communication network. Due to the fact that set-points are predefined, it does not require to solve any optimization problem.

References

[1] M. E. Baran, H. Hooshyar, Z. Shen, and A. Q. Huang, "Accommodating high pv penetration on distribution feeders." *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 1039–1046, 2012.

[2] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities." *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 36–46, 2013.

[3] K. S. Turitsyn, P. Sulc, S. Backhaus, and M. Chertkov, "Options for control of reactive power by distributed photovoltaic generators." *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1063–1073, 2011.

[4] M. Farivar, R. Neal, C. R. Clarke, and S. H. Low, "Optimal inverter var control in distribution systems with high pv penetration," *CoRR*, 2011.

[5] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. McGraw-hill New York, 1994, vol. 7.

[6] O. Palizban and K. Kauhaniemi, "Hierarchical control structure in microgrids with distributed generation: Island and grid-connected mode," *Renewable and Sustainable Energy Reviews*, vol. 44, pp. 797–813, 2015.

[7] R. on Electric Sector Failure Scenarios and I. Analyses, "Electric power research institute," *National Electric Sector Cybersecurity Organization Resource Report*, September 2013.

[8] H. D. Chiang and M. E. Baran, "On the existence and uniqueness of load flow solution for radial distribution power networks," *IEEE Transactions on Circuits and Systems*, vol. 37, no. 3, pp. 410–416, 1990.

[9] E. Dall'Anese and G. B. Giannakis, "Sparsity-leveraging reconfiguration of smart distribution systems," *CoRR*, vol. abs/1303.5802, 2013.

[10] H. Bevrani, *Robust power system frequency control*. Springer, 2009, vol. 85.

[11] K. Ogata and Y. Yang, *Modern control engineering*, 3rd ed. Prentice-Hall Englewood Cliffs, 1997.

[12] D. Shelar and S. Amin, "Security assessment of electricity distribution networks under der node compromises," *IEEE Transactions on Control of Networked Systems (submitted for review)*, pp. –, 2015.

[13] J. Schiffer, R. Ortega, A. Astolfi, J. Raisch, and T. Sezi, "Conditions for stability of droop-controlled inverter-based microgrids," *Automatica*, vol. 50, no. 10, pp. 2457–2469, 2014.

[14] C. Greacen, R. Engel, and T. Quetchenbach, "A guidebook on grid interconnection and islanded operation of mini-grid power systems up to 200 kw," Lawrence Berkeley National Laboratory and Schatz Energy Research Center, Tech. Rep., 2013.

[15] J. von Appen, M. Braun, T. Stetz, K. Diwold, and D. Geibel, "Time in the sun: The challenge of high pv penetration in the german electric grid," *Power and Energy Magazine, IEEE*, vol. 11, no. 2, pp. 55–64, March 2013.

[16] F. Dörfler, J. W. Simpson-Porco, and F. Bullo, "Plug-and-play control and optimization in microgrids," in *53rd IEEE Conference on Decision and Control, CDC 2014, Los Angeles, CA, USA, December 15-17, 2014*, 2014, pp. 211–216.

[17] E. Mallada, C. Zhao, and S. H. Low, "Optimal load-side control for frequency regulation in smart grids," *CoRR*, vol. abs/1410.2931, 2014.

[18] D. Shelar and S. Amin, "Analyzing vulnerability of electricity distribution networks to DER disruptions," in *American Control Conference, ACC 2015, Chicago, IL, USA, July 1-3, 2015*, 2015, pp. 2461–2468. [Online]. Available: http://dx.doi.org/10.1109/ACC.2015.7171101

[19] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *Power Systems, IEEE Transactions on*, vol. 19, no. 2, pp. 905–912, May 2004.

[20] R. Wood, "Bilevel network interdiction models: Formulations and solutions," in *Wiley Encyclopedia of Operations Research and Management Science*, 2011.

[21] M. Farivar and S. H. Low, "Branch flow model: Relaxations and convexification." in *CDC*. IEEE, 2012, pp. 3672–3679.

[22] H. Chan, A. Perrig, B. Przydatek, and D. X. Song, "SIA: secure information aggregation in sensor networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 69–102, 2007.

[23] H. Chan, H. Hsiao, A. Perrig, and D. Song, "Secure distributed data aggregation," *Foundations and Trends in Databases*, vol. 3, no. 3, pp. 149–201, 2011.