Evaluating Resilience of Electricity Distribution Networks via A Modification of Generalized Benders Decomposition Method

Devendra Shelar, Saurabh Amin, and Ian Hiskens

Abstract

This article presents an optimization-based approach to evaluate the resilience of electricity Distribution Networks (DNs) to cyber-physical failure events. In our model, an attacker targets multiple DN components to maximize the minimum loss to the operator. The operator can respond to the attack in one of two ways: (i) Coordinated emergency response via pre-emptive tripping and control of loads and/or Distributed Generators (DGs); (ii) Uncoordinated autonomous disconnections, possibly leading to an uncontrolled cascade of failures. Evaluating resilience under response (i) entails solving a Bilevel Mixed-Integer Second-Order Cone Program (BiMISOCP) which is computationally challenging to solve due to mixed-integer variables in the inner-level (operator) subproblem and non-linear power flow constraints. We develop an algorithm based on the Generalized Benders' Decomposition (GBD) method that achieves reasonable tradeoff between computational time and solution accuracy. In each iteration of GBD, a generalized Benders cut is added to the master (attacker) subproblem, in which a linear expression in the attack variables is constrained to be greater than a certain value ϵ. In our modified algorithm, we introduce a criticality parameter which exploits the structural insights on power flow over radial DNs and selects appropriate values of ϵ for each generalized Benders cut. We evaluate DN resilience under response (ii) by sequentially computing autonomous disconnects of DGs and loads in response to attack-induced failures and resulting voltage bound violations. Our approach can be used to estimate the gain in resilience under response (i), relative to (ii), for different values of attacker's resource budget.

Index Terms

Cyber-Physical Security, Network Resilience, Smart Grids, Generalized Benders Decomposition

Manuscript resubmitted on May 15, 2020. This work was supported by awards: AFOSR "Building attack resilience into complex networks", NSF CAREER (CNS-1453126), and "Modeling & Analysis of Load Ensembles" (ECCS-1810144).

D. Shelar and S. Amin are with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology (MIT), Cambridge, MA 02139 USA (e-mail: {shelard, amins}@mit.edu, phone: 857-253-8964).

I. A. Hiskens is with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109 USA (e-mail: hiskens@umich.edu).

I. Introduction

Despite the ongoing modernization of electricity distribution networks (DNs), many distribution system operators (DSOs) face both strategic and operational challenges in ensuring a reliable and secure service to their customers. The integration of distributed generators (DGs) and new monitoring and control capabilities has enabled flexible operations, which can be utilized to respond to a class of failure events, e.g. sudden voltage drop [1–3]. However, these capabilities also expose the vulnerabilities of DNs to adversaries [4–6]. Particularly, cyber-physical failures to DNs can result in contingencies that cause cascading network outages [7–9]. In this article, we argue that the flexibility of modern DNs can be leveraged to generate a timely and effective response to cyber-physical failures. We present a systematic approach for evaluating the DN resilience under currently feasible response capabilities.

For a given cyber-physical failure model and an operational response capability of the DSO, our optimization-based approach can be used to evaluate the *worst-case* post-contingency loss due to various factors, such as the impact of voltage degradation and costs of load control, load shedding, and line losses. By evaluating this loss for different response (control) operations, we can compute their relative *value* in maintaining the DN resilience against the given class of failures. From a strategic viewpoint, this computation is useful for knowing which control capabilities, if deployed in the DN, will be most effective in response to contingencies arising from such failures. From an operational viewpoint, it can help the DSO to implement the response in a timely manner to limit the uncontrolled outages resulting from the triggering of automatic protection mechanisms.

Indeed, defining the appropriate operational response capability, the cyber-physical failure model, and the nature of attacker-operator interaction are all crucial aspects of our problem, which we discuss next.

Firstly, we consider three different operations supported by modern DNs; see Fig. 1. Response (a) refers to remote control by the control center; response (b) - autonomous disconnects of components due to activation of local protection systems; and response (c) - emergency control by the Substation Automation (SA) systems. In our model, response (c) is comprised of load control and preemptive tripping of components (loads and/or DGs). Response (b) is *uncoordinated* in that it is based on local checks of operating bounds at the DN nodes. In contrast, response (a) and (c) utilize information from DN meters that includes node-level consumption, distributed generation, and nodal voltages. We assume that the response (c) subsumes (b) by making decisions that are *coordinated* across the SA system. Hence, (b) and (c) are never simultaneously active.

Secondly, we study a generic attack model in which the attacker-induced failure compromises one of the two

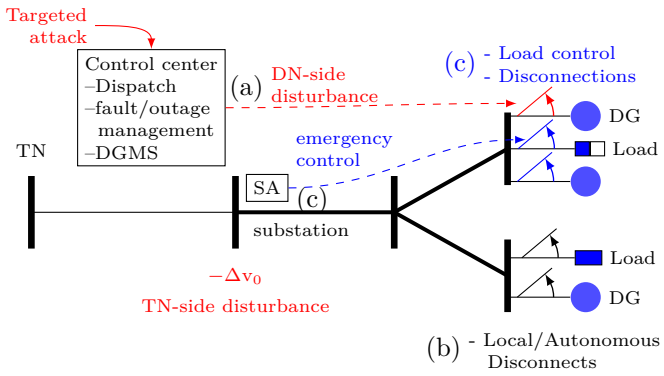


Fig. 1: DSO operations (blue) and attack model (red).

network-wide response capabilities of the DSO. The SA systems (response (c)) were recently provided cyber-security re-perimeterisation by NERC [10]. In contrast, control center operations (response (a)) are still prone to back channel attacks by remote entities [11]. Therefore, we focus on a specific attack scenario in which the DG Management System (DGMS) – which is part of response (a) as shown in Fig. 1– is compromised by the attacker [12]. In fact, the impact of such security failures may be aggravated due to a failure in the adjoining transmission network (TN). We model the impact of TN-side failure as a voltage sag (drop in the substation voltage), and that of the security failures in DGMS as supply disturbances, i.e. DG tripping, at DN nodes. Thus, this attack model can capture the effect of contingencies resulting from simultaneous TN and DN failures.

Thirdly, we develop a computationally tractable approach to address the problem of determining the *worst-case* post-contingency loss when the DSO responds to the attacker actions with response (b) or (c). For the case of response (c), we formulate a bilevel mixed-integer second-order cone program (BiMISOCP), which captures the sequential nature of attacker-operator interaction (Sec. II). The inner (operator) problem consists of mixed-binary variables which model response (c), and the second-order cone constraints model the non-linear power flows (NPF) over a radial DN. The operator's objective is to minimize the post-contingency loss. The outer (attacker) problem is to determine an attack that will maximize the DSO's loss, assuming the DSO responds optimally. The worst case post-contingency loss for response (c) is given by the maximin value of the BiMISOCP.

To compute the post-contingency loss under response (b), we present a two-step approach (Sec. V). For a given attack, the first step evaluates the impact of cascading failures by determining the DG disconnections. The second step determines the effect of DG disconnects on the nodal voltages and evaluates its impact on the load control/shedding. Then, we present a randomized algorithm to estimate the worst-case post-contingency loss under a maximally disruptive attacker strategy.

Several papers have used bilevel formulations for security assessment of power systems [3, 5, 7–9, 13]. When the

inner problem does not have integer variables, the original bilevel problem can be transformed into a single-level problem via a KKT-based reformulation. However, in general, BiMISOCPs with mixed-integer variables in the inner problem are extremely challenging to solve, and have received limited attention in the literature. Even under linear constraints, the resulting bilevel mixed-integer linear program (BiMILP), is still hard to solve due to integer variables in the inner problem. Previous works have utilized a relaxation technique to reformulate this BiMILP as a single-level MILP, which can be solved using an advanced branch-and-bound algorithm [14, 15]). Recent papers have proposed intersection cuts [16, 17], and disjunction cuts [18, 19] to introduce stronger cuts. However, these approaches only solve a weak relaxation of the original BiMILP [20, 21]. Other methods for solving BiMILPs include the Generalized Benders Decomposition (GBD) method [21] and column constraint generation [22]. However, these methods cannot be applied to solve our BiMISOCP, again due to the presence of integer variables in the inner problem.

We address the abovementioned challenge by exploiting some structural results on non-linear power flows on a radial DN topology (Sec. III), and using these insights to generate more effective cuts for the inner (operator) problem. Essentially, our computational approach first reformulates the original BiMISOCP as an equivalent min-cardinality disruption problem, and then applies an algorithm based on the GBD method. In each iteration of the GBD method, a generalized Benders cut is added to the master (attacker) subproblem, in which a linear expression in the attack variables is constrained to be greater than a certain value ϵ. In our algorithm, we introduce a criticality parameter to select appropriate values of ϵ for each generalized Benders cut by exploiting the structure of our problem (Sec. IV). The computational results demonstrate that this modification achieves a good tradeoff between the computational speed and the optimality gap (Sec. VI).

II. Modeling and Problem formulation

Now, we describe our generic approach to evaluate DN resilience, and then present our sequential attacker-operator bilevel problem formulation.

A. Evaluating resilience of DNs

Generically, a system's resilience is defined as "its ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" [23]. To systematically evaluate a DN's resilience, we need to select both a class of adverse events and the DN's ability to respond to those events. In our setup, the class of disruptions is denoted by $\mathcal{D}_{\mathrm{k}}$, where k is attacker's resource constraint. We also consider a set of operator responses denoted by $\mathcal{U}$. Then, we denote by $\mathcal{L}_{\mathrm{Mm}}$ the post-contingency loss which is a measure of the maximum reduction in system performance under $\mathcal{D}_{\mathrm{k}}$;

see Fig. 2. Let $\mathcal{L}_{\max}$ denote the loss incurred when all loads and DGs are disconnected. Then, $\mathcal{R}_{\text{Mm}} := 100(1-\mathcal{L}_{\text{Mm}}/\mathcal{L}_{\max})$ i.e., the percentage drop in system performance, can be viewed as a metric of the DN resilience under the response capabilities $\mathcal{U}$ against attacks in $\mathcal{D}_{\text{k}}$.

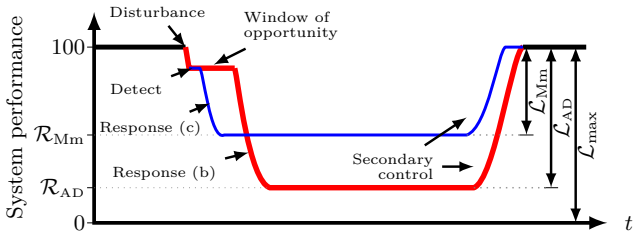


Fig. 2: Performance under various response capabilities.

To compare the DN resilience under response (c) with the case of autonomous disconnections (b), we need to estimate the maximum loss corresponding to response (b) that would be induced by an attack in $\mathcal{D}_{\text{k}}$. Let the automatic disconnect actions be denoted by u_{nr}, resulting network state by x_{nr}, and the corresponding loss by $\mathcal{L}_{\text{AD}} = L(u_{\text{nr}}, x_{\text{nr}})$. Then, the resilience metric of the DN under autonomous disconnections (AD) can be written as $\mathcal{R}_{\text{AD}} = 100(1 - \mathcal{L}_{\text{AD}}/\mathcal{L}_{\max})$.

Fig. 2 qualitatively illustrates the evolution of system performance over time. Initially, the DN is operating under the nominal conditions. Then, due to the TN/DN-side disturbances, the system performance degrades. If the operator fails to respond in a timely manner (in less than a few seconds), then an uncontrolled cascade can occur due to response (b), resulting in a loss $\mathcal{L}_{\text{AD}}$. However, to regain nominal operation, the operator eventually undertakes secondary control actions involving transformers or capacitor banks. Then, the nodal voltages recover, allowing the disconnected components to reconnect and operate within safety bounds.

By evaluating the post-contingency loss due to a timely DSO response, and comparing it with the loss under the autonomous disconnections, we can estimate the *value* of the timely response toward improving the DN's resilience. We assume that all the devices within the DN are networked in response (c). Hence, $\mathcal{R}_{\text{Mm}} \geqslant \mathcal{R}_{\text{AD}}$, and we can evaluate the relative value of operational response (or equivalently, the improvement in DN resilience) as $(\mathcal{R}_{\text{Mm}} - \mathcal{R}_{\text{AD}})$; see Sec. VI.

B. BiMISOCP formulation for $\mathcal{L}_{Mm}$

Now, we describe our bilevel program to evaluate $\mathcal{L}_{\text{Mm}}$ over a radial DN for specific attacker and operator models.

We model the DN as a tree network of node set $\mathcal{N} \bigcup \{0\}$ and line set $\mathcal{E}$. Also, without loss of generality, we assume that each node of the DN has a load and a DG. Furthermore, we consider the constant power model for both loads and DGs. We refer the reader to Table IV in the Appendix for definitions of key notation.

We formulate a bilevel problem to model the sequential interaction between the strategic attacker (leader) and the

operator (follower). First, we model the effect of a TN-side disruption on the DN as a drop in the substation voltage $\Delta \mathrm{v}_0$. Next, we consider a specific attack model where the attacker disrupts a subset of DGs in the DN. We denote an attacker-induced failure by $d \in \{0,1\}^{\mathcal{N}}$, where $d_i = 1$ indicates that the DG at node i is disrupted, $d_i = 0$ otherwise. Let k denote the attacker's resource budget. For a given TN-side disruption $\Delta \mathrm{v}_0$ and attacker action d, we consider that the operator can respond by exercising load control, changing the DG output, and/or disconnecting the loads and DGs, if necessary. We denote the operator response (c) by $u = (\beta, pg, qg, kc, kg)$, and use $x = (pc, qc, p, q, P, Q, \mathrm{v}, \ell)$ to denote the post-contingency network state. Finally, we denote by $L(u, x)$ the loss function for a given operator response and network state. Now, we state our problem as follows:

$$
\begin{aligned}
&\mathcal{L}_{\mathrm{Mm}} \coloneqq \max\nolimits_{d \in \{0,1\}^{\mathcal{N}}} \ \mathcal{C}_{\mathrm{Mm}}(d) \\
&\text{s.t.} \qquad \textstyle\sum_{i \in \mathcal{N}} d_i \leqslant \mathrm{k}, \qquad (1) \\
&\mathcal{C}_{\mathrm{Mm}}(d) \coloneqq \min\nolimits_{u,x} L(u, x) \qquad \text{s.t.}
\end{aligned}
$$

$$
\mathrm{v}_0 = \mathbf{v^{nom}} - \Delta \mathrm{v}_0 \qquad (2)
$$

$$
kg_i \geqslant d_i \qquad \forall\ i \in \mathcal{N} \qquad (3)
$$

$$
pg_i \leqslant \overline{\mathbf{pg}}_i (1 - d_i) \qquad \forall\ i \in \mathcal{N} \qquad (4)
$$

$$
pg_i \leqslant \overline{\mathbf{pg}}_i (1 - kg_i) \qquad \forall\ i \in \mathcal{N} \qquad (5)
$$

$$
pg_i \geqslant 0 \qquad \forall\ i \in \mathcal{N} \qquad (6)
$$

$$
qg_i \geqslant -\eta_i pg_i, \qquad qg_i \leqslant \eta_i pg_i \qquad \forall\ i \in \mathcal{N} \qquad (7)
$$

$$
kg_i \in \{0,1\}, \qquad kc_i \in \{0,1\} \qquad \forall\ i \in \mathcal{N} \qquad (8)
$$

$$
\beta_i \geqslant (1 - kc_i)\, \underline{\beta}_i, \qquad \beta_i \leqslant (1 - kc_i) \qquad \forall\ i \in \mathcal{N} \qquad (9)
$$

$$
pc_i = \beta_i \overline{\mathbf{pc}}_i, \qquad qc_i = \beta_i \overline{\mathbf{qc}}_i \qquad \forall\ i \in \mathcal{N} \qquad (10)
$$

$$
kg_i \geqslant \underline{\mathbf{vg}}_i - \mathrm{v}_i, \qquad kg_i \geqslant \mathrm{v}_i - \overline{\mathbf{vg}}_i \qquad \forall\ i \in \mathcal{N} \qquad (11)
$$

$$
kc_i \geqslant \underline{\mathbf{vc}}_i - \mathrm{v}_i, \qquad kc_i \geqslant \mathrm{v}_i - \overline{\mathbf{vc}}_i \qquad \forall\ i \in \mathcal{N} \qquad (12)
$$

$$
p_i = pc_i - pg_i, \qquad q_i = qc_i - qg_i \qquad \forall\ i \in \mathcal{N} \qquad (13)
$$

$$
P_{ij} = \textstyle\sum_{k:(j,k) \in \mathcal{E}} P_{jk} + p_j + \mathbf{r}_{ij} \ell_{ij} \qquad \forall\ (i,j) \in \mathcal{E} \qquad (14)
$$

$$
Q_{ij} = \textstyle\sum_{k:(j,k) \in \mathcal{E}} Q_{jk} + q_j + \mathbf{x}_{ij} \ell_{ij} \qquad \forall\ (i,j) \in \mathcal{E} \qquad (15)
$$

$$\mathrm{v}_j = \mathrm{v}_i - 2\mathbf{r}_{ij}P_{ij} - 2\mathbf{x}_{ij}Q_{ij} + \left|\mathbf{z}_{ij}^2\right|\ell \quad \forall\ (i,j) \in \mathcal{E} \tag{16}$$

$$\ell_{ij}\mathrm{v}_i = P_{ij}^2 + Q_{ij}^2 \quad \forall\ (i,j) \in \mathcal{E} \tag{17}$$

where $\mathcal{L}_{\mathrm{Mm}}$ denotes the Max-min (Mm) post-contingency under response (c) against $\mathcal{D}_{\mathrm{k}}$. For a fixed attack, the operator's objective is to minimize the post-contingency loss $L\left(u,x\right)$, and the attacker's objective is to choose an attack that maximizes the minimum post-contingency loss.

We define $L(u,x)$ as the sum of the following costs: (i) cost due to loss of voltage regulation, (ii) cost of load control, (iii) cost of load shedding, and (iv) cost of line losses:

$$\begin{aligned} L(u,x) = \mathrm{W}^{\mathrm{VR}}\left\|\mathbf{v}^{\mathbf{nom}} - \mathrm{v}\right\|_{\infty} + \textstyle\sum_{i\in\mathcal{N}}\ \mathrm{W}_i^{\mathrm{LC}}\left(\mathbf{1}-\beta_i\right)\overline{\mathbf{pc}}_i \\ + \textstyle\sum_{i\in\mathcal{N}}\ \left(\mathrm{W}_i^{\mathrm{LS}} - \mathrm{W}_i^{\mathrm{LC}}\right)kc_i\overline{\mathbf{pc}}_i + \mathrm{W}^{\mathrm{LL}}\textstyle\sum_{ij\in\mathcal{E}}\mathbf{r}_{ij}\ell_{ij}, \end{aligned} \tag{18}$$

where for load at node i, $\mathrm{W}_i^{\mathrm{LC}} \in \mathbb{R}_+$ denotes the cost of per unit load controlled, $\mathrm{W}_i^{\mathrm{LS}} \in \mathbb{R}_+$ and $\mathrm{W}_i^{\mathrm{LS}} \geqslant \mathrm{W}_i^{\mathrm{LC}}$ is the cost in dollars of per unit load shed; $\mathrm{W}^{\mathrm{LL}} \in \mathbb{R}_+$ is the cost of unit power lost in line losses; and $\mathrm{W}^{\mathrm{VR}} \in \mathbb{R}_+$ is the cost of unit absolute deviation of nodal voltage from the nominal value $\mathbf{v}^{\mathbf{nom}}$. The weight $\mathrm{W}_i^{\mathrm{LS}} - \mathrm{W}_i^{\mathrm{LC}}$ is chosen to enable proper counting of the cost of load control when the load is disconnected.

Explanation of constraints: Eq. (1) states that the attacker can disrupt at most k nodes. Eq. (2) models the impact of a TN-side disruption in terms of sudden drop in substation voltage; (3) states that if the attacker disrupts a DG at node i, then that DG becomes non-operational, and is *effectively disconnected* from the DN; (4)-(7) determine the feasible space for a DG's power output; (6) states that the active power output of DG is always non-negative; (7) states that the magnitude of a DG's reactive power output can atmost be $\eta_i \geqslant 0$ times its active power output; and (4) (resp. (5)) combined with (6) and (7) state that the active and reactive power output of DG is zero if it is disconnected due to attacker (resp. operator) action.

Eq. (8) captures the binary constraints of the connectivity variables; (9) and (10) together model that if a load is connected to a DN, the operator may change the actual consumption of the load to a fraction of its nominal demand via direct load control; and (11) models that a DG will disconnect if the nodal voltage violates either of the DG's operating voltage bounds, which is required according to the IEEE standard rules for interconnection of DGs [24]. Similarly, a load at node $i \in \mathcal{N}$ will disconnect if either of its operating voltage bounds is violated (12).

Eq. (13) models the net nodal power consumption; (14) (resp. (15)) is the active (resp. reactive) power conservation equation; (16) is the voltage drop equation; and (17) models the current-voltage-power relationship [25].

Eq. (17) is a non-convex equation due to which the operator subproblem becomes challenging to solve. Furthermore,

the operator response and the corresponding network state may not be unique. However, the convex relaxation of (17) can be written as follows [26]:

$$\ell_{ij}\mathrm{v}_i \geqslant P_{ij}^2 + Q_{ij}^2 \qquad \forall\ (i,j) \in \mathcal{E}. \tag{19}$$

Let $\mathcal{D}_\mathrm{k} := \{d \in \{0,1\}^\mathrm{N} \mid \sum_{i\in\mathcal{N}} d_i \leqslant \mathrm{k}\}$ denote the set of feasible attacker strategies. Next, we can denote an operator response strategy as $u \in \mathcal{U}$, where $\mathcal{U} := \{(\beta, pg, qg, kc, kg) \in \mathbb{R}^{5\mathrm{N}} \mid (5)-(9) \text{ hold}\}$. Finally, we can denote the set of response strategies feasible after an attack d by $\mathcal{U}(d) := \{u \in \mathcal{U} \mid \text{such that } (3)-(4) \text{ hold}\}$.

For a $u \in \mathcal{U}$, let $\mathcal{X}(u) = \{x \in \mathbb{R}^{5|\mathcal{N}|+3|\mathcal{E}|} \mid (2), (10)-(16), (19) \text{ hold}\}$ denote the set of feasible post-contingency states. Then, we can succinctly model the attacker-operator interaction in the presence of TN-side disturbance as follows:

$$\begin{aligned} \mathcal{L}_\mathrm{Mm} \ := \ & \max_{d\in\mathcal{D}_\mathrm{k}} \quad \mathcal{C}_\mathrm{Mm}(d) \\ & \text{s.t.} \quad \mathcal{C}_\mathrm{Mm}(d) := \min_{u\in\mathcal{U}(d), x\in\mathcal{X}(u)} \ L\left(u,x\right). \end{aligned} \tag{Mm}$$

Thus, the attacker's (resp. operator's) objective is to maximize (resp. minimize) the loss L subject to DG and load models, nonlinear power flows, TN-side disruption, and the failure impact captured by $u \in \mathcal{U}(d)$. We refer the problem (Mm) as the *Budget-k-max-loss* problem.

C. BiMILP formulation for $\hat{\mathcal{L}}_{Mm}$

Solving a bilevel problem can be computationally difficult, especially when the inner subproblem is an MISOCP. To check whether using linear power flow (LPF) approximation provides any computational advantage, we propose an analogous Bilevel Mixed-Integer Linear Problem (BiMILP) based on LPF. Therefore, consider the classical *LinDistFlow* model [27]:

$$P_{ij} = \textstyle\sum_{k:(j,k)\in\mathcal{E}} P_{jk} + p_j \qquad \forall\ (i,j) \in \mathcal{E} \tag{20}$$

$$Q_{ij} = \textstyle\sum_{k:(j,k)\in\mathcal{E}} Q_{jk} + q_j \qquad \forall\ (i,j) \in \mathcal{E} \tag{21}$$

$$\mathrm{v}_j = \mathrm{v}_i - 2\left(\mathbf{r}_{ij}P_{ij} + \mathbf{x}_{ij}Q_{ij}\right) \qquad \forall\ (i,j) \in \mathcal{E}, \tag{22}$$

where (20)-(21) are the approximate power conservation equations and (22) is the voltage drop equation.

We approximate the loss function in (18) as the sum of following costs: (i) cost due to loss of voltage regulation, (ii) cost of load control, and (iii) cost of load shedding:

$$\begin{aligned} \widehat{L}(u,x) = \mathrm{W}^\mathrm{VR}\left\|\mathbf{v}^\mathbf{nom} - \mathrm{v}\right\|_\infty + \textstyle\sum_{i\in\mathcal{N}} \ \mathrm{W}_i^\mathrm{LC}\left(\mathbf{1}-\beta_i\right)\overline{\mathbf{pc}}_i \\ + \textstyle\sum_{i\in\mathcal{N}} \ \left(\mathrm{W}_i^\mathrm{LS} - \mathrm{W}_i^\mathrm{LC}\right) kc_i\overline{\mathbf{pc}}_i, \end{aligned} \tag{23}$$

where we omit the line loss term for the sake of BiMILP formulation.

Let $\widehat{\mathcal{X}}$ denote the set of post-contingency states x that satisfy the constraints (2), (10)-(13), (17), and (20)-(22). Again, we can denote the attacker-operator interaction under linear power flow (LPF) constraints as follows:

$$\begin{aligned} \hat{\mathcal{L}}_{\mathrm{Mm}} \;:=\; & \max_{d \in \mathcal{D}_{\mathrm{k}}} \quad \hat{\mathcal{C}}_{\mathrm{Mm}}(d) \\ & \text{s.t.} \quad \hat{\mathcal{C}}_{\mathrm{Mm}}(d) := \min_{u \in \mathcal{U}(d), x \in \widehat{\mathcal{X}}(u)} \; \widehat{L}\,(u, x)\,. \end{aligned} \tag{$\widehat{\mathrm{Mm}}$}$$

Note that current-magnitude-squared variables ℓ do not affect the loss function $\widehat{L}$, and do not impact the choice of other decision variables in ($\widehat{\mathrm{Mm}}$) as ℓ only appear in (17). Hence, the problem ($\widehat{\mathrm{Mm}}$) is still effectively a BiMILP despite having a non-linear equation (17).

To summarize, our problem is to determine the maximin optimal attacker-operator strategies to compute the worst-case post-contingency loss $\mathcal{L}_{\mathrm{Mm}}$ (resp. $\hat{\mathcal{L}}_{\mathrm{Mm}}$) for non-linear (resp. linear) power flow model.

D. Assumptions

We assume that DN lines have positive, but small impedances, i.e., $0 < \mathbf{r}_{ij} \ll 1, 0 < \mathbf{x}_{ij} \ll 1 \quad \forall\, (i,j) \in \mathcal{E}$, and that voltage lower bounds are positive, i.e., $\underline{\mathbf{vc}}_i > 0, \underline{\mathbf{vg}}_i > 0 \quad \forall\, i \in \mathcal{N}$. These are rather mild assumptions which hold true for DNs in practice [25, 26].

We also assume the following *No Reverse Power Flow* condition. For $i \in \mathcal{N}$, let $\mathcal{N}_i \subseteq \mathcal{N}$ denote the subset of nodes that belong to the subtree rooted at node i.

Definition 1. *We say that a DN is operating under the* No Reverse Power Flow *condition (NRPF) if*

$$\textstyle\sum_{j \in \mathcal{N}_i} \quad p_j \geqslant 0, \qquad \sum_{j \in \mathcal{N}_i} \quad q_j \geqslant 0 \qquad \forall\, i \in \mathcal{N}.$$

Under the NRPF condition, the flows computed using either linear or nonlinear power flow constraints are non-negative, i.e. on any DN line, power does not flow towards the substation. Hence, the name "no reverse power flow".

In this paper, we assume that the NRPF condition always holds, even when all DGs are producing maximum output, i.e. $pg_i = \overline{\mathbf{pg}}_i$ and $qg_i = \eta_i \overline{\mathbf{pg}}_i \;\forall\, i \in \mathcal{N}$. An important consequence of the NRPF condition is that the convex relaxation of (17) is exact [26], i.e., there is a unique optimal solution to the operator subproblem such that inequality (19) is tight.

III. Theoretical Results

In this section, we present the structural results based on linear and non-linear power flows in radial DNs.

For fixed p and q, let $\widehat{P}, \widehat{Q}, \hat{\mathrm{v}}$ and $\widehat{\ell}$ be the linear power flow (LPF) solutions of (2), (17) and (20)-(22). Since $\widehat{P}, \widehat{Q}, \hat{\mathrm{v}}$ do not depend on $\widehat{\ell}$ and are linear functions of p and q, $\widehat{P}, \widehat{Q}, \hat{\mathrm{v}}$ and $\widehat{\ell}$ can be solved for in $\mathcal{O}(|\mathcal{N}|)$ time.

Again, for fixed p and q, let (P, Q, v, ℓ) be the solution of the problem:

$$\begin{aligned} \min_{P,Q,\mathrm{v},\ell} \quad & \textstyle\sum_{(i,j)\in\mathcal{E}} \mathbf{r}_{ij}\ell_{ij} \\ \text{s.t.} \quad & (2), (14)-(16), (19). \end{aligned} \tag{24}$$

Note that problem (24) is the same as the optimal power flow problem [26] such that the lower and upper bounds for the net nodal consumption at each node are equal to p_i and q_i. Furthermore, problem (24) is a SOCP and has a cost function that is strictly increasing in ℓ. Therefore, under NRPF, it has a unique solution [26].

Let $\mathcal{F}$ and $\mathcal{G}$ be sets of quantities such that $\mathcal{F} = \{P_{ij}, Q_{ij}, \ell_{ij}\}_{(i,j)\in\mathcal{E}}$ and $\mathcal{G} = \{\mathrm{v}_i\}_{i\in\mathcal{N}}$. Also, let $\widehat{\mathcal{F}}$ and $\widehat{\mathcal{G}}$ denote the corresponding sets of LPF quantities. Let $\mathcal{H} = \{(P_{ij}, \widehat{P}_{ij}), (Q_{ij}, \widehat{Q}_{ij}), (\ell_{ij}, \widehat{\ell}_{ij})\}_{(i,j)\in\mathcal{E}}$ and $\mathcal{I} = \{(\mathrm{v}_i, \hat{\mathrm{v}}_i)\}_{i\in\mathcal{N}}$ be the sets consisting of tuples each with an entry of the NPF quantity and its corresponding LPF quantity. Let $\mathcal{J} = \{(p_i, pc_i, pg_i), (q_i, qc_i, qg_i)\}_{i\in\mathcal{N}}$ and $\mathcal{M} = \{p_i, q_i\}_{i\in\mathcal{N}}$.

The following lemma states that increasing the active (resp. reactive) consumption at a node has equal and opposite effects as compared to that of increasing the active (resp. reactive) generation at the same node. (We refer the reader to Appendix B for the proofs of the technical results.)

Lemma 1.

$$\frac{\partial e}{\partial a} = \frac{\partial e}{\partial b} = -\frac{\partial e}{\partial c} \quad \forall\ e \in \mathcal{F} \cup \widehat{\mathcal{F}} \cup \mathcal{G} \cup \widehat{\mathcal{G}}, (a, b, c) \in \mathcal{J}.$$

The following proposition states that the power flows and the current magnitude on any DN line as computed using NPF (resp. LPF) is increasing (resp. non-decreasing) with increasing net nodal consumption. On the other hand, the nodal voltages as computed using NPF or LPF are strictly decreasing in the net nodal consumption. Furthermore, the impact of a change in consumption is strictly larger for the NPF values than for the LPF values.

Proposition 1. *Under NRPF, the following hold:*

$$\frac{\partial f}{\partial c} > \frac{\partial \hat{f}}{\partial c} \geqslant 0 > \frac{\partial \hat{v}}{\partial c} > \frac{\partial v}{\partial c} \quad \forall\ (f, \hat{f}) \in \mathcal{H}, (v, \hat{v}) \in \mathcal{I}, c \in \mathcal{M}.$$

Intuitively speaking, Prop. 1 holds because increasing net consumption reduces the DN voltage at all nodes, which in turn, increases the power flows and the current magnitudes on all DN lines.

The following proposition helps determine the DG output under optimal operator response as follows:

Proposition 2. *Under NRPF,*

$$pg_i^\star = \widehat{pg}_i^\star \quad = \overline{\mathbf{pg}}_i(1 - kg_i^\star) \qquad \forall\ i \in \mathcal{N}$$

$$qg_i^\star = \widehat{qg}_i^\star \quad = \eta_i\overline{\mathbf{pg}}_i(1 - kg_i^\star) \qquad \forall\ i \in \mathcal{N}.$$

Prop. 2 implies that under NRPF, the active and reactive power capability of connected DGs will be fully exhausted leaving no room for response via DG output control. An important consequence of Prop. 2 is that the operator response can be simplified to β, kc, kg since the DG output is uniquely determined by whether it is connected or not.

Furthermore, with a slight abuse of notation, we restrict the set $\mathcal{U}$ to be the projection of the set $\{u \in \mathbb{R}^{5\mathrm{N}}$ such that $qg_i = \eta_i pg_i = \eta_i\overline{\mathbf{pg}}_i(1-kg_i) \quad \forall\ i \in \mathcal{N}$ and $(8)-(9)$ hold$\}$ onto the $(\beta, kc, kg)-$space. Then, we denote the operator response by $u = (\beta, kc, kg)$ such that $u \in \mathcal{U}$.

The next proposition states the impact of change in net nodal consumption of a downstream node on the power flows, current and voltage magnitudes, is larger than that due to an equivalent change in net consumption at an upstream node.

Proposition 3. *Consider $k, l \in \mathcal{N}$ such that $k \prec l$. Let $\mathcal{Z}_{kl} = \{(p_k, p_l), (q_k, q_l)\}$. Then, under NRPF,*

$$\frac{\partial f}{\partial c_l} > \frac{\partial f}{\partial c_k} > 0 > \frac{\partial v}{\partial c_k} > \frac{\partial v}{\partial c_l} \qquad \forall\ f \in \mathcal{F}, v \in \mathcal{G}, (c_k, c_l) \in \mathcal{Z}_{kl}$$

$$\frac{\partial \hat{f}}{\partial c_l} \geqslant \frac{\partial \hat{f}}{\partial c_k} \geqslant 0 > \frac{\partial \hat{v}}{\partial c_k} \geqslant \frac{\partial \hat{v}}{\partial c_l} \qquad \forall\ \hat{f} \in \widehat{\mathcal{F}}, \hat{v} \in \widehat{\mathcal{G}}, (c_k, c_l) \in \mathcal{Z}_{kl}$$

The next proposition states that for any fixed attacker action, the post-contingency loss computed under the optimal operator response using NPF is no worse than the corresponding loss computed using the LPF.

Proposition 4. $\mathcal{C}_{Mm}(d) > \widehat{\mathcal{C}}_{Mm}(d) \qquad \forall\ d \in \mathcal{D}_{\mathrm{k}}$.

The next proposition states that the resilience of the DN computed using ($\widehat{\mathrm{Mm}}$) is greater than the value obtained by solving (Mm).

Proposition 5. $\mathcal{R}_{Mm} \leqslant \widehat{\mathcal{R}}_{Mm}$.

Consider $i, j \in \mathcal{N}$ such that $i \prec j$ (i.e., j is a successor node of i). The following result states that if (i) the lower voltage bound, the nominal active and reactive power demand, load control parameter, and the cost coefficient of load control at i are at most the corresponding values at j, and (ii) the cost coefficient of load shedding at i is at least as much as that at j, then, in an optimal operator response, the upstream load being shed implies that the downstream load is also shed.

Proposition 6. *Let $i, j \in \mathcal{N}$ such that $i \prec j$. Then,*

$$\left.\begin{array}{ll} \underline{\mathbf{vc}}_i \leqslant \underline{\mathbf{vc}}_j, & \overline{\mathbf{pc}}_i \leqslant \overline{\mathbf{pc}}_j \\ \underline{\beta}_i \leqslant \underline{\beta}_j, & \overline{\mathbf{qc}}_i \leqslant \overline{\mathbf{qc}}_j \\ W_i^{LC} \leqslant W_j^{LC}, & W_i^{LS} \geqslant W_j^{LS} \end{array}\right\} \implies kc_i^\star \leqslant kc_j^\star. \tag{25}$$

Again, consider $i, j \in \mathcal{N}$ such that $i \prec j$. The following result states that if (i) DGs at both i and j are not attacked, (ii) DG at i has a capacity larger than that of the DG at j, and (iii) the voltage lower bound at i is smaller than that at j, then, in an optimal operator response, the upstream DG being disconnected implies that the downstream DG is also disconnected.

Proposition 7. *Consider $i, j \in \mathcal{N}$ such that $i \prec j$. Then,*

$$\left.\begin{array}{ll} & \underline{\mathbf{vg}}_i \leqslant \underline{\mathbf{vg}}_j \\ d_i = 0, & d_j = 0 \\ \overline{\mathbf{pg}}_i \geqslant \overline{\mathbf{pg}}_j, & \eta_i \geqslant \eta_j \end{array}\right\} \implies kg_i^\star \leqslant kg_j^\star. \tag{26}$$

Propositions 6 and 7 characterize the notion of keeping the more beneficial ("superior") DN components connected. That is, if the operator cannot keep the "superior" components connected that help reduce the overall loss and provide more flexibility in operation, then the operator must have been forced to disconnect the "inferior" components. In Sec. IV, we will use these results to add cuts to the operator subproblem and evaluate their effect on the computational speedup in Sec. VI.

IV. Evaluating $\mathcal{R}_{\text{Mm}}$ - a Modified GBD Method

Our approach for evaluating $\mathcal{R}_{\text{Mm}}$ relies on using a modified Generalized Benders Decomposition (GBD) algorithm [28] to approximately solve (Mm) on a reformulated problem. The overall approach is as follows. First, we argue that $\mathcal{L}_{\text{Mm}}$ can be obtained by solving an equivalent *Min-cardinality* problem instead. Then, we apply the GBD algorithm, which decomposes the min-cardinality problem into a master (attacker) problem (an integer program) and an operator subproblem (a mixed-integer program), and then solves these two problems in an iterative manner, until either an optimal min-cardinality attack is obtained or all the attacks are exhausted.

A. Min-cardinality disruption problem

Recall that in problem (Mm), the attacker's goal is to determine an optimal attack of size at most k (attack resource). On the other hand, in the min-cardinality problem, the attacker computes a disruption with as few attacked DN nodes

as possible to induce a loss to the operator greater than a pre-specified threshold target post-contingency loss, denoted $\mathcal{L}_{\text{target}}$. The min-cardinality problem is equivalent to (Mm); see [29] for additional details.

Now, we describe the GBD method to solve the min-cardinality problem. For given load and DG connectivity vectors kc and kg, we define a **configuration** vector as $\kappa := (kc, kg)$. Given an attack vector d, let $\mathcal{K}(d) := \{(kc, kg) \in \{0,1\}^{2\mathrm{N}}$ such that (3) holds$\}$, i.e. $\mathcal{K}(d)$ denotes the set of all possible post-disruption configuration vectors that the operator can choose from. Then, for a fixed attack d and a fixed configuration vector $\kappa \in \mathcal{K}(d)$, consider the following second-order cone program:

$$\begin{aligned} \mathcal{P}(d,\kappa) \;:=\; & \min_{\beta\in[0,1]^{\mathrm{N}}} \; L(u,x) \\ & \text{s.t. } u = (\beta,\kappa), u \in \mathcal{U}, x \in \mathcal{X}(u). \end{aligned} \tag{O-SOCP}$$

Note that (O-SOCP) may be infeasible as the chosen κ may violate (11) or (12) in the set of constraints $\mathcal{X}(u)$. In this case, the value of $\mathcal{P}(d,\kappa)$ is set to ∞.

Suppose that, for a given DN, we are concerned with a TN-side disturbance $\Delta \mathrm{v}_0$ and a target $\mathcal{L}_{\text{target}}$ post-contingency loss. We say that an attack-induced disruption $d \in \mathcal{D}_{\mathrm{k}}$ *defeats* a configuration $\kappa \in \mathcal{K}(d)$ if $\mathcal{P}(d,\kappa) \geqslant \mathcal{L}_{\text{target}}$, and is *successful* if it defeats *every* $\kappa \in \mathcal{K}(d)$. The above definition is analogous to the definition of successful attack considered in [7]. We can now state the *Min-cardinality disruption* problem as follows:

$$\begin{aligned} \min_{d\in\{0,1\}^{\mathcal{N}}} \quad & \textstyle\sum_{i\in\mathcal{N}} d_i \\ \text{s.t.} \quad & \mathcal{P}(d,\kappa) \geqslant \mathcal{L}_{\text{target}} \quad \forall\ \kappa \in \mathcal{K}(d). \end{aligned} \tag{MCP}$$

If there exists an optimal solution of the problem (MCP), say $d^\star$, then it is a *min-cardinality disruption* corresponding to $\mathcal{L}_{\text{target}}$ because it is successful and has minimum number of attacked nodes.

However, problem (MCP) is not tractable in its current form because the number of constraints is equal to the cardinality of set $\mathcal{K}(d)$ which can be exponential in N, and verifying each constraint ($\mathcal{P}(d,\kappa) \geqslant \mathcal{L}_{\text{target}}$) is itself an SOCP. The GBD algorithm can be applied to address this issue.

B. Modified Generalized Benders Decomposition

The algorithm decomposes (MCP) into two relatively simpler problems: attacker MILP master problem (A-MIP) and operator MISOCP subproblem (O-MISOCP), which are then solved in an iterative manner. In fact, in each iteration, one needs to solve (A-MIP), (O-MISOCP), and the dual of the problem in (O-SOCP), as discussed below. Fig. 3 summarizes the overall approach.

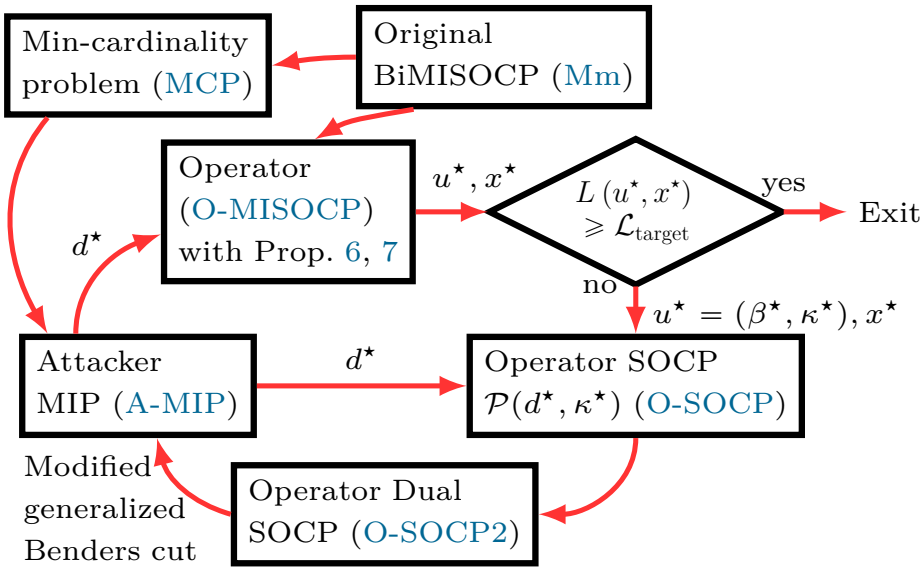


Fig. 3: Computational approach to solve (Mm).

The attacker MIP can be written as follows:

$$\begin{aligned} \min_{d\in\{0,1\}^{\mathcal{N}}} \quad & \textstyle\sum_{i\in\mathcal{N}} d_i \\ \text{s.t.} \quad & \text{set of generalized Benders cuts.} \end{aligned} \tag{A-MIP}$$

The master problem is initialized with only the integrality and budget constraints on the attack variables, and without any generalized Benders cut. In each iteration, solving the master problem (A-MIP), which is a bounded MIP, if feasible, yields an attack $d^\star$. Then, this attack vector is used as an input parameter for the operator subproblem (O-MISOCP). For a fixed disruption $d^\star$, the operator subproblem is the same as the inner problem of (Mm):

$$\begin{aligned} \min_{u\in\mathcal{U}(d^\star), x\in\mathcal{X}(u)} \quad & L(u,x) \\ \text{s.t.} \quad & (25), (26). \end{aligned} \tag{O-MISOCP}$$

The problem (O-MISOCP) is also a bounded MIP because the load and DGs have bounded feasible space. If (O-MISOCP) is feasible, it yields an optimal operator response $u^\star$ and network state $x^\star$ for the disruption $d^\star$. If the operator's loss $L(u^\star, x^\star)$ exceeds the target loss $\mathcal{L}_{\text{target}}$, the algorithm terminates having successfully determined an optimal min-cardinality attack. Otherwise, $L(u^\star, x^\star) < \mathcal{L}_{\text{target}}$ which implies that $d^\star$ is not a successful disruption. In this case, we need to generate a generalized Benders cut to eliminate $d^\star$ from the feasible space of (A-MIP).

Note that problem (O-SOCP) with parameters ($d^\star$, $\kappa^\star$) can be simplified and rewritten as the following problem:

$$\min_w \; c^\top w$$

$$\begin{aligned} \text{s.t. } Aw &\geqslant b + Bd^\star \\ \left\|E^i w + f^i\right\|_2 &\leqslant {g^i}^\top w + h^i \qquad \forall\ i \in [1\,..\,\mathrm{N}], \end{aligned} \tag{O-SOCP2}$$

where $\|\cdot\|_2$ is the L-squared norm; w is the primal decision vector variable; A, B, and E^i for $i \in [1\,..\,\mathrm{N}]$ are matrices; b, f^i and g^i for $i \in [1\,..\,\mathrm{N}]$ are vectors of appropriate dimensions; and $h^i s$ are scalars. The N second-order cone constraints correspond to (19).

The dual of problem (O-SOCP2) is as follows:

$$\begin{aligned} \max_{\lambda \geqslant \mathbf{0}} \quad & (b + Bd^\star)^\top \lambda + \sum_{i=1}^{\mathrm{N}} \left({f^i}^\top \alpha^i - \beta^i h^i\right) \\ \text{s.t.} \quad & c - A^\top \lambda + \sum_{i=1}^{\mathrm{N}} \left({E^i}^\top \alpha^i - \beta^i g^i\right) = \mathbf{0} \\ & \left\|\alpha^i\right\|_2 \leqslant \beta^i \qquad \forall\ i \in [1\,..\,\mathrm{N}] \end{aligned} \tag{D-SOCP2}$$

We solve the dual problem (thanks to strong duality, the optimal values are the same) in (D-SOCP2) to compute $\mathcal{P}(d^\star, \kappa^\star)$ and an optimal dual solution $(\lambda^\star, \alpha^{i\star}, \beta^{i\star})$. This furnishes a *generalized Benders cut*, which is added to the master problem in the next iteration. In particular, if the dual problem in (D-SOCP2) has an optimal solution $(\lambda^\star, \alpha^{i\star}, \beta^{i\star})$, and its optimal value is $L^\star$, then

$$(b + Bd)^\top \lambda^\star + \textstyle\sum_{i=1}^{\mathrm{N}} \left({f^i}^\top \alpha^i - \beta^i h^i\right) \geqslant L^\star + \epsilon \tag{27}$$

is the desired generalized Benders cut where ϵ is a non-negative number. In a classical generalized Benders cut the value of ϵ is 0. If the inner subproblem of (Mm) were convex, such a cut would indeed be useful in eliminating sub-optimal attacker strategies [28]. However, this cut is not useful in the presence of discrete inner variables, i.e. it does not eliminate any attack vector.

Hereafter, we refer to the generalized Benders cut as simply the Benders cut. Note that $d^\star$ does not satisfy the Benders cut constraint when $\epsilon > 0$ because $(b + Bd^\star)^\top \lambda^\star + \sum_{i=1}^{\mathrm{N}} \left({f^i}^\top \alpha^i - \beta^i h^i\right) = \mathcal{P}(d^\star, \kappa^\star) = L^\star < L^\star + \epsilon$, where the first equality holds because of strong duality in second-order cone programs. Thus, choosing $\epsilon > 0$ is a modification to the Benders cut which will help eliminate $d^\star$ from attacker's set of feasible strategies. However, due to numerical issues, an off-the-shelf solver "stalls" sometimes, and is unable to generate dual vector values required for the Benders cut. To address this issue, we add the following cut:

$$\textstyle\sum_{(i \in \mathcal{N}: d_i^\star = 1)} d_i + \sum_{(i \in \mathcal{N}: d_i^\star = 1)} (1 - d_i) \leqslant \mathrm{N} - 1, \tag{28}$$

which definitely eliminates $d^\star$.

Thus, in each iteration, we eliminate suboptimal attacks from the feasible space of (A-MIP). Hence, the new master problem obtained by adding a Benders cut is a stronger relaxation of (MCP). Consequently, we get a progressively tighter lower bound on the minimum cardinality of the attack as the iteration continues, until we get a successful attack. Since there are a finite number of attacks, whether successful or not, the GBD algorithm is bound to terminate.

Note that the same algorithm depicted in Fig. 3 is also applicable for solving the BiMILP ($\widehat{\text{Mm}}$). In this case, instead of solving an MISOCP and SOCP, the algorithm would simply solve an MILP and an LP.

C. Choosing ϵ using a criticality parameter

The Benders cut, when simplified, is of the form $\sum_{i\in\mathcal{N}} C_i d_i \geqslant \epsilon^j$, where $C = \lambda^{\star\top} B$ is the coefficient vector, and $\epsilon^j > 0$ is a scalar chosen for the j^{th} added Benders cut. The choice of ϵ^j in the generation of a Benders cut is an important issue in our implementation of the GBD algorithm. One way would be to choose a constant value of ϵ for each Benders cut. However, if we choose too large an ϵ then many attacks (possibly including the optimal attacks) would be eliminated from the set of feasible attacker strategies in (A-MIP). This introduces an approximation error as a result of which, the obtained min-cardinality attack may not be optimal. If we choose too small an ϵ, then in each iteration only the current min-cardinality attack vector is eliminated resulting in performance no better than brute force over all attacks.

To address this issue, we present a further modification of the Benders cut by proposing a heuristic to assign varying values for ϵ in each iteration. Suppose that in iteration j, the optimal attack vector obtained is d^j and the dual coefficient vector is C^j. Let $\mathrm{k}^j := \sum_i d_i^j$ be the cardinality of d^j. Let σ^j be a permutation of nodes such that $C^j_{\sigma^j(1)} \geqslant C^j_{\sigma^j(2)} \geqslant \cdots \geqslant C^j_{\sigma^j(\mathrm{N})}$, with the ties broken by lexicographical ordering. Here $l = \sigma^j(i)$ indicates that node $l \in \mathcal{N}$ has the i^{th} highest value in the vector C^j. Let $\mathrm{m} \in [1\,..\,\mathrm{N}]$ be a parameter, which we call a *criticality parameter*. Let $\mathrm{e}^j := \min(\mathrm{N}, \mathrm{m} + \mathrm{k}^j)$ and $\mathrm{s}^j = \mathrm{e}^j - \mathrm{k}^j + 1$. Then, one can choose ϵ for the $(j+1)^{th}$ iteration as follows:

$$\epsilon^{j+1} = \underbrace{C^j_{\sigma^j(\mathrm{s}^j)} + C^j_{\sigma^j(\mathrm{s}^j+1)} + \cdots + C^j_{\sigma^j(\mathrm{e}^j)}}_{\mathrm{k}^j \text{ terms}}$$

Essentially, we exclude the top $\min(\mathrm{m}, \mathrm{N} - \mathrm{k}^j)$ values, and then take the sum of next k^j coefficients. Again, as m increases, the ϵ^j value decreases, thereby allowing the GBD algorithm to explore more number of attacks. As a result, one would expect the optimality gap to be lower and the computational time to be higher than the case when m is small.

An intuitive reason for why this heuristic works well is as follows. By Prop. 3, we get the insight that the downstream

nodes in a DN are critical. Therefore, the attacker may attack as many downstream nodes as he can subject to his resource constraint. However, in this case the attacker may fail to exploit the cascading nature of the attack. Specifically, the attacker may be better off by not disrupting a few downstream nodes, and instead using his budget on compromising a few upstream nodes. Due to such an attack, the downstream DGs, which are anyway more likely to face voltage bound violations, may be disconnected due to the operator response. That is why choosing a lower value of ϵ^j allows the GBD algorithm to explore attacks that do not compromise the most critical nodes (as suggested by the dual coefficients in the Benders cut). Essentially, the dual coefficients C^j do not capture the cascading effect due to further disconnection of other DGs and loads because we fix the configuration vector for solving the SOCP. Thus, C^j do not properly capture the true "criticality" of the DG nodes by ignoring the cascading effects. Therefore, varying the criticality parameter m allows the algorithm to explore attacks on DGs whose criticality as indicated by C^j value is less. As we show in Sec. VI, the GBD algorithm with variable value for ϵ takes significantly fewer iterations compared with brute force or the GBD algorithm with a constant ϵ.

V. Evaluating $\mathcal{R}_{\text{AD}}$ - A Two-Step Approach

A. Autonomous disconnect model - Response (b)

To model the network state under response (b), we propose the following two-step approach. In the first step, we compute the subset of DGs which will autonomously disconnect due to the attacker-induced failure as well as due to the resulting voltage bound violations. In the second step, we determine the subset of loads facing voltage bound violations caused by the DG disconnects in the first step. Since voltage bound violations are typically indicative of faults, DGs are disconnected a lot sooner than the loads as a precautionary measure to avoid feeding current to a fault. That's why we focus on only DG disconnections in the first step.

Now, we provide the details of our two-step approach. For a fixed operator action $u \in \mathcal{U}$, let $\mathcal{Z}$ denote the set of network states x that satisfy the constraints (2), (10), (11), (13)-(16) and (19). Note that $\mathcal{X}(u) \subseteq \mathcal{Z}(u)$ because $\mathcal{X}(u)$ has an additional constraint (12). For a fixed attacker action $d \in \mathcal{D}_{\text{k}}$, let $(u^\star_{\text{in}}(d), x^\star_{\text{in}}(d))$ denote the intermediate autonomous disconnect action and the resulting corresponding network state. We will extract the information about disconnected DGs and the nodal voltages from this intermediate action and network state $(u^\star_{\text{in}}(d), x^\star_{\text{in}}(d))$ to compute the final autonomous disconnect action and the post-contingency state denoted by $(u^\star_{\text{nr}}, x^\star_{\text{nr}})$. We formulate a problem

to compute $(u^{\star}_{\text{in}}(d), x^{\star}_{\text{in}}(d))$ as follows:

$$\begin{aligned} \min_{u_{\text{in}}, x_{\text{in}}} \quad & L\left(u_{\text{in}}, x_{\text{in}}\right) & \\ \text{s.t.} \quad & u_{\text{in}} \in \mathcal{U}(d), & x_{\text{in}} \in \mathcal{Z}\left(u_{\text{in}}\right) \\ & \beta_i^{\text{in}} = 1 & \forall\ i \in \mathcal{N}, \end{aligned} \tag{P-IN}$$

where the intermediate state does not require the loads to satisfy the voltage bound constraint. Note that the load control parameters are set to unity to model the fact that under autonomous disconnections, the operator will not be able to exercise load control.

Next, to compute $(u^{\star}_{\text{nr}}, x^{\star}_{\text{nr}})$, we extract the data of DG connectivity vector $kg^{\text{in}\star}$ and voltage data $\text{v}^{\text{in}\star}$ from the intermediate action-state pair $(u^{\star}_{\text{in}}(d), x^{\text{in}\star}(d))$. Then, we use this data to parameterize the following problem:

$$\begin{aligned} \min_{u_{\text{nr}}, x_{\text{nr}}} \quad & L\left(u_{\text{nr}}, x_{\text{nr}}\right) & \\ \text{s.t.} \quad & u_{\text{nr}} \in \mathcal{U}, & x_{\text{nr}} \in \mathcal{X}(u_{\text{nr}}) \\ & \beta_i^{\text{nr}} = kc_i^{\text{nr}} & \forall\ i \in \mathcal{N} \\ & kg_i^{\text{nr}} \geqslant kg_i^{\text{in}\star}(d) & \forall\ i \in \mathcal{N} \\ & kc_i^{\text{nr}} \geqslant \text{v}_i - \text{v}_i^{\text{in}\star}(d) & \forall\ i \in \mathcal{N} \end{aligned} \tag{P-FN}$$

The optimal solution of the above problem will provide us $(u^{\star}_{\text{nr}}, x^{\star}_{\text{nr}})$, i.e the final autonomous disconnect action and the post-contingency state.

Algorithm 1 summarizes the execution of the two-step approach. It takes as input an initial attack-induced contingency d, and generates automatic disconnect actions for one or more components due to the uncontrolled cascade. Note that the load control parameter $\beta_i = 1$ throughout the cascading disconnects of DGs, unless the load becomes fully disconnected, in which case it switches to $\beta_i = 0$. The final connectivity vector $u^{\star}_{\text{nr}}$ corresponds to a situation where all the connected components satisfy voltage bounds, and can be used to compute the corresponding post-contingency loss $L\left(u^{\star}_{\text{nr}}, x^{\star}_{\text{nr}}\right)$.

B. Randomized algorithm for lower bounding $\mathcal{L}_{AD}$

For each cardinality k, we can compute the worst case loss under response (b) using brute force. However, that would require evaluating loss over combinatorially many $\binom{\text{N}}{\text{k}}$ attacks. Therefore, we present a randomized algorithm to compute worst case loss under the autonomous disconnections; see Algorithm 2.

The algorithm performs the following steps: for each random permutation of nodes, for each attack cardinality k,

Algorithm 1 Uncontrolled cascade under response (b)

Input: attacker action d (initial contingency)

$u^\star_{\rm nr}, x^\star_{\rm nr} \leftarrow$ GetCascadeFinalState(d)
function GetCascadeFinalState(d)
  Compute $u^\star_{\rm in}(d), x^\star_{\rm in}(d)$ by solving (P-IN)
  Extract parameters $(kg^{\rm in\star}, {\rm v}^{\rm in\star})$ from $(u^\star_{\rm in}, x^\star_{\rm in})$
  Instantiate (P-FN) with parameters $(kg^{\rm in\star}, {\rm v}^{\rm in\star})$
  Solve (P-FN) to compute the final state $u^\star_{\rm nr}, x^\star_{\rm nr}$
  return $u^\star_{\rm nr}, x^\star_{\rm nr}$
end function

Algorithm 2 Random attacks and approximately worst case attack for autonomous disconnections

Input: Z (number of random permutations)

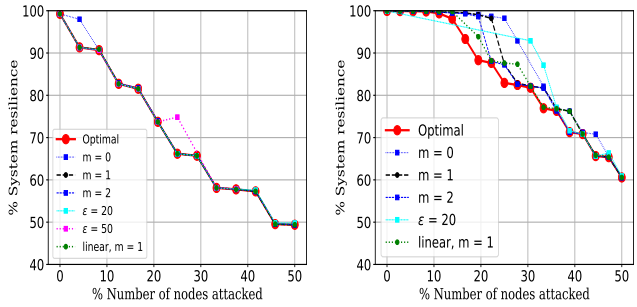
Initialize $Y = \mathbf{0}_{{\rm N}\times Z}$ and $V = \mathbf{0}_{\rm N}$
for $t \in [1\,..\,Z]$ **do**
  Generate a random permutation σ of nodes $\mathcal{N}$
  Reset $d = \mathbf{0}$
  for k $= 1\,..\,$N **do**
    Set $d_{\sigma({\rm k})} = 1$ // k cardinality attack
    $(u_{\rm nr}, x_{\rm nr}) \leftarrow$ GetCascadeFinalState(d) // Refer Algorithm 1 for GetCascadeFinalState
    $Y[{\rm k}, t] \leftarrow L(u_{\rm nr}, x_{\rm nr})$
  end for
end for
for k $\in [1\,..\,{\rm N}]$ **do**
  $V[{\rm k}] \leftarrow \max_{t\in[Z]} Y[{\rm k}, t]$
end for
return Y, V

it disrupts the first k nodes in that permutation, and computes the loss due to autonomous component disconnects (using Algorithm 1). Then, for each attack cardinality, it chooses the maximum among all computed losses. As shown in Sec. VI, for any randomly chosen attack of cardinality k $<$ N, if we disrupt one more DG, then the loss incurred under autonomous disconnections will increase. This monotonicity of increasing loss for increasing attack cardinality cannot be shown if we simply choose N + 1 random attacks of cardinalities k $\in [0\,..\,{\rm N}]$, and plot the loss values *vs.* k. This is the main idea behind Algorithm 2. Next, we show in Sec. VI, how Algorithm 2 and the modified GBD algorithm helps compute the *value of timely response*.

VI. Computational Results

We present computational results to show: (a) the value of timely operator response compared to autonomous disconnections; (b) comparison of the solutions of our GBD approach with the optimal solution (generated for small networks by brute force); and (c) the scalability of our approach to larger networks. We refer the reader to the appendix for the setup of our computational study.

Solution accuracy of the modified GBD method: For a fixed cardinality k, we compute the optimal loss $\mathcal{L}^\star$ using brute force over all disruptions. Then, we use $\mathcal{L}^\star$ as the parameter $\mathcal{L}_{\text{target}}$ for the problem (MCP). If the GBD algorithm applied to (MCP) computes a successful attack with the same cardinality k, then indeed we have obtained the optimal attack of cardinality k. Fig. 4 shows that our GBD method with variable ϵ choices performs very well in computing



(a) N = 24 (b) N = 36

Fig. 4: Accuracy of GBD algorithm and its variants in computing resilience metric in comparison to brute force.

optimal attacks. The sub-optimality resulting from the introduction of ϵ in the generalized Benders cuts decreases as the criticality parameter m increases; see Sec. IV-C.

Performance of the modified GBD method: Table I compares the computational time and solution accuracy of the GBD method with constant ϵ and variable ϵ choices. We also show the results for our solution approach applied to the ($\widehat{\text{Mm}}$), where the optimal attacks are then used to evaluate operator's loss using NPF constraints. Table II shows the benefits of adding cuts (25) and (26) on the computational time required to solve the operator subproblem.

	N = 24			N = 36		
	opt. gap	iterations	time	opt. gap	iterations	time
$\epsilon = 10$	0.00%	4096	3112.4s	0.00%	10000*	12537s
$\epsilon = 20$	0.00%	4094	3098.9s	50.0%	4190	5045.3s
$\epsilon = 50$	8.33%	1596	815.3s	–	–	–
m = 0	8.33%	17	1.49s	27.78	22	6.44s
m = 1	8.33%	123	13.43s	22.22%	230	46.12s
m = 2	5.56%	496	85.90s	16.67%	1828	825.44s
l, m = 0	8.33%	22	2.25s	27.78%	29	4.97s
l, m = 1	8.33%	161	22.65s	16.67%	198	54.42s

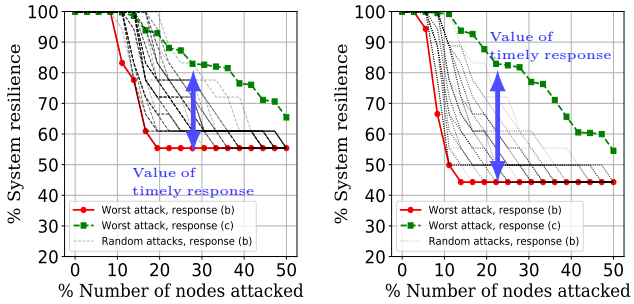
TABLE I: Computational time vs. ϵ choices. The first (resp. second) three rows correspond to fixed (resp. variable) ϵ choices for the GBD method. The last two rows correspond to the BD method for ($\widehat{\text{Mm}}$), and then evaluated using NPF constraints. Results show that GBD method with variable ϵ provides significant computational speedup, while still retaining solution accuracy.

Value of timely response: Recall that in Sec. I, we used post-contingency loss to define the resilience metric for SA system response ($\mathcal{R}_{\text{Mm}}$) and autonomous disconnection ($\mathcal{R}_{\text{AD}}$) cases; and that $\mathcal{R}_{\text{Mm}} \geqslant \mathcal{R}_{\text{AD}}$. Fig. 5 compares the

		N = 24	N = 36	N = 118
m = 0	with cuts	2.30s	4.60s	87.34s
	no cuts	1.87s	4.55s	88.83s
m = 1	with cuts	9.74s	24.66s	613.42s
	no cuts	10.66s	28.29s	2949.04s

TABLE II: Computational speedup due to cuts. These experiments were carried with variable ϵ choices for parameter $m \in \{0, 1\}$. Adding the cuts (25)-(26) become significantly beneficial for large networks, as m increases.

resiliency values for the two cases (response (c) versus autonomous disconnection (b)) for varying number of nodes attacked, where computation of $\mathcal{R}_{\text{Mm}}$ (resp. $\mathcal{R}_{\text{AD}}$) involves using the GBD algorithm (resp. Algorithm 1). In Fig. 5, the resilience curve due to response (b) under random attacks is obtained by using Algorithm 2 in the Sec. V-B.



(a) $\Delta v_0 = 0$ (b) $\Delta v_0 = 0.02$

Fig. 5: Value of timely response (N = 36).

Indeed, under autonomous disconnections, we find that the voltage bound violations cause even the non-disrupted DGs to disconnect resulting in a cascade. However, under operator response, the SA detects these voltage bound violations, and *preemptively* exercises load control and/or disconnects the loads/DGs to reduce the total number of non-disrupted DGs from being disconnected, and minimize the impact of the attack. The difference between the two resiliency curves gives the value of timely response via the SA system. The intermediate curves in Fig. 5 correspond to the DN resilience under random attacks and autonomous disconnections. Finally, when both a TN-side disturbance and a DN attack are simultaneous, the resilience metric of the DN decreases; see Fig. 5b.

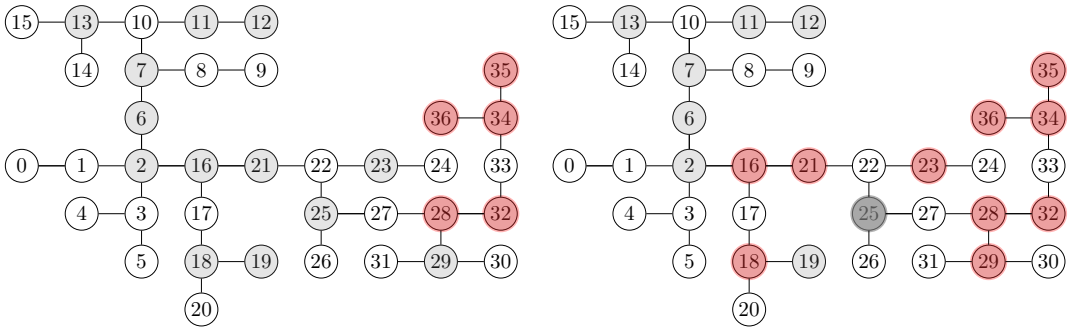
Scalability of GBD algorithm: We tabulate the computational time required by the GBD algorithm to compute min-cardinality attacks for different network sizes and varying values of the resilience metric $\mathcal{R}_{\text{target}} = 100\,(1 - \mathcal{L}_{\text{target}}/\mathcal{L}_{\text{max}})$; see Table III. Note that even for N = 118 nodes, which has 2^{118} configuration vectors, the GBD algorithm finishes computations in ≈10 minutes. In comparison, for N = 36 node network, the brute force method took ≈24 hours. The failure cases in Table III correspond to the cases where there does not exist an attack vector that exceeds the target loss values.

Attacker's downstream strategy: Fig. 6 shows the optimal attacker strategy as computed by brute force for attack cardinality k = 5 (Fig. 6a) and k = 10 (Fig. 6b) on the modified IEEE test network with N = 36. It shows that the

Entries are resilience metric of DN (in percentage), number of iterations (written in brackets), time (in seconds), attack cardinality.			
$\mathcal{R}_{\text{target}}$	N = 24	N = 36	N = 118
99	91.33, (3), 1.46, 1	98.18, (111), 13.01, 8	98.94, (10), 10.6, 6
95	91.33, (3), 1.46, 1	87.97, (112), 13.26, 9	94.19, (19), 15.89, 14
90	82.78, (8), 1.96, 3	87.97, (112), 13.26, 9	89.89, (29), 23.29, 23
85	82.78, (8), 1.96, 3	82.58, (122), 16.36, 11	84.97, (95), 90.75, 39
80	74.61, (18), 2.93, 5	76.94, (137), 20.69, 13	79.71, (86), 613.42, 52
75	74.61, (18), 2.93, 5	71.05, (171), 32.35, 15	Failure
65	58.17, (54), 8.01, 8	60.56, (230), 56.65, 18	
55	49.53, (112), 17.13, 11	Failure	
45	Failure		

TABLE III: Resiliency metric evaluated using GBD algorithm. The realized resilience metric can significantly fall short of the target resilience metric ($\mathcal{R}_{\text{target}} = 100\,(1 - \mathcal{L}_{\text{target}}/\mathcal{L}_{\max})$); for e.g., when the attack cardinality changes from 8 to 9, the resilience for 36-node network decreases sharply from 98.18% to 87.97%. This means that the 36-node DN is at least 85% (actual value 87.97%) resilient to k = 9 cardinality attacks.

attacker has a preference to attack downstream nodes (shown as red nodes) because that would result in maximum post-contingency loss. In Fig. 6b, we can see that even though node 25 is not attacked, it still gets disconnected due to the cascading nature of the attack (shown as dark gray node).



(a) k = 5 (b) k = 10

Fig. 6: Modified IEEE 36 node test network. DG nodes are indicated by gray color.

VII. Concluding remarks

In this article, we developed an approach to evaluate the resilience of DNs under a class of cyber and physical disruptions. We considered an attack model that involves a TN-side voltage disturbance, and DN-side supply-demand disturbance due to simultaneous DG disruptions. We formulated the overall problem as a BiMISOCP, and demonstrated a solution approach based on the GBD method modified by introducing a criticality parameter. Our computational approach for solving BiMISOCPs with binary variables in the inner problem fills an existing gap in the literature, and is applicable to other resource allocation problems in power systems. We also estimated the value of timely operator response which involves preemptive load control or component disconnections implemented via substation automation. Future work involves refining our attacker-operator interaction model onto DNs with microgrid islanding capabilities, and improving algorithmic approaches for quicker system performance recovery.

Problem (Mm) considers the problem of determining attack strategy that will minimize the system performance considering the optimal immediate operator response. However, the operator can gradually connect back the DGs and

the loads to restore the system performance. Here, we argue that the problem of determining optimal attack considering operator's immediate response and gradual recovery can also be posed as a BiMISOCP. Consider a set $\mathcal{T}$ of timesteps $\{0, 1, \cdots, \mathrm{T}\}$, where a period $t \in \mathcal{T}$ denotes a timestep during the system performance recovery. Let u^t denote the operator response during timestep t; x^t the corresponding network state; and $\mathcal{Y}(u^{t-1})$ the set of available operator actions in time step t based on the recovery constraints. Then, the problem can be written as:

$$\begin{aligned} \mathcal{L}_{\mathrm{REC}} \coloneqq \max_{d \in \mathcal{D}_{\mathrm{k}}} \quad & \min_{\{u^t, x^t\}_{t \in \mathcal{T}}} \quad \sum_{t \in \mathcal{T}} L\left(u, x^t\right) \\ & \text{s.t. } u^0 \in \mathcal{U}(d), x^0 \in \mathcal{X}\left(u^t\right) \\ & \quad u^t \in \mathcal{Y}(u^{t-1}), x^t \in \mathcal{X}\left(u^t\right). \end{aligned} \tag{REC}$$

Problem (REC) is also a BiMISOCP, however, the number of mixed-binary variables in the inner problem increases linearly with the number of time steps. Our future work includes extending the solution approach we developed in this paper for solving this large-scale BiMISOCP.

References

[1] A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks," in *Proceedings of the 2010 ACC*, 2010.

[2] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, Feb 2015.

[3] D. Shelar, S. Amin, and I. Hiskens, "Towards resilience-aware resource allocation and dispatch in electricity distribution networks," *Book Ch., Control of Energy Markets & Grids*, 2018.

[4] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, 2016.

[5] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack Detection and Identification in Cyber-Physical Systems," *IEEE Trans. on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[6] ——, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *2011 50th IEEE Conference on Decision and Control and European Control Conference*, 2011, pp. 2195–2201.

[7] D. Bienstock and A. Verma, "The N-k Problem in Power Grids: New Models, Formulations, and Numerical Experiments," *SIAM J. on Optimization*, vol. 20, no. 5, pp. 2352–2380, Jun. 2010.

[8] J. Salmeron, K. Wood, and R. Baldick, "Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids,"

IEEE Trans. Power Syst., vol. 24, no. 1, pp. 96–104, 2009.

[9] K. C. Sou, H. Sandberg, and K. Johansson, "Computing Critical k -Tuples in Power Networks," *Power Systems, IEEE Trans. on*, vol. 27, no. 3, pp. 1511–1520, 2012.

[10] NERC Reliability Standards, "CIP-005-5 – Cyber Security - Electronic Security Perimeter(s)," 2015.

[11] R. Lee, M. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center," 2015.

[12] 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., 2014.

[13] D. Shelar and S. Amin, "Security Assessment of Electricity Distribution Networks Under DER Node Compromises," *IEEE Trans. on Control of Net. Syst.*, vol. 4, no. 1, pp. 23–36, 2017.

[14] J. T. Moore and J. F. Bard, "The mixed integer linear bilevel programming problem," *Operations research*, vol. 38, no. 5, pp. 911–921, 1990.

[15] P. Xu and L. Wang, "An exact algorithm for the bilevel mixed integer linear programming problem under three simplifying assumptions," *Computers & Operations Research*, vol. 41, 2014.

[16] M. Fischetti, I. Ljubić, M. Monaci, and M. Sinnl, "A New General-Purpose Algorithm for Mixed-Integer Bilevel Linear Programs," Tech. Rep. 6, 2016.

[17] ——, "On the use of intersection cuts for bilevel optimization," *Mathematical Programming*, vol. 172, no. 1, Nov 2018.

[18] L. Wang and P. Xu, "The Watermelon Algorithm for The Bilevel Integer Linear Programming Problem," *SIAM Journal on Optimization*, vol. 27, no. 3, pp. 1403–1430, 2017.

[19] L. Lozano and J. C. Smith, "A Value-Function-Based Exact Approach for the Bilevel Mixed-Integer Programming Problem," *Operations Research*, 2017.

[20] R. Wood, "Bilevel Network Interdiction Models: Formulations and Solutions," in *Wiley Encyclopedia of Operations Research and Management Science*, 2011.

[21] B. Hua, R. Baldick, and K. Wood, "Interdiction of a Mixed-Integer Linear System," *INFORMS*, 01/2019 2019.

[22] B. Zeng and Y. An, "Solving bilevel mixed integer program by reformulations and decomposition," *Optimization online*, 2014.

[23] National Infrastructure Advisory Council, "Critical Infrastructure Resilience Final Report and Recommendations," 2009.

[24] "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, April 2018.

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

[26] L. Gan, N. Li, U. Topcu, and S. H. Low, "Exact Convex Relaxation of Optimal Power Flow in Radial Networks," *IEEE Trans. on Automatic Control*, vol. 60, no. 1, pp. 72–87, 2015.

[27] M. Baran and F. F. Wu, "Optimal sizing of capacitors placed on a radial distribution system," *IEEE Trans. on Power Delivery*, vol. 4, no. 1, pp. 735–743, 1989.

[28] A. M. Geoffrion, "Generalized Benders decomposition," *Journal of Optimization Theory and Applications*, no. 4, 1972.

[29] D. Shelar, S. Amin, and I. Hiskens, "Evaluating resilience of electricity distribution networks via a modification of generalized benders decomposition method - Technical Report," 2020. [Online]. Available: https://arxiv.org/abs/1812.01746

[30] W. H. Kersting, *Distribution System Modeling and Analysis*. CRC Press, 2012.

Devendra Shelar is Postdoctoral Associate in LIDS at MIT. He works on developing resilient control algorithms for cyberphysical systems against extreme weather events and security attacks. His research leverages ideas from large-scale optimization, scheduling, and game theory. Dr. Shelar received his Ph.D. in Computational Science and Engineering from MIT, 2019.

Saurabh Amin is Associate Professor in the Department of CEE and core member of the LIDS at MIT. He received his Ph.D. in Systems Engineering from the UC Berkeley in 2011. His fields of interests include control and optimization, applied game theory, and networks. His research focuses on the design and implementation of resilient control algorithms for networked infrastructures systems.

Ian A. Hiskens is the Vennema Professor of Engineering in the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor. His research interests lie at the intersection of power system analysis and systems theory. He is a Fellow of IEEE and a Fellow of Engineers Australia. Dr. Hiskens is a Chartered Professional Engineer in Australia and the 2020 recipient of the M.A. Sargent Medal from Engineers Australia.

Appendix

DN parameters	
$\mathcal{N}$	set of nodes in DN
$\mathcal{E}$	set of edges in DN
0	substation node label
$\mathrm{N} = \lvert\mathcal{N}\rvert$	number of non-substation nodes in DN
$\mathbf{j}$	complex square root of -1, $\mathbf{j} = \sqrt{-1}$
$\mathbf{v^{nom}}$	nominal squared voltage magnitude (1 pu)
v_0	squared voltage magnitude at substation node
Nodal quantities of node $i \in \mathcal{N}$	
v_i	squared voltage magnitude at node i
$\overline{\mathbf{pc}}_i + \mathbf{j}\overline{\mathbf{qc}}_i$	nominal demand at node i
$\overline{\mathbf{pg}}_i + \mathbf{j}\overline{\mathbf{qg}}_i$	nominal generation at node i
η_i	$\max_{qg_i, pg_i \neq 0}(\lvert qg_i\rvert / pg_i)$ maximum ratio of absolute reactive power to active power
$pc_i + \mathbf{j}qc_i$	actual power consumed at node i
$pg_i + \mathbf{j}qg_i$	actual power generated at node i
$p_i + \mathbf{j}q_i$	net power consumed at node i
$\underline{\mathbf{vc}}_i, \overline{\mathbf{vc}}_i$	lower, upper voltage bounds for load at node i
$\underline{\mathbf{vg}}_i, \overline{\mathbf{vg}}_i$	lower, upper voltage bounds for DG at node i
kg_i	0 if DG at node i is connected to DN; 1 otherwise
kc_i	0 if load at node i is connected to DN; 1 otherwise
β_i	fraction of demand satisfied at node i
$\underline{\beta}_i$	lower bound of load control parameter β_i
$x \in \mathbb{R}^{6\mathrm{N}-3}$	$x = (p, q, P, Q, \mathrm{v}, \ell)$ the network state
Parameters of edge $(i,j) \in \mathcal{E}$	
$P_{ij} + \mathbf{j}Q_{ij}$	power flowing from node i to node j
$\mathbf{r}_{ij}, \mathbf{x}_{ij}$	resistance and reactance of line $(i,j) \in \mathcal{E}$
ℓ_{ij}	square of magnitude of current on line (i,j)
Precedence relationship between nodes $i, j \in \mathcal{N}, i \neq j$	
$i \prec j$	Node i precedes node j if i lies on the path connecting j and the substation node 0
Cyber-physical failure parameter	
$\Delta\mathrm{v}_0$	Drop in substation voltage due to transmission network-side disturbance.
Attack variables	
$d \in \{0,1\}^{\mathcal{N}}$	$d_i = 1$ if DG at node i is disrupted; 0 otherwise.
Operator response variables	
u	$u = (\beta, pg, qg, kc, kg)$ an operator response
Generic math notation	
$[a \,..\, b]$	integer interval set for $a, b \in \mathbb{Z}$

TABLE IV: Table of Notations.

A. Setup for Computational Study

We consider three networks: 24 node, and modified IEEE 36 node and 118 node networks. Each line has an identical impedance of $\mathbf{r}_{ij} = 0.01, \mathbf{x}_{ij} = 0.02$. Half of the nodes have a DG and half have a load. Hence, the maximum cardinality of an attack in our computational study will be half the number of the nodes in the DN. Consider a parameter $\alpha = \frac{6}{\mathrm{N}}$. Before the contingency, each DG has active power output of $\overline{\mathbf{pg}}_i = \alpha$, and each load has a demand of $\overline{\mathbf{pc}}_i = 1.25\alpha$. Thus, we assume 80% DG penetration since the total DG output is 80% of the total demand. The voltage bounds are $\underline{\mathbf{vc}}_i = 0.9$, $\overline{\mathbf{vc}}_i = 1.1$, $\underline{\mathbf{vg}}_i = 0.92$ and $\overline{\mathbf{vg}}_i = 1.08$. The reactive power values are chosen to be exactly one third that of the corresponding active power value, i.e. a 0.95 (lagging) power factor for each load and DG. The values are chosen

such that the total net active power demand in the DN is 0.75 pu, and the lowest voltage in the network before any contingency is close to $\underline{\mathbf{vg}}$. The maximum load control parameter is $\underline{\beta}_i = 0.8$, i.e. at most 20% of each load demand can be curtailed. For the sake of simplicity, we assume that all DGs and loads are homogeneous. The values of cost coefficients are chosen to be $\mathrm{W}^{\mathrm{LC}} = 100/\overline{\mathbf{pc}}_i, \mathrm{W}^{\mathrm{VR}} = 100$ and $\mathrm{W}^{\mathrm{LS}} = 1000/\overline{\mathbf{pc}}_i$.

B. Proofs of Technical Results in Sec. III

For $i \in \mathcal{N}$, let $\mathcal{P}_i \subseteq \mathcal{E}$ denote the subset of DN edges on the path from the substation node 0 to node i. For $i, j \in \mathcal{N}$, let $\mathbf{R}_{ij}$ (resp. $\mathbf{X}_{ij}$) denote the sum of resistances (resp. reactances) of the edges common to $\mathcal{P}_i$ and $\mathcal{P}_j$, i.e.,

$$\mathbf{R}_{ij} \coloneqq \textstyle\sum_{((k,l)\in\mathcal{P}_i\cap\mathcal{P}_j)} \mathbf{r}_{kl}, \qquad \mathbf{X}_{ij} \coloneqq \textstyle\sum_{((k,l)\in\mathcal{P}_i\cap\mathcal{P}_j)} \mathbf{x}_{kl}.$$

Let $\mathcal{N}_i \subseteq \mathcal{N}$ be the subset of nodes that form the subtree rooted at node i, which includes node i, and let $\mathcal{W}_i \subseteq \mathcal{E}$ be the subset of edges that form the subtree $\mathcal{N}_i$. Then, the following equations can be derived using recursion on the radial tree topology.

$$\widehat{P}_{ij} = \textstyle\sum_{k\in\mathcal{N}_j} p_k \qquad \forall\ (i,j) \in \mathcal{E} \tag{29}$$

$$\widehat{Q}_{ij} = \textstyle\sum_{k\in\mathcal{N}_j} q_k \qquad \forall\ (i,j) \in \mathcal{E} \tag{30}$$

$$\hat{\mathrm{v}}_j = \mathbf{v}^{\mathbf{nom}} - 2\textstyle\sum_k (\mathbf{R}_{jk}p_k + \mathbf{X}_{jk}q_k) \quad \forall\ j \in \mathcal{N} \tag{31}$$

$$P_{ij} = \widehat{P}_{ij} + \textstyle\sum_{(k,l)\in\mathcal{W}_i} \mathbf{r}_{kl}\ell_{kl} \qquad \forall\ (i,j) \in \mathcal{E} \tag{32}$$

$$Q_{ij} = \widehat{Q}_{ij} + \textstyle\sum_{(k,l)\in\mathcal{W}_i} \mathbf{x}_{kl}\ell_{kl} \qquad \forall\ (i,j) \in \mathcal{E} \tag{33}$$

$$\begin{aligned} \mathrm{v}_j = \hat{\mathrm{v}}_j - 2\textstyle\sum_{(k,l)\in\mathcal{E}}(\mathbf{R}_{jl}\mathbf{r}_{kl} + \mathbf{X}_{jl}\mathbf{x}_{kl})\ell_{kl} + \\ \textstyle\sum_{(k,l)\in\mathcal{P}_j}(\mathbf{r}_{kl}^2 + \mathbf{x}_{kl}^2)\ell_{kl} \end{aligned} \tag{34}$$

Thus, we can write $(\widehat{P}, \widehat{Q}, \hat{\mathrm{v}})$ as functions of (p, q) and (P, Q, v) as functions of (p, q, ℓ).

Now, the objective in problem (24) is strictly increasing in (p, q, ℓ) and p_i and q_i is fixed $\forall\ i \in \mathcal{N}$. Furthermore, we have assumed the NRPF condition. Hence, as shown in [26], the solution of problem (24) is unique. Thus, even ℓ can be considered a function of (p, q).

Proof of Lemma 1. The Lemma follows from the fact that $(\widehat{P}, \widehat{Q}, \hat{\mathrm{v}})$ and (P, Q, v, ℓ) are functions of (p, q) and by a straightforward application of (13). ■

Consider the iterative Backward-Forward Sweep (BFS) algorithm [30] used to compute the NPF values, which we

modify to consider the TN-side voltage disturbance. Let $(P^t, Q^t, \mathrm{v}^t, \ell^t)$ be the values computed in t^{th} iteration of the FBS algorithm.

Initialization:

$$\mathrm{v}_i^0 = \mathbf{v^{nom}} - \Delta \mathrm{v}_0 \qquad \forall\ i \in \mathcal{N}\backslash\{0\} \tag{35}$$

$$\mathrm{v}_0^t = \mathbf{v^{nom}} - \Delta \mathrm{v}_0 \qquad \forall\ t \in [1\ ..\ \mathrm{T}] \tag{36}$$

$$\ell_{ij}^0 = 0, P_{ij}^0 = \widehat{P}_{ij}, Q_{ij}^0 = \widehat{Q}_{ij} \qquad \forall\ (i,j) \in \mathcal{E}. \tag{37}$$

Backward Sweep: Starting from the leaf nodes to the substation node, compute:

$$\ell_{ij}^t = \left((P_{ij}^{t-1})^2 + (Q_{ij}^{t-1})^2 \right) / \mathrm{v}_i^{t-1} \qquad \forall\ (i,j) \in \mathcal{E} \tag{38}$$

$$P_{ij}^t = p_j + \mathbf{r}_{ij}\ell_{ij}^t + \textstyle\sum_{k:(j,k)\in\mathcal{E}} P_{jk}^t \qquad \forall\ (i,j) \in \mathcal{E} \tag{39}$$

$$Q_{ij}^t = q_j + \mathbf{x}_{ij}\ell_{ij}^t + \textstyle\sum_{k:(j,k)\in\mathcal{E}} Q_{jk}^t \qquad \forall\ (i,j) \in \mathcal{E}. \tag{40}$$

Forward Sweep: Starting from the children nodes of the substation node to the leaf nodes, compute $\forall\ (i,j) \in \mathcal{E}$:

$$\mathrm{v}_j^t = \mathrm{v}_i^t - 2\left(\mathbf{r}_{ij}P_{ij}^t + \mathbf{x}_{ij}Q_{ij}^t\right) + (\mathbf{r}_{ij}^2 + \mathbf{x}_{ij}^2)\ell_{ij}^t. \tag{41}$$

The BFS algorithm is bound to converge under mild assumptions of power flows in the DNs, for e.g., small line losses, small line impedances; see [13] for technical definitions of these assumptions.

Proof of Prop. 1. Let $\{(P^t, Q^t, \mathrm{v}^t, \ell^t)\}_{t=1}^{\mathrm{T}}$ be the values computed by the BFS algorithm in iteration $t = [1\ ..\ \mathrm{T}]$ where T is a fixed large number of iterations. Now, suppose that p_k increases marginally to $p_k + \Delta p_k$, while all other consumption values remain constant. Let $\{(\breve{P}^t, \breve{Q}^t, \breve{\mathrm{v}}^t, \breve{\ell}^t)\}_{t=1}^{\mathrm{T}}$ be the new values computed by the BFS algorithm.

From (39) and (40), we get:

$$\breve{P}_{ij}^0 = P_{ij}^0 + \Delta p_k \quad \forall\ (i,j) \in \mathcal{P}_k \tag{42a}$$

$$\breve{P}_{ij}^0 = P_{ij}^0 \qquad \forall\ (i,j) \in \mathcal{E}\backslash\mathcal{P}_k \tag{42b}$$

$$\breve{Q}_{ij}^0 = Q_{ij}^0 \qquad \forall\ (i,j) \in \mathcal{E}. \tag{42c}$$

By applying (38) and (42), we get

$$\breve{\ell}_{ij}^1 > \ell_{ij}^1 \qquad \forall\ (i,j) \in \mathcal{P}_k \tag{43a}$$

$$\breve{\ell}_{ij}^{1} = \ell_{ij}^{1} \qquad \forall\ (i,j) \in \mathcal{E} \backslash \mathcal{P}_k. \tag{43b}$$

Next, from (41) and (43), we get:

$$\breve{\mathrm{v}}_i^1 < \mathrm{v}_i^1 \qquad \forall\ i \in \mathcal{N},$$

which, in turn, implies

$$\breve{\ell}_{ij}^{2} > \ell_{ij}^{2} \qquad \forall\ (i,j) \in \mathcal{E}.$$

Now, by making an inductive argument based on (38)-(41), we can show that

$$\breve{\ell}_{ij}^{t} > \ell_{ij}^{t} \quad \forall\ (i,j) \in \mathcal{E}, t \geqslant 2.$$

Furthermore, we can also show that

$$\breve{\ell}_{ij}^{t} - \breve{\ell}_{ij}^{t-1} > \ell_{ij}^{t} - \ell_{ij}^{t-1} \quad \forall\ (i,j) \in \mathcal{E}, t \geqslant 2.$$

(The proof of the previous equation requires a further detailed analysis which is provided in [29].) Thus, $\breve{\ell}_{ij}^{t}$ and ℓ_{ij}^{t} are the t^{th} terms of two monotonically increasing and converging sequences such that the difference between consecutive terms of the former sequence are strictly greater than the corresponding difference of the latter. Therefore, the relative ordering also remains true for the converged values in the final iteration, i.e.,

$$\breve{\ell}_{ij} > \ell_{ij} \quad \forall\ (i,j) \in \mathcal{E}.$$

Then, by applying (32)-(34), we can show that

$$\begin{aligned}
\breve{P}_{ij} - P_{ij} > \breve{P}_{ij}^{0} - P_{ij}^{0} \ &\geqslant 0 \qquad \forall\ (i,j) \in \mathcal{E} \\
\breve{Q}_{ij} - Q_{ij} > \breve{Q}_{ij}^{0} - Q_{ij}^{0} \ &= 0 \qquad \forall\ (i,j) \in \mathcal{E} \\
\breve{\mathrm{v}}_i - \mathrm{v}_i < \breve{\mathrm{v}}_i^{0} - \mathrm{v}_i^{0} \ &< 0 \qquad \forall\ i \in \mathcal{N}.
\end{aligned}$$

Then, taking the limit $\Delta p_k \to 0$,

$$\frac{\partial P_{ij}}{\partial p_k} > \frac{\partial \widehat{P}_{ij}}{\partial p_k} \geqslant 0 > \frac{\partial \hat{\mathrm{v}}_l}{\partial p_k} > \frac{\partial \mathrm{v}_l}{\partial p_k} \quad \forall\ (i,j) \in \mathcal{E}, l \in \mathcal{N}.$$

We conclude the proof by noting that a similar argument can be made had q_k been increased instead of p_k. ■

Proof of Prop. 2. The proof follows from the application of Prop. 1 and Lemma 1. Essentially, increasing DG output will result in reduced line losses and better DN voltage profile. These effects directly help lower operator loss. However, the improved voltage profile may also help further reduce the load control and connect back disconnected loads, if any. This is true because of the NRPF condition, and as a result increasing voltages will not lead to violation of upper voltage bounds. ■

Proof of Prop. 3. Let $(P^t, Q^t, \mathrm{v}^t, \ell^t)$ (resp. $(\breve{P}^t, \breve{Q}^t, \breve{\mathrm{v}}^t, \breve{\ell}^t)$) be the values computed in t^{th} iteration of the BFS algorithm when p_k (resp. p_l) is increased by Δp. Applying (29) and (30), we get

$$\breve{P}^0_{ij} = P^0_{ij} + \Delta p_k \quad \forall\ (i,j) \in \mathcal{P}_l \backslash \mathcal{P}_k \tag{44a}$$

$$\breve{P}^0_{ij} = P^0_{ij} \quad \forall\ (i,j) \in \mathcal{E} \backslash (\mathcal{P}_l \backslash \mathcal{P}_k) \tag{44b}$$

$$\breve{Q}^0_{ij} = Q^0_{ij} \quad \forall\ (i,j) \in \mathcal{E}. \tag{44c}$$

This is because when the consumption at l increases, the additional power has to travel a path $\mathcal{P}_l$ that subsumes the path $\mathcal{P}_k$. The rest of the proof is similar to that of Prop. 1. Essentially, we again show that:

$$\breve{\ell}_{ij} > \ell_{ij} \qquad \forall\ (i,j) \in \mathcal{E},$$

and, therefore,

$$\breve{P}_{ij} - P_{ij} > 0, \quad \breve{Q}_{ij} - Q_{ij} > 0 \qquad \forall\ (i,j) \in \mathcal{E}$$

$$\breve{\mathrm{v}}_i - \mathrm{v}_i < 0 \qquad \forall\ i \in \mathcal{N}.$$

The proof completes by taking the limit $\Delta p \to 0$. ■

Proof of Prop. 4. Let $(u^\star, x^\star)$ be the optimal solution of the problem $\mathcal{C}_{\mathrm{Mm}}(d)$. For the fixed operator response $u^\star$, the p and q vectors are uniquely determined. Let $\widehat{x}$ be the LPF solution for the p and q vectors. By applying Prop. 1, we can show that $\mathbf{v^{nom}} \geqslant \widehat{\mathrm{v}} \geqslant \mathrm{v}$. Therefore, we can claim that $(u^\star, \widehat{x})$ is a feasible solution for the problem $\widehat{\mathcal{C}}_{\mathrm{Mm}}(d)$.

Now, $L(u^\star, x^\star) - \widehat{L}(u^\star, \widehat{x}) = \mathrm{W}^{\mathrm{VR}}(\|\mathbf{v^{nom}} - \mathrm{v}^\star\|_\infty - \|\mathbf{v^{nom}} - \widehat{\mathrm{v}}\|_\infty) + \mathrm{W}^{\mathrm{LL}} \sum_{ij \in \mathcal{E}} \mathbf{r}_{ij} \ell^\star_{ij} \geqslant 0$, because both these terms are non-negative. ■

Proof of Prop. 5. Let $d^\star$ and $\hat{d}^\star$ be the optimal attacker strategies to problems (Mm) and ($\widehat{\mathrm{Mm}}$), respectively. Then, $\mathcal{L}(d^\star) \geqslant \mathcal{L}(\hat{d}^\star) \geqslant \widehat{\mathcal{L}}(\hat{d}^\star)$, where the first inequality holds because of optimality of $d^\star$, and the second inequality holds because of Prop. 4. The proof completes by applying the definitions of $\mathcal{R}_{\mathrm{Mm}}$ and $\widehat{\mathcal{R}}_{\mathrm{Mm}}$. ■

Proof of Prop. 6. Suppose for contradiction that $u \in \mathcal{U}$ is an optimal response such that $kc_i = 1$, $kc_j = 0$, and $\beta_j = a$ for some value $a \in [\underline{\beta}_j, 1]$. Then, we construct a response $\breve{u}$ which is exactly the same as u except that $\breve{kc}_i = 0$, $\breve{kc}_j = 1$, and $\breve{\beta}_i = a$. Let x and $\breve{x}$ be the corresponding network states. By Prop. 3, $\breve{\ell} < \ell$ and $\mathbf{v^{nom}} > \breve{\mathrm{v}} > \mathrm{v} \geqslant \underline{\mathbf{vc}}$. Therefore, $\breve{x}$ satisfies voltage bounds, and $\breve{u}$ is a feasible operator strategy. Also, by Prop. 1 and Prop. 3, the cost of voltage deviation and the cost of line loss is smaller because the increase in active and reactive load at i (i.e. $a\overline{\mathbf{pc}}_i$ and $a\overline{\mathbf{qc}}_i$) is at most equal to the reduction in active and reactive load at j ($a\overline{\mathbf{pc}}_j$ and $a\overline{\mathbf{qc}}_j$)).

Now, the cost of load control and shedding in response $\breve{u}$ is no worse than that in u ($\because \mathrm{W}_j^{\mathrm{LC}} + \mathrm{W}_i^{\mathrm{LC}}(1-a) \leqslant \mathrm{W}_i^{\mathrm{LC}} + \mathrm{W}_j^{\mathrm{LC}}(1-a)$). Moreover, the improved voltage profile may allow further reduction in cost of load control/shedding. Thus, u cannot be an optimal response. ■

Proof of Prop. 7. Suppose for contradiction that $u \in \mathcal{U}$ is an optimal response such that $kg_i = 1$, and $kg_j = 0$. Then, we can construct a response $\breve{u}$ which is exactly the same as u except that $\breve{kg}_i = 0$, because i was not disrupted by the attacker. Then, the cost of voltage deviations and line losses in response $\breve{u}$ is lesser than that in u by Prop. 3 and the fact that the decrease in active and reactive output at i (i.e. $\overline{\mathbf{pg}}_i$ and $\eta_i\overline{\mathbf{pg}}_i$) is smaller than the increase in active and reactive output at j (i.e. $\overline{\mathbf{pg}}_j$ and $\eta_j\overline{\mathbf{pg}}_j$). Thus, u cannot be an optimal response. ■