Resilience of Electricity Distribution Networks
Part II: Leveraging Microgrids

Devendra Shelar, Saurabh Amin, and Ian Hiskens

Abstract—**Advances in microgrids powered by Distributed Energy Resources (DERs) make them an attractive response capability for improving the resilience of electricity distribution networks (DNs). This paper presents an approach to evaluate the value of implementing a timely response using microgrid operations and DER dispatch in the aftermath of a disruption event, involving strategic compromise of multiple DN components. Firstly, we extend the resiliency assessment framework in [1] and develop a sequential (bilevel) model of attacker-operator interactions on a radial DN with one or more microgrids. Particularly, the operator response includes microgrid operations under various islanding configurations (regimes), and single- or multi-master operation of DERs in providing grid-forming services as well as frequency and voltage regulation. Secondly, we introduce a restoration problem in which the operator gradually reconnects the disrupted components over multiple periods to restore the nominal performance of the DN. The first problem, formulated as a bilevel mixed-integer problem, is solved using a Benders decomposition method. The second problem, formulated as a multi-period mixed-integer problem, can be solved using a greedy algorithm. Our results illustrate the benefit of using microgrids in reducing the operator's losses, both immediately after the disruption event and during the restoration process.**

Index Terms—**Cyber-physical systems, network security, smart grids, bilevel optimization, microgrids**

I. Introduction

Modern electricity Distribution Networks (DNs) are prone to risks of service interruptions due to the failures of unreliable, and often insecure, cyber and physical components. Recent disruptions caused by natural disasters [2] and security attacks [3, 4] highlight the vulnerability of DNs to cyberphysical failures. In this article, we investigate the use of microgrid technologies such as microgrid islanding and dispatch of Distributed Energy Resources (DERs) [4, 5, 6] toward improving DN resilience. Historically, the idea of DER-powered microgrids as a response mechanism has been considered for responding to reliability failures [4, 6, 7]. Indeed, microgrids have been implemented to support the reliability targets of critical facilities such as hospitals, industrial plants, and military bases. However, their technological feasibility (and related operational aspects) in responding to security failures has received limited attention. We address this issue by building on our work in [1], and focus on evaluating the effectiveness of DER-powered microgrids in limiting post-contingency losses after a disruption.

We model the sequential interaction between a DN operator and an external adversary as follows [1]:

$$\mathcal{L}_{\mathrm{Mm}} := \max_{d \in \mathcal{D}_{\mathrm{k}}} \min_{u \in \mathcal{U}(d)} L(u, x) \qquad \text{s.t.} \quad x \in \mathcal{X}(u), \quad \text{(P1)}$$

where $d \in \mathcal{D}_{\mathrm{k}}$ denotes an attacker strategy, $u \in \mathcal{U}(d)$ an operator response strategy, $x \in \mathcal{X}$ the network state, and L the composite loss function, the details of which are presented in Sec. IV. In [1], we argued that cyberphysical disruptions to DNs can lead to operating bound violations and cause uncontrolled or forced disconnects of DN components. Specifically, we modeled the impact of attacker-induced disconnects of DN components as supply-demand disturbances, and the impact of TN-side disturbances as voltage deviations at the substation node. Then, we considered preemptive load control and component disconnects as operator response actions for the generic setting when the attacker's (resp. operator's) goal is to maximize (resp. minimize) the post-contingency losses. We introduced $\mathcal{R}_{\mathrm{Mm}} := 100\,(1 - \mathcal{L}_{\mathrm{Mm}}/\mathcal{L}_{\max})$ as a resilience metric of the DN, where $\mathcal{L}_{\max}$ (chosen for sake of normalization) denotes the operator loss when all DN components are disconnected; see Fig. 1. Finally, we evaluated the value of optimal response as the total reduction in post-contingency losses relative to the case of autonomous (local protection driven) disconnections, i.e. $\mathcal{R}_{\mathrm{Mm}} - \mathcal{R}_{\mathrm{AD}}$, where $\mathcal{R}_{\mathrm{AD}} = 100\,(1 - \mathcal{L}_{\mathrm{AD}}/\mathcal{L}_{\max})$.

In this article, we consider another bilevel formulation:

$$\mathcal{L}_{\mathrm{MG}} := \max_{d \in \mathcal{D}_{\mathrm{k}}^{\mathrm{m}}} \min_{u \in \mathcal{U}_{\mathrm{m}}(d)} L_{\mathrm{m}}(u, x) \quad \text{s.t.} \ x \in \mathcal{X}_{\mathrm{m}}(u), \quad \text{(P2)}$$

where the network model $\mathcal{X}_{\mathrm{m}}$, and the loss function L_{m} are extended to capture microgrid operations (Sec. II) and DER dispatch and regulation aspects (Sec. III); the set of attacker strategies $\mathcal{D}_{\mathrm{k}}^{\mathrm{m}}$ and the set of operator strategies $\mathcal{U}_{\mathrm{m}}$ are also modified to capture attacker-operator interactions for DNs with DER-powered microgrids (Sec. IV). The maximin value of (P2), $\mathcal{L}_{\mathrm{MG}}$, denotes the worst-case post-contingency loss incurred by the operator for the given microgrid and DER capabilities; see Fig. 1. Then, $\mathcal{R}_{\mathrm{MG}} := 100\,(1 - \mathcal{L}_{\mathrm{MG}}/\mathcal{L}_{\max})$ can be viewed as a resilience metric of the DN under microgrid-enabled op-

Devendra Shelar and Saurabh Amin are with Department of Civil and Environmental Engineering, Massachusetts Institute of Technology, 77 Massachusetts Avenue 1-241, 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).

erator response. Furthermore, the relative value of timely microgrid response (or equivalently, the improvement in DN resilience due to microgrids) can be evaluated as $(\mathcal{R}_{\mathrm{MG}} - \mathcal{R}_{\mathrm{Mm}})$. We posit that advances in DER-enabled microgrids and emergency control operations at the substation level can be leveraged to implement timely resiliency-improving response actions (less than a few seconds after a disturbance event).
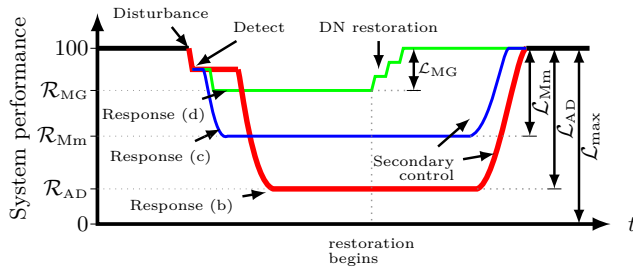

Fig. 1: Performance under various response capabilities.

In [1], we considered three operator response models:

(a) Remote control by the control center during normal conditions;

(b) Autonomous (protection driven) disconnection of individual components (tripping of DGs or loads under nodal violations in operating conditions); and

(c) Emergency control by a secure Substation Automation (SA) system.

As in [1], it is assumed that the emergency control actions (c) subsume the autonomous actions (b) by making decisions that are coordinated across the SA system. Hence, (b) and (c) are never simultaneously active. Furthermore, in this paper, we consider the following extension of (c):

(d) Emergency control by the SA involving microgrid islanding and DER dispatch.

Analogous to [1], we consider that the SA system can detect the disrupted components from changes in measurements of net nodal consumption. By using knowledge of the attack the SA can compute and implement the operator response in a timely manner. For our purposes, response (d) is an optimal second-stage response in (P2). Our analysis relies on the premise that such response can be implemented via modern SA systems during disruptions. Indeed, the continued improvements in SA system disturbance detection and control capabilities can further assist in restoration operations.

The resiliency of a system also reflects how quickly it can rebound to its nominal state after a disruption [1, 8]. Microgrids can provide partial demand satisfaction during the system restoration process, especially during the time when the DN is fully disconnected from the TN. We consider an admittedly simple, but practically relevant, multi-period DN restoration problem in which the disrupted DN components are gradually restored over several periods; refer to "DN restoration" in Fig. 1. Our goal in this problem is to compute an operator strategy in each time period (roughly, on the order of a few minutes). Such

a strategy is comprised of reconnecting disrupted components, modifying the microgrid islanding configuration, and dispatching the DERs within individual microgrids.

Our modeling approach addresses some key issues regarding microgrid and DER operations. In particular, we allow for the formation of one or more microgrid islands in radial DNs. When all the microgrids are connected to the transmission network (TN), the DN is operating in the *grid-connected* regime. If none of the microgrids are connected to the TN, then the DN is operating in the *fully-islanded* regime. In our approach, the DN can also operate in a *partially-islanded* regime, in which some of the microgrids are connected to the TN while other microgrids are not. In both partially- and fully- islanded regimes, each microgrid can operate as an isolated microgrid or as part of a larger microgrid. To model power flows in each of the microgrids, we introduce a natural extension of the LinDistFlow equations. The resulting network model captures DN operations in all the above-mentioned regimes (Sec. II). We limit attention to linear power flows mainly for the ease of exposition.

Importantly, we consider the parallel operation of multiple DERs for the provision of *grid-forming* services, which involve providing voltage and frequency references, as well as maintaining voltage and frequency within operating bounds (i.e. *regulation* services). When a microgrid is connected to the TN, the bulk generators provide the grid-forming services. However, when a microgrid is disconnected from the TN, then at least one DER within that microgrid must provide the grid-forming services [5]. Depending on the number of grid-forming DERs within a microgrid, one can consider two modes of DER operation under islanded regimes, namely Single-Master Operation (with a single grid-forming DER) and Multi-Master Operation (with more than one grid-forming DER) [5]. Our model is sufficiently flexible to capture both the single- and multi-master modes of DER operation. In addition to voltage regulation, we also consider frequency regulation, which becomes important for microgrids due to the low inertia of the DERs. By using the appropriate droop control equations, we capture both frequency and voltage regulation aspects resulting from multiple DERs operating in parallel within a microgrid (Sec. III).

Our main contributions are as follows:

(⋆) We capture the different microgrid regimes as well as DER operating modes by developing a new mixed-integer linear network model. This modeling approach enables us to formulate (P2) as a Bilevel Mixed-Integer Problem (BiMIP). In [1], we showed that (P1) is also a BiMIP, and can be solved using a Benders Decomposition (BD) algorithm. In Sec. IV, we show that this algorithm can be applied to the extended formulation (P2).

(⋆) Our network model is also well-suited for formulating a DN restoration problem as a multi-period Mixed-Integer Problem (MIP). In our restoration problem, the network state in any period only depends on the operator response actions in that period, and the

network state in the previous period. We exploit this feature and propose a greedy heuristic that seeks to reconnect the disrupted components in each period such that the post-contingency losses for that period are minimized (Sec. VI).

II. Multi-Microgrid DN model

In this section, we develop a model of a radial DN with one or more microgrids. This network model extends the LinDistFlow model [9] to multi-microgrid settings.

We distinguish between two operating stages o and c, which denote the pre- and post- contingency stage, respectively. The network is initially in o stage, and after the disturbance event enters the c stage; see Sec. IV for details on the disturbance model. Let $\eta \in \{o, c\}$ denote the operating stage of the network. We define the network state as $x^\eta := (p^\eta, q^\eta, P^\eta, Q^\eta, v^\eta, f^\eta)^\top$, where each of these entries are themselves vectors of appropriate dimensions, and are described in Table I.

In our DN model, we consider a radial network consisting of one or more microgrids. We refer to a distribution line $(i,j) \in \mathcal{M} \subseteq \mathcal{E}$ as a microgrid *connecting line* if it connects a microgrid to the TN or to other microgrids; see Fig. 2. Here $\mathcal{M}$ denotes a given fixed set of connecting lines. For a connecting line $(i,j) \in \mathcal{M}$, we use $kl^\eta_{ij} = 0$ (resp. $kl^\eta_{ij} = 1$) to indicate that it is in the closed (resp. open) state. The DN operating regimes are defined according to the states of the connecting lines:

- *Grid-connected regime* when all connecting lines are closed (i.e $kl^\eta_{ij} = 0 \quad \forall \ (i,j) \in \mathcal{M}$),
- *Fully-islanded regime* when all connecting lines are open (i.e. $kl^\eta_{ij} = 1 \quad \forall \ (i,j) \in \mathcal{M}$), or
- *Partially-islanded regime* when there exists at least two connecting lines such that one of them is closed and the other is open (i.e. $\exists \ (i,j), (m,n) \in \mathcal{M}$ such that $kl^\eta_{ij} = 0$ and $kl^\eta_{mn} = 1$).

Let $\{\mathcal{N}_1, \cdots, \mathcal{N}_{|\mathcal{M}|}\}$ denote the set of disjoint microgrid subnetworks of the DN, where each $\mathcal{N}_i$ for $i \in \{1, \cdots, |\mathcal{M}|\}$ denotes a connected subnetwork when all connecting lines are open, i.e. $kl^\eta_{mn} = 1$ for all $(m, n) \in \mathcal{M}$. For each subnetwork $\mathcal{N}_i$, let $\mathcal{M}_i \subseteq \mathcal{M}$ denote the set of connecting lines which need to be open for $\mathcal{N}_i$ to be completely isolated (i.e. autonomously operating). A *microgrid island* is formed when an individual microgrid or a connected subnetwork of more than one microgrid no longer receives power supply from the TN. Also, let $\mathcal{P}_i$ denote the set of lines along the path connecting node i to the substation node. For example, in Fig. 2 the set of connecting lines for the subnetwork $\mathcal{N}_1 = \{1, 2\}$ is $\mathcal{M}_1 = \{(0,1), (2,3), (2,5)\}$. For this example, $\mathcal{P}_5 = \{(0,1), (1,2), (2,5)\}$. Also, if $kl^\eta_{01} = 1$, $kl^\eta_{23} = 0$, and $kl^\eta_{25} = 1$, then the microgrid $\mathcal{N}_3$ is operating as an isolated island, whereas microgrids $\mathcal{N}_1$ and $\mathcal{N}_2$ are operating together as part of one larger microgrid island.

Remark 1. The smaller microgrids are typically used for supplying power to a critical facility (e.g. hospital, university, prison). In our model, these microgrids can be

DN parameters

$\mathcal{N}$	set of nodes in DN
$\mathcal{E}$	set of edges in DN
0	substation node label
$\mathcal{M} \subseteq \mathcal{E}$	set of microgrid connecting lines
$\mathcal{N}_i \subseteq \mathcal{N}$	nodes belonging to i^{th} microgrid
$\mathcal{M}_i \subseteq \mathcal{M}$	set of lines which if open isolate the ith microgrid
$\mathbf{j}$	complex square root of -1, $\mathbf{j} = \sqrt{-1}$
$\mathbf{v^{nom}}$	nominal squared voltage magnitude (1 pu)
$\mathbf{f^{nom}}$	nominal system frequency (1 pu)
$\mathcal{P}_i \subseteq \mathcal{E}$	lines on the path between node i and substation node

DER categories

$\mathcal{S}$	set of DERs
$\mathcal{S}_{gf} \subseteq \mathcal{S}$	set of grid-forming DERs
$\mathcal{S} \subseteq \mathcal{S}_{gf}$	set of PQ Inverter (PQI)-controlled DERs
$\mathcal{S}_{pq}^{fixed} \subseteq \mathcal{S}_{pq}$	set of PQI-controlled DERs with fixed setpoints
$\mathcal{S}_{pq}^{var} \subset \mathcal{S}_{pq}$	set of PQI-controlled DERs with controllable setpoints
$\mathcal{S}_{gf}^{utility} \subseteq \mathcal{S}_{gf}$	set of utility-owned grid-forming DERs
$\mathcal{S}_{gf}^{facility} \subseteq \mathcal{S}_{gf}$	set of facility level microgrid-specific grid-forming DERs
$\mathcal{S}_{gi} = \mathcal{S}_{gf} \bigcup \mathcal{S}_{pq}^{var}$	set of grid-interactive DERs

Nodal quantities of node $i \in \mathcal{N}$

v_i	squared voltage magnitude at node i
f_i	system frequency measured at node i
$\underline{vc}_i, \overline{vc}_i$	lower, upper voltage bounds for load i
$\underline{vg}_i, \overline{vg}_i$	lower, upper voltage bounds for DG i
$\underline{fc}_i, \overline{fc}_i$	lower, upper frequency bounds for load i
$\underline{fg}_i, \overline{fg}_i$	lower, upper frequency bounds for DG i
$\overline{pc}_i + \mathbf{j}\overline{qc}_i$	nominal demand at node i
$pc_i + \mathbf{j}qc_i$	actual power consumed at node i
$kc_i \in \{0, 1\}$	0 if load 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
$\overline{pg}_i + \mathbf{j}\overline{qg}_i$	nominal generation of DG $i \in \mathcal{S}_{pq}^{fixed}$
$pg_i + \mathbf{j}qg_i$	actual power generated by DG $i \in \mathcal{S}_{pq}^{fixed}$
$kg_i \in \{0, 1\}$	0 if DG $i \in \mathcal{S}_{pq}^{fixed}$ is connected to DN; 1 otherwise

Quantities of DER $s \in \mathcal{S}$

$j(s)$	the DN node where the DER $s \in \mathcal{S}_{gf}$ is located
$J(S) \subseteq \mathcal{N}$	the set of DN nodes where the DERs in the set $S \subseteq \mathcal{S}$ are located
$\underline{pn}_s, \overline{pn}_s$	lower, upper active power bounds of microsource $s \in \mathcal{S}_{gf}$
$\underline{qn}_s, \overline{qn}_s$	lower, upper reactive power bounds of microsource $s \in \mathcal{S}_{gf}$
$pn_s + \mathbf{j}qn_s$	total power supplied by microsource $s \in \mathcal{S}_{gf}$
$\underline{pe}_s, \overline{pe}_s$	lower, upper active power bounds of storage $s \in \mathcal{S}_{gf}$
$\underline{qe}_s, \overline{qe}_s$	lower, upper reactive power bounds of storage $s \in \mathcal{S}_{gf}$
$pe_s + \mathbf{j}qe_s$	total power supplied by storage $s \in \mathcal{S}_{gf}$
$kr_s \in \{0, 1\}$	1 if DER $s \in \mathcal{S}_{gf}$ contributes to grid-forming services
$pr_s + \mathbf{j}qr_s$	total power supplied by DER $s \in \mathcal{S}_{gf}$
$\mathbf{pr}_s^{ref}, \mathbf{qr}_s^{ref}$	active, reactive power references of DER $s \in \mathcal{S}_{gf}$
$\mathbf{f}_s^{ref}, \mathbf{v}_s^{ref}$	frequence, voltage references of DER $s \in \mathcal{S}_{gf}$

Parameters of edge $(i,j) \in \mathcal{E}$

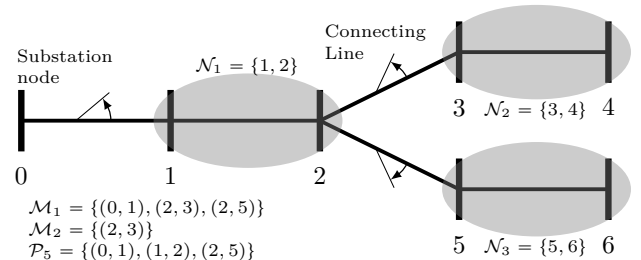|	
$kl_{ij} \in \{0, 1\}$	1 if (i,j) is switched open; 0 otherwise
$P_{ij} + \mathbf{j}Q_{ij}$	power flowing from node i to node j
$\mathbf{r}_{ij}, \mathbf{x}_{ij}$	resistance and reactance of line $(i,j) \in \mathcal{E}$

TABLE I: Table of Notation.

Fig. 2: Multi-microgrid DN model.

leveraged to supply power to the DN during emergency conditions (fully- or partially-islanded regimes).

Now, we describe the constraints related to the power flows, nodal frequencies and load connectivity in microgrids. Unless explicitly stated, the following constraints are valid for either operating stage $\eta \in \{o, c\}$.

1) *Power flows:* A connecting line permits power flow through it if and only if it is *closed*. We model this constraint as follows:

$$\left| P_{ij}^{\eta} \right| \leqslant \left(1 - kl_{ij}^{\eta} \right) \mathbf{M} \qquad \forall \, (i,j) \in \mathcal{M} \tag{1a}$$

$$\left| Q_{ij}^{\eta} \right| \leqslant \left(1 - kl_{ij}^{\eta} \right) \mathbf{M} \qquad \forall \, (i,j) \in \mathcal{M}, \tag{1b}$$

where $\mathbf{M}$ is a large constant. This typical modeling trick to use a constraint of the type $|a - c| \leqslant y\mathbf{M}$ where $y \in \{0, 1\}$, enforces an equality $a = c$ only when $y = 0$; otherwise the equality is not binding. We use this trick repeatedly to model various other constraints of a similar type.

2) *Voltage drop:* The voltage drop along a non-connecting line $(i,j) \notin \mathcal{M}$ is given by the standard voltage drop equation of the LinDistFlow model [9]:

$$\mathrm{v}_j^{\eta} = \mathrm{v}_i^{\eta} - 2\mathbf{r}_{ij} P_{ij}^{\eta} - 2\mathbf{x}_{ij} Q_{ij}^{\eta} \quad \forall \, (i,j) \in \mathcal{E} \backslash \mathcal{M}. \tag{2}$$

However, for a connecting line, the voltage drop constraint is active only if it is closed, and is inactive, otherwise, i.e.

$$\left| \mathrm{v}_j^{\eta} - \left(\mathrm{v}_i^{\eta} - 2\mathbf{r}_{ij} P_{ij}^{\eta} - 2\mathbf{x}_{ij} Q_{ij}^{\eta} \right) \right| \leqslant kl_{ij}^{\eta} \mathbf{M} \quad \forall \, (i,j) \in \mathcal{M}. \tag{3}$$

3) *Nodal frequencies:* In islanded regimes, the DER(s) must provide grid-forming and regulation services [5, 10]. Moreover, a microgrid island can have multiple DERs operating in parallel. We assume that DERs can rapidly synchronize their frequencies to a common value with the help of power electronics [5]. This value can be regarded as the island's frequency. To model that the nodal frequencies within a microgrid island are identical in steady state, we can write:

$$f_i^{\eta} = f_j^{\eta} \quad \forall \, i, j \in \mathcal{N}_k \text{ and } \forall \, k = 1, \cdots, |\mathcal{M}|,$$

which is equivalent to writing:

$$f_i^{\eta} = f_j^{\eta} \qquad \forall \, (i,j) \in \mathcal{E} \backslash \mathcal{M}, \tag{4}$$

because if a line (i,j) is not a connecting line, i.e. $(i,j) \in \mathcal{E} \backslash \mathcal{M}$, then nodes i and j both belong to the same microgrid. Generically, frequency of every microgrid island can be different from the frequency of the TN-connected substation node. Moreover, the frequencies of any two microgrid islands that are not connected to each other can also be different. We model this constraint as follows:

$$\left| f_i^{\eta} - f_j^{\eta} \right| \leqslant kl_{ij}^{\eta} \mathbf{M} \qquad \forall \, (i,j) \in \mathcal{M}. \tag{5}$$

Finally, we model the constraint that the load gets disconnected (i.e. $kc_i^{\eta} = 1$) when the nodal frequency violates the safe operating bounds:

$$kc_i^{\eta} \geqslant \underline{\mathbf{fc}}_i - f_i^{\eta}, \qquad kc_i^{\eta} \geqslant f_i^{\eta} - \overline{\mathbf{fc}}_i \qquad \forall \, i \in \mathcal{N}. \tag{6}$$

III. DISTRIBUTED ENERGY RESOURCES (DERs)

We now introduce a generic taxonomy of DERs that is relevant to microgrid operations (see [11]) and a model which captures both single- and multi-master operating modes of DERs. Refer to Fig. 3 for DER categories and Table II for a comparison of their capabilities.
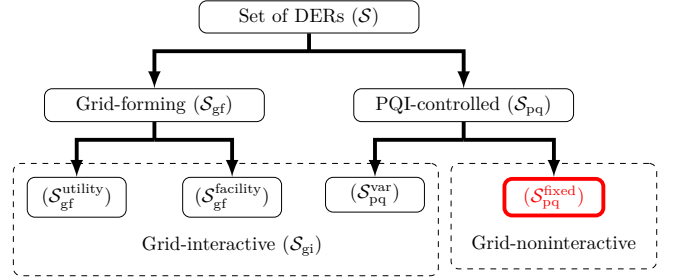

Fig. 3: Basic taxonomy of DERs [11].

Attribute	Grid-noninteractive ($\mathcal{S}_{\mathrm{pq}}^{\mathrm{fixed}}$)	Grid-interactive ($\mathcal{S}_{\mathrm{gi}} = \mathcal{S}_{\mathrm{gf}} \bigcup \mathcal{S}_{\mathrm{pq}}^{\mathrm{var}}$)
Power output	fixed	variable/responsive to grid conditions
Controllable by response (a)	yes (remote set-point control)	no (can act as zero output source while being connected)
Controllable by response (b)	yes (due to operating bound violations)	no (LVRT & LFRT available)
Controllable by response (c)	yes	N/A
Controllable by response (d)	yes	yes

(a) Grid-interactive vs. grid-noninteractive DERs.

Attribute	PQI-controlled DERs with variable setpoints ($\mathcal{S}_{\mathrm{pq}}^{\mathrm{var}}$)	Grid-forming ($\mathcal{S}_{\mathrm{gf}}$)
Grid-forming	no	yes (under specific islanding conditions)
Output control	Remote setpoint control	Droop-based control

(b) PQI-controlled vs. grid-forming DERs.

Attribute	Utility-owned ($\mathcal{S}_{\mathrm{gf}}^{\mathrm{utility}}$)	Facility level ($\mathcal{S}_{\mathrm{gf}}^{\mathrm{facility}}$)
Ownership	Utility	Facility
Islanding condition	microgrid not connected to TN but can stay connected to other microgrid(s) (explained later in (7))	microgrid operates as an isolated island (explained later in (8))

(c) Utility (operator) owned grid-forming DERs vs. facility level grid-forming DERs.

TABLE II: Comparison of DER categories.

DER classification: Our classification is based on the output behaviour and service capabilities of DERs. First, we distinguish between grid-forming DERs (which provide voltage and frequency references) and DERs whose active (P) and reactive (Q) power output is controlled by PQ inverters. We denote the sets of grid-forming and PQ Inverter (PQI-) controlled DERs by $\mathcal{S}_{\mathrm{gf}}$ and $\mathcal{S}_{\mathrm{pq}}$, respectively. Then, there are a further two sub-categories of PQI-controlled DERs: those whose PQ setpoints can be remotely controlled (denoted by $\mathcal{S}_{\mathrm{pq}}^{\mathrm{var}}$), and others whose PQ setpoints are fixed (denoted by $\mathcal{S}_{\mathrm{pq}}^{\mathrm{fixed}}$). Since the

output of the DERs belonging to the set $\mathcal{S}_{\text{pq}}^{\text{fixed}}$ does not vary with the grid conditions, they can be considered as grid-noninteractive DERs. On the other hand, since the output of the DERs in the sets $\mathcal{S}_{\text{gf}}$ and $\mathcal{S}_{\text{pq}}^{\text{var}}$ can change with grid-conditions, we consider them as grid-interactive DERs (denoted by $\mathcal{S}_{\text{gi}}$); see Table IIa. In order to distinguish the DERs in set $\mathcal{S}_{\text{pq}}^{\text{fixed}}$, we refer to them as distributed generators (DGs). Since the output of these DGs cannot be changed, if operating bound violations occur, then they need to be disconnected either by remote means or through autonomous disconnections.

In contrast, the grid-interactive DERs can stay connected to the DN as zero output sources even under fluctuations in the network state. Particularly, we assume that these DERs are fitted with low-voltage and low-frequency ride through (LVRT and LFRT) functionalities. This allows DERs to stay connected to the DN during temporary voltage and frequency bound violations at nodes. Furthermore, the output of grid-interactive DERs can be changed by two control mechanisms. In the case of grid-forming DERs ($\mathcal{S}_{\text{gf}}$), droop-based primary control is activated under specific islanding conditions. In the case of DERs in the set $\mathcal{S}_{\text{pq}}^{\text{var}}$, their active-reactive (PQ) setpoints can be controlled by the SA system; see Table IIb.

Let $\mathcal{N}_{\mathcal{I}} \subseteq N$ denote a microgrid island within the DN. Also, let $J(S)$ be the set of DN nodes where DERs in the set $S \subseteq \mathcal{S}$ are located, with $j(s) = i$ indicating that DER s is connected to node i. Recall from Sec. II that a microgrid island can consist of one or more microgrids. Based on the number of DERs contributing to grid-forming services, a microgrid island can be in the following operating modes [5]:

1) Single-Master Operation (SMO): One DER operates as a single grid-forming DER (i.e. $|J(\mathcal{S}_{\text{gf}}) \bigcap \mathcal{N}_{\mathcal{I}}| = 1$), while all other DERs operate in the PQ mode.
2) Multi-Master Operation (MMO): More than one DER (but not necessarily all) operate as grid-forming DERs (i.e. $|J(\mathcal{S}_{\text{gf}}) \bigcap \mathcal{N}_{\mathcal{I}}| \geqslant 2$).

In multi-master operation, the output of multiple grid-forming DERs changes based on nodal voltage and frequency values under the droop control constraints. These constraints ensure appropriate power sharing among DERs based on their capacities. The nodal frequencies (resp. voltages) are used for active (resp. reactive) power sharing. Our network model for radial DNs is sufficiently flexible to allow DN operations in both SMO and MMO modes.

Finally, there are two sub-categories of grid-forming DERs, namely utility (or operator) owned grid-forming DERs and grid-forming DERs belonging to some facilities such as hospitals or other high priority loads. Each of these categories contributes to grid-forming services depending on the specific islanding conditions; see Table IIc. Let $kr_s^{\eta} = 1$ if the islanding condition for DER $s \in \mathcal{S}_{\text{gf}}$ is satisfied, and $kr_s^{\eta} = 0$ otherwise. The two main islanding conditions of interest are as follows:

1) A utility grid-forming DER contributes to grid-forming services when the node to which it belongs becomes a part of a microgrid island (i.e. the node is not connected to the TN). Consider a DER $s \in \mathcal{S}_{\text{gf}}^{\text{utility}}$ and a microgrid $\mathcal{N}_k$ such that $j(s) = i \in \mathcal{N}_k$. Then, DER s contributes to grid-forming if and only if $\mathcal{N}_k$ is not connected to the TN, or equivalently, at least one connecting line along the path connecting node i to the substation is open, i.e.

$$kr_s^{\eta} = 1 \iff \exists \, (m,n) \in \mathcal{M}\bigcap\mathcal{P}_i \text{ such that } kl_{mn}^{\eta} = 1.$$

We formulate this condition using the following mixed-integer linear constraints:

$$kr_s^{\eta} \geqslant kl_{mn}^{\eta} \qquad \forall \, (m,n) \in \mathcal{M}\bigcap\mathcal{P}_i \qquad (7a)$$

$$kr_s^{\eta} \leqslant \sum_{(m,n)\in(\mathcal{M}\bigcap\mathcal{P}_i)} kl_{mn}^{\eta}. \qquad (7b)$$

2) The facility level DERs (denoted by $\mathcal{S}_{\text{gf}}^{\text{facility}}$) also contribute to grid-forming services when the microgrid to which they belong operates as an isolated island (i.e. not connected to the TN nor to any other microgrid). Consider a DER $s \in \mathcal{S}_{\text{gf}}^{\text{facility}}$ and a microgrid $\mathcal{N}_i$ such that $j(s) \in \mathcal{N}_i$. Then, DER s contributes to grid-forming if and only if all the connecting lines connecting the microgrid $\mathcal{N}_i$ to the TN and other microgrids are open, i.e.

$$kr_s^{\eta} = 1 \iff kl_{mn}^{\eta} = 1 \, \forall \, (m,n) \in \mathcal{M}_i.$$

We formulate this condition using the following mixed-integer linear constraints:

$$kr_s^{\eta} \geqslant \left(\sum_{(m,n)\in\mathcal{M}_i} kl_{mn}^{\eta} \right) - (|\mathcal{M}_i| - 1) \qquad (8a)$$

$$kr_s^{\eta} \leqslant kl_{mn}^{\eta} \qquad \forall \, (m,n) \in \mathcal{M}_i. \qquad (8b)$$

DER output model: Next, we describe the output model for the DERs. Each grid-forming DER $s \in \mathcal{S}_{\text{gf}}$ consists of a microsource and a storage device (batteries or flywheels) [5]. The microsource supplies active power (quadrants I or II) in all three regimes. Thus, the output of the microsource is constrained as follows:

$$Gn_s[pn_s^{\eta} \quad qn_s^{\eta}]^{\top} \leqslant hn_s \quad \forall \, s \in \mathcal{S}_{\text{gf}}, \qquad (9)$$

where $Gn_s \in \mathbb{R}^{6\times 2}$ is a matrix and $hn_s \in \mathbb{R}^6$ is a vector that represents the polytope as shown in Fig. 4a.

For the sake of modeling simplicity, we assume that the storage device supplies active power only in the islanded regimes, whereas it consumes active power in the grid-connected regime (quadrants III and IV); see Fig. 4. One justification for this restriction is that the life of a storage device significantly degrades with frequent charging/discharging cycles [5]. Indeed, advances in storage technology make them viable sources of power supply even in the grid-connected regime. Still our modeling assumption is relevant to situations where fixed storage capacity is set aside as contingency reserve to be used in islanded regimes. Thus, the output of a storage device is constrained as follows:

$$Ge_s[pe_s^{\eta} \quad qe_s^{\eta}]^{\top} + H_s kr_s^{\eta} \leqslant he_s \quad \forall \, s \in \mathcal{S}_{\text{gf}}, \qquad (10)$$

where the $Ge_s, H_s \in \mathbb{R}^{8 \times 2}$ are matrices and $he_s \in \mathbb{R}^8$ is a vector such that the DER operates in quadrants III and IV when $kr_s^\eta = 0$; and in quadrants I and II when $kr_s^\eta = 1$; see Fig. 4b.

The total output of the DER is given by:

$$\begin{aligned} pr_s^\eta &= pn_s^\eta + pe_s^\eta && \forall \ s \in \mathcal{S}_{\mathrm{gf}} \\ qr_s^\eta &= qn_s^\eta + qe_s^\eta && \forall \ s \in \mathcal{S}_{\mathrm{gf}}. \end{aligned} \qquad (11)$$

On the other hand, PQI-controlled DERs $(\mathcal{S}_{\mathrm{pq}})$ consist only of a microsource, and do not have a storage device. Thus, their output is constrained as in Fig. 4a. We can simply assume that $\forall \ s \in \mathcal{S}_{\mathrm{pq}}, \ pe_s^\eta = qe_s^\eta = 0$.
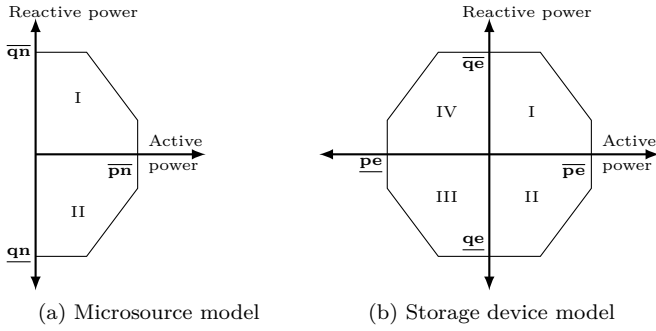

(a) Microsource model (b) Storage device model

Fig. 4: DER output model [12].

Droop control equations: We model the regulation services provided by one or more grid-forming DERs using voltage and frequency droop control equations [10]. This allows the DERs to adjust their active and reactive power outputs based on local voltage and frequency measurements, thus eliminating the need for explicit coordination among DERs (for the purpose of regulation).

The output changes of a grid-forming DER $s \in \mathcal{S}_{\mathrm{gf}}$ depend on whether or not it is contributing to regulation (i.e. $kr_s^\eta = 1$ or 0) based on the islanding conditions (see (7) and (8)). Then, the classical voltage droop equation [10] can be refined to model the reactive power output of a grid-forming DER as follows (see Fig. 5a):

$$\left| v_i^\eta - \left(\mathbf{v}_s^{\mathrm{ref}} - \mathbf{mq}_s(qr_s^\eta - \mathbf{qr}_s^{\mathrm{ref}}) \right) \right| \leqslant (1 - kr_s^\eta)\mathbf{M}$$
$$\forall \ s \in \mathcal{S}_{\mathrm{gf}}, i \in \mathcal{N} \ \text{ and } \ i = j(s). \qquad (12)$$

Eq. (12) implies that when a DER provides regulation, it contributes more (resp. less) reactive power as the voltage drops (resp. rises) relative to a reference value.

Similarly, the classical frequency droop control equation [10] can be refined to model the active power output of a grid-forming DER as follows (see Fig. 5b):

$$\left| f_i^\eta - \left(\mathbf{f}_s^{\mathrm{ref}} - \mathbf{mp}_s \left(pr_s^\eta - \mathbf{pr}_s^{\mathrm{ref}} \right) \right) \right| \leqslant (1 - kr_s^\eta)\mathbf{M}$$
$$\forall \ s \in \mathcal{S}_{\mathrm{gf}}, i \in \mathcal{N} \ \text{ and } \ i = j(s). \qquad (13)$$

Eq. (13) ensures proper power sharing in the sense that DERs can adjust their active power contributions for frequency regulation depending on their individual capacities. The reference setpoints $(\mathbf{f}_s^{\mathrm{ref}}, \mathbf{v}_s^{\mathrm{ref}}, \mathbf{pr}_s^{\mathrm{ref}}, \mathbf{qr}_s^{\mathrm{ref}})$ and the

droop coefficients $(\mathbf{mp}_s, \mathbf{mq}_s)$ are given constants.[1]

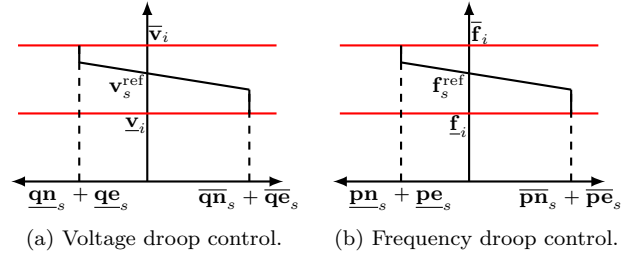(a) Voltage droop control. (b) Frequency droop control.

Fig. 5: Droop control model [10].

As in [1], we assume that each node has a DG (i.e. a grid-noninteractive DER) without loss of generality. Then, similar to the loads, we model the dependence of DG connectivity on the nodal voltage and frequency as follows:

$$kg_i^\eta \geqslant \underline{\mathbf{vg}}_i - v_i^\eta, \quad kg_i^\eta \geqslant v_i^\eta - \overline{\mathbf{vg}}_i \quad \forall \ i \in \mathcal{N}, \qquad (14)$$
$$kg_i^\eta \geqslant \underline{\mathbf{fg}}_i - f_i^\eta, \quad kg_i^\eta \geqslant f_i^\eta - \overline{\mathbf{fg}}_i \quad \forall \ i \in \mathcal{N}. \qquad (15)$$

Eqs. (14)-(15) imply that a DG will disconnect if the corresponding nodal voltage or frequency violates safe operating bounds.

The net power consumed at a node i is the power consumed by the load minus the power generated by the DGs and other grid-interactive DERs at that node, i.e.

$$p_i^\eta = pc_i^\eta - pg_i^\eta - \sum_{s \in \mathcal{S}_{\mathrm{gi}}|j(s)=i} pr_s^\eta \qquad \forall \ i \in \mathcal{N} \quad (16a)$$
$$q_i^\eta = qc_i^\eta - qg_i^\eta - \sum_{s \in \mathcal{S}_{\mathrm{gi}}|j(s)=i} qr_s^\eta \qquad \forall \ i \in \mathcal{N}. \quad (16b)$$

Finally, we summarize the LinDistFlow and connectivity constraints described in [1] as follows:

$$P_{ij}^\eta = \sum_{k:(j,k)\in\mathcal{E}} P_{jk}^\eta + p_j^\eta \qquad \forall \ (i,j) \in \mathcal{E} \qquad (17)$$

$$Q_{ij}^\eta = \sum_{k:(j,k)\in\mathcal{E}} Q_{jk}^\eta + q_j^\eta \qquad \forall \ (i,j) \in \mathcal{E} \qquad (18)$$

$$pg_i^\eta = (1 - kg_i^\eta)\overline{\mathbf{pg}}_i \qquad \forall \ i \in \mathcal{N} \qquad (19)$$

$$qg_i^\eta = (1 - kg_i^\eta)\overline{\mathbf{qg}}_i \qquad \forall \ i \in \mathcal{N} \qquad (20)$$

$$pc_i^\eta = \beta_i^\eta \overline{\mathbf{pc}}_i, \quad qc_i^\eta = \beta_i^\eta \overline{\mathbf{qc}}_i \qquad \forall \ i \in \mathcal{N} \qquad (21)$$

$$(1 - kc_i^\eta)\underline{\beta}_i \leqslant \beta_i^\eta \leqslant (1 - kc_i^\eta) \quad \forall \ i \in \mathcal{N} \qquad (22)$$

$$kc_i^\eta \geqslant \underline{\mathbf{vc}}_i - v_i^\eta, \quad kc_i^\eta \geqslant v_i^\eta - \overline{\mathbf{vc}}_i \forall \ i \in \mathcal{N}. \qquad (23)$$

This completes the discussion of our multi-regime microgrid network model with parallel operation of DERs.

IV. Bilevel Optimization Problem

In [1], we modeled the sequential interaction between the attacker and operator as a bilevel mixed-integer problem (BiMIP). We now extend this model to include microgrid operations and DER dispatch capabilities. Our revised BiMIP formulation considers multi-regime microgrid

---

[1]The secondary control of voltage and frequency regulation could change the reference setpoints of the DERs, namely the voltage, frequency, active and reactive power setpoints [13]. Secondary control may also include changing the droop coefficients of the DERs [14]. However, for the sake of simplicity, we consider primary (but not secondary) control in this paper.

operations with multiple DERs/DGs. It also accounts for TN-side voltage and frequency disturbances as part of the overall disturbance model.

TN-side disruption: We consider TN-side disturbance in our attack model because the DN can face significant loss if the attacker targets the DN during an active TN failure event. In general, a TN-side disturbance (e.g. failure of a transmission line or bulk generator) can impact the system frequency as well as the substation voltage of the DN, and this can influence the attacker's strategy. We model the impact of a TN-side failure as a perturbation in the substation voltage and frequency, denoted Δv_0 and Δf_0, respectively. Then, the voltage and frequency at the substation node in the post-contingency stage can be written:

$$v_0^c = \mathbf{v^{nom}} - \Delta v_0, \tag{24}$$
$$f_0^c = \mathbf{f^{nom}} - \Delta f_0. \tag{25}$$

DN-side disruption: For the sake of consistency, we consider the same model of DN-side disruption as in [1], i.e. an attacker-induced compromise of the DG management system (DGMS) results in simultaneous disruption of multiple DGs. We model this attack as follows:

$$kg_i^c \geqslant d_i \quad \forall \quad i \in \mathcal{N}. \tag{26}$$

Let k denote the maximum number of DGs that the attacker can disrupt. Then, the set of all possible attacker strategies, denoted $\mathcal{D}_k^m$, is given by

$$\mathcal{D}_k^m = \{d \in \{0,1\}^{\mathcal{N}} \mid \textstyle\sum_{i \in \mathcal{N}} d_i \leqslant k\}.$$

Unlike DGs (set $\mathcal{S}_{pq}^{fixed}$), the output of grid-interactive DERs (set $\mathcal{S}_{gi}$) changes depending on the grid conditions. In particular, the DER output either changes autonomously based on the droop control equations, or the DERs are explicitly coordinated by the SA. The DERs are not vulnerable under our assumed disruption model because they are not affected by the compromised DGMS.

Note that the above-mentioned disruption model can be extended to other types of attacks, including disruption of loads or circuit breakers. One can model such attacks as follows:

$$kc_i^c \geqslant dc_i \qquad \forall \; i \in \mathcal{N}$$
$$kl_{ij}^c \geqslant dl_{ij} \qquad \forall \; (i,j) \in \mathcal{E},$$

where $dc \in \{0,1\}^{\mathcal{N}}$ and $dl \in \{0,1\}^{\mathcal{E}}$ denote the corresponding attacks for loads and DN lines, respectively. Thus, despite its simplicity, our approach to modeling DN-side disruptions can be applied to capture the physical impact of a broad class of security failure scenarios. This class includes Distributed Denial-of-Service (DDoS) attacks on the power grid components that can result in simultaneous failures [15, 16, 17]. Another relevant attack scenario is motivated by the vulnerabilities of Internet connected customer-side devices (e.g. smart inverters, air conditioners, water heaters), also known as Internet-of-Things (IoT) devices [15]. An adversary can hack into these components

via a cyberattack, create an IoT botnet, and can access them via the internet. Indeed, recent work in cybersecurity of power systems has identified risk of correlated failures (e.g. simultaneous on/off events) induced/caused by IoT botnets [16]. In our disruption model, the impact of such an attack can be straightforwardly modeled by load/DG/line disconnects, leading to a sudden supply-demand disturbance. However, a single point of failure such as a cyberattack on the DGMS is perhaps a more critical threat to DNs with significant penetration of DGs.

Remark 2. Another attack model that is well-studied in the literature considers false-data injection attacks to a (small) subset of sensors in order to inject biases in state estimates, while being undetected by anamoly detectors [18, 19, 20]. Available results include identification and security of "critical" sensors and attack-resilient state estimation. However, a less commonly studied aspect is that of incorrect control actions that could be implemented as a result of biased state estimation. Based on our previous work [21], one can argue that our disruption model can be tailored to capture the changes in supply/demand of network nodes due to disruption of DGs/loads and/or component disconnect actions that may be induced by successful false-data injection attacks on sensor data used by the control center.

Remark 3. Our disruption model can be extended to the compromise of grid-interactive DERs as well; see, for example, [22] in which DERs in $\mathcal{S}_{pq}^{var}$ are compromised by setpoint manipulation.

Operator response model: Recall the response capabilities (a), (b), (c) and (d) from Sec. I. Since our attack model is concerned with compromised DGMS, we rule out response (a) as an operator response. We considered (b) and (c) in [1]; see Fig. 1. Our underlying assumption is that (c) is not prone to cyberattacks, because distribution utilities are being regulated under NERC CIP standards [23], which provide specific guidelines for secure *reperimeterisation* of the substation cyber infrastructure. We consider the response (d) to be executed by the SA, and thus assume that it is also secure.

The responses (b) and (c) do not consider grid-interactive DERs nor microgrid islanding capabilities. In contrast, (d) utilizes both these capabilities, in addition to load control and preemptive disconnection of components. Particularly, we model the operator response (d) as follows: $u := (kl, kr, pr, qr, \beta, kc, kg)$. Then, the set of all response strategies, denoted $\mathcal{U}_m$, can be defined as $\mathcal{U}_m := \{0,1\}^{\mathcal{M}} \times \{0,1\}^{\mathcal{S}_{gf}} \times (\mathbb{R} \times \mathbb{R})^{\mathcal{S}_{gi}} \times \mathcal{B} \times \{0,1\}^{\mathcal{N}} \times \{0,1\}^{\mathcal{N}}$. Moreover, given the attacker-induced disruption d, let the set $\mathcal{U}_m(d) := \{u \in \mathcal{U}_m \mid (26) \text{ holds}\}$ denote the set of feasible response strategies available to the operator after the disruption.

For the sake of simplicity, we consider that in the pre-contingency stage, the DN is in the grid-connected regime and all components are connected. That is, there are no microgrid islands ($kl^o = \mathbf{0}$), and all the loads and DGs are connected to the DN ($kc^o = \mathbf{0}$ and $kg^o = \mathbf{0}$).

Consequently, the grid-forming DERs are not contributing to regulation in the pre-contingency stage o, i.e. $kr_s^o = 0$ for all $s \in \mathcal{S}$. We also assume the output of the grid-interactive DERs in mode o to be zero, i.e. $pr_s^o = qr_s^o = 0$ for all $s \in \mathcal{S}_{\mathrm{gi}}$. These are not restrictive assumptions, however they allow us to straightforwardly compare the effectiveness of each of the response (b), (c) and (d).

Post-contingency costs: The post-contingency loss incurred by the operator, denoted L_{m}, is the sum of the following costs: (i) cost due to loss of voltage and frequency regulation, (ii) cost of load control, (iii) cost of load shedding, and (iv) cost of islanding:

$$
\begin{aligned}
L_{\mathrm{m}} =&\, W_{\mathrm{VR}} \|\mathbf{v^{nom}} - v\|_\infty + W_{\mathrm{FR}} \|\mathbf{f^{nom}} - f\|_\infty \\
&+ W_{\mathrm{LC}} \sum_{i \in \mathcal{N}} (1 - \beta_i) \overline{\mathbf{pc}}_i \\
&+ (W_{\mathrm{LS}} - W_{\mathrm{LC}}) \sum_{i \in \mathcal{N}} kc_i \overline{\mathbf{pc}}_i \\
&+ W_{\mathrm{MG}} \sum_{(i,j) \in \mathcal{M}} kl_{ij},
\end{aligned}
\tag{27}
$$

where $W_{\mathrm{LC}} \in \mathbb{R}_+$ denotes the cost of per unit load control, $W_{\mathrm{LS}} \in \mathbb{R}_+$ and $W_{\mathrm{LS}} \geqslant W_{\mathrm{LC}}$ is the cost of per unit load shed, W_{MG} is the cost of a single islanding control action, $W_{\mathrm{VR}} \in \mathbb{R}_+$ is the cost of the largest deviation of nodal voltage from the nominal value $\mathbf{v^{nom}} = 1$ pu, and W_{FR} is the cost of the largest deviation of nodal frequency from the nominal value $\mathbf{f^{nom}} = 1$ pu.

For a given operator response $u \in \mathcal{U}_{\mathrm{m}}$, let $\mathcal{X}_{\mathrm{m}}(u)$ denote the set of post-contingency states x that satisfy the constraints (1)-(25). Then, we can restate our bilevel formulation (P2) as:

$$
\begin{aligned}
\mathcal{L}_{\mathrm{MG}} := \max_{d \in \mathcal{D}_{\mathrm{k}}^{\mathrm{m}}} \min_{u \in \mathcal{U}_{\mathrm{m}}(d)}\; & L_{\mathrm{m}}(u, x^c) \\
\text{s.t. } & x^c \in \mathcal{X}_{\mathrm{m}}(u).
\end{aligned}
\tag{P-MG}
$$

Since (P-MG) is a BiMIP with the same mathematical structure as the BiMIP in [1], we solve it using the Benders Decomposition algorithm that we developed in [1].

V. COMPUTATIONAL STUDY

Now, we present computational results to: (i) compare the output value of our BD algorithm with the optimal value (generated for small networks by simple enumeration); (ii) compare the DN resilience under response capabilities (b), (c) and (d); and (iii) show the scalability of our approach to realistically large DN network sizes $N \in \{24, 36, 118\}$.

Setup for computational study: We consider three networks: modified IEEE 24-, 36-, and 118-node networks; see Fig. 10 in the Appendix. The set of connecting lines $\mathcal{M}$ are shown with thick edges. The individual microgrid networks $\mathcal{N}_1, \cdots, \mathcal{N}_{|\mathcal{M}|}$ can be obtained by setting $kl_{ij} = 1 \;\forall\; (i,j) \in \mathcal{M}$. Each line $(i,j) \in \mathcal{E}$ has an identical impedance of $\mathbf{r}_{ij} = 0.01, \mathbf{x}_{ij} = 0.02$. Half of the nodes have a DG each and half have a load each. Consider a parameter $\alpha = \frac{6}{N}$. Before the contingency, each DG has active power output of $\overline{\mathbf{pg}}_i = \alpha$, and each load has a demand of $\overline{\mathbf{pc}}_i = 1.25\alpha$. 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 $W_{\mathrm{LC}} = 100/\overline{\mathbf{pc}}_i, W_{\mathrm{VR}} = 100, W_{\mathrm{FR}} = 100, W_{\mathrm{LS}} = 1000/\overline{\mathbf{pc}}_i, W_{\mathrm{MG}} = 400$. Each microgrid has one utility grid-forming (GF) DER and one facility-GF DER. Consider a parameter $\gamma = (\sum_{i \in \mathcal{N}} \overline{\mathbf{pc}}_i)/(8 |\mathcal{M}|)$. Then, each facility level DER has the following parameters: $\forall\; s \in \mathcal{S}_{\mathrm{gf}}^{\mathrm{facility}}, \overline{\mathbf{pn}}_s = \overline{\mathbf{pe}}_s = \overline{\mathbf{qn}}_s = \overline{\mathbf{qe}}_s = \gamma, \mathbf{mp}_s = 0.02, \mathbf{mq}_s = 0.04$; and, each utility-owned DER has the following parameters: $\forall\; s \in \mathcal{S}_{\mathrm{gf}}^{\mathrm{utility}}, \overline{\mathbf{pn}}_s = \overline{\mathbf{pe}}_s = \overline{\mathbf{qn}}_s = \overline{\mathbf{qe}}_s = 2\gamma, \mathbf{mp}_s = 0.1, \mathbf{mq}_s = 0.2$. These parameters are chosen such that the total capacity of grid-noninteractive DGs is 80% of the total demand, whereas the total capacity of all grid-interactive DERs is 75% of the total demand of all loads. However, the total capacity of grid-interactive DERs may not be fully available to meet the demand because the microgrids are typically not of exact uniform size and topology, and the storage devices supply power only under the specific islanding configurations.

Benders Decomposition vs. Simple Enumeration: We evaluate the ability of our implementation of the BD algorithm to compute optimal attacks in the islanding regime for small ($N \in \{24, 36\}$) networks. For each possible cardinality of attack we first compute the optimal attack with maximum loss using simple enumeration. Then we fix the maximum loss as $\mathcal{L}_{\mathrm{target}}$ for the BD algorithm. If the BD algorithm can find an attack with the same cardinality, then indeed the BD algorithm has computed the optimal attack. Otherwise, it has computed a suboptimal attack.
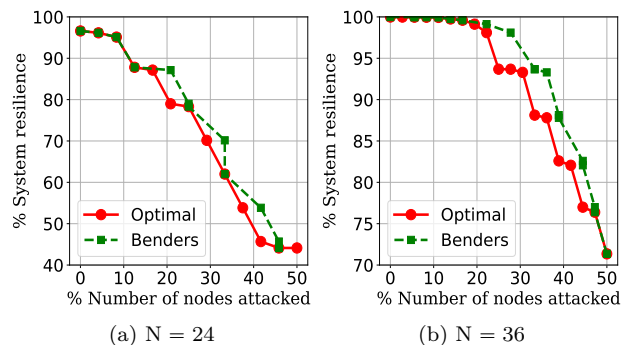

Fig. 6: System resilience ($\mathcal{R} = 100 (1 - \mathcal{L}/\mathcal{L}_{\max})$) vs. k. Near-optimal performance of BD algorithm.

The results of the BD algorithm implemented for solving (P-MG) are shown in Fig. 6. Naturally, the attack cardinality computed by BD algorithm is greater than or equal to the optimal min-cardinality computed using simple enumeration. In some cases, however, the BD algorithm does not obtain the optimal attack. The BD algorithm

involves iteratively eliminating sub-optimal attacks using Benders cuts [1]. Each cut involved an ϵ which results in a tradeoff between the accuracy and computational time. For a very small choice of ϵ, the BD algorithm eliminates exactly one sub-optimal attack in each iteration, and performs as worse as simple enumeration. For a large value of ϵ, relatively more attacks, including optimal attacks are eliminated. Hence, the BD algorithm terminates faster although with some loss of optimality. Still, for both 24- and 36-node networks, the BD algorithm computes attacks whose cardinalities are at most 8-23% more than the cardinalities of the corresponding optimal attacks.

Value of timely response: In [1], we used post-contingency loss to define the metric of resilience for autonomous disconnections ($\mathcal{R}_{\text{AD}}$) and operator response without microgrid capabilities ($\mathcal{R}_{\text{Mm}}$). In Sec. I, we introduced an analogously defined metric of resilience for operator response involving microgrid islanding and DER dispatch capabilities ($\mathcal{R}_{\text{MG}}$). Fig. 7 compares the resiliency values for the three cases for varying attack cardinalities, where computation of $\mathcal{R}_{\text{MG}}$ and $\mathcal{R}_{\text{Mm}}$ involves using the BD algorithm to solve the corresponding BiMIPs, and $\mathcal{R}_{\text{AD}}$ is computed using Algorithm "Uncontrolled cascade under autonomous disconnections (response (b))" in [1]. Indeed, under response (d), the SA triggers microgrid islanding and DER dispatch in a preemptive manner to reduce the impact of the attack. This leads to a smaller loss in comparison to using just load control and/or component disconnects (that is, response (c)). Indeed, our computational results validate that $\mathcal{R}_{\text{MG}} \geqslant \mathcal{R}_{\text{Mm}} \geqslant \mathcal{R}_{\text{AD}}$. The difference between the dashed (green) and solid (red) curves in Fig. 7 indicate the value of response (d) relative to response (b). The difference between the dashed (green) and cross-marked (blue) curves indicate the relative value of timely response (d) over response (c).

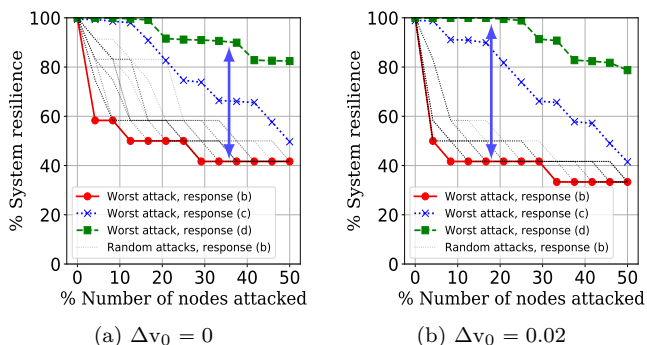(a) $\Delta\mathrm{v}_0 = 0$ (b) $\Delta\mathrm{v}_0 = 0.02$

Fig. 7: DN resilience under varying attacker-operator interaction scenarios. (The blue double-sided arrows indicate the value of timely microgrid response relative to the autonomous disconnections case.)

Scalability of the BD algorithm: We tabulate the performance of the BD algorithm in terms of its computational time and number of iterations 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. We also note the cardinalities of attacks output by the BD algorithm as well as the corresponding DN resilience. Note that the N = 118 node network has 2^{118} possible configuration vectors. Still, with $\mathcal{R}_{\text{target}} = 80\%$, the BD algorithm computes an attack in $\approx$ 1 minute. In comparison, for the N = 36 node network, the simple enumeration method took $\approx$ 6 hours.

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	98.91, (15), 0.41, 6	98.95, (10), 0.37, 5	98.95, (8), 2.48, 4
95	91.33, (16), 0.46, 7	94.12, (12), 0.51, 7	94.28, (15), 3.91, 11
90	82.8, (18), 0.57, 9	88.23, (17), 0.91, 11	89.73, (20), 10.62, 16
85	82.8, (18), 0.57, 9	81.9, (20), 1.23, 14	83.49, (29), 28.79, 25
80	78.73, (21), 0.74, 12	71.46, (21), 1.75, 15	79.9, (40), 67.38, 36

TABLE III: Resiliency metric evaluated using the BD algorithm for 24-, 36- and 118-node networks. The realized resilience metric can significantly fall short of the target resilience metric ($\mathcal{R}_{\text{target}} = 100\,(1 - \mathcal{L}_{\text{target}}/\mathcal{L}_{\text{max}})$); for example, when the attack cardinality changes from 6 to 7, the percentage resilience for the 24-node network decreases sharply from 98.91% to 91.33%. This means that the 24-node DN is at least 90% (actual value 91.33%) resilient to k = 7 cardinality attacks.

VI. MULTI-PERIOD DN RESTORATION

We recall that the resilience of a system is related to its ability to not only minimize the impact of a disturbance, but also quickly recover from it; see Fig. 1. Our attack model assumes that a compromise of the DGMS leads to remote disconnection of multiple DGs. However, the actual functionality of disconnected DGs is not compromised. In response (d), we consider that the SA has the ability to detect and obtain knowledge of the complete attack. Moreover, the SA can also control DG connectivity. We now discuss how the SA can restore the disrupted DGs, and bring the DN back to its nominal performance. In this section, we present a simple MIP that models the process of restoring system performance.

Our model of the DN restoration process entails progressively reconnecting the disrupted DGs, and eventually restoration to the grid-connected mode of DN operation. We consider a multi-period horizon $\mathcal{T} = \{0, 1, \cdots, \mathrm{T}\}$ where the end of the 0th period coincides with the time when the restoration actions begin; see Fig. 1. Let a period be denoted by $t \in \mathcal{T}$, where each period t is of fixed time duration (say, a few minutes). Furthermore, the operator response at period t is denoted by u^t. Let $\mathrm{T} = t_{\text{res}} + 1$, where $t_{\text{res}} \in \mathbb{Z}_+$ denotes the earliest time period when all disrupted DGs can be restored.

A TN-disturbance may clear any time, before or after the DG reconnections. However, since our analysis is focused on determining worst-case resilience of the DN, we assume that the TN-side disturbance clears after the disrupted DGs are fully reconnected, i.e. beyond time T. Under the assumed detection and response capabilities of

the SA, the restoration action begins only after $t = 0$. Thus, the operator control actions in the 0th time period are the same as the initial contingency response, i.e. $u^0 = u^c$. Similarly, the operator control actions remain unchanged after the restoration actions are complete until just prior to the TN-disturbance clearing. Therefore, without loss of generality we can assume that $t_2 = \mathrm{T}$, and restrict our analysis to the horizon $\mathcal{T}$.

We consider two types of constraints to model the restoration actions of the operator across time periods: monotonicity constraints and resource constraints. Consider a period $t \in \{1, 2, \cdots, \mathrm{T}\}$. The monotonicity constraints for period t are:

$$kl_{ij}^t \leqslant kl_{ij}^{t-1} \quad \forall\, (i,j) \in \mathcal{M}, \tag{28a}$$
$$kg_i^t \leqslant kg_i^{t-1} \quad \forall\, i \in \mathcal{N}. \tag{28b}$$

Eq. (28a) implies that during the restoration process, once a connecting line is closed, it remains closed until the restoration process is completed. Similarly, (28b) implies that a disconnected DG becomes operational after being reconnected, and then remains operational until the restoration is complete. The monotonicity constraints can be justified based on the practical consideration that frequently changing the status of connecting lines can create large fluctuations in nodal voltages and frequencies of the microgrids due to the low inertia of DERs. Moreover, the battery life of storage devices would reduce due to frequent changes from charging modes (quadrants III and IV) to discharging modes (quadrants I and II), and vice versa; see Fig. 4.

The resource constraint merely limits the number of DG reconnections. Specifically, we consider that during period t, at most G^t DGs can be reconnected, where G^t denotes the restoration budget for that period:

$$\sum_{i \in \mathcal{S}_{\mathrm{pq}}^{\mathrm{fixed}}} kg_i^t \geqslant \sum_{i \in \mathcal{S}_{\mathrm{pq}}^{\mathrm{fixed}}} kg_i^{t-1} - \mathrm{G}^t. \tag{29}$$

Restrictions on the number of connecting line closing operations can be similarly considered. Eq. (29) can also be justified in a way similar to that of the monotonicity constraints. Naturally, the operator wants to avoid a large number of simultaneous DG reconnections as that could lead to large voltage and frequency fluctuations.

We must choose T large enough so that all disrupted DGs can be reconnected over the horizon $\mathcal{T}$. This implies $\mathrm{T} = \min\{t' \mid \sum_{t=1}^{t'} \mathrm{G}^t \geqslant \mathrm{k}\} + 1$. Also, we assumed that the TN-side disturbance ceases to exist at the last time period. We model this as:

$$\mathrm{v}_0^t = \begin{cases} \mathbf{v^{nom}} - \Delta\mathrm{v}_0 & \text{if } t \neq \mathrm{T} \\ \mathbf{v^{nom}} & \text{if } t = \mathrm{T} \end{cases} \tag{30a}$$

$$f_0^t = \begin{cases} \mathbf{f^{nom}} - \Delta f_0 & \text{if } t \neq \mathrm{T} \\ \mathbf{f^{nom}} & \text{if } t = \mathrm{T}. \end{cases} \tag{30b}$$

Let $\mathcal{Y}_{\mathrm{m}}^t(u^{t-1})$ denote the feasible set of response strategies for u^t, i.e. $\mathcal{Y}_{\mathrm{m}}^t(u^{t-1}) = \{u^t \in \mathcal{U}_{\mathrm{m}} \mid \text{such that (28)} - (29) \text{ hold}\}$. Also, given an operator response $u \in \mathcal{U}_{\mathrm{m}}$, let $\mathcal{X}_{\mathrm{m}}^t(u)$ denote the set of network states x^t which satisfy

the constraints (1)-(14) and (30). Hence, the restoration problem can be posed as:

$$\mathcal{L}_{\mathrm{res}}(d) := \min_{\{u^t\}_{t\in\mathcal{T}}} \sum_{t\in\mathcal{T}} L_{\mathrm{m}}\left(u^t, x^t\right)$$
$$\text{s.t.} \quad u^0 \in \mathcal{U}_{\mathrm{m}}(d) \tag{P3}$$
$$u^t \in \mathcal{Y}_{\mathrm{m}}^t(u^{t-1}) \quad \forall\, t = 1, \cdots, \mathrm{T}$$
$$x^t \in \mathcal{X}_{\mathrm{m}}^t(u^t) \quad \forall\, t = 0, \cdots, \mathrm{T}.$$

Problem (P3) is a Mixed-Integer Problem (MIP), and can be solved using off-the-shelf MIP solvers. However, due to the large number of binary variables, it can become computational expensive to solve for larger networks. In fact, we solve (P3) using a simple greedy algorithm; see Algorithm 1. In each period, the operator simply chooses that response which minimizes the post-contingency loss during that time period subject to the monotonicity and resource constraints. Algorithm 1 is based on the feature that the network state in any period depends only on the operator actions in that period, and the network state in the previous period. The algorithm returns with the operator actions, resulting network state, and corresponding post-contingency loss for each time period.

Algorithm 1 Greedy Algorithm

1: $u^0, x^0 \leftarrow \underset{u \in \mathcal{U}_{\mathrm{m}}(d)}{\mathrm{argmin}} \quad L_{\mathrm{m}}(u, x) \quad \text{s.t.} \quad x \in \mathcal{X}(u)$.
2: **for** $t = 1, \cdots, \mathrm{T}$ **do**
3: $\quad u^t, x^t \leftarrow \underset{u \in \mathcal{Y}_{\mathrm{m}}^t(u^{t-1})}{\mathrm{argmin}} \quad L_{\mathrm{m}}(u, x) \quad \text{s.t.} \quad x \in \mathcal{X}_{\mathrm{m}}^t(u)$.
4: $\quad L^t \leftarrow L_{\mathrm{m}}(u^t, x^t)$
5: **end for**
6: **return** $\{u^t, x^t, L^t\}_{t\in\mathcal{T}}$

Fig. 8 shows the system performance during the restoration of the DN over multiple time periods for different resource constraints. For each system restoration curve, we chose G^t to be a constant for all time periods $t \in \mathcal{T}$. One can see that after the TN-side and DN-side disturbances, the system performance drops. Then, as disrupted components are connected, the system performance progressively recovers. Also, the post-contingency losses are higher for larger TN-side disturbances. However, as the restoration budget increases, the system recovers faster.
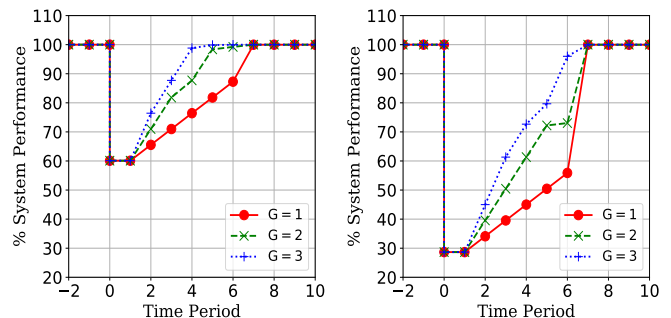
(a) $\Delta\mathrm{v}_0 = 0.1$ (b) $\Delta\mathrm{v}_0 = 0.2$

Fig. 8: Multi-period DN restoration (N = 36).

MIP vs. Greedy Recovery Algorithm: Fig. 9 shows the comparison of the system performance recovery curves obtained using Algorithm 1 and by directly solving the large-scale MIP for N = 24 and N = 36 node networks. The TN-side voltage disturbance for both the networks is set to Δv_0 = 0.2. In this experiment, we set the time limit of the (Gurobi) solver to 7200 seconds. While solving the large-scale MIP for N = 36 and G = 3 we were able to achieve an optimality gap of 16.54% after 2 hours. However, Algorithm 1 was able to attain the same system performance recovery curve using the default solver settings (no presolve and Simplex method), and compute the near-optimal solution in approximately 10 seconds.
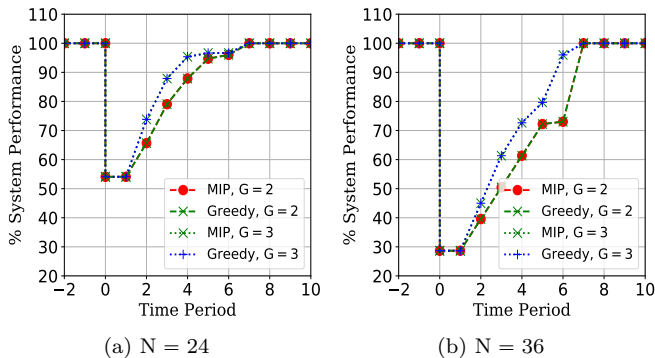

(a) N = 24 (b) N = 36

Fig. 9: Near-optimal performance of Greedy Algorithm 1.

In order to implement the response computed in (P3), the SA may need to coordinate with the individual microgrid controllers. A detailed description of such a communication architecture is beyond the scope of this paper. We refer the reader to [24] for a hierarchical control architecture which can support the coordination between SA and individual microgrid controllers.

VII. CONCLUDING REMARKS

In this paper and its companion paper [1], we developed a quantitative framework to evaluate DN resilience, which is its ability to minimize the impact of a disturbance, and to restore the DN back to full load supply. It has been shown that the impact of a broad class of cyberphysical failure scenarios can be modeled as DN-side disruption of multiple components and/or disturbances in substation voltage and frequency. We developed a novel network model which captures operation of microgrid(s) under various regimes, and single-/multi-master operation of DERs. Various operator response strategies were considered: from load control and component disconnects to microgrid islanding and DER dispatch. Furthermore, we formulated the attacker-operator interactions as bilevel mixed-integer problems, and developed a computational approach to efficiently solve these problems using a Benders decomposition algorithm. Restoration of DN performance over multiple time periods was considered, and a greedy algorithm was presented for solving this problem. Our computational results show the value of timely response under varying operator capabilities in minimizing the impact of disruption.

Even though a linear power flow was used and only basic aspects of microgrid operations have been considered, the paper provides a rich and flexible modeling framework for analyzing DN resilience for more sophisticated attack and response capabilities. Other cyber-physical security scenarios can be similarly analyzed by considering a clear demarcation between the vulnerable and the securely controllable DN components. The computational approach for solving the bilevel formulation arising from the linear power flow approximation can, in principle, be extended to convex (second-order cone) relaxations of the nonlinear power flow model. This approach may be useful for optimal resource allocation [12] and security investments for DNs [22]. The framework also provides the basis for resiliency assessment of other smart infrastructure networks.

REFERENCES

[1] D. Shelar, S. Amin, and I. Hiskens, "Resilience of Electricity Distribution Networks - Part I: Cyber-physical Disruption Models," *arXiv e-prints*, p. arXiv:1812.01746, Dec 2018.

[2] C. Chen, J. Wang, F. Qiu, and D. Zhao, "Resilient Distribution System by Microgrids Formation After Natural Disasters," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 958–966, March 2016.

[3] R. Lee, M. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center," http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf, 2015.

[4] H. Qi, X. Wang, L. M. Tolbert, F. Li, F. Z. Peng, P. Ning, and M. Amin, "A Resilient Real-Time System Design for a Secure and Reconfigurable Power Grid," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 770–781, Dec 2011.

[5] J. A. P. Lopes, C. L. Moreira, A. G. Madureira, F. O. Resende, X. Wu, N. Jayawarna, Y. Zhang, N. Jenkins, F. Kanellos, and N. Hatziargyriou, "Control strategies for microgrids emergency operation," in *2005 International Conference on Future Power Systems*, Nov 2005, p. 6.

[6] T. L. Vandoorn, J. C. Vasquez, J. D. Kooning, J. M. Guerrero, and L. Vandevelde, "Microgrids: Hierarchical Control and an Overview of the Control and Reserve Management Strategies," *IEEE Industrial Electronics Magazine*, vol. 7, no. 4, pp. 42–55, Dec 2013.

[7] N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay, "Microgrids: An Overview of Ongoing Research, Development, and Demonstration Projects," *IEEE Power & Energy Magazine*, vol. July/August, p. 19, 08/2007 2007.

[8] National Infrastructure Advisory Council, "Critical Infrastructure Resilience Final Report and Recommendations," September 2009. [Online]. Available: https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

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

[10] J. A. P. Lopes, C. L. Moreira, and A. G. Madureira, "Defining control strategies for MicroGrids islanded operation," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 916–924, May 2006.

[11] F. Katiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas, "Microgrids management," *IEEE Power and Energy Magazine*, vol. 6, no. 3, pp. 54–65, May 2008.

[12] D. Shelar, S. Amin, and I. Hiskens, "Towards Resilience-Aware Resource Allocation and Dispatch in Electricity Distribution Networks," *Book chapter in Springer/IMA volume on The Control of Energy Markets and Grids*, 2018.

[13] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical Control of Droop-Controlled AC and DC Microgrid–A General Approach Toward Standardization," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158–172, Jan 2011.

[14] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero, and F. Bullo, "Secondary Frequency and Voltage Control of Islanded Microgrids via Distributed Averaging," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 11, pp. 7025–7038, Nov 2015.

[15] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," *2017 North American Power Symposium (NAPS)*, pp. 1–6, 2017.

[16] S. Soltan, P. Mittal, and H. V. Poor, "Protecting the Grid against IoT Botnets of High-Wattage Devices," *CoRR*, vol. abs/1808.03826, 2018.

[17] Y. Yuan, Z. Li, and K. Ren, "Modeling Load Redistribution Attacks in Power Systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, June 2011.

[18] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011.

[19] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart Grid Data Integrity Attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013.

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

[21] D. Shelar, P. Sun, S. Amin, and S. Zonouz, "Compromising Security of Economic Dispatch in Power System Operations," in *47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, June 2017, pp. 531–542.

[22] D. Shelar and S. Amin, "Security Assessment of Electricity Distribution Networks Under DER Node Compromises," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 23–36, March 2017.

[23] NERC Reliability Standards, "CIP-005-5 – Cyber Security - Electronic Security Perimeter(s)," December 2015. [Online]. Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf

[24] N. J. Gil and J. A. P. Lopes, "Hierarchical Frequency Control Scheme for Islanded Multi-Microgrids Operation," in *2007 IEEE Lausanne Power Tech*, July 2007, pp. 473–478.

APPENDIX

(a) 24 node network.
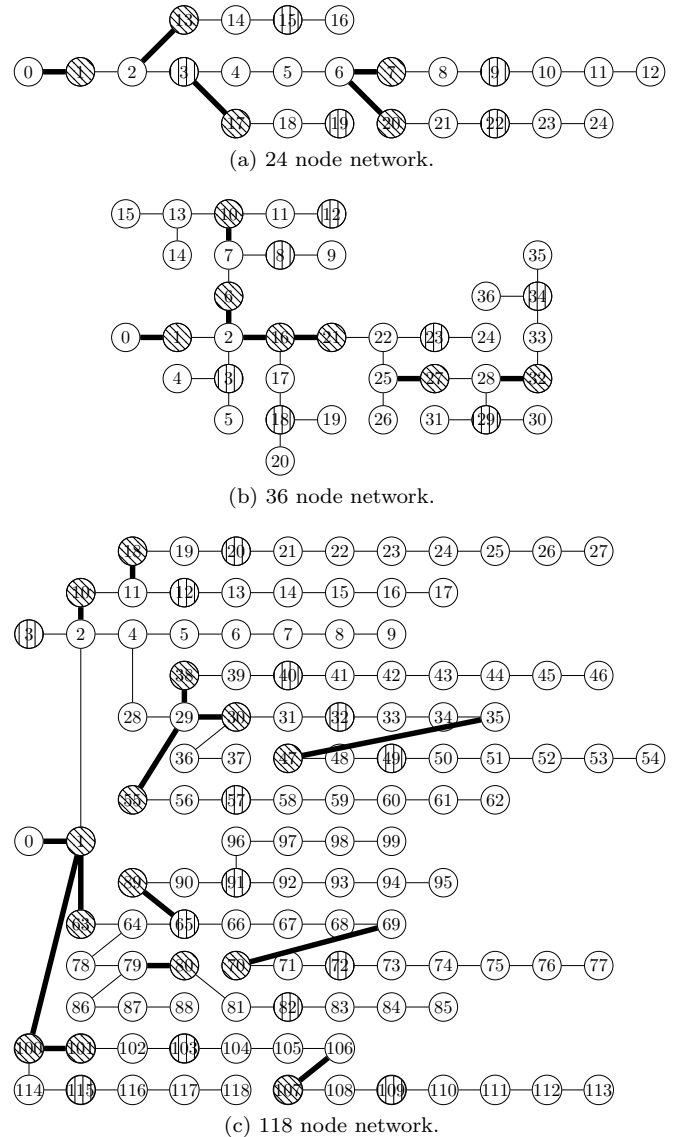
(b) 36 node network.

(c) 118 node network.

Fig. 10: Modified IEEE test networks. Connecting lines are indicated by thick edges. Utility-owned (resp. facility level) grid-forming DERs are indicated by northwest (resp. vertical) lines.