Security Assessment of Electricity Distribution Networks under DER Node Compromises

Devendra Shelar and Saurabh Amin

***Abstract*—This article focuses on the security assessment of electricity distribution networks (DNs) with vulnerable distributed energy resource (DER) nodes. The adversary model is simultaneous compromise of DER nodes by strategic manipulation of generation set-points. The loss to the defender (DN operator) includes loss of voltage regulation and cost of induced load control under supply-demand mismatch caused by the attack. A 3-stage Defender-Attacker-Defender (DAD) game is formulated: in Stage 1, the defender chooses a security strategy to secure a subset of DER nodes; in Stage 2, the attacker compromises a set of vulnerable DERs and injects false generation set-points; in Stage 3, the defender responds by controlling loads and uncompromised DERs. Solving this trilevel optimization problem is hard due to nonlinear power flows and mixed-integer decision variables. To address this challenge, the problem is approximated by tractable formulations based on linear power flows. The set of critical DER nodes and the set-point manipulations characterizing the optimal attack strategy are characterized. An iterative greedy approach to compute attacker-defender strategies for the original nonlinear problem is proposed. These results provide guidelines for optimal security investment and defender response in pre- and post-attack conditions, respectively.**

I. Introduction

Integration of distributed energy resources (DERs) such as solar photovoltaic (PV) and solar thermal power generation with electricity distribution networks (DNs) is a major aspect of smart grid development [1]. Some reports estimate that, by 2050, solar PVs will contribute up to 23.7 % of the total electricity generation in the US. Large-scale deployment of PVs can be utilized to improve grid reliability, reduce dependence on bulk generators (especially, during peak demand), and decrease network losses (at least, up to a certain penetration level) [2]. Harnessing these capabilities requires secure and reliable operation of cyber-physical components such as smart inverters, DER controllers, and communication network between DERs and remote control centers. Thus, reducing cyber-physical security risks is a crucial aspect of the design and operation of DNs [3], [4], [5], [6], [7]. This article focuses on the problem of security assessment of DNs under threats of DER node disruptions by a malicious adversary.

We are specifically interested in limiting the loss of voltage regulation and supply-demand mismatch that can result from the simultaneous compromise of multiple PV nodes on a distribution feeder. It is well known that the active power curtailment and reactive power control are two desirable capabilities that can help maintain the operational requirements in DNs with large-scale penetration of DERs with intermittent nature [2], [8], [9]. In this paper, we investigate the specific ways in which these capabilities need to be built into the PV deployment designs, and show that properly chosen security strategies can protect DNs against a class of security attacks.

Our work is motivated by recent progress in three topics: **(T1)** Interdiction and cascading failure analysis of power grids (especially, transmission networks) [10], [11]; **(T2)** Cyber-physical security of networked control systems [3], [4], [5], [6], [12]; and **(T3)** Optimal power flow and optimal control of distribution networks with DERs [2], [9], [13].

Existing work in **(T1)** employs state-of-the-art computational methods for solving large-scale, mixed integer programs for interdiction/cascade analysis of transmission networks assuming direct-current (DC) power flow models. Since our focus is on security assessment of DNs, we also need to model reactive power demand, in addition to the active power flows. In this work, we consider standard DN model with constant power loads and PVs [9], [13], but we restrict our attention to tree networks. This enables us to obtain structural results on optimal attack strategies (including the critical PV nodes and their setpoints). We show that these structural results also provide guidelines for investment in deploying IT security solutions, especially in geographically diverse DNs.

The adversary model in this paper considers simultaneous PV node compromises by false-data injection attacks. Thanks to the recent progress in **(T2)**, similar models have been proposed for a range of cyber-physical systems [4], [5]. Our model is motivated by the DER failure scenarios proposed by power system security experts [14]. These scenarios consider shutdown of PV systems when an external threat agent compromises the DERs by a direct attack, or by manipulating the power generation set-points sent from the control center to individual DER nodes/controllers; see Fig. 1.

In our model, the attacker's objective is to impose loss of voltage regulation to the defender (i.e., network operator), and also induce him to exercise load control in order to reduce the supply-demand mismatch immediately after the attack. The defender's primary concern in post-attack conditions is to reduce the costs due to loss of voltage regulation and load control. Hence, in our model, the line losses are assigned relatively lesser weight. For a fixed attack, solving

Manuscript submitted on September 3, 2015

D. Shelar and S. Amin are with the Department of Civil and Environmental Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: shelard,amins@mit.edu).

This work was supported by EPRI grant for "Modeling the Impact of ICT Failures on the Resilience of Electric Distribution Systems" (contract ID: 10000621), and NSF project "FORCES" (award #: CNS-1239054).

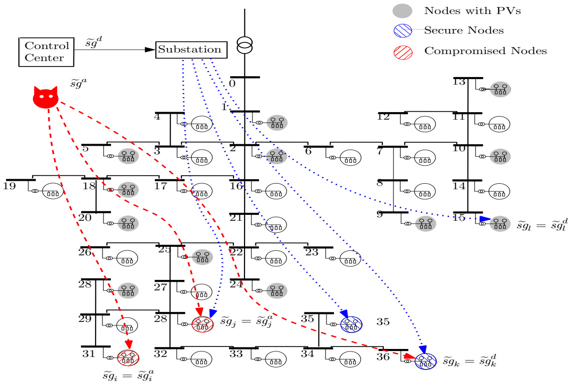


Fig. 1: Illustration of the DER failure scenario proposed in [14] on a modified IEEE 37-node network.

the problem of defender response via load control and the control of uncompromised PVs is similar to the recent results in **(T3)**, i.e., convex relaxations of optimal power flow (OPF) problem.

Our main contribution is analysis of a three-stage sequential security game posed in §II. In Stage 1, the defender invests in securing a subset of PV nodes but cannot ensure security of all nodes due to budget constraints; in Stage 2, the resource-constrained attacker compromises a subset of vulnerable PV nodes and manipulates their set-points; in Stage 3, the defender responds by regulating the supply-demand mismatch. This defender-attacker-defender (DAD) game models both strategic investment decisions (Stage 1) and operation of DN during attacker-defender interaction (Stages 2-3). Solving the DAD game is a hard problem due to nonlinear power flow, PV constraints, and mixed-integer decision variables.

In Sec. III, we provide tractable approximations of the sub-game induced for a fixed defender security strategy, i.e., the attacker-defender interaction in Stages 2-3; see Thm. 1. These approximations can be efficiently solved, and hold under the assumption of no reverse power flows, small impedances, and small line losses. Next we show structural results for the master-problem (i.e., optimal attack for fixed defender response), and the sub-problem (i.e., optimal defender response for fixed attack). For the master-problem, we derive the false set-points that the attacker will introduce in any compromised PV (Thm. 2), and also propose computational methods to solve for attack vectors, i.e., PV nodes whose compromise will cause maximum loss to the defender (Propositions 3 and 4). For the sub-problem, we utilize the convex relaxations of OPF to compute optimal defender response for a fixed attack (Lemma 3), and under a restricted set of conditions, provide a range of new set-points for the uncompromised PVs (Prop. 2). These results lead to a greedy approach, which efficiently computes the optimal attack and defender response (Algorithm 3). We prove optimality of the greedy approach for DNs with identical resistance-to-reactance ratio (Thm. 3), and show that the approach efficiently obtains optimal attack strategy and defender response for a broad range of conditions (§V). Thanks to the structural results on optimal attack strategy, our greedy approach has significantly better computational performance than standard techniques to solve bilevel optimization problems (e.g., Benders decomposition [11]). Finally, we provide a characterization of the optimal security strategy for Stage 1 decision by the defender, albeit for symmetric DNs (§IV, Thm. 4).

II. Problem Formulation

A. Distribution network model

We summarize the standard network model of radial electric distribution systems [15], [16], [17], [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 voltage magnitude. We assume that the magnitude of substation voltage $|V_0|$ is constant. Let $I_j \in \mathbb{C}$ denote the current flowing from node i to node j on line $(i,j) \in \mathcal{E}$, and $\ell_j := |I_j|^2$ the square of the magnitude of the current. A distribution line $(i,j) \in \mathcal{E}$ 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 $\mathbf{j} = \sqrt{-1}$.

The voltage regulation requirements of the DN under *nominal* no attack conditions govern that:

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

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

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

where $\underline{\mu}$ and $\overline{\mu}$ are the *hard* voltage safety bounds for any nodal voltage, and $0 < \underline{\mu} < \min_{i \in \mathcal{N}} \underline{\nu}_i \leqslant \max_{i \in \mathcal{N}} \overline{\nu}_i < \overline{\mu}$.

1) Load model: We consider constant power loads [18]. Let $sc_i := pc_i + \mathbf{j}qc_i$ denote the power consumed by a load at node i, where pc_i and qc_i are the real and reactive components. Let $\mathrm{sc}_i^{\mathrm{nom}} := \mathrm{pc}_i^{\mathrm{nom}} + \mathbf{j}\mathrm{qc}_i^{\mathrm{nom}}$ denote the *nominal* power demanded by a node i, where $\mathrm{pc}_i^{\mathrm{nom}}$ and $\mathrm{qc}_i^{\mathrm{nom}}$ are the real and reactive components of $\mathrm{sc}_i^{\mathrm{nom}}$. Under our assumptions, for all $i \in \mathcal{N}$, $pc_i \leqslant \mathrm{pc}_i^{\mathrm{nom}}$ and $qc_i \leqslant \mathrm{qc}_i^{\mathrm{nom}}$, i.e., the actual power consumed at each node is upper bounded by the nominal demand:

$$\forall \quad i \in \mathcal{N}, \quad sc_i \leqslant \mathrm{sc}_i^{\mathrm{nom}}. \tag{3}$$

2) PV model:[1] Let $sg_i := pg_i + \mathbf{j}qg_i$ denote the power generated by the PV connected to node i, where pg_i and qg_i denote the active and reactive power, respectively. Following [13], [9], sg_i is bounded by the apparent power capability of the inverter, which is a given constant $\overline{\mathrm{sp}}_i$. We denote the PV set-point by $\mathrm{sp}_i = \mathbf{Re}(\mathrm{sp}_i) + \mathbf{jIm}(\mathrm{sp}_i)$, where $\mathbf{Re}(\mathrm{sp}_i)$ and

[1] We use the term PV to denote the complete PV-inverter assembly attached to a node of DN.

$\mathbf{Im}(\mathrm{sp}_i)$ are the real and reactive components. The power generated at each node is constrained as follows:

$$\forall \quad i \in \mathcal{N}, \quad sg_i \leqslant \mathrm{sp}_i \in \mathcal{S}_i, \tag{4}$$

where $\mathcal{S}_i := \{\mathrm{sp}_i \in \mathbb{C} \quad | \quad \mathbf{Re}(\mathrm{sp}_i) \geqslant 0 \text{ and } |\mathrm{sp}_i| \leqslant \overline{\mathrm{sp}}_i\}$. The set of configurable set-points is denoted by $\mathcal{S} := \prod_{i\in\mathcal{N}} \mathcal{S}_i$.

We denote the net power consumed at node i by $s_i := sc_i - sg_i$. In our model, a DN can be fully specified by the tuple $\langle \mathcal{G}, |V_0|, z, \mathrm{sc}^{\mathrm{nom}}, \overline{\mathrm{sp}}\rangle$, where $z, \mathrm{sc}^{\mathrm{nom}}, \overline{\mathrm{sp}}$ are row vectors of appropriate dimensions, and are assumed to be constant.

3) Power flow equations:The 3-phase balanced nonlinear power flow (NPF) on line $(i, j) \in \mathcal{E}$ is given by [15]:

$$S_j = \textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + sc_j - sg_j + z_j\ell_j \tag{5a}$$

$$\nu_j = \nu_i - 2\mathbf{Re}(\bar{z}_j S_j) + |z_j|^2 \ell_j \tag{5b}$$

$$\ell_j = \frac{|S_j|^2}{\nu_i}, \tag{5c}$$

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; (5a) is the power conservation equation; (5b) relates the voltage drop and the power flows; and (5c) is the current-voltage-power relationship. For the NPF model (5), we define a state as follows:

$$\mathrm{x} := [\nu, \ell, sc, sg, S],$$

where $\mathrm{x} \in \mathbb{R}_+^{2N} \times \mathbb{C}^{3N}$, and ν, ℓ, sc, sg, and S are row vectors of appropriate dimensions. Let $\mathcal{F}$ denote the set of all states x that satisfy (2), (3), (4) and the NPF model (5), and define the set of all states with *no reverse power flows* as follows:

$$\mathcal{X} := \{\mathrm{x} \in \mathcal{F} | S \geqslant 0\}.$$

The linear power flow (LPF) approximation of (5) is:

$$\widehat{S}_j = \textstyle\sum_{k:(j,k)\in\mathcal{E}} \widehat{S}_k + \widehat{sc}_j - \widehat{sg}_j \tag{6a}$$

$$\widehat{\nu}_j = \widehat{\nu}_i - 2\mathbf{Re}(\bar{z}_j \widehat{S}_j) \tag{6b}$$

$$\widehat{\ell}_j = \frac{|\widehat{S}_j|^2}{\widehat{\nu}_i}, \tag{6c}$$

where $\widehat{\mathrm{x}} := [\widehat{\nu}, \widehat{\ell}, \widehat{sc}, \widehat{sg}, \widehat{S}]$ is a state of the LPF model, and analogous to the NPF model, define the set of LPF states $\widehat{\mathrm{x}}$ with no reverse power flows as $\widehat{\mathcal{X}}$.

B. Notation and definitions

All vectors are row vectors, unless otherwise stated. For two vectors c and d, $c \odot d$ denotes their Hadamard product.

Let $K_j := \frac{r_j}{x_j}$ be the resistance-to-reactance ($\mathbf{r}/\mathbf{x}$) ratio for line $(i, j) \in \mathcal{E}$, and let $\underline{K}$ and $\overline{K}$ denote the minimum and maximum of the K_js over all $(i, j) \in \mathcal{E}$. We say that PVs at nodes j and k are homogeneous with respect to each other if their set-point configurations as well as their apparent power capabilities are identical, i.e., $\mathrm{sp}_j = \mathrm{sp}_k$ and $\overline{\mathrm{sp}}_j = \overline{\mathrm{sp}}_k$. Similarly, two loads at nodes j and k are homogeneous if $\mathrm{sc}_j^{\mathrm{nom}} = \mathrm{sc}_k^{\mathrm{nom}}$.

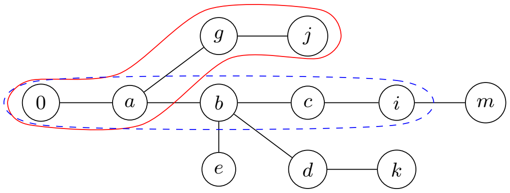


Fig. 2: Precedence description of the nodes for a tree network. Here, $j \prec_i k$, $e =_i k$, $b \prec k$, $\mathcal{P}_j = \{a, g, j\}$, $\mathcal{P}_i \cap \mathcal{P}_j = \{a\}$.

For any given node $i \in \mathcal{N}$, let $\mathcal{P}_i$ be the path from the root node to node i. Thus, $\mathcal{P}_i$ is an ordered set of nodes starting from the root node and ending at node i, excluding the root node; see Fig. 2. 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., $Z_{ij} := \sum_{k\in\mathcal{P}_i\cap\mathcal{P}_j} z_k$, and denote the resistive (real) and inductive (imaginary) components of Z_{ij} by R_{ij} and X_{ij}, respectively.

Finally, we define some useful terminology for the tree network $\mathcal{G}$. Let H denote the height of $\mathcal{G}$, and let $\mathcal{N}_h$ denote the set of nodes on level h for $h = 1, 2, \cdots, H$. For any node $i \in \mathcal{N}$, h_i denotes the level of node i; $\mathcal{C}_i$ the set of children nodes of node i; Λ_i the set of nodes in the subtree rooted at node i; Λ_i^j the set of nodes in the subtree rooted at node i until level h_j, where $j \in \Lambda_i$; $\mathcal{N}_L$ the set of leaf nodes, i.e., $\mathcal{N}_L := \{j \in \mathcal{N} \mid \nexists\ k \in \mathcal{N} \text{ s.t. } (j, k) \in \mathcal{E}\}$.

C. Defender-Attacker-Defender security game

We consider a 3-stage sequential game between a defender (network operator) and an attacker (external threat agent).

- **Stage 1:** The defender chooses a security strategy $u \in \mathcal{U}_B$ to secure a subset of PVs;
- **Stage 2:** The attacker chooses from the set of PVs that were not secured by the defender in Stage 1, and manipulates their set-points according to a strategy $\psi := [\mathrm{sp}^{\mathrm{a}}, \delta] \in \Psi_M(u)$;
- **Stage 3:** The defender responds by choosing the set-points of the uncompromised PVs and, if possible, impose load control at one or more nodes according to a strategy $\phi := [\mathrm{sp}^{\mathrm{d}}, \gamma] \in \Phi(u, \psi)$.

In this Stackelberg game, $\mathcal{U}_B$ and $\Phi(u, \psi)$ denote the set of defender actions in Stage 1 and 3, respectively; and $\Psi_M(u)$ denotes the set of attacker strategies in Stage 2. Formally, the defender-attacker-defender [DAD] game is as follows:

$$[\mathrm{DAD}]\ \mathcal{L} := \min_{u\in\mathcal{U}_B}\ \max_{\psi\in\Psi_M}\ \min_{\phi\in\Phi}\ \mathrm{L}(\mathrm{x}(u, \psi, \phi)) \tag{7}$$

$$
\begin{aligned}
\text{s.t.} \quad & \mathrm{x}(u,\psi,\phi) \in \mathcal{X} && \text{(8a)}\\
& sc(u,\psi,\phi) = \gamma \odot \mathrm{sc}^{\mathrm{nom}} && \text{(8b)}\\
& sg(u,\psi,\phi) = u \odot \mathrm{sp}^{\mathrm{d}} + (\mathbf{1}_N - u)\\
& \qquad \odot \left[\delta \odot \mathrm{sp}^{\mathrm{a}} + (\mathbf{1}_N - \delta) \odot \mathrm{sp}^{\mathrm{d}}\right], && \text{(8c)}
\end{aligned}
$$

where (8b) specifies that the *actual power consumed* at node i is equal to the power demand scaled by the corresponding load control parameter $\gamma_i \in [\underline{\gamma}_i, 1]$ chosen by the defender.

The constraint (8c) models the net effect of defender choice u_i in Stage 1, the attacker choice $(\mathrm{sp}^{\mathrm{a}}_i, \delta_i)$ in Stage 2, and the defender choice $\mathrm{sp}^{\mathrm{d}}_i$ in Stage 3 on the *actual power generated* at node i. Thus, (8c) is the *adversary model* of $[\mathrm{DAD}]$ game: the PV i is compromised *if and only if* it was not secured by the defender ($u_i = 0$) *and* was targeted by the attacker ($\delta_i = 1$). Specifically, if i is compromised, $\mathrm{sp}_i = \mathrm{sp}^{\mathrm{a}}_i$, where $\mathrm{sp}^{\mathrm{a}}_i = \mathbf{Re}(\mathrm{sp}^{\mathrm{a}}_i) + \mathbf{jIm}(\mathrm{sp}^{\mathrm{a}}_i)$ is the false set-point chosen by the attacker (different from the nominal set-point). The set-points of non-compromised PVs are governed by the defender, i.e., if PV i is not compromised $\mathrm{sp}_i = \mathrm{sp}^{\mathrm{d}}_i$. Note that our adversary model assumes that the PV's power output, sg, quickly attain the set-points specified by (8c), i.e., the model does not consider dynamic set-point tracking.[2]

The loss function in $[\mathrm{DAD}]$ is defined as follows:

$$
\mathrm{L}(\mathrm{x}(u,\psi,\phi)) := \mathrm{L}_{\mathrm{VR}}(\mathrm{x}) + \mathrm{L}_{\mathrm{LC}}(\mathrm{x}) + \mathrm{L}_{\mathrm{LL}}(\mathrm{x}), \qquad (9)
$$

where L_{VR} denotes the cost due to loss of voltage regulation; L_{LC} the cost of load control (i.e., the loss due to partially satisfied demand); L_{LL} the total line losses. These costs are defined as follows:

$$
\begin{aligned}
\mathrm{L}_{\mathrm{VR}}(\mathrm{x}) &:= \|W \odot (\underline{\nu} - \nu)_+\|_\infty && \text{(10a)}\\
\mathrm{L}_{\mathrm{LC}}(\mathrm{x}) &:= \|C \odot (1 - \gamma) \odot \mathrm{pc}^{\mathrm{nom}}\|_1 && \text{(10b)}\\
\mathrm{L}_{\mathrm{LL}}(\mathrm{x}) &:= \|r \odot \ell\|_1, && \text{(10c)}
\end{aligned}
$$

where $W, C \in \mathbb{R}^N_+$. Here, W_i is the weight assigned to violation of voltage bound, C_i is the cost of shedding unit load at node i, and r denotes the vector of resistances. Note that L_{VR} is the maximum of the weighted non-negative difference between the lower bound $\underline{\nu}_i$ and nodal voltage square ν_i. Since the defender's primary concern during the contingencies created by the attacker is to limit L_{VR} and L_{LC}, the weights W_i and C_i are chosen such that L_{LL} is relatively small compared to L_{VR} and L_{LC}.

Admittedly, the loss function (9) does not consider the cost of PV control and the cost of energy spillage [19]. However, our formulation is aimed toward security assessment of DNs where the DER owners *participate* in VAR control, perhaps in return of a pre-specified compensation by the operator/defender. Alternatively, the DERs may be *required* to contribute reactive power during contingency scenarios; e.g. sudden supply-demand mismatch. We now describe each stage in more detail:

Stage 1 [Security Investment]:The set of defender actions is:

$$
\mathcal{U}_B := \{u \in \{0,1\}^{\mathcal{N}} \mid \|u\|_0 \leqslant B\},
$$

where $B \leqslant |\mathcal{N}|$ denotes a security budget. Since, securing control-center's communication to every PV node in a geographically diverse DN might be costly/impractical, we impose that the maximum number of nodes the defender can secure is B. A defender's choice $u \in \mathcal{U}_B$ implies that a PV at node i is secure if $u_i = 1$ (i.e. PV at node i cannot be compromised), and vulnerable to attack if $u_i = 0$. Let $\mathcal{N}_s(u) := \{i \in \mathcal{N} | u_i = 1\}$ and $\mathcal{N}_v(u) := \mathcal{N} \backslash \mathcal{N}_s(u)$ denote the set of secure and vulnerable nodes, for a defender choice u.[3]

Stage 2 [Attack]:Let $\Psi_M(u) := \mathcal{S}(u) \times \mathcal{D}_M(u)$ denotes the set of attacker actions for a defender's choice u, where

$$
\begin{aligned}
\mathcal{S}(u) &:= \textstyle\prod_{i \in \mathcal{N}_v(u)} \mathcal{S}_i \times \prod_{j \in \mathcal{N}_s(u)} \{0 + 0\mathbf{j}\}\\
\mathcal{D}_M(u) &:= \{\delta \in \{0,1\}^{\mathcal{N}} \mid \delta \leqslant \mathbf{1}_N - u, \ \|\delta\|_0 \leqslant M\},
\end{aligned}
$$

and $M \leqslant |\mathcal{N}_v|$ is the maximum number of PVs that the attacker can compromise. This limit accounts for the attacker's resource constraints (and/or restrict his influence based on his knowledge of PV vulnerabilities). The attacker *simultaneously* compromises a subset of vulnerable PV nodes by introducing incorrect set-points (see the adversary model (8c)), and increase the loss L (see (9)). The attacker's choice is denoted by $\psi := \left[\mathrm{sp}^{\mathrm{a}}, \delta\right] \in \Psi_M(u)$, where sp^{a} denotes the vector of incorrect set-points chosen by the attacker, and $\delta \in \mathcal{D}_M$ denotes the attack vector that indicates the subset of PVs compromised. A PV at node i is compromised if $\delta_i = 1$, and not compromised if $\delta_i = 0$.

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

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

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

D. Assumptions

In general, $[\mathrm{DAD}]$ is a non-convex, non-linear, tri-level optimization problem with mixed-integer decision variables. Hence, it is a computationally hard problem. Our goals are:

(i) to provide structural insights about the optimal attacker and defender strategies of the $[\mathrm{DAD}]$ game;

[2] Note that, under this adversary model, the impact of PV compromise is different than the impact of a natural event, e.g. cloud cover, during which $pg = \mathbf{0}$. The reactive power contribution may be non-negative during a natural event; however, as we show in §III-C, a compromised PV always contributes reactive power equal to the negative of apparent power capability to the DN.

[3] Note that when we say a node is secure, we mean that the PV at that node is not prone to compromise by the attacker. From a practical viewpoint, the defender can secure a PV node by investing in node security solutions such as installing intrusion prevention/detection systems (IPS/IDS) [12]. These security solutions are complementary to the device hardening technologies that can secure the PV-inverter assembly. Our focus is on security against an external threat agent interested in simultaneously compromising multiple PVs. Thus, we restrict our attention to node security solutions.

(ii) to approximate the non-linear (hard) problem by formulating computationally tractable variants based on linear power flow models.

To address these goals we make the following assumptions:

$(\mathbf{A0})_\mathbf{0}$ **Voltage quality:** In no attack (nominal) conditions, the voltage quality bounds (1) are satisfied by both $\mathcal{X}$ and $\widehat{\mathcal{X}}$.

$(\mathbf{A0})_\mathbf{1}$ **Safety:** Safety bounds (2) are always satisfied, i.e., $\forall\ (u, \psi, \phi) \in \mathcal{U}_B \times \Psi \times \Phi$, $\forall\ \mathrm{x}(u, \psi, \phi) \in \mathcal{X}$, $\underline{\mu}\mathbf{1}_N \leqslant \nu \leqslant \overline{\mu}\mathbf{1}_N$.

$(\mathbf{A0})_\mathbf{2}$ **No reverse power flows:** Power flows from the substation node towards the downstream nodes, i.e., $\widehat{S} \geqslant 0$. This implies that $\forall\ \hat{\mathrm{x}} \in \widehat{\mathcal{X}},\ \hat{\nu} \leqslant \nu_0\mathbf{1}_N$; similarly, for NPF model.

$(\mathbf{A0})_\mathbf{3}$ **Small impedance:** All power flows are in the per unit (*p.u.*) system, i.e., $\nu_0 = 1$ and $\forall\ (i, j) \in \mathcal{E},\ |S_j| < 1$. Furthermore, the resistances and reactances are small, i.e.,

$$\forall\ (i, j) \in \mathcal{E}, r_j \leqslant \frac{\underline{\mu}^2}{4\underline{\mu}+8} < 1,\ x_j \leqslant \frac{\underline{\mu}^2}{4\underline{\mu}+8} < 1,$$

and the common path resistances and reactances are also smaller than 1, i.e., $R_{ii} \leqslant 1$ and $X_{ii} \leqslant 1\ \forall\ i \in \mathcal{N}$.

$(\mathbf{A0})_\mathbf{4}$ **Small line losses:** The line losses are very small compared to the power flows, i.e., $\forall\ \mathrm{x} \in \mathcal{X},\ z \odot \ell \leqslant \epsilon_0 S$, where ϵ_0 is a small positive number. [4]

$(\mathbf{A0})_0$-$(\mathbf{A0})_1$ are standard assumptions. $(\mathbf{A0})_2$ assumes that the PV penetration level is such that the net demand is always positive. In real-world DNs, both r_js and x_js are typically around 0.01 $(\mathbf{A0})_3$. Also, residential load power factors ($^{pc_j}/_{|sc_j|}$) are in range of 0.88-0.95. For these values, one can show that $\epsilon_0 \approx 0.05$ $(\mathbf{A0})_4$. We will denote $(\mathbf{A0})_0$-$(\mathbf{A0})_4$ by **(A0)** .

Now, let $\epsilon := (1-\epsilon_0)^{-H} - 1$, and consider another linear power flow model (which we call the ϵ-LPF model):

$$\check{S}_j = \textstyle\sum_{k:(j,k)\in\mathcal{E}} \check{S}_k + (1+\epsilon)(\check{sc}_j - \check{sg}_j) \tag{11a}$$

$$\check{\nu}_j = \check{\nu}_i - 2\mathbf{Re}(\bar{z}_j\check{S}_j) \tag{11b}$$

$$\check{\ell}_j = \frac{|\check{S}_j|^2}{\check{\nu}_i}, \tag{11c}$$

and $\check{\mathrm{x}} := \left[\check{\nu}, \check{\ell}, \check{sc}, \check{sg}, \check{S}\right]$ is a state of ϵ-LPF model, and $\check{\mathcal{X}}$ is the set of all states $\check{\mathrm{x}}$ with no reverse power flows (analogously defined as $\mathcal{X}$ and $\widehat{\mathcal{X}}$). Note that for $\epsilon = 0$, (11) becomes (6).

We will consider two variants of the [DAD] game (7)-(8):

$$[\widehat{\text{DAD}}]\ \widehat{\mathcal{L}} := \min_{u\in\mathcal{U}_B}\ \max_{\psi\in\Psi_M}\ \min_{\phi\in\Phi}\ \widehat{\mathrm{L}}(\hat{\mathrm{x}}(u, \psi, \phi))$$

$$\text{s.t.}\quad \hat{\mathrm{x}}(u, \psi, \phi) \in \widehat{\mathcal{X}}, (8b), (8c)$$

$$[\widecheck{\text{DAD}}]\ \check{\mathcal{L}} := \min_{u\in\mathcal{U}_B}\ \max_{\psi\in\Psi_M}\ \min_{\phi\in\Phi}\ \check{\mathrm{L}}(\hat{\mathrm{x}}(u, \psi, \phi))$$

$$\text{s.t.}\quad \check{\mathrm{x}}(u, \psi, \phi) \in \check{\mathcal{X}}, (8b), (8c)$$

where $\widehat{\mathrm{L}}(\hat{\mathrm{x}}) := \mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}}) + \mathrm{L}_{\mathrm{LC}}(\hat{\mathrm{x}})$, and $\check{\mathrm{L}}(\check{\mathrm{x}}) := \mathrm{L}_{\mathrm{VR}}(\check{\mathrm{x}}) + \mathrm{L}_{\mathrm{LC}}(\check{\mathrm{x}})$ are the loss functions for $[\widehat{\text{DAD}}]$ and $[\widecheck{\text{DAD}}]$, respectively. Note that the loss functions $\widehat{\mathrm{L}}$ and $\check{\mathrm{L}}$ do not have the line losses term. The optimal loss L of $[\widehat{\text{DAD}}]$ and $[\widecheck{\text{DAD}}]$ are denoted by $\widehat{\mathcal{L}}$ and $\check{\mathcal{L}}$, respectively. Our results in §III-IV show that $[\widehat{\text{DAD}}]$ (resp. $[\widecheck{\text{DAD}}]$) help provide under (resp. over) approximation of [DAD]; and the derivation of structural properties of optimal strategies in both $[\widehat{\text{DAD}}]$ and $[\widecheck{\text{DAD}}]$ is analogous to one another.

We will, henceforth, abuse the notation, and use Ψ and Φ to denote $\Psi_M(u)$ and $\Phi(u, \psi)$, respectively.

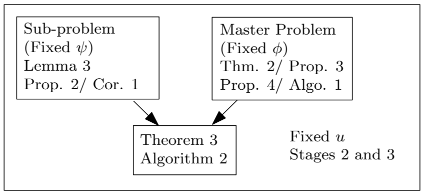


Fig. 3: Outline of Technical Results in §III

III. Attacker-Defender Sub-game

In this section, we consider the sub-game (Stages 2 and 3) induced by a fixed defender security strategy u in Stage 1:

$$[\text{AD}]\quad \mathcal{L}^u\ := \max_{\psi\in\Psi}\ \min_{\phi\in\Phi}\ \mathrm{L}(\mathrm{x}(u, \psi, \phi))\quad \text{s.t.}\quad (8)$$

Analogous to the variants of [DAD], $[\widehat{\text{DAD}}]$ and $[\widecheck{\text{DAD}}]$, we define two variants of the sub-game [AD]: $[\widehat{\text{AD}}]$ (resp. $[\widecheck{\text{AD}}]$) with $\widehat{\mathcal{X}}$ (resp. $\check{\mathcal{X}}$) in (8a). The optimal losses of $[\widehat{\text{AD}}]$ and $[\widecheck{\text{AD}}]$ are denoted by $\widehat{\mathcal{L}}^u$ and $\check{\mathcal{L}}^u$), respectively.

For simplicity and *without loss of generality*, we focus on case for $u = \mathbf{0}$; i.e., no node is secured by the defender in Stage 1. With further abuse of notation, for a strategy profile $(\mathbf{0}, \psi, \phi)$, we denote $\mathrm{x}(\mathbf{0}, \psi, \phi)$ by $\mathrm{x}(\psi, \phi)$ as the solution of NPF model. Similarly, redefine $\hat{\mathrm{x}}(\psi, \phi)$ and $\check{\mathrm{x}}(\psi, \phi)$. We also drop the superscript u from $\mathcal{L}^u$, $\widehat{\mathcal{L}}^u$ and $\check{\mathcal{L}}^u$.

Following the computational approach in the literature to solve (bilevel) interdiction problems [10], [20], we define the master-problem $[\text{AD}]^{\mathrm{a}}$ (resp. sub-problem $[\text{AD}]^{\mathrm{d}}$) for fixed $\phi \in \Phi$ (resp. fixed $\psi \in \Psi$):

$$[\text{AD}]^{\mathrm{a}}\quad \psi^*(\phi) \in \operatorname{argmax}_{\psi\in\Psi} \mathrm{L}(\mathrm{x}(\psi, \phi))\quad \text{s.t.}\quad (8),$$

$$[\text{AD}]^{\mathrm{d}}\quad \phi^*(\psi) \in \operatorname{argmin}_{\phi\in\Phi} \mathrm{L}(\mathrm{x}(\psi, \phi))\quad \text{s.t.}\quad (8).$$

Similarly, define master- and sub- problems $[\widehat{\text{AD}}]^{\mathrm{a}}$ and $[\widehat{\text{AD}}]^{\mathrm{d}}$ (resp. $[\widecheck{\text{AD}}]^{\mathrm{a}}$ and $[\widecheck{\text{AD}}]^{\mathrm{d}}$) for the variants $[\widehat{\text{AD}}]$ (resp. $[\widecheck{\text{AD}}]$).

Sec. III-A focuses on bounding the optimal loss for [AD] with the losses in $[\widehat{\text{AD}}]$ and $[\widecheck{\text{AD}}]$. We focus on the master- and sub- problems in §III-B and §III-C, respectively. This leads to an iterative approach in §III-D to solve the sub-games [AD], $[\widehat{\text{AD}}]$, $[\widecheck{\text{AD}}]$. Fig. 3 provides an outline of these results.

[4] Equivalently, ϵ_0 is an upper bound on the maximum ratio of the magnitudes of line losses and the power flows, i.e., $\epsilon_0 = \max_{(i,j)\in\mathcal{E}, P_j\neq 0, Q_j\neq 0} \max\left(^{r_j\ell_j}/_{P_j}, ^{x_j\ell_j}/_{Q_j}\right)$.

A. Upper and Lower Bounds on $\mathcal{L}$

Theorem 1. *Let (ψ^*, ϕ^*), $(\widehat{\psi}^*, \widehat{\phi}^*)$ and $(\check{\psi}^*, \check{\phi}^*)$ be optimal solutions to $[\text{AD}]$, $[\widehat{\text{AD}}]$ and $[\widecheck{\text{AD}}]$, respectively; and denote the optimal losses by $\mathcal{L}$, $\widehat{\mathcal{L}}$, $\check{\mathcal{L}}$, respectively. Then,*

$$\widehat{\mathcal{L}} \leqslant \mathcal{L} \leqslant \check{\mathcal{L}} + \tfrac{\underline{\mu}N}{2\underline{\mu}+4}. \tag{14}$$

To prove Thm. 1, we first prove a preliminary result that relates $\mathrm{x}(\psi, \phi)$, $\widehat{\mathrm{x}}(\psi, \phi)$, and $\check{\mathrm{x}}(\psi, \phi)$:

Proposition 1. *For a fixed strategy profile $(\psi, \phi) \in \Psi \times \Phi$,*

$$\widehat{S} \leqslant S \leqslant \check{S}, \quad \widehat{\nu} \geqslant \nu \geqslant \check{\nu}, \quad \widehat{\ell} \leqslant \ell \leqslant \check{\ell}.$$

Hence,

$$\left.\begin{array}{l} \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}) \leqslant \mathrm{L}_{\mathrm{VR}}(\mathrm{x}) \leqslant \mathrm{L}_{\mathrm{VR}}(\check{\mathrm{x}}) \\ \mathrm{L}_{\mathrm{LC}}(\widehat{\mathrm{x}}) = \mathrm{L}_{\mathrm{LC}}(\mathrm{x}) = \mathrm{L}_{\mathrm{LC}}(\check{\mathrm{x}}) \\ \mathrm{L}_{\mathrm{LL}}(\widehat{\mathrm{x}}) \leqslant \mathrm{L}_{\mathrm{LL}}(\widehat{\mathrm{x}}) \leqslant \mathrm{L}_{\mathrm{LL}}(\check{\mathrm{x}}) \end{array}\right\} \implies \mathrm{L}(\widehat{\mathrm{x}}) \leqslant \mathrm{L}(\mathrm{x}) \leqslant \mathrm{L}(\check{\mathrm{x}}). \tag{15}$$

Prop. 1 implies that any attack ψ that increases $\widehat{\mathcal{L}}$ in $[\widehat{\text{AD}}]$ (relative to the no attack case), also increases $\mathcal{L}$ in $[\text{AD}]$ and $\check{\mathcal{L}}$ in $[\widecheck{\text{AD}}]$, respectively. The converse need not be true, i.e., an attack that increases $\mathcal{L}$ in $[\text{AD}]$ (resp. $\check{\mathcal{L}}$ in $[\widecheck{\text{AD}}]$) need not increase $\widehat{\mathcal{L}}$ in $[\widehat{\text{AD}}]$ (resp. $\mathcal{L}$ in $[\text{AD}]$). Similarly, any defender response ϕ that reduces $\check{\mathcal{L}}$ (resp. $\mathcal{L}$), also reduces $\mathcal{L}$ (resp. $\widehat{\mathcal{L}}$). Again, the converse statements do not apply here.

Proof: The relationships $\widehat{S} \leqslant S$ and $\widehat{\nu} \geqslant \nu$ are proved in [21].

The rest of the proof of Prop. 1 utilizes two lemmas.

Lemma 1. *Consider a fixed $(\psi, \phi) \in \Psi \times \Phi$. The following holds: $sc = \widehat{sc} = \check{sc}$, $sg = \widehat{sg} = \check{sg}$, and*

$$\check{S} = (1+\epsilon)\widehat{S} \tag{16a}$$

$$\check{\nu} - \nu_0\mathbf{1}_N = (1+\epsilon)(\widehat{\nu} - \nu_0\mathbf{1}_N) \tag{16b}$$

$$\forall\ (i,j) \in \mathcal{E} \begin{cases} S_j = \sum_{k\in\Lambda_j} s_k + z_k\ell_k & \text{(17a)} \\ \widehat{S}_j = \sum_{k\in\Lambda_j} s_k & \text{(17b)} \end{cases}$$

$$\forall\ j \in \mathcal{N} \begin{cases} \widehat{\nu}_j = \nu_0 - 2\sum_{k\in\mathcal{N}} \mathbf{Re}(\bar{Z}_{jk}s_k) & \text{(18a)} \\ \check{\nu}_j = \nu_0 - 2(1+\epsilon)\sum_{k\in\mathcal{N}} \mathbf{Re}(\bar{Z}_{jk}s_k) & \text{(18b)} \\ \widehat{\nu}_j = \nu_0 - 2\sum_{k\in\mathcal{P}_j} \mathbf{Re}(\bar{z}_k\widehat{S}_k). & \text{(18c)} \\ \check{\nu}_j = \nu_0 - 2\sum_{k\in\mathcal{P}_j} \mathbf{Re}(\bar{z}_k\check{S}_k). & \text{(18d)} \end{cases}$$

Proof: Recursively apply the power flow models (5), (6), and (11), from the root node to leaf nodes. ■

Lemma 2. *For a fixed $(\psi, \phi) \in \Psi \times \Phi$,*

$$\forall \quad (i,j) \in \mathcal{E}, \quad S_j \leqslant \tfrac{\widehat{S}_j}{(1-\epsilon_0)^{H-|\mathcal{P}_j|+1}}. \tag{19}$$

Proof:

We apply induction from leaf nodes to the root node. **Base case:** For any leaf node $k \in \mathcal{N}_L$,

$$z_k\ell_k \overset{(\mathbf{A0})_4}{\leqslant} \epsilon_0 S_k \overset{(17a)}{=} \epsilon_0(s_k + z_k\ell_k)$$

$$\therefore z_k\ell_k \leqslant \tfrac{\epsilon_0 s_k}{1-\epsilon_0} \overset{(17b)}{=} \tfrac{\epsilon_0\widehat{S}_k}{1-\epsilon_0}.$$

Now, for any $j \in \mathcal{N}\backslash\mathcal{N}_L$,

$$z_j\ell_j \overset{(\mathbf{A0})_4}{\leqslant} \epsilon_0 S_j \overset{(5a)}{=} \epsilon_0\big[\textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j + z_j\ell_j\big]$$

$$\therefore z_j\ell_j \leqslant \tfrac{\epsilon_0}{1-\epsilon_0}\big[\textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j\big].$$

Adding $\sum S_k + s_j$ on both the sides:

$$\underbrace{\textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j + z_j\ell_j}_{S_j} \leqslant \tfrac{1}{1-\epsilon_0}\big[\textstyle\sum_{k:(j,k)\in\mathcal{E}} S_k + s_j\big].$$

Inductive step: By inductive hypothesis (IH) on $\mathcal{C}_j$,

$$S_j \overset{\text{(IH)}}{\leqslant} \tfrac{1}{(1-\epsilon_0)^{H-|P_k|+2}}\big[\textstyle\sum_{k:(j,k)\in\mathcal{E}} \widehat{S}_k + s_j\big]$$

$$= \tfrac{\widehat{S}_j}{(1-\epsilon_0)^{H-|P_j|+1}} \quad (\because |\mathcal{P}_j| = |\mathcal{P}_k| - 1).$$

■

From Lemma 2, for any $(i,j) \in \mathcal{E}$,

$$S_j \leqslant \tfrac{\widehat{S}_j}{(1-\epsilon_0)^{H-|\mathcal{P}_j|+1}} \leqslant \tfrac{\widehat{S}_j}{(1-\epsilon_0)^{H}} = (1+\epsilon)\widehat{S}_j \overset{(16a)}{=} \check{S}_j. \tag{20}$$

For nodal voltages,

$$\begin{aligned} \nu_j &\overset{(5b)}{=} \nu_i - 2\mathbf{Re}(\bar{z}_jS_j) + |z|_j^2\,\ell_j \\ &\geqslant \nu_i - 2\mathbf{Re}(\bar{z}_jS_j) \\ &\overset{(20)}{\geqslant} \nu_i - 2\mathbf{Re}(\bar{z}_j\check{S}_j). \end{aligned} \tag{21}$$

Applying (21) recursively from the node j till root node:

$$\nu_j \geqslant \nu_0 - 2\textstyle\sum_{k\in\mathcal{P}_j} \mathbf{Re}(\bar{z}_k\check{S}_k) \overset{(18d)}{=} \check{\nu}_j.$$

Thus, $\widehat{S}_j \leqslant S_j \leqslant \check{S}_j$ and $\widehat{\nu}_j \geqslant \nu_j \geqslant \check{\nu}_j$. Furthermore,

$$\widehat{S}_j \leqslant S_j \leqslant \check{S}_j \overset{(\mathbf{A0})_2}{\implies} \left|\widehat{S}_j\right|^2 \leqslant |S_j|^2 \leqslant \left|\check{S}_j\right|^2$$

$$\implies \tfrac{|\widehat{S}_j|^2}{\widehat{\nu}_j} \leqslant \tfrac{|S_j|^2}{\nu_j} \leqslant \tfrac{|\check{S}|^2}{\check{\nu}_j} \implies \widehat{\ell} \leqslant \ell \leqslant \check{\ell}.$$

Finally, (15) immediately follows from (9), (10), and (14). ■

*Proof of **Theorem 1**:*
For any $\mathrm{x} \in \mathcal{X}$,

$$\mathrm{L}_{\mathrm{LL}}(\mathrm{x}) \overset{(5c)}{=} \sum_{(i,j)\in\mathcal{E}} \frac{r_j(P_j^2+Q_j^2)}{\nu_i} \overset{(\mathbf{A0})_1,(\mathbf{A0})_3}{\leqslant} \frac{2}{\underline{\mu}} \sum_{(i,j)\in\mathcal{E}} r_j \overset{(\mathbf{A0})_3}{\leqslant} \frac{\underline{\mu}N}{2\underline{\mu}+4} \tag{22}$$

Hence,

$$\begin{aligned} \check{\mathcal{L}} &= \check{\mathrm{L}}(\check{\mathrm{x}}(\check{\psi}^*, \check{\phi}^*(\check{\psi}^*))) \\ &\geqslant \check{\mathrm{L}}(\check{\mathrm{x}}(\psi^*, \check{\phi}^*(\psi^*))) && \text{(by optimality of } \check{\psi}^*) \\ &\geqslant \check{\mathrm{L}}(\mathrm{x}(\psi^*, \check{\phi}^*(\psi^*))) && \text{(by Proposition 1)} \\ &\overset{(22)}{\geqslant} \mathrm{L}(\mathrm{x}(\psi^*, \check{\phi}^*(\psi^*))) - \tfrac{\underline{\mu}N}{2\underline{\mu}+4} \\ &\geqslant \mathrm{L}(\mathrm{x}(\psi^*, \phi^*(\psi^*))) - \tfrac{\underline{\mu}N}{2\underline{\mu}+4} && \text{(by optimality of } \phi^*) \\ &= \mathcal{L} - \tfrac{\underline{\mu}N}{2\underline{\mu}+4}. \end{aligned}$$

Similarly, one can show $\mathcal{L} \geqslant \widehat{\mathcal{L}}$. ■

Thm. 1 implies that the value of the sub-game $[\text{AD}]$ with NPF can be lower (resp. upper) bounded by the value of $[\widehat{\text{AD}}]$ (resp. $[\widecheck{\text{AD}}]$). Our subsequent results show that both $[\widehat{\text{AD}}]$ and $[\widecheck{\text{AD}}]$ admit computationally efficient solutions.

B. Optimal defender response under fixed attacker strategy ψ

We consider the sub-problem $[\mathrm{AD}]^{\mathrm{d}}$, i.e., the problem of computing optimal defender response $\phi^*(\psi)$ for a fixed attack ψ. The proofs for this subsection are in Appendix.

The following Lemma shows that $[\mathrm{AD}]^{\mathrm{d}}$ is a Second-Order Cone Program (SOCP), and hence, can be solved efficiently.

Lemma 3. *Let $\mathcal{X}_{CPF} := conv(\mathcal{X})$, i.e., $\mathcal{X}_{CPF}$ is the set of states x satisfying (2)-(4), (5a), (5b), and the relaxation of (5c):*

For a fixed $\psi \in \Psi$, the problem of minimizing $\mathrm{L}(\mathrm{x}(\psi, \phi))$ subject to $\mathrm{x} \in \mathcal{X}_{CPF}$, (8b), (8c) is a SOCP. Its optimal solution, $\phi^{**}(\psi)$, is also optimal for $[AD]^{\mathrm{d}}$.

For fixed ψ (attack) and fixed load control parameter γ (e.g. when changing γ is not allowed), the following proposition provides a range of optimal defender set-points $\widehat{\mathrm{sp}}^{d*}$ and $\check{\mathrm{sp}}^{d*}$ for LPF and ϵ-LPF models, respectively. Note that, if γ is fixed, $\mathrm{L}_{\mathrm{LC}}(\hat{\mathrm{x}})$ is also fixed. Then, the defender set-points can be chosen by using $\mathrm{L}_{\mathrm{VR}}(\hat{\mathrm{x}})$ as a loss function, instead of $\widehat{\mathrm{L}}(\hat{\mathrm{x}})$. Similar argument holds for $\check{\mathrm{L}}(\check{\mathrm{x}})$.

Proposition 2. *Consider $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$ with fixed $\gamma \in \Gamma$. Then $\forall i \in \mathcal{N}$,*

$$\delta_i = 0 \implies \left|\widehat{\mathrm{sp}}_i^{d*}\right| = \overline{\mathrm{sp}}_i, \quad \angle\widehat{\mathrm{sp}}_i^{d*} \in [\operatorname{arccot}\overline{K}, \operatorname{arccot}\underline{K}].$$

Furthermore, if the DN has identical $\mathbf{r}/\mathbf{x} \equiv K$ ratio, then

$$\delta_i = 0 \implies \left|\widehat{\mathrm{sp}}_i^{d*}\right| = \overline{\mathrm{sp}}_i, \quad \angle\widehat{\mathrm{sp}}_i^{d*} = \operatorname{arccot} K. \tag{23}$$

Similar results hold for $[\widecheck{\mathrm{AD}}]^{\mathrm{d}}$.

C. Optimal attack under fixed defender response ϕ

Now, we focus on the master problem $[\mathrm{AD}]^{\mathrm{a}}$, i.e., the problem of computing optimal attack for a fixed defender response ϕ. The following Theorem characterizes the optimal attacker set-point be denoted $\mathrm{sp}_i^{a*} = \mathbf{Re}(\mathrm{sp}_i^{a*}) + \mathbf{jIm}(\mathrm{sp}_i^{a*})$, when $\delta_i^* = 1$ (i.e. PV at node i is targeted by the attacker).

Theorem 2. *Consider $[\mathrm{AD}]^{\mathrm{a}}$ for a fixed $\delta \in \mathcal{D}_M$ (i.e., the PVs compromised by the attacker are specified by δ and the only decision variables in $[\mathrm{AD}]^{\mathrm{a}}$ are sp^{a}). Then*

$$\forall\ i \in \mathcal{N} \text{ s.t. } \delta_i = 1, \quad \mathrm{sp}_i^{a*} = 0 - \boldsymbol{j}\overline{\mathrm{sp}}_i. \tag{24}$$

Same holds for both $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ and $[\widecheck{\mathrm{AD}}]^{\mathrm{a}}$.

Proof: If $\delta_i = 1$, then $pg_i = \widehat{pg}_i = \mathbf{Re}(\mathrm{sp}_i) = \mathbf{Re}(\mathrm{sp}_i^{a*})$.

We first prove the simpler case for $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$. From (6), one can check that as functions of $\widehat{pg}_i$, $\widehat{P}$ is strictly decreasing, $\widehat{Q}$ is constant, and $\hat{\nu}$ is strictly increasing. Hence, $\widehat{\mathrm{L}}(\psi, \phi_f)$ is strictly increasing in $\widehat{pg}_i$ (because L_{VR} is non-decreasing as $\hat{\nu}$ is decreasing; L_{LC} is constant). Hence, to minimize the loss L, the attacker chooses $\mathbf{Re}(\widehat{\mathrm{sp}}_i^{a*}) = 0$. Similarly, $\mathbf{Im}(\widehat{\mathrm{sp}}_i^{a*}) = 0$. Similarly, we can show that in $[\widecheck{\mathrm{AD}}]^{\mathrm{a}}$, $\check{\mathrm{sp}}^{a*} = \mathbf{0}$.

Now, we prove the case for $[\mathrm{AD}]^{\mathrm{a}}$ by contradiction. Suppose that there exists $i \in \mathcal{N}$ s.t. $\mathbf{Re}(\mathrm{sp}_i^{a*}) > 0$. Then we can construct another attacker strategy $\widetilde{\psi}^* = [\widetilde{\delta}, \widetilde{\mathrm{sp}}^{\mathrm{a}}]$ that can further maximize L, such that $\mathbf{Re}(\mathrm{sp}_i^{a*}) = 0$, holding all else equal, i.e., $\widetilde{\delta} = \delta, \forall\ j \in \mathcal{N},\ \mathbf{Im}(\widetilde{\mathrm{sp}}_j^{\mathrm{a}}) = \mathbf{Im}(\mathrm{sp}_j^{a*}), \forall\ j \in \mathcal{N} : j \neq i,\ \mathbf{Re}(\widetilde{\mathrm{sp}}_j^{\mathrm{a}}) = \mathbf{Re}(\mathrm{sp}_j^{a*})$.

Let $(\mathrm{sp}^{\mathrm{a}}, \ell)$ be the decision variables for $[\mathrm{AD}]^{\mathrm{a}}$, as for fixed ϕ, the other decision variables P, Q, ν can then be written as affine functions of $(\mathrm{sp}^{\mathrm{a}}, \ell)$ from (5). Let $(\mathrm{sp}^{\mathrm{a}*}, \ell^*)$ (resp. $(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \widetilde{\ell})$) be the solution to $[\mathrm{AD}]^{\mathrm{a}}$ when $\psi = \psi^*$ (resp. $\psi = \widetilde{\psi}$).

Let $f \in \mathbb{R}_+^N$ such that, for any $(i, j) \in \mathcal{E}$, $f_j(\mathrm{sp}^{\mathrm{a}}, \ell) := \frac{P_j^2 + Q_j^2}{\nu_i}$. Let $f^* = f(\mathrm{sp}^{\mathrm{a}*}, \ell^*)$, $f' = f(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \ell^*)$, and $\widetilde{f} = f(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \widetilde{\ell})$.

Since $(\mathrm{sp}^{\mathrm{a}*}, \ell^*)$ and $(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \widetilde{\ell})$ are solutions to $[\mathrm{AD}]^{\mathrm{a}}$, they satisfy (5c). Hence, $f^* = \ell^*$, and $\widetilde{f} = \widetilde{\ell}$. Furthermore, it can be checked that $f' > f^*$. We want to show that $\widetilde{f} > f'$. Assume that $\widetilde{f} > f'$. Then, $\widetilde{f} > f^*$. Hence, $\mathrm{L}(\widetilde{\mathrm{x}}) > \mathrm{L}(\mathrm{x}^*)$, (because, $\mathrm{L}_{\mathrm{VR}}(\widetilde{\mathrm{x}}) > \mathrm{L}_{\mathrm{VR}}(\mathrm{x}^*)$, $\mathrm{L}_{\mathrm{LC}}(\widetilde{\mathrm{x}}) = \mathrm{L}_{\mathrm{LC}}(\mathrm{x}^*)$, $\mathrm{L}_{\mathrm{LL}}(\widetilde{\mathrm{x}}) > \mathrm{L}_{\mathrm{LL}}(\mathrm{x})$). However, this is a contradiction, as it violates the optimality of $\mathrm{sp}^{\mathrm{a}*}$. By similar logic, we can show that $\forall\ i \in \mathcal{N},\ \mathbf{Im}(\mathrm{sp}_i^{\mathrm{a}*}) = -\overline{\mathrm{sp}}_i$.

We now prove that $\widetilde{f} > f'$, with the help of an illustrative diagram (see Fig. 4).

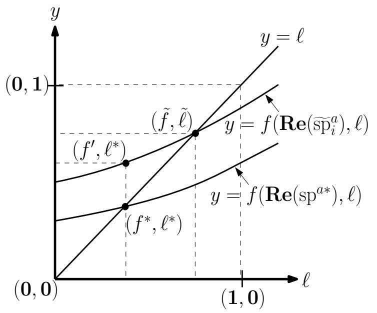

y
$y = \ell$
$(\mathbf{0}, \mathbf{1})$
$(\tilde{f}, \tilde{\ell})$
$y = f(\mathbf{Re}(\widetilde{\mathrm{sp}}_i^a), \ell)$
(f', ℓ^*)
$y = f(\mathbf{Re}(\mathrm{sp}^{a*}), \ell)$
(f^*, ℓ^*)
$(\mathbf{0}, \mathbf{0})$
$(\mathbf{1}, \mathbf{0})$
ℓ

Fig. 4: Illustrative diagram showing how ℓ changes with sp^{a}

Note that from (5), one can show that for any ℓ, $f(\mathbf{Re}(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \ell)) > f(\mathbf{Re}(\mathrm{sp}^{\mathrm{a}*}, \ell))$. Now, consider the $(j, k)^{th}$ entry of Jacobian $\mathbf{J}_f(\ell)$.

$$\partial_{\ell_k} f_j = \frac{\nu_i \left(2P_j \partial_{\ell_k} P_j + 2Q_j \partial_{\ell_k} Q_j\right)}{\nu_i^2} - \frac{(P_j^2 + Q_j^2)\partial_{\ell_k} \nu_i}{\nu_i^2}$$

$$\begin{aligned}
\therefore \quad 0 &\overset{(A2)}{\leqslant} \partial_{\ell_k} f_j \overset{(A3)}{<} \frac{(2r_k + 2x_k)}{\nu_i} + \frac{(4R_{ik}r_k + 4X_{ik}x_k)}{\nu_i^2} \\
\implies \quad & 0 \leqslant \partial_{\ell_k} f_j \overset{(A3)}{<} (r_k + x_k)(2/\mu + 4/\mu^2) \quad \leqslant 1 \\
\implies \quad & 0 \leqslant \partial_{\ell_k} f_j < 1.
\end{aligned}$$

At $\ell = \mathbf{0}$, $f > \mathbf{0}$, and each entry of Jacobian $\mathbf{J}_f(\ell)$ is positive and smaller than 1. Hence, f intersects the hyperplane $y = \ell$, exactly once. Furthermore, $f(\mathbf{Re}(\widetilde{\mathrm{sp}}^{\mathrm{a}}, \ell)) > f(\mathbf{Re}(\mathrm{sp}^{\mathrm{a}*}, \ell))$. Hence, we can conclude that $\widetilde{\ell} = \widetilde{f} > f' > f^* = \ell^*$. ■

Fig. 5 shows the optimal attacker set-point sp_i^{a*} for $\delta_i^* = 1$, and the defender set-points for the PVs for $\delta_j^* = 0$.

Thanks to Thm. 2, sc and sg are determined by δ and ϕ (since optimal $\mathrm{sp}^{\mathrm{a}*}$ is given by (24)). Thus, for given (δ, ϕ),

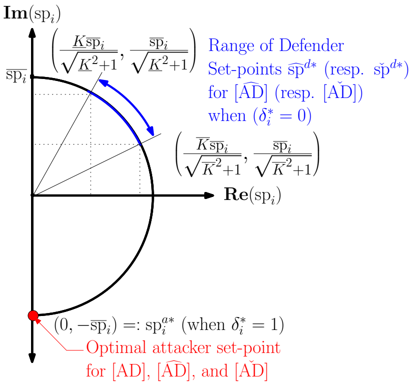

$\mathbf{Im}(\mathrm{sp}_i)$
$\left(\frac{\underline{K}\overline{\mathrm{sp}}_i}{\sqrt{\underline{K}^2+1}}, \frac{\overline{\mathrm{sp}}_i}{\sqrt{\underline{K}^2+1}}\right)$
Range of Defender
Set-points $\widehat{\mathrm{sp}}^{d*}$ (resp. $\check{\mathrm{sp}}^{d*}$)
for $[\widehat{\mathrm{AD}}]$ (resp. $[\check{\mathrm{AD}}]$)
when $(\delta_i^* = 0)$
$\overline{\mathrm{sp}}_i$
$\left(\frac{\overline{K}\overline{\mathrm{sp}}_i}{\sqrt{\overline{K}^2+1}}, \frac{\overline{\mathrm{sp}}_i}{\sqrt{\overline{K}^2+1}}\right)$
$\mathbf{Re}(\mathrm{sp}_i)$
$(0, -\overline{\mathrm{sp}}_i) =: \mathrm{sp}_i^{a*}$ (when $\delta_i^* = 1$)
Optimal attacker set-point
for [AD], $[\widehat{\mathrm{AD}}]$, and $[\check{\mathrm{AD}}]$

Fig. 5: Optimal attacker set-points (Thm. 2) and range for optimal defender set-points (Prop. 2).

loss function can be denoted as $\mathrm{L}(\mathrm{x}(\left[\mathbf{0} - \mathbf{j}\overline{\mathrm{sp}}, \delta\right], \phi))$; and [AD] can be restated as follows:

$$\mathcal{L} \quad = \quad \max_{\delta \in \mathcal{D}_M} \ \min_{\phi \in \Phi} \ \mathrm{L}(\mathrm{x}(\delta, \phi)) \quad \text{s.t.} \quad (8), (24)$$

Same holds for $[\widehat{\mathrm{AD}}]$ (resp. $[\check{\mathrm{AD}}]$) and $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ (resp. $[\check{\mathrm{AD}}]^{\mathrm{a}}$).

Let $\Delta_j(\widehat{\nu}_i)$ (resp. $\Delta_\delta(\widehat{\nu}_i)$) be the change in nodal voltage at node i caused due to compromise of PV at node j (resp. compromise of PVs due to attack vector δ). Similarly, define $\Delta_j(\check{\nu}_i)$ and $\Delta_\delta(\check{\nu}_i)$. The following Lemma is proved in the Appendix.

Lemma 4. *If ϕ is fixed, then*

$$\forall\ i, j \in \mathcal{N} \begin{cases} \Delta_j(\widehat{\nu}_i) = 2\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \boldsymbol{j}\overline{\mathrm{sp}}_j)) & \text{(25a)} \\ \Delta_j(\check{\nu}_i) = 2(1+\epsilon)\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \boldsymbol{j}\overline{\mathrm{sp}}_j)) & \text{(25b)} \end{cases}$$

$$\forall\ \delta \subseteq \mathcal{D}_M \begin{cases} \Delta_\delta(\widehat{\nu}_i) = \sum_{j:\delta_j=1} \Delta_j(\widehat{\nu}_i) & \text{(26a)} \\ \Delta_\delta(\check{\nu}_i) = \sum_{j:\delta_j=1} \Delta_j(\check{\nu}_i) & \text{(26b)} \end{cases}$$

For a fixed $\phi \in \Phi$, let $\widehat{\mathcal{D}}_M^i(\phi)$ be the set of optimal attack vectors that maximize LPF voltage bounds violation at a pivot node, say i. Formally,

$$\widehat{\mathcal{D}}_M^i(\phi) \ := \operatorname*{argmax}_{\delta \in \mathcal{D}_M} W_i(\underline{\nu}_i - \widehat{\nu}_i) \ \text{ s.t. } \widehat{\mathrm{x}}(\delta, \phi) \in \widehat{\mathcal{X}}, (8b), (8c) \tag{27}$$

Let $\widehat{\mathcal{D}}_M^* := \cup_{i \in \mathcal{N}} \widehat{\mathcal{D}}_M^i$, and $\widehat{\delta}^i \in \widehat{\mathcal{D}}_M^i$ denote any vector in $\widehat{\mathcal{D}}_M^i$. Similarly, define $\check{\mathcal{D}}_M^i(\phi)$, $\check{\mathcal{D}}_M^*(\phi)$, and $\check{\delta}^i$.

Using Lemma 4, Algorithm 1 computes optimal $\widehat{\delta}^*$ to maximize L_{VR} for a fixed defender action $\phi \in \Phi$ [17]. In each iteration, the Algorithm selects one node as a pivot node. For a pivot node, say i, a set of target nodes $\widehat{\delta}^i$ is determined by selecting M nodes with largest $\Delta_j(\widehat{\nu}_i)$ (see Algorithm 5 in Appendix). Applying Lemma 4, the final nodal voltage at the current pivot node i is given by $\widehat{\nu}_i - \Delta_{\widehat{\delta}^i}(\widehat{\nu}_i)$. The attack strategy that maximizes L_{VR} is the set $\widehat{\delta}^k$ corresponding to a pivot node k that admits maximum voltage bound violation when PVs specified by $\widehat{\delta}^k$ are compromised.

The following proposition shows that Algorithm 1 is optimal for DNs with identical $^{\mathbf{r}}\!/_{\mathbf{x}}$ ratio.

Algorithm 1 Optimal Attack for Fixed Defender Response

```
1: $\widehat{\delta}^*(\phi) \leftarrow$ OptimalAttackForFixedResponse($\phi$)
2: procedure OptimalAttackForFixedResponse($\phi$)
3:     Compute state vector for no attack $\widehat{\mathrm{x}}(\mathbf{0}, \phi) \in \widehat{\mathcal{X}}$
4:     for $i \in \mathcal{N}$ do
5:         $\widehat{\delta}^i \leftarrow$ GetPivotNodeOptimalAttack($i, \mathrm{sp}^{\mathrm{d}}$), and calculate $\Delta_{\widehat{\delta}^i}(\widehat{\nu}_i)$ using Lemma. 4
6:         Calculate new voltage value $\widehat{\nu}_i' \leftarrow \widehat{\nu}_i - \Delta_{\widehat{\delta}^i}(\widehat{\nu}_i)$
7:     end for
8:     $k \leftarrow \operatorname{argmax}_{i \in \mathcal{N}} W_i(\underline{\nu}_i - \widehat{\nu}_i')$
9:     return $\widehat{\delta} \leftarrow \widehat{\delta}^k$ (Pick $\widehat{\delta}^k$ which maximally violates (1))
10: end procedure
11: procedure GetPivotNodeOptimalAttack($i, \mathrm{sp}^{\mathrm{d}}$)
12:     $(J, \mathcal{N}_{g^i}, m') \leftarrow$ OptimalAttackHelper($i, \mathrm{sp}^{\mathrm{d}}$)
13:     Randomly choose $M - m'$ nodes from $\mathcal{N}_{g^i}$ to form $\mathcal{N}'$
14:     return $\widehat{\delta}^i \in \mathcal{D}_M$ such that $\widehat{\delta}_k^i = 1 \iff k \in J \cup \mathcal{N}'$
15: end procedure
```

Proposition 3. *For a fixed $\phi \in \Phi$, let $\widehat{\delta}$ be the optimal attack vector computed by Algorithm 1. Then $\widehat{\delta}$ is also an optimal solution of $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$. Same holds for $[\check{\mathrm{AD}}]^{\mathrm{a}}$.*

Proof: Note that for fixed $\phi \in \Phi$, maximizing $\widehat{\mathrm{L}}(\widehat{\delta}, \phi)$ (resp. $\check{\mathrm{L}}(\widehat{\delta}, \phi))$ is equivalent to maximizing $\mathrm{L}_{\mathrm{VR}}(\widehat{\delta}, \phi)$ (resp. $\mathrm{L}_{\mathrm{VR}}(\check{\delta}, \phi)$). Let $\widehat{\delta}^*$ be the optimal solution to $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$.

Case (i). $\mathrm{L}_{\mathrm{VR}}(\widehat{\delta}^*, \phi) = 0$. Then Algorithm 1 computes $\widehat{\delta}^*$ trivially, because $0 = \mathrm{L}_{\mathrm{VR}}(\widehat{\delta}^*, \phi) \geqslant \mathrm{L}_{\mathrm{VR}}(\widehat{\delta}, \phi)) \geqslant 0$. Hence, $\mathrm{L}_{\mathrm{VR}}(\widehat{\delta}, \phi)) = \mathrm{L}_{\mathrm{VR}}(\widehat{\delta}^*, \phi) = 0$.

Case (ii). $\mathrm{L}_{\mathrm{VR}}(\widehat{\delta}^*, \phi) > 0$. Let $\widehat{\nu}_j(\delta, \phi)$ denote the nodal voltage at node j after the attack δ. Since, $\widehat{\delta} = \widehat{\delta}^k$, for some pivot node $k \in \mathcal{N}$ (see Algorithm 1), $\widehat{\delta}^k$ maximally violates (1) over all $\widehat{\delta}^i$, i.e.,

$$\forall\ i \in \mathcal{N}, \quad \underline{\nu}_k - \widehat{\nu}_k(\widehat{\delta}^k, \phi) \geqslant \underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^i, \phi), \tag{28}$$

where $\widehat{\delta}^i$ is the optimal pivot node attack as computed by Algorithm 1 for node i, i.e.,

$$\forall\ i \in \mathcal{N},\ \forall\ \delta \in \mathcal{D}_M \quad \underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^i, \phi) \geqslant \underline{\nu}_i - \widehat{\nu}_i(\delta, \phi). \tag{29}$$

Let $i = \operatorname{argmax}_{j \in \mathcal{N}} W_j(\underline{\nu}_j - \widehat{\nu}_j(\widehat{\delta}^*, \phi))_+$. Furthermore, since $\mathrm{L}_{\mathrm{VR}}(\widehat{\delta}^*, \phi) > 0$,

$$\mathrm{L}_{\mathrm{VR}}(\widehat{\delta}^*, \phi) = W_i(\underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^*, \phi)) \tag{30}$$

$$\begin{aligned} &\therefore \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\widehat{\delta}, \phi)) = \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\widehat{\delta}^k, \phi)) \\ &\overset{(10a)}{=} \max_{j \in \mathcal{N}} W_j(\underline{\nu}_j - \widehat{\nu}_j(\widehat{\delta}^k, \phi))_+ \quad \overset{(28)}{\geqslant} W_i(\underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^i, \phi)) \\ &\overset{(29)}{\geqslant} W_i(\underline{\nu}_i - \widehat{\nu}_i(\widehat{\delta}^*, \phi)) \quad \overset{(30)}{=} \mathrm{L}_{\mathrm{VR}}(\widehat{\mathrm{x}}(\widehat{\delta}^*, \phi)). \end{aligned}$$

Furthermore, for a fixed ϕ $\mathrm{L}_{\mathrm{LC}}(\widehat{\mathrm{x}}(\widehat{\delta}, \phi)) = \mathrm{L}_{\mathrm{LC}}(\widehat{\mathrm{x}}(\widehat{\delta}^*, \phi))$. Hence, $\widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\widehat{\delta}, \phi)) \geqslant \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\widehat{\delta}^*, \phi))$. ■

We now show that the effect of PV compromise at either node j or k on the node i depends upon the locations of nodes j and k relative to node i. The following Proposition states that if node j is upstream to node k relative to the pivot node i ($j \prec_i k$), then the PV compromise at node k impacts on $\widehat{\nu}_i$ more than the PV compromise on node j; and if $j =_i k$, then the effect of PV compromise at j, k on $\widehat{\nu}_i$ is identical.

Proposition 4. *[17] Consider $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$. Let nodes $i, j, k \in \mathcal{N}$ where i is the pivot node, $\mathrm{sp}^{\mathrm{d}}_j = \mathrm{sp}^{\mathrm{d}}_k$, and $\overline{\mathrm{sp}}_j = \overline{\mathrm{sp}}_k$. If $j \prec_i k$ (resp. $j =_i k$), then $\Delta_j(\widehat{\nu}_i) < \Delta_k(\widehat{\nu}_i)$ (resp. $\Delta_j(\widehat{\nu}_i) = \Delta_k(\widehat{\nu}_i)$).*

Same holds true for $[\widecheck{\mathrm{AD}}]^{\mathrm{a}}$.

Prop. 4 implies that, broadly speaking, compromising downstream PVs is advantageous to the attacker than compromising the upstream PVs. The following illustrative example suggests that compromising PVs by means of clustered attacks are more beneficial to the attacker than distributed attacks.

Example 1. Consider the $[\widehat{\mathrm{AD}}]^{\mathrm{a}}$ with $M = 2$ instantiated on the DN in Fig. 2. Assume that all loads and PVs are homogeneous, all lines have equal impedances, i.e., $\forall i \in \mathcal{N}, sc_i = sc_a, \mathrm{sp}^{\mathrm{d}}_i = \mathrm{sp}^{\mathrm{d}}_a, \overline{\mathrm{sp}}_i = \overline{\mathrm{sp}}_a, z_i = z_a$. By Prop. 2, the outputs of all the PVs are fixed and identical to each other.

Let $\alpha = 2(\mathbf{Re}(\bar{z}_a(sc_a - \mathrm{sp}^{\mathrm{d}}_a)))$, and $\beta = 2(\mathbf{Re}(\bar{z}_a(\mathbf{Re}(\mathrm{sp}^{\mathrm{d}}_a) + \mathbf{j}(\mathbf{Im}(\mathrm{sp}^{\mathrm{d}}_a) + \overline{\mathrm{sp}}_a))))$. Then ν values for different attack vectors are given in Table I. The optimal attack compromises nodes i and m, which is a cluster attack.

Attacked Nodes	ν_m	ν_j	ν_k
$\varnothing$	$\nu_0 - 23\alpha$	$\nu_0 - 13\alpha$	$\nu_0 - 40\alpha$
$\{i, m\}$	$\nu_0 - 23\alpha - 9\beta$	$\nu_0 - 13\alpha - 2\beta$	$\nu_0 - 20\alpha - 4\beta$
$\{j, m\}$	$\nu_0 - 23\alpha - 6\beta$	$\nu_0 - 13\alpha - 4\beta$	$\nu_0 - 20\alpha - 3\beta$
$\{k, m\}$	$\nu_0 - 23\alpha - 7\beta$	$\nu_0 - 13\alpha - 2\beta$	$\nu_0 - 20\alpha - 6\beta$
$\{g, j\}$	$\nu_0 - 23\alpha - 2\beta$	$\nu_0 - 13\alpha - 5\beta$	$\nu_0 - 20\alpha - 2\beta$
$\{d, k\}$	$\nu_0 - 23\alpha - 4\beta$	$\nu_0 - 13\alpha - 2\beta$	$\nu_0 - 20\alpha - 7\beta$

TABLE I: ν vs Different Attack Combinations

Consequently, our results (see §IV) on security strategy in Stage 1 show that the defender should utilize his security strategy to deter cluster attacks.

D. A greedy approach for solving $[\widehat{\mathrm{AD}}]$, $[\widecheck{\mathrm{AD}}]$ and $[\mathrm{AD}]$

We now utilize results for sub- and master-problems to solve $[\mathrm{AD}]$. Consider the following assumption:

(A1) DN has identical $^{\mathbf{r}}\!/\mathbf{x} \equiv K$ ratio, i.e., $\forall\ j \in \mathcal{N}, K_j = K$.

In this subsection, we first present an algorithm to solve $[\widehat{\mathrm{AD}}]$ and $[\widecheck{\mathrm{AD}}]$ under (A1). Then we propose its extension, a greedy iterative approach, for solving $[\mathrm{AD}]$ under the general case.

Under (A1), the optimal defender set-points $\widehat{\mathrm{sp}}^{\mathrm{d}*}$ and $\widecheck{\mathrm{sp}}^{\mathrm{d}*}$ are as specified by Prop. 2, and hence fixed. For fixed optimal $\widehat{\mathrm{sp}}^{\mathrm{d}*}$ (resp. $\widecheck{\mathrm{sp}}^{\mathrm{d}*}$), we can solve the problem $[\widehat{\mathrm{AD}}]$ (resp. $[\widecheck{\mathrm{AD}}]$) by using Benders Cut method [20]. However, we present a computationally faster algorithm, Algorithm 2 that computes attacker's candidate optimal attack vectors $\widehat{\mathcal{D}}^*_M$ (resp. $\widecheck{\mathcal{D}}^*_M$) using Lemma 4.

Lemma 5. *Under (A0), (A1), for any two fixed $\widehat{\gamma}^1, \widehat{\gamma}^2 \in \Gamma$, $\widehat{\mathcal{D}}^*_M([\widehat{\mathrm{sp}}^{\mathrm{d}*}, \widehat{\gamma}^1]) = \widehat{\mathcal{D}}^*_M([\widehat{\mathrm{sp}}^{\mathrm{d}*}, \widehat{\gamma}^2])$.*

Proof: The computation of $\widehat{\mathcal{D}}^*_M(\phi)$ depends on $\Delta_j(\widehat{\nu}_i)$ values which depend only on sp^{d}, and not on $\widehat{\gamma}$ (see Lemma 4). ■

Given $\widehat{\mathrm{sp}}^{\mathrm{d}} \in \mathcal{S}$, it can be checked that Algorithm 2, in fact, computes $\widehat{\mathcal{D}}^i_M(\widehat{\mathrm{sp}}^{\mathrm{d}})$, and $\widehat{\mathcal{D}}^*_M(\widehat{\mathrm{sp}}^{\mathrm{d}}) = \bigcup_{i \in \mathcal{N}} \widehat{\mathcal{D}}^i_M(\widehat{\mathrm{sp}}^{\mathrm{d}})$ is the set of candidate optimal attack vectors.

Algorithm 2 computes the set of attacks $\widehat{\mathcal{D}}^*_M(\widehat{\mathrm{sp}}^{\mathrm{d}*})$, and iterates over each $\widehat{\delta} \in \widehat{\mathcal{D}}^*_M(\widehat{\mathrm{sp}}^{\mathrm{d}*})$. In each iteration, since $\mathrm{sp}^{\mathrm{d}} = \widehat{\mathrm{sp}}^{\mathrm{d}*}$ is fixed, the sub-problem $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$ reduces to an LP over the variable γ. Let $\widehat{\gamma}^*(\widehat{\delta})$ be the solution to the LP. Then, $\widehat{\phi}^*(\widehat{\delta}) = \left[\widehat{\mathrm{sp}}^{\mathrm{d}*}, \widehat{\gamma}^*(\widehat{\delta})\right]$ is the optimal solution to $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$. Choosing $\widehat{\delta}^* = \mathrm{argmax}_{\widehat{\delta} \in \widehat{\mathcal{D}}^*_M} \mathrm{L}(\widehat{\mathrm{x}}(\widehat{\delta}, \widehat{\phi}^*(\widehat{\delta})))$, Algorithm 2 computes the solution to be $(\widehat{\delta}^*, \widehat{\phi}^*(\widehat{\delta}^*))$ to the problem $[\widehat{\mathrm{AD}}]$. Similarly, we can use Algorithm 2 to solve $[\widecheck{\mathrm{AD}}]$ under (A1).

Algorithm 2 Solution to $[\widehat{\mathrm{AD}}]$ for DNs with identical $^{\mathbf{r}}\!/\mathbf{x}$

```
$(\widehat{\delta}^*, \widehat{\phi}^*, \widehat{\mathcal{L}}) \leftarrow$ GREEDY-ONE-SHOT()
procedure GREEDY-ONE-SHOT()
    $\widehat{\mathcal{L}} = 0$, $\widehat{\delta}^* = \mathbf{0}$, $\widehat{\gamma}^* = \mathbf{1}$, $\widehat{\mathrm{sp}}^{\mathrm{d}*}$ as in Prop. 2
    Let $\widehat{\mathcal{D}}^i_M =$ GETPIVOTNODEOPTIMALATTACKSET($i, \widehat{\mathrm{sp}}^{\mathrm{d}*}$)
    $\widehat{\mathcal{D}}^*_M = \bigcup_{i \in \mathcal{N}} \widehat{\mathcal{D}}^i_M$
    For each $\widehat{\delta} \in \widehat{\mathcal{D}}^*_M$, compute $\widehat{\gamma}^*(\widehat{\delta})$ by solving $[\widehat{\mathrm{AD}}]^{\mathrm{d}}$ as an
  LP in $\gamma$. Let $\widehat{\phi}^*(\widehat{\delta}) = \widehat{\mathrm{sp}}^{\mathrm{d}*}, \widehat{\gamma}^*(\delta)))$
    Let $\widehat{\delta}^* := \mathrm{argmax}_{\widehat{\delta} \in \widehat{\mathcal{D}}^*_M} \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\widehat{\delta}, \widehat{\gamma}^*(\widehat{\delta}), \widehat{\mathrm{sp}}^{\mathrm{d}*}))$
    return $\widehat{\delta}^*, \widehat{\phi}^* = \widehat{\phi}^*(\widehat{\delta}^*), \widehat{\mathcal{L}} = \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\widehat{\delta}^*, \widehat{\phi}^*))$
end procedure
procedure GETPIVOTNODEOPTIMALATTACKSET($i$, $\mathrm{sp}^{\mathrm{d}}$)
    $(J, \mathcal{N}_{g^i}, m') \leftarrow$ OPTIMALATTACKHELPER($i$, $\mathrm{sp}^{\mathrm{d}}$)
    return $\mathcal{D}^i_M \leftarrow \{\widehat{\delta} \in \mathcal{D}_M | \widehat{\delta}_k = 1$ iff $k \in J \cup$
  $\mathcal{N}'$, where $\mathcal{N}' \subseteq \mathcal{N}_{g^i}$ and $|\mathcal{N}'| = M - m'\}$
end procedure
```

Theorem 3. *Under (A0), (A1), let $(\widehat{\delta}, \widehat{\phi})$ be a solution computed by Algorithm 2. Then $(\widehat{\delta}, \widehat{\phi})$ is also an optimal solution to $[\widehat{\mathrm{AD}}]$. Similar result holds for $[\widecheck{\mathrm{AD}}]$.*

Proof: Under (A1), $\mathrm{sp}^{\mathrm{d}} = \widehat{\mathrm{sp}}^{\mathrm{d}*}$ is fixed (Prop. 2). Then, for any $\gamma \in \Gamma$, by Lemma 5 and Prop. 3, the optimal attack $\widehat{\delta}^*$ belongs to the set $\widehat{\mathcal{D}}^*_M(\widehat{\mathrm{sp}}^{\mathrm{d}*})$. Algorithm 2 iterates over the attack vectors $\delta \in \widehat{\mathcal{D}}^*_M$, computes $\widehat{\gamma}^*(\delta)$ by solving an LP, and calculates the loss $\widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\delta, \widehat{\phi}^*(\delta)))$. Finally, it returns the solution corresponding to the maximum loss. Similarly, Algorithm 2 also computes the optimal solution for $[\widecheck{\mathrm{AD}}]$. ■

Proposition 5. *Under (A0), (A1), $\widehat{\mathcal{D}}^*_M(\widehat{\mathrm{sp}}^{\mathrm{d}*}) = \widecheck{\mathcal{D}}^*_M(\widecheck{\mathrm{sp}}^{\mathrm{d}*})$.*

Proof: Under (A1), the PV set-points are as specified by Prop. 2. Hence, $\widehat{\mathrm{sp}}^{\mathrm{d}*} = \widecheck{\mathrm{sp}}^{\mathrm{d}*}$. Furthermore, $\forall\ j \in \mathcal{N}, \Delta_j(\widecheck{\nu}_i) = (1+\epsilon)\Delta_j(\widehat{\nu}_i)$. Hence, the sequence of partitions of the nodes for every pivot node is the same in both the LPF and the ϵ-LPF model. Hence, $\widehat{\mathcal{D}}^*_M(\widehat{\mathrm{sp}}^{\mathrm{d}*}) = \widecheck{\mathcal{D}}^*_M(\widecheck{\mathrm{sp}}^{\mathrm{d}*})$. ■

We, now, describe an iterative greedy approach to compute the solution to $[\mathrm{AD}]$ that uses the optimal attacker strategy for fixed defender response (refer Algorithm 1).

Algorithm 3 initializes ϕ_c to the optimal defender response under no attack. In the first step of the iterative approach, the attacker assumes some defender response ϕ_c to be fixed, and computes the optimal attack strategy $\delta_c(\phi_c)$ using the greedy Algorithm 1. Then in the second step, the defender computes a new defense strategy ϕ_c optimal for fixed δ_c by solving the SOCP, and updates the defender response. If $\mathrm{L}(\mathrm{x}(\delta_c, \phi_c)) > \mathrm{L}(\mathrm{x}(\delta^*, \phi^*))$, then the current best solution (δ^*, ϕ^*) is updated to (δ_c, ϕ_c). Then in the next iteration, the attacker uses this new defender response to update his attack strategy, and so on and so forth. If this δ_c has already been discovered in some previous iteration, the algorithm terminates successfully, with δ^*, ϕ^* as the required optimal attack plan, and the corresponding optimal defense. The algorithm terminates unsuccessfully if the number of iterations exceeds a maximum limit.

Algorithm 3 Iterative Algorithm for Greedy Approach

```
$(\delta^*, \phi^*, \mathcal{L}) \leftarrow$ GREEDY-ITERATIVE()
procedure GREEDY-ITERATIVE
    Let $\delta^* \leftarrow \mathbf{0}, \mathcal{L}^* \leftarrow 0, \delta_c \leftarrow \mathbf{0}, iter \leftarrow 0, \Upsilon \leftarrow \varnothing, \phi_c, \phi^*, \Upsilon$
    For $\delta = \delta_c$ compute $\phi^*$ by solving SOCP $[\mathrm{AD}]^{\mathrm{d}}$ (Lem. 3)
    $\phi_c \leftarrow \phi^*, \mathcal{L}^* \leftarrow \mathrm{L}(\tilde{\mathrm{x}}(\delta, \phi^*))$
    for $iter \leftarrow 0, 1, \ldots, maxIter$ do
        $\delta_c \leftarrow$ OPTIMALATTACKFORFIXEDRESPONSE($\phi_c$)
                // If $\delta_c$ previously found, successfully terminate
        if $\delta_c \in \Upsilon$ then return $\delta^*, \phi^*$
        else $\Upsilon = \Upsilon \cup \{\delta_c\}$        // Store the current best attack vector
        Compute $\phi_c$ by solving SOCP $[\mathrm{AD}]^{\mathrm{d}}$ Lem. 3
        if $\mathrm{L}(\tilde{\mathrm{x}}(\delta_c, \phi_c)) > \mathcal{L}^*$ then
            $\delta^* \leftarrow \delta_c, \phi^* \leftarrow \phi_c, \mathcal{L}^* \leftarrow \mathrm{L}(\tilde{\mathrm{x}}(\delta, \phi^*))$
        end if
    end for                    // Maximum Iteration Limit reached
    Return $\delta^*, \phi^*, \mathcal{L}^*$          // Return the last best solution
end procedure                  // Algo terminates unsuccessfully
```

Note that in each iteration, the size of Υ increases by 1, hence, the algorithm is bound to terminate after exhausting all possible attack vectors.

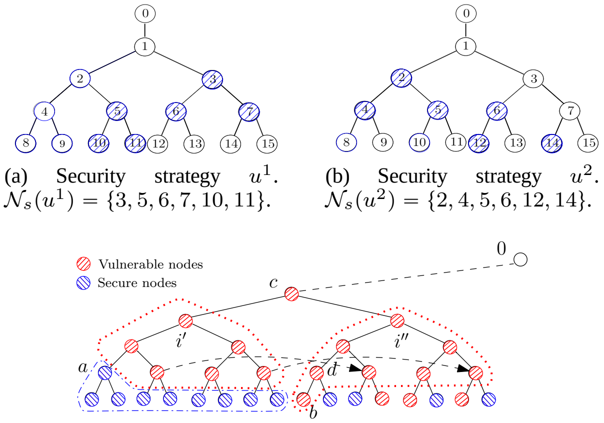
Prop. 5 and Thm. 3 can be applied for any $u \in \mathcal{U}_B$, since if the DN has identical $\mathbf{r}/\mathbf{x}$ ratio, sp^{d} are also fixed.

IV. SECURING DERS TO WORST-CASE ATTACKS

In this section, we consider the defender problem of optimal security investment in Stage 1. For simplicity, we restrict our attention to DNs that satisfy the following assumption:

(A2) Symmetric Network. For every $i \in \mathcal{N}$, for any two nodes $j, k \in \mathcal{C}_i$, Λ_j and Λ_k are symmetrically identical about node i. That is, $z_j = z_k$, $|\mathcal{C}_j| = |\mathcal{C}_k|$, $\mathrm{sc}_j^{\mathrm{nom}} = \mathrm{sc}_k^{\mathrm{nom}}$, $\underline{\nu}_j = \underline{\nu}_k$, $W_j = W_k$, and $C_j = C_k$. However, all the PVs are homogeneous, i.e., $\forall\, j, k \in \mathcal{N}$, $\overline{\mathrm{sp}}_j = \overline{\mathrm{sp}}_k$.

Let B be a fixed security budget. Let $u, \tilde{u} \in \mathcal{U}_B$, $u \neq \tilde{u}$, be two security strategies. Strategy u is *more secure* than strategy $\tilde{u}$ (denoted by $u \preccurlyeq \tilde{u}$) under NPF (resp. LPF), if $\mathcal{L}^u \leqslant \mathcal{L}^{\tilde{u}}$ (resp. $\widehat{\mathcal{L}}^u \leqslant \widehat{\mathcal{L}}^{\tilde{u}}$). Finally, we ask what is the best security strategy u^*, such that for $u = u^*$, $\mathcal{L}^u$ is minimized. Fig. 6 shows two possible security strategies u^1 (Fig. 6a) and u^2 (Fig. 6b). If we compare u^1 and u^2, while transitioning from u^1 to strategy u^2, 3 secure nodes in Λ_2 subtree go up a level each, while 3 secure nodes in Λ_3 subtree go down a level each. Then, between u^1 and u^2, which strategy is more secure? In this section, we provide insights about optimal security strategies under (A2), which help show that u^2 is more secure than u^1.



(a) Security strategy u^1. $\mathcal{N}_s(u^1) = \{3, 5, 6, 7, 10, 11\}$.

(b) Security strategy u^2. $\mathcal{N}_s(u^2) = \{2, 4, 5, 6, 12, 14\}$.

(c) A possible security strategy on a tree DN.

Fig. 6: Different defender security strategies.

Algorithm 4 computes an optimal security strategy $[\widehat{\mathrm{DAD}}]$ under (A0)-(A2). It initially assigns all nodes to be vulnerable. Then, PV nodes are secured sequentially in a bottom-up manner towards the root node. If the security budget is not adequate to secure a full level, the nodes in that level are uniformly secured and the remaining nodes are not secured.

Theorem 4. *Assume (A0), (A1), (A2). Let $\hat{u}^*$ be the security strategy computed by Algorithm 4. Furthermore, with $u = \hat{u}^*$, let $(\widehat{\psi}^*, \widehat{\phi}^*)$ be the solution computed by Algorithm 2. Then, $(\hat{u}^*, \widehat{\psi}^*, \widehat{\phi}^*)$ is an optimal solution to $[\widehat{\mathrm{DAD}}]$. Similar result holds for $[\mathrm{DAD}]$.*

Consider any security strategy $u \in \mathcal{U}_B$ such that

$$u = \begin{bmatrix} \underbrace{u_1}_{1} & \underbrace{u_2}_{2} & \cdots & \underbrace{1}_{a} & \cdots & \underbrace{0}_{b} & \cdots & \underbrace{u_N}_{N} \end{bmatrix}. \tag{31}$$

Construct $\tilde{u}$ from u as follows:

$$\tilde{u} = \begin{bmatrix} \underbrace{u_1}_{1} & \underbrace{u_2}_{2} & \cdots & \underbrace{0}_{a} & \cdots & \underbrace{1}_{b} & \cdots & \underbrace{u_N}_{N} \end{bmatrix}, \tag{32}$$

i.e., $\tilde{u}_i = u_i \quad \forall \quad i \in \mathcal{N} \backslash \{a, b\}$. Similarly, let $\delta \in \mathcal{D}_M(u)$ such that $\delta_a = 0, \delta_b = 1$; and construct $\tilde{\delta}$ from δ as in (32) such that $\tilde{\delta}_i = \delta_i \quad \forall \quad i \in \mathcal{N} \backslash \{a, b\}$. Note that, $\tilde{\delta} \in \mathcal{D}_M(\tilde{u})$.

Algorithm 4 Optimal security strategy

```
$\hat{u}^* \leftarrow$OPTIMALSECURIRTYSTRATEGY()
procedure OPTIMALSECURIRTYSTRATEGY()
    $n_s \leftarrow 0, h \leftarrow H, \hat{u} \leftarrow \mathbf{0}$        // Initialize all nodes to vulnerable nodes
    For each $h \in [1, 2, \ldots, H]$, let $\alpha_h \leftarrow \sum_{j=h}^{H} |\mathcal{N}_j|$
    Let $h' \leftarrow \mathrm{argmax}_{h \in [1,\ldots,H] : \alpha_h \geqslant M}\, h$
    Let $\forall\, h \in [h', \ldots, H], \forall\, i \in \mathcal{N}_h$, $\hat{u}_i \leftarrow 1$.
    Let $\mathcal{N}'_{h'} \subseteq \mathcal{N}_{h'}$ be a set of uniformly chosen $M - \alpha_{h'+1}$ nodes on level $h'$.
    For each $i \in \mathcal{N}'_{h'}$, $\hat{u}_i \leftarrow 1$
    return $\hat{u}$
end procedure
```

In the following sequence of propositions, we compare the security strategies u and $\tilde{u}$ under various conditions. (See proofs of the propositions 6, 7, and 8 in the Appendix.)

Proposition 6. *Assume (A0), (A1), (A2). Let $u \in \mathcal{U}_B$ (resp. $\widetilde{u} \in \mathcal{U}_B$) be as in (31) (resp. (32)). If $b \in \Lambda_a$, then $u \preccurlyeq \widetilde{u}$.*

Starting with any strategy $u' \in \mathcal{U}_B$, Prop. 6 can be applied recursively to obtain a more secure strategy $u \in \mathcal{U}_B : u' \preccurlyeq u$, which has the property that if a node i is secure, then all its successor nodes (i.e. all nodes in subtree Λ_i) are also secured by the defender, i.e.,

$$\forall\ i \in \mathcal{N},\ u_i = 1 \implies \forall\ j \in \Lambda_i,\ u_j = 1 \tag{33}$$

Proposition 7. *Assume (A0), (A1), (A2). Let $u \in \mathcal{U}_B$ (resp. $\widetilde{u} \in \mathcal{U}_B$) be as in (31) (resp. (32)). Let $A_u = \{(i,j) \in \mathcal{N} \times \mathcal{N} \mid u_i = 1, u_j = 0, h_i \geqslant h_j + 1\}$. If u satisfies (33), and $(a,b) \in \text{argmax}_{(i,j)\in A_u} |\mathcal{P}_i \cap \mathcal{P}_j|$, then $u \preccurlyeq \widetilde{u}$.*

Again, starting with any strategy $u' \in \mathcal{U}_B$, we can apply Prop. 7 recursively to obtain a more secure strategy $u \in \mathcal{U}_B : u' \preccurlyeq u$, in which, if a node is secure, then all nodes in lower levels are also secured by the defender, i.e.,

$$\forall\ i,j \in \mathcal{N},\ (u_i = 1 \text{ and } h_j > h_i) \implies u_j = 1 \tag{34}$$

Thus, Prop. 7 is a generalization of Prop. 6.

Proposition 8. *Assume (A0), (A1), (A2). Let $u \in \mathcal{U}_B$ be such that u satisfies (34). Let $h' = \text{argmin}_{(\exists\ a \in \mathcal{N}_h : u_a = 1)} h$. If the secure nodes on level h' are uniformly distributed over the level h', i.e., $|\mathcal{C}_j \cap \mathcal{N}_s| \in \{T, T+1\},\ \forall\ j \in \mathcal{N}_{h'}$, where $T \in \mathbb{Z}_+$, then u is an optimal security strategy, i.e., $\forall\ \widetilde{u} \in \mathcal{U}_B,\ \widetilde{u} \preccurlyeq u$.*

Prop. 8 implies that there exists an optimal security strategy in which there is a top-most level with PV nodes that are uniformly chosen for security investment.

Proof of Thm. 4: Let $u^{*1} \in \mathcal{U}_B$ be any optimal security strategy. From u^{*1}, by sequentially applying Prop. 6, Prop. 7, and Prop. 8, we can obtain an optimal security strategy u^{*2} that satisfies (33), (34), and has the top-most level with secure nodes having uniformly distributed secured nodes.

Now, let $\widehat{u}^*$ be the output of Algorithm 4. Since in Algorithm 4, nodes are secured from the leaf nodes to the root node level-by-level, $\widehat{u}^*$ also satisfies (33) and (34). The Algorithm 4 also secures the top-most level with secure nodes with uniformly distributed secured nodes, $\widehat{u}^*$ is the same as u^{*2} upto a homomorphic transformation.

Finally, we argue that under (A0)-**(A2)**, $\widehat{u}^*$ can be combined with previous results to obtain full solution of $[\widehat{\text{DAD}}]$. Under (A1), the defender set-points are fixed. Since, $\widehat{u}$ and $\widehat{\text{sp}}^{\text{d}*}$ are both fixed, we can compute the set of candidate optimal attack vectors $\widehat{\mathcal{D}}^*_M$, by considering only vulnerable PVs. Then for a fixed $\delta \in \widehat{\mathcal{D}}^*_M$, the sub-problem $[\widehat{\text{AD}}]^{\text{d}}$ reduces to an LP in γ. Hence, Algorithm 2 solves for $(\widehat{\psi}^*, \widehat{\phi}^*)$, the optimal solution of $[\widehat{\text{AD}}]$ for $u = \widehat{u}$, by iterating over $\delta \in \widehat{\mathcal{D}}^*_M$. The strategy profile $(\widehat{u}^*, \widehat{\psi}^*, \widehat{\phi}^*)$, thus obtained, is an optimal solution to for DNs that satisfy (A0), (A1), (A2). Similarly, we can solve $[\widecheck{\text{DAD}}]$. ■

Propositions 6 and 7 capture the attacker preference for the downstream PVs, whereas Prop. 8 capture the attacker preference for cluster attacks. Hence, the optimal security strategy has distributed secured nodes.

Let us revisit the security strategies u^1 and u^2 in Fig. 6: which one is better? Firstly, we use symmetricity (A2) to argue that securing nodes 2, 4, 5 is equivalent to securing nodes 3, 6, 7. Then, Λ_3 subtree of u^2 has more distributed secured nodes than Λ_2 in u^1. Hence, strategy 2 is better. Thm. 4 will, of course, give the optimal security strategy $\widehat{u}^*$ in which nodes $\mathcal{N}_s(\widehat{u}^*) = \{8, 9, 10, 12, 13, 14\}$, or other homomorphic strategies of $\widehat{u}^*$.

We state without proof the following Proposition:

Proposition 9. 1) *Under (A0), (A1), (A2), any attack vector in $\widehat{\mathcal{D}}^*_M$, can be considered as a homomorphic transformation of an element of a subset of $\widehat{\mathcal{D}}^*_M$ which is at most of size $|\mathcal{N}_v| \leqslant N$.*

2) *Under (A0), (A1), if $\forall\ i,j,k \in \mathcal{N}$ such that $\overline{\text{sp}}_j > 0$ and $\overline{\text{sp}}_k > 0$, $\Delta_j(\widehat{\nu}_i) \neq \Delta_k(\widehat{\nu}_i)$, then $\left|\widehat{\mathcal{D}}^*_M\right| = N$.*

Due to Thm. 4 and Prop. 9, we can compute the optimal solution for $[\widehat{\text{DAD}}]$, in $\mathcal{O}(poly(N))$. Same holds for $[\widecheck{\text{DAD}}]$.

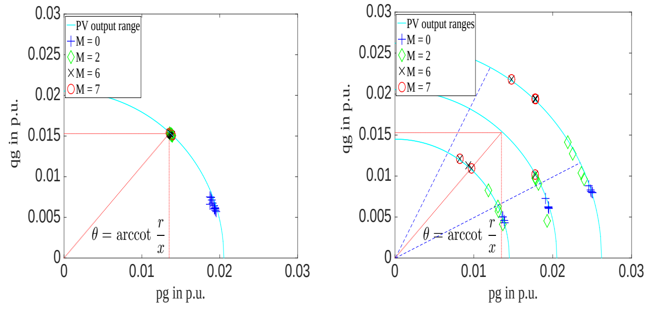
V. Computational Study

We describe a set of computational experiments to evaluate the performance of the iterative Greedy Approach (GA) in solving [AD]; see Algorithm 3. (We again assume $u = \mathbf{0}$.) We compare the optimal attack strategies and optimal defender set-points obtained from GA with the corresponding solutions obtained by conducting an exhaustive search (or Brute Force(BF)), and by implementing the Benders Cut (BC) algorithm. We refer the reader to [10], [20], for the BC algorithm adopted here[5]. The abbreviations BC-LPF and BC-NPF denote the solutions obtained by applying optimal attack strategies from $[\widehat{\text{AD}}]$ to LPF and NPF, respectively. Importantly the experiments illustrate the impact of attacker's resource (M) and defender's load control capability $\underline{\gamma}$ on the optimal value of [AD]. The code for this computational study can be obtained by contacting the authors.

Network Description:Our prototypical DN is a modified IEEE 37-node network; see Fig. 1. We consider two variants of this network: homogeneous and heterogeneous. **Homogeneous Network ($\mathcal{G}^I$)** has 14 homogeneous PVs with randomly assigned node locations, loads with equal nominal demand, and lines with identical $\mathbf{r}/\mathbf{x}$ ratio. Table II (in appendix) lists the parameter values of $\mathcal{G}^I$. **Heterogeneous Network ($\mathcal{G}^H$)** has same topology as $\mathcal{G}^I$, but has heterogeneous PVs (chosen at random from 3 different PV apparent power capabilities), heterogeneous loads, and lines with different $\mathbf{r}/\mathbf{x}$ ratios. The location of PV nodes, the total nominal generation capacity, and the total nominal demand in $\mathcal{G}^H$ is roughly similar to the corresponding values for $\mathcal{G}^I$. **PV output vs M.** Fig. 7 compares the PV output (sg) of uncompromised PVs that form part of defender response in $\mathcal{G}^I$ and $\mathcal{G}^H$ for different M. When $M = 0$ (no attack),

[5] In the BC-implementation of [20], the inner sub-problem is in LP. To apply BC to $[\widehat{\text{AD}}]$, the non-linearity due to (4) is addressed by fixing the set-points according to Prop. 2. In our implementation, we choose $\angle\widehat{\text{sp}}^{\text{d}*} = \arctan K_{avg}$, where $K_{avg} := \frac{\sum_{(i,j)\in\mathcal{E}} r_j}{\sum_{(i,j)\in\mathcal{E}} x_j}$ is the ratio of sum of resistances over all the lines to the sum of reactances over all the lines.

there are no voltage violations, and the defender minimizes $\mathrm{L_{LL}}$ by producing more $pg > qg$. For $M > 0$, the voltage bounds are violated. To limit $\mathrm{L_{VR}}$, the defender responds by increasing qg; and the output of uncompromised PVs lie in a neighborhood of $\theta = \operatorname{arccot} \mathbf{r}/\mathbf{x}$. For the case of $\mathcal{G}^H$ (Fig. 7b), the set-points of the uncompromised PVs are more spread out for voltage regulation over different $\mathbf{r}/\mathbf{x}$ ratios (Prop. 2). In Fig. 7b the three semi-circles correspond to the uncompromised PVs with different apparent power capabilities. These observations on defender response validate Prop. 2.



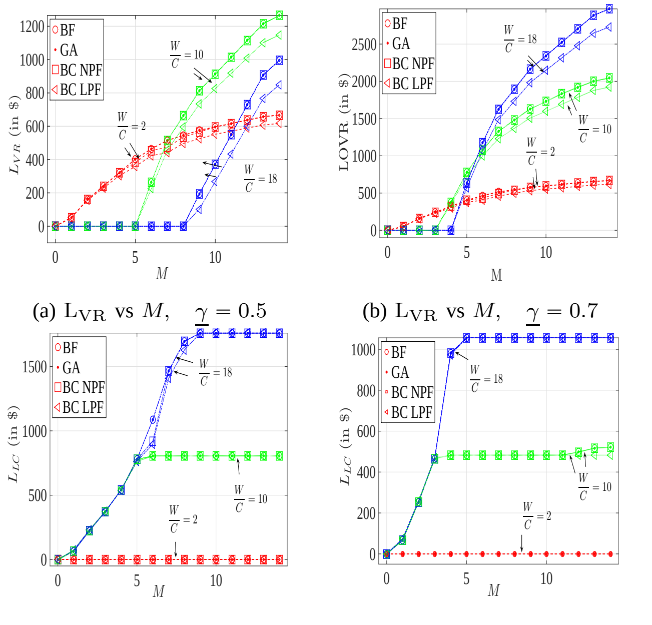
(a) Homogeneous network (b) Heterogeneous network

Fig. 7: Reactive Power Vs Real Power Output of PVs.

GA *vs.* BC-NPF, BC-LPF and BF. Fig. 8 compares results obtained from *BC-NPF*, *GA*, and *BF* on $\mathcal{G}^I$. We consider two cases with the maximum controllable load percentage $\underline{\gamma} = 50$ % and $\underline{\gamma} = 70$ %. For each case, we vary M from 0 to $|\mathcal{N}_v| = 14$; and also vary $\mathbf{W}/\mathbf{C}$ ratios to capture the effect of different weights on the terms $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$.

In our study, $\mathbf{W}/\mathbf{C} = 2$ roughly corresponds to the maximum W/C ratio for which the defender does not exercise load control, because the cost of doing load control is too high, i.e., at optimum defender response, $\gamma^* = \mathbf{1}_N$. In contrast, $\mathbf{W}/\mathbf{C} = 18$ roughly corresponds to the minimum W/C ratio for which the defender exercises maximum load control (i.e. $\gamma^* = \underline{\gamma}$). We also consider an intermediate ratio, $\mathbf{W}/\mathbf{C} = 10$. L ***vs.* M.** Both $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$ are zero when there is no attack. As M increases, one or both $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$ start increasing. This indicates that as more PVs are compromised, the defender incurs $\mathrm{L_{VR}}$, and in addition, he imposes load control to better regulate the DN. Indeed, after the false set-points (THm. 2) are used to compromise PVs, the net load in the DN increases. Without load control, the voltages at some nodes drop below the lower bounds, increasing $\mathrm{L_{VR}}$. Hence, the defender exercises load control, and changes the set-points of uncompromised PVs such that $\mathrm{L_{VR}} + \mathrm{L_{LC}}$ is minimized.

Perhaps the more interesting observation is that as M increases, $\mathrm{L_{LC}}$ first increases rapidly but then flattens out. This can be explained as follows. Depending on the W/C ratio, there is a subset of downstream loads that are beneficial in terms of the value that defender can obtain by controlling them. That is, if the loads belonging to this subset are controlled, the decrease in $\mathrm{L_{VR}}$ outweighs the increase in $\mathrm{L_{LC}}$, hence, the defender imposes load control on these downstream loads to reduce the $\mathrm{L_{VR}} + \mathrm{L_{LC}}$. In contrast, controlling the loads outside this subset, increases $\mathrm{L_{LC}}$ more than the decrease in $\mathrm{L_{VR}}$. Hence, the defender satisfies the demand at these loads fully. Hence, $\mathrm{L_{LC}}$ increases until load control capability in the subset of beneficial downstream loads to the defender is fully exhausted. The size of this subset depends on the W/C ratio. The higher the ratio, the larger the size of the subset of the loads beneficial to the defender. Hence, the value of M, at which the $\mathrm{L_{LC}}$ cost curve flattens out, increases as the W/C ratio increases.



(a) $\mathrm{L_{VR}}$ vs M, $\underline{\gamma} = 0.5$ (b) $\mathrm{L_{VR}}$ vs M, $\underline{\gamma} = 0.7$

(c) $\mathrm{L_{LC}}$ vs M, $\underline{\gamma} = 0.5$ (d) $\mathrm{L_{LC}}$ vs M, $\underline{\gamma} = 0.7$

Fig. 8: $\mathrm{L_{VR}}$ and $\mathrm{L_{LC}}$ vs M for $\mathcal{G}^I$. The results of $\mathcal{G}^H$ are more or less similar to those of $\mathcal{G}^I$.

The cost curve for $\mathrm{L_{VR}}$ also shows interesting behavior as the number of compromised PV nodes increases (Fig. 8a and 8b). The marginal increase in $\mathrm{L_{VR}}$ for every additional PV compromised reduces as M increases. This observation can be explained by the fact that the attacker prefers to compromise downstream nodes over upstream ones (Prop. 4). Initially, the attacker is able to rapidly increase L by compromising more beneficial downstream nodes. However, as the downstream nodes are eventually exhausted, the attacker has to target the relatively less beneficial upstream nodes. Hence, the reduction in marginal increase of $\mathrm{L_{VR}}$.

In $\mathrm{L_{VR}}$ plots, for small M, $\mathbf{W}/\mathbf{C} = 2$ curves are lower than the $\mathbf{W}/\mathbf{C} = 10$ curves which in turn are lower than the $\mathbf{W}/\mathbf{C} = 18$ curves. But, for larger M, this order reverses. The M where these lines cross each other decreases, as the $\underline{\gamma}$ increases. The reason is for some intermediate value of M, the defender exhausts the load control completely, and then the L increases at rates in the same order of increasing $\mathbf{W}/\mathbf{C}$ values. Finally, for $\underline{\gamma} = 0.7$, the M where defender exhausts the load control completely is smaller than that in $\underline{\gamma} = 0.5$.

The Greedy Approach (GA) is better than Benders Cut

(BC) method because GA calculates the exact impact the PV compromises will have on a pivot node. BC overestimates the impact of PV compromises that are not the ancestors to the pivot nodes. Therefore, the feasible region probed by BC at every iteration is larger than the feasible region probed in the corresponding iteration of GA. Hence, although GA converges to a solution in 2-3 iterations, BC in most cases does not converge to the optimal solution even in 200 iterations.

VI. Concluding Remarks

We focused on the security assessment of tree-like DNs for an adversary model in which multiple DERs (in this case, PV nodes) are compromised. The adversary can be a threat agent, who can compromise the operation of DERs, or a malicious insider in the control center. We considered a composite loss function that primarily accounts for the attacker's impact on voltage regulation and induced load control. The security assessment problem is formulated as a three-stage Defender-Attacker-Defender ([DAD]) sequential game. Our main technical contributions include: (i) Approximating the [DAD] game that has nonlinear power flow model and mixed-integer decision variables with tractable formulations based on linear power flow; and (ii) characterization of structural properties of security investments in Stage 1 and the optimal attack in Stage 2 (i.e., the choice of DER node locations and the choice of false set-points).

Future work includes: (a) Extending Theorems 1 and 2 to cases where reverse power flows are permissible (e.g., when the DN is not under heavy loading conditions and the attacker can cause DER generation to exceed the demand); (b) Designing greedy algorithm to solve [AD] and proving optimality guarantees of Theorems 3 and 4 for DNs with heterogeneous $\mathbf{r}/\mathbf{x}$ ratio, and heterogeneous PVs or loads. Finally, we believe that the ideas proposed in this paper are also applicable to security assessment of water DNs under threats that can cause multiple sources to be compromised and lead to sudden loss in hydraulic head and/or loss of supply to consumers.

References

[1] 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. [Online]. Available: http://dblp.uni-trier.de/db/journals/tsg/tsg4.html#MaCHM13

[2] I. A. Hiskens, "What's smart about the smart grid?" in *DAC*, S. S. Sapatnekar, Ed. ACM, 2010, pp. 937–939. [Online]. Available: http://dblp.uni-trier.de/db/conf/dac/dac2010.html#Hiskens10

[3] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *Automatic Control, IEEE Transactions on*, vol. 59, no. 6, pp. 1454–1467, 2014.

[4] Y. Mo, T. H. jin Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," in *Proceedings of the IEEE*, 2012, pp. 195–209.

[5] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Automat. Contr.*, vol. 58, no. 11, pp. 2715–2729, 2013. [Online]. Available: http://dx.doi.org/10.1109/TAC.2013.2266831

[6] K. C. Sou, H. Sandberg, and K. Johansson, "Computing critical k -tuples in power networks," *Power Systems, IEEE Transactions on*, vol. 27, no. 3, pp. 1511–1520, Aug 2012.

[7] A. Teixeira, K. C. Sou, H. Sandberg, and K. Johansson, "Secure control systems: A quantitative risk management approach," *Control Systems, IEEE*, vol. 35, no. 1, pp. 24–45, Feb 2015.

[8] B. A. Robbins, Domnguez-Garcia, and A. D. Tonkoski, "Optimal reactive power dispatch for voltage regulation in unbalanced distribution systems," *IEEE Transactions on Power Systems*.

[9] 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. [Online]. Available: http://dblp.uni-trier.de/db/journals/pieee/pieee99.html#TuritsynSBC11

[10] 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. [Online]. Available: http://dx.doi.org/10.1109/tpwrs.2004.825888

[11] ——, "Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids," *Power Systems, IEEE Transactions on*, vol. 24, no. 1, pp. 96–104, Feb. 2009. [Online]. Available: http://dx.doi.org/10.1109/tpwrs.2008.2004825

[12] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '11. New York, NY, USA: ACM, 2011, pp. 355–366. [Online]. Available: http://doi.acm.org/10.1145/1966913.1966959

[13] M. Farivar, R. Neal, C. R. Clarke, and S. H. Low, "Optimal inverter var control in distribution systems with high pv penetration," *CoRR*, vol. abs/1112.5594, 2011. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr1112.html#abs-1112-5594

[14] A. Lee, "Electric sector failure scenarios and impact analyses," National Electric Sector Cybersecurity Organization Resource (NESCOR), Electric Power Research Institute (EPRI), Palo Alto, California, Tech. Rep., June 2014. [Online]. Available: http://www.smartgrid.epri.com/doc/NESCOR%20failure%20scenarios%2006-30-14a.pd

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

[16] E. Dall'Anese and G. B. Giannakis, "Sparsity-leveraging Reconfiguration of Smart Distribution Systems," *ArXiv e-prints*, Mar. 2013.

[17] 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

[18] M. Farivar and S. H. Low, "Branch flow model: Relaxations and convexification." in *CDC*. IEEE, 2012, pp. 3672–3679. [Online]. Available: http://dblp.uni-trier.de/db/conf/cdc/cdc2012.html#FarivarL12

[19] R. Tonkoski, L. Lopes, and T. El-Fouly, "Coordinated active power curtailment of grid connected pv inverters for overvoltage prevention," *Sustainable Energy, IEEE Transactions on*, vol. 2, no. 2, pp. 139–147, April 2011.

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

[21] L. Gan, N. Li, U. Topcu, and S. Low, "Exact convex relaxation of optimal power flow in radial networks," *Automatic Control, IEEE Transactions on*, vol. 60, no. 1, pp. 72–87, Jan 2015.

Parameters	Values
$r + \mathbf{j}x$	$(0.33 + 0.38\mathbf{j})\ \Omega$
$\mathrm{pc}_i^{\mathrm{nom}}$	$15\ kW$
$\mathrm{qc}_i^{\mathrm{nom}}$	$4.5\ kvar$
$\overline{\mathrm{sp}}_i$	$11.55\ kVA$
$\lvert V_0 \rvert$	$4\ kV$
C	7 \$ per kW

TABLE II: Parameters of the Homogeneous Network

Appendix

For a pivot node $i \in \mathcal{N}$, Algorithm 5 computes a sequence of sets of nodes in decreasing order of $\Delta_j(\widehat{\nu}_i)$ values.

This sequence is used to compute the optimal attacks that maximize voltage bounds violation at node i.

Algorithm 5 Helper procedures

```
procedure OptimalAttackHelper($i$, $\widehat{\mathrm{sp}}^{\mathrm{d}}$)
    For each $j \in \mathcal{N}$ compute $\Delta_j(\widehat{\nu}_i)$ using Lemma 4
    Create a sequence of sets $\{\mathcal{N}_j^i\}_{j=1}^N$ such that
      i) $\mathcal{N} = \bigcup_{j=1}^N \mathcal{N}_j^i$, $\forall\, 1 \leqslant j, k, \leqslant N$, $\mathcal{N}_j^i \cap \mathcal{N}_k^i = \varnothing$
      ii) if $1 \leqslant l \leqslant N$, $j, k \in \mathcal{N}_l^i$, then $\Delta_j(\widehat{\nu}_i) = \Delta_k(\widehat{\nu}_i)$, and
      iii) if $1 \leqslant l < m \leqslant N$, $j \in \mathcal{N}_l^i, k \in \mathcal{N}_m^i$, then $\Delta_j(\widehat{\nu}_i) > \Delta_k(\widehat{\nu}_i)$.
    Let, for $j \in [1, \dots, N], m_j^i \leftarrow |\mathcal{N}_j^i|$, $M_j^i := \sum_{k=1}^{j-1} m_k^i$.
    Let $g^i \leftarrow \mathrm{argmin}_{j \in [1,\dots,N], M_j^i \geqslant M} \quad j$.
    $J \leftarrow \bigcup_{j=1}^{g^i-1}, \mathcal{N}_{g^i}$, $m' = M - M_{g^i-1}^i$
    return $J$, $\mathcal{N}_{g^i}$, $m'$
end procedure
```

Proof of Lemma 3: $(\mathbf{A0})_1$ implies that a feasible solution exists for $[\mathrm{AD}]^{\mathrm{d}}$. Since, $\mathcal{X} \subset \mathcal{X}_{\mathrm{CPF}}$, a feasible solution $\tilde{\mathrm{x}} \in \mathcal{X}_{\mathrm{CPF}}$ also exists for $[\widetilde{\mathrm{AD}}]^{\mathrm{d}}$. Let $(\widetilde{\phi}, \widetilde{\ell})$ denote the decision variables for $[\widetilde{\mathrm{AD}}]^{\mathrm{d}}$. Note that, for a fixed ψ, $\tilde{\mathrm{x}}$ is an affine in $(\widetilde{\phi}, \widetilde{\ell})$, and can be computed using (5a) and (5b).

Now, L is convex in $\widetilde{\phi}$ (because the L_{VR} is a maximum over affine functions, and both L_{LC} and L_{LL} are affine in $(\widetilde{\phi}, \widetilde{\ell})$. Also, Φ is a convex compact set. Further, for a fixed ϕ, L is strictly increasing in $\widetilde{\ell}$ (because, L_{VR} is non-decreasing in $\widetilde{\ell}$ as $\tilde{\nu}$ is affine decreasing in $\widetilde{\ell}$; L_{LC} does not change with $\widetilde{\ell}$; L_{LL} is strictly increasing in ℓ). From Thm. 1 [18], $(\widetilde{\phi}^*, \widetilde{\ell}^*)$ can be computed using a SOCP. To argue that $\widetilde{\ell}^*$ satisfy (5c), assume for contradiction that $\exists\ (i,j) \in \mathcal{E}$, s.t. $\widetilde{\ell}_j^* > \left|\tilde{S}_j^*\right|^2/\tilde{\nu}_i^*$. Then, construct $(\phi^*, \widetilde{\ell}')$ such that $\forall\ j \in \mathcal{N}\ : j \neq i$, $\widetilde{\ell}_j' = \widetilde{\ell}_j^*$, and $\widetilde{\ell}_i' = \left|\tilde{S}_j^*\right|^2/\tilde{\nu}_i^*$. Since $\forall\ (j,k) \in \mathcal{E}$, $\left|\tilde{S}_k\right|^2/\tilde{\nu}_j$ is strictly decreasing in $\widetilde{\ell}_i$, $\forall\ (j,k) \in \mathcal{E} :\ \widetilde{\ell}_k' \geqslant \left|\tilde{S}_k^*\right|^2/\tilde{\nu}_j^* > \left|\tilde{S}_k'\right|^2/\tilde{\nu}_j'$. Hence, one can further minimize the loss function by choosing a new feasible solution $(\phi^*, \widetilde{\ell}')$, thus violating the optimality of $(\widetilde{\phi}^*, \widetilde{\ell}^*)$. ■

Proof of Prop. 2:

Let (d_i, θ_i) denote $\widehat{\mathrm{sp}}_i^{\mathrm{d}}$ in the polar coordinates, i.e., $d_i = \left|\widehat{\mathrm{sp}}_i^{\mathrm{d}}\right|, \theta_i = \angle\widehat{\mathrm{sp}}_i^{\mathrm{d}}$.

For $\delta_i = 0$, $\widehat{\mathrm{sp}}_i = \widehat{\mathrm{sp}}_i^{\mathrm{d}}$. Then from (18a),

$$\forall\ j \in \mathcal{N},\ \widehat{\nu}_j = \widehat{\nu}_j' + 2d_i(R_{ij}\cos\theta_i + X_{ij}\sin\theta_i), \tag{35}$$

where $\widehat{\nu}_j' = \nu_0 - 2\sum_{k \in \mathcal{N}, k \neq j} \mathbf{Re}(\bar{Z}_{jk}s_k) - 2\mathbf{Re}(\bar{Z}_{ij}sc_j)$. Note that $\widehat{\nu}_j'$ does not depend on (d_i, θ_i).

It is clear from (35) that $\widehat{\nu}_j$ is greater if $\theta_i \in [0, \pi/2]$ than if $\theta_i \in [-\pi/2, 0]$. Furthermore, the impedances are positive. Hence, $\forall\ j, \partial_{d_i}\widehat{\nu}_j = 2(R_{ij}\cos\theta_i + X_{ij}\sin\theta_i) > 0$. Hence, $\partial_{d_i}\mathrm{L}_{\mathrm{VR}} > 0$. But, from (4), $d_i \leqslant \overline{\mathrm{sp}}_i$. Hence, $d_i^* = \overline{\mathrm{sp}}_i$. Further, $\partial_{\theta_i}\widehat{\nu}_j = 2d_i(-R_{ij}\sin\theta_i + X_{ij}\cos\theta_i)$.

$$\partial_{\theta_i}\widehat{\nu}_j \begin{cases} > 0 & \text{if} \quad \theta_i \in [0, \mathrm{arccot}(R_{ij}/X_{ij})) \\ = 0 & \text{if} \quad \theta_i = \mathrm{arccot}(R_{ij}/X_{ij})) \\ < 0 & \text{if} \quad \theta_i \in (\mathrm{arccot}(R_{ij}/X_{ij})), \pi/2] \end{cases}$$

Now, $\mathrm{arccot}\,\overline{K} \leqslant \mathrm{arccot}(X_{ij}/R_{ij}) \leqslant \mathrm{arccot}\,\underline{K}$. Hence,

$$\forall \quad j \in \mathcal{N}, \quad \partial_{\theta_i}\widehat{\nu}_j \quad \begin{cases} < 0 & \text{if } \theta_i > \quad \mathrm{arccot}\,\underline{K} \\ > 0 & \text{if } \theta_i < \quad \mathrm{arccot}\,\overline{K} \end{cases} \tag{36}$$

Suppose, for contradiction, $\theta_i^* \notin [\mathrm{arccot}\,\overline{K}, \mathrm{arccot}\,\underline{K}]$. Holding all else equal, for $\theta_i = \widetilde{\theta}_i$, let $\widehat{\nu}(\widetilde{\theta}_i)$ and $\mathrm{L}_{\mathrm{VR}}(\widetilde{\theta}_i)$ be the $\widehat{\nu}$ and L_{VR}. From (36), for any $\widetilde{\theta}_i \in [\mathrm{arccot}\,\overline{K}, \mathrm{arccot}\,\underline{K}]$, $\widehat{\nu}(\widetilde{\theta}_i) > \widehat{\nu}(\widetilde{\theta}_i^*)$. Since, $\mathrm{L}_{\mathrm{VR}} > \mathrm{L}_{\mathrm{LL}} \geqslant 0$, $\mathrm{L}_{\mathrm{VR}}(\widetilde{\theta}_i) < \mathrm{L}_{\mathrm{VR}}(\widetilde{\theta}_i^*)$, violating the optimality of $\widetilde{\theta}_i^*$. Furthermore, under identical $\mathbf{r}/\mathbf{x}$ ratio, $\underline{K} = \overline{K} = K$, which implies $\theta_i = \mathrm{arccot}\,K$. ■

Proof of Lemma 4: Let $\Delta_j(\mathrm{sp}_j)$ denote the change in the set-point of PV j after it is compromised. By Theorem 2, $\Delta(\mathrm{sp}_j) = \mathrm{sp}_j^{\mathrm{d}} - (0 - \mathbf{j}\overline{\mathrm{sp}}_j) = \mathrm{sp}^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_j$; and by linearity in (18a),

$$\Delta_j(\nu_i) = 2\mathbf{Re}(\bar{Z}_{ij}\Delta_j(\mathrm{sp}_j)) = 2\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_j)).$$

Again, by invoking the linearity in (18a), (26a) follows. Similarly, one can show (25b) and (26b). ■

Proof of Prop. 4: From (18a), when $\delta_j = 1$, i.e., the PV j is compromised, only the power supplied at node j changes.

$$\therefore \Delta_j(\widehat{\nu}_i) = 2\mathbf{Re}(\bar{Z}_{ij}\mathrm{sp}_j^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_j).$$

Due to linearity, the first part of Prop. 4 holds true. Now,

$$j <_i k \implies \mathcal{P}_i \cap \mathcal{P}_j \subset \mathcal{P}_i \cap \mathcal{P}_k \implies Z_{ij} < Z_{ik}.$$

$$\begin{aligned} \therefore \Delta_j(\widehat{\nu}_i) &= 2\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_j)) \\ &< 2\mathbf{Re}(\bar{Z}_{ik}(\mathrm{sp}_k^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_k)) = \Delta_k(\widehat{\nu}_i) \end{aligned}$$

Similarly, we can prove the case for $j =_i k$.

Under the ϵ-LPF model, $\Delta_j(\check{\nu}_i) = 2(1+\epsilon)\mathbf{Re}(\bar{Z}_{ij}(\mathrm{sp}_j^{\mathrm{d}} + \mathbf{j}\overline{\mathrm{sp}}_j))$. The rest of the proof follows similarly. ■

Proof of Prop. 6: Let (δ^*, ϕ^*) and $(\widetilde{\delta}^*, \widetilde{\phi}^*)$, denote the optimal solutions of $[\widehat{\mathrm{AD}}]$ with $u = \widehat{u}$ (resp. $u = \widetilde{u}$). (A1) $\implies$ $\mathrm{sp}^{\mathrm{d}*}$ is fixed (Prop. 2). Hence, ϕ^* depends only on δ^*, and not u. Then, let $\phi^*(\delta)$ denote optimal defender response to δ. We want to show $\widehat{\mathcal{L}}^{\widetilde{u}} \leqslant \widehat{\mathcal{L}}^u$.

Case $\widetilde{\delta}_a^* = 0$. Then $\widetilde{\delta}^* \in \mathcal{D}_M(u)$. Thus, $\widehat{\mathcal{L}}^{\widetilde{u}} = \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\widetilde{u}, \widetilde{\delta}^*, \phi^*(\widetilde{\delta}^*))) = \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(u, \widetilde{\delta}^*, \phi^*(\widetilde{\delta}^*))) \leqslant \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(u, \delta^*, \phi^*(\delta^*)))$, where the inequality follows by optimality of δ^*.

Case $\widetilde{\delta}_a^* = 1$. Let $\delta \in \mathcal{D}_M(u) : \delta_a = 0, \delta_b = 1, \forall i \in \mathcal{N}\backslash\{a,b\}, \delta_i = \widetilde{\delta}_i^*$. Then, $\delta \in \mathcal{D}_M(u)$. Since $b \in \Lambda_a$, $\forall\ i \in \mathcal{N},\ a \preceq_i b$. Hence, by Prop. 4, $\forall\ i \in \mathcal{N},\ \Delta_b(\widehat{\nu}_i) \geqslant \Delta_a(\widehat{\nu}_i)$. Then, by Lemma 4, for fixed ϕ, $\Delta_\delta(\widehat{\nu}) \geqslant \Delta_{\widetilde{\delta}^*}(\widehat{\nu})$. Hence, $\widehat{\mathcal{L}}^{\widetilde{u}} = \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\widetilde{u}, \widetilde{\delta}^*, \phi^*(\widetilde{\delta}^*))) \leqslant \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(\widetilde{u}, \widetilde{\delta}^*, \phi^*(\delta))) \leqslant \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(u, \delta, \phi^*(\delta))) \leqslant \widehat{\mathrm{L}}(\widehat{\mathrm{x}}(u, \delta^*, \phi^*(\delta^*))) = \widehat{\mathcal{L}}^u$. Here, the first (resp. last) inequality follows due to optimality of $\phi^*(\widetilde{\delta}^*)$ (resp. δ^*). Hence, $u \preccurlyeq \widetilde{u}$. ■

Proof of Prop. 7: Let $c = \mathrm{argmax}_{(i \in \mathcal{P}_a \cap \mathcal{P}_b)}\, h_i$, be the lowest common ancestor of a and b. Let $i', i'' \in \mathcal{C}_c\ :\ a \in \Lambda_{i'}$ and $b \in \Lambda_{i''}$. From Thm. 3, we know that the optimal attack δ^* will be a pivot node attack $\widehat{\delta}^i$ for some node, say $i \in \mathcal{N}$. Let $\mathcal{N}' = \Lambda_{i'} \cup \Lambda_{i''}$.

Case $i \in \mathcal{N}'$**.** Now $u_j = 1 \ \forall \ j \in \Lambda_{i'} \backslash \Lambda^a_{i'} \cup \{a\}$ by maximality of $|\mathcal{P}_a \cap \mathcal{P}_b|$. Similarly, $u_j = 0 \ \forall \ j \in \Lambda^d_{i''} \cup \{b\}$. Thus, $\forall \ j \in \Lambda_{i'}$ s.t. $u_j = 0$ there exists a separate node $k \in \Lambda_{i''}$ such that j and k are homomorphic, and $u_k = 0$ (see Fig. 6c). Hence, the subtree $\Lambda_{i''}$ is more vulnerable than the subtree $\Lambda_{i'}$, and it will be more beneficial for the attacker to target a pivot node in $\Lambda_{i''}$. Now, $i \in \Lambda_{i''}$, and $\forall \ i \in \Lambda_{i''}, \ a \prec_i b$. We obtain, by Prop. 4, $\Delta_a(\widehat{\nu}_i) < \Delta_b(\widehat{\nu}_i)$.

Case $i \notin \mathcal{N}'$**.** Then $a =_i b$, and by Prop. 4, $\Delta_a(\widehat{\nu}_i) = \Delta_b(\widehat{\nu}_i)$.

We now want to show that $\widehat{\mathcal{L}}^{\widetilde{u}} \leqslant \widehat{\mathcal{L}}^{u}$. The rest of the proof follows along the same lines as the proof of Prop. 6.

■

Proof of Prop. 8: Similar to the proof of Prop. 7. ■