

Optimization-Based Resiliency Verification in Microgrids via Maximal Adversarial Set Characterization

Nawaf Nazir*, Thiagarajan Ramachandran, Saptarshi Bhattacharya, Ankit Singhal,
Soumya Kundu, and Veronica Adetola

Abstract—Critical energy infrastructures are increasingly relying on advanced sensing and control technologies for efficient and optimal utilization of flexible energy resources. Algorithmic procedures are needed to ensure that such systems are designed to be resilient to a wide range of cyber-physical adversarial events. This paper provides a robust optimization framework to quantify the range of adversarial perturbations that a system can accommodate without violating pre-specified resiliency metrics. An inner-approximation of the set of adversarial events which can be mitigated by the available flexibility is constructed using an optimization based approach. The proposed algorithm is illustrated on an islanded microgrid example: a modified IEEE 123-node feeder with distributed energy resources. Simulations are carried out to validate that the resiliency metrics are met for any event sampled from the constructed adversarial set for varying levels of available flexibility (energy reserves).

I. INTRODUCTION

Decarbonization, digitalization, and decentralization are driving the evolution of the energy infrastructures worldwide in the 21st century [1]. There are incentives towards low carbon solutions (including, but not limited to, renewable energy resources), most of which are located at the customer sites (e.g., rooftop solar panels). On the other hand, advanced sensing and control technologies, coupled with ubiquitous communication infrastructure, are creating a digital platform for efficient and optimal utilization of distributed energy resources. Fueled by these and other drivers, microgrids are fast emerging as viable energy infrastructure. Microgrids are a group of flexible energy resources operating together locally as a single controllable entity, satisfying certain reliability, power quality, and adequacy standards [2]. Safe and reliable operation of microgrids via optimal coordination of the flexible energy resources has drawn much attention in recent works [3]. Several works, including [4], have shown how microgrids with multiple energy sources can minimize the cost of energy and increase the resilience of energy supply to critical loads. In [5], data-driven methods have been used to study the impact of uncertainties in the renewable generation on microgrid resiliency, whereas in [6], resiliency metrics are incorporated into the microgrid planning problem. A robust optimization framework for microgrid operation is

presented in [7], which calculates the reserves required to ensure robustness under modeled uncertainties.

The resiliency of energy systems, e.g., microgrids, against various cyber and physical adversarial events, including malicious attacks, have been studied in the literature [8]–[11]. One type of such attacks includes injecting measurement errors to renewable generation output. Such errors can be constant offsets or potentially time-varying, and left untreated, may eventually lead to ramp-induced attacks [12]. Another class of attacks include *replay attacks* [13], whereby the measured renewable generation output is maliciously changed to reflect the true generation at a previous time stamp, thus impacting dispatch decisions. A third class of attacks entails corruption of state estimation, whereby the estimated physical quantities required for dispatch decisions (such as load setpoints) are maliciously changed [14], [15]. Specifically, load-setpoint change attacks often cause maximal impact when affected during specific hours of the day (for example, during 12 - 7 PM, when the load typically rises to hit an evening peak). A final class of attacks is coordinated attacks, whereby an attacker often has access to multiple critical information of the system, and can maliciously pose threats in a coordinated manner, from multiple sources (such as malicious under-estimation of load coupled with over-estimation of renewable capacity). Examples of such cyber-physical attacks can be found in [12], [16], [17]. In addition to attacks, other physical events such as generator outage, loss of solar generation due to cloud coverage, etc., could also lead to violations of critical operational constraints (such as serviceability of critical loads), as considered in this work.

The main contribution of the paper is to identify the set of cyber-physical adversarial events that the microgrid is guaranteed to be resilient against, via optimal use of available flexible energy resources. An optimization problem is set up to construct an inner approximation of the tolerable adversarial set. The rest of the paper is organized as follows. Sec. II presents the microgrid model that will be used in this paper and presents baseline optimization results without considering the uncertainty due to adversarial events. Sec. III provides the robust version of the microgrid optimization problem that calculates optimal reserves required to manage the adversarial events. Sec. IV provides the adversarial set characterization technique that is used to determine an inner approximation of the set of adversarial events that the microgrid can handle. Simulation results showing various case studies on the baseline model, robust model and adversarial set characterization are shown in Sec. V. Finally, Sec. VI

The authors are with the Electricity Infrastructure and Buildings Division at the Pacific Northwest National Laboratory, Richland, WA 99354, USA. S. Kundu holds a joint appointment as an Adjunct Faculty within the Department of Electrical and Biomedical Engineering at the University of Vermont, Burlington, VT 05405, USA.

*Corresponding Author. Email: nawaf.nazir@pnnl.gov.

provides the conclusions and the scope for future work.

II. BASELINE OPTIMIZATION

Let us begin by presenting a formulation of the optimal dispatch problem in a microgrid with various distributed energy resources, including solar photovoltaics (PVs), diesel generators (DGs), and energy storage (ES) units. We introduce a few notations for the following mathematical description. Let \mathcal{N} denote the set of all bus indices, and $\mathcal{L} \subseteq \mathcal{N} \times \mathcal{N}$ denote the set of all branches. We use $V_{n,k}$ to denote the multi-phase voltage vector at bus $n \in \mathcal{N}$, at time k . The net apparent power injection at bus n , at time k , is denoted by $S_{n,k}^{\text{net}} = P_{n,k}^{\text{net}} + jQ_{n,k}^{\text{net}}$, where $P_{n,k}^{\text{net}}$ and $Q_{n,k}^{\text{net}}$ are the respective active and reactive power components. Likewise, the Table I lists the symbols denoting the apparent, active, and reactive power associated with each of the energy resources and loads at bus n , at time k . Let $E_{n,k}^{\text{es}}$ be the storage state of

APPARENT, ACTIVE, REACTIVE	UNIT	CONVENTION
$\{S_{n,k}^{\text{pv}}, P_{n,k}^{\text{pv}}, Q_{n,k}^{\text{pv}}\}$	solar PV	injection
$\{S_{n,k}^{\text{dg}}, P_{n,k}^{\text{dg}}, Q_{n,k}^{\text{dg}}\}$	diesel generator	injection
$\{S_{n,k}^{\text{es}}, P_{n,k}^{\text{es}}, Q_{n,k}^{\text{es}}\}$	energy storage	injection
$\{S_{n,k}^{\text{load}}, P_{n,k}^{\text{load}}, Q_{n,k}^{\text{load}}\}$	load	consumption

TABLE I: Notations used for nodal power exchange

charge (SoC). Furthermore, let $i_{n,m,k}$ be the complex vector denoting the multi-phase current flowing from bus n to bus m (i.e., $n \rightarrow m$), at time k . Let $S_{n,m,k}$, $P_{n,m,k}$ and $Q_{n,m,k}$ denote, respectively, the apparent, active, and reactive branch power-flow from $n \rightarrow m$, at time k . Let $Z_{n,m} = Z_{m,n}$ be the impedance matrix of the branch $(n, m) \in \mathcal{L}$. Furthermore, we define (with $(\cdot)^*$ denoting conjugate transpose):

$$W_{n,k} := V_{n,k} \cdot V_{n,k}^*, \quad I_{n,m,k} := i_{n,m,k} \cdot i_{n,m,k}^*.$$

The distribution network power-flow equations can be expressed in the Branch Flow Model (BFM) [18] as:

$$\begin{bmatrix} W_{n,k} & S_{n,m,k} \\ S_{n,m,k}^* & I_{n,m,k} \end{bmatrix} = \begin{bmatrix} V_{n,k} \\ i_{n,m,k} \end{bmatrix} \begin{bmatrix} V_{n,k} \\ i_{n,m,k} \end{bmatrix}^* \quad (1a)$$

$$W_{n,k} = W_{m,k} - (S_{n,m,k} Z_{n,m}^* + Z_{n,m} S_{n,m,k}) + Z_{n,m} I_{n,m,k} Z_{n,m}^* \quad (1b)$$

$$S_{n,k}^{\text{net}} + \text{diag}(S_{n,m,k} - Z_{n,m} I_{n,m,k}) = \sum_{o:m \rightarrow o} \text{diag}(S_{m,o,k}) \quad (1c)$$

The nonlinearity of the power-flow equations in (1) render the resulting optimal dispatch problem non-convex (and NP-hard). While convex relaxations of the power-flow have been proposed in the literature (see [19] and the references therein), in this paper, we adopt a linearized power-flow model which typically yields acceptable solutions [20]. In particular, the linearized BFM model [18] is given as below:

$$0 = W_{n,k} - W_{m,k} + (S_{n,m,k} Z_{n,m}^* + Z_{n,m} S_{n,m,k}) \quad (2a)$$

$$0 = \text{diag}(S_{n,m,k}) - \sum_{o:m \rightarrow o} \text{diag}(S_{m,o,k}) + S_{n,k}^{\text{net}} \quad (2b)$$

Next, based on the convention in Table I, the net active and reactive power injections at each bus n satisfy the relations:

$$P_{n,k}^{\text{net}} = P_{n,k}^{\text{pv}} + P_{n,k}^{\text{dg}} + P_{n,k}^{\text{es}} - P_{n,k}^{\text{load}} \quad (3a)$$

$$Q_{n,k}^{\text{net}} = Q_{n,k}^{\text{pv}} + Q_{n,k}^{\text{dg}} + Q_{n,k}^{\text{es}} - Q_{n,k}^{\text{load}} \quad (3b)$$

The power system operational reliability and safety dictate imposing certain constraints on the bus voltages and the line flows, as follows:

$$|\text{diag}(S_{n,m,k})| \leq \bar{S}_{n,m} \quad (4a)$$

$$\underline{V}^2 \leq \text{diag}(W_{n,k}) \leq \bar{V}^2 \quad (4b)$$

where \underline{V} and \bar{V} are, respectively, the maximum and minimum allowable voltage limits (e.g., specified by ANSI C84.1 Standard), while $\bar{S}_{n,m}$ is the maximum limit on the line-flow.

The inequality constraints that govern the solar PV and diesel power generation is given by the following:

$$|S_{n,k}^{\text{pv}}| \leq \bar{S}_n^{\text{pv}}, \quad |S_{n,k}^{\text{dg}}| \leq \bar{S}_n^{\text{dg}}, \quad (5)$$

where \bar{S}_n^{pv} denotes the inverter capacity at bus n , and \bar{S}_n^{dg} is the rated size of the diesel generator at bus n .

Finally, the energy storage units are associated with a state-of-charge (SoC) dynamics, as well as limits on the charging/discharging rates, limits on the SoC (i.e., storage size), and the inverter capacity, as follows:

$$E_{n,k+1}^{\text{es}} = E_{n,k}^{\text{es}} - P_{n,k}^{\text{es}} \Delta t \quad (6a)$$

$$\underline{E}_n^{\text{es}} \leq E_{n,k}^{\text{es}} \leq \bar{E}_n^{\text{es}} \quad (6b)$$

$$-\bar{P}_n^{\text{es}} \leq P_{n,k}^{\text{es}} \leq \bar{P}_n^{\text{es}} \quad (6c)$$

$$|S_{n,k}^{\text{es}}| = \sqrt{(P_{n,k}^{\text{es}})^2 + (Q_{n,k}^{\text{es}})^2} \leq \bar{S}_n^{\text{es}} \quad (6d)$$

where \bar{P}_n^{es} is the maximum absolute limit on charging (and discharging power), while \bar{E}_n^{es} and $\underline{E}_n^{\text{es}}$ are the respective maximum and minimum limits of SoC. The storage inverter capacity is denoted by \bar{S}_n^{es} .

The decision variables (i.e., dispatchable quantities) considered in this work are:

$$u := \left(\mathbf{P}_k^{\text{pv}}, \mathbf{Q}_k^{\text{pv}}, \mathbf{P}_k^{\text{dg}}, \mathbf{Q}_k^{\text{dg}}, \mathbf{P}_k^{\text{es}}, \mathbf{Q}_k^{\text{es}}, \mathbf{P}_k^{\text{load}}, \mathbf{Q}_k^{\text{load}} \right)$$

where the bold-faced $\mathbf{P}_k^{\text{pv}} = [P_{n,k}^{\text{pv}}]$ denotes the vector of the solar active power variables at all buses, at time k , and likewise for the rest. The following additional physical constraints are placed on the solar and load dispatch.

- *Solar curtailment:* In a predictive optimization setting, we assume the availability of solar forecast $\hat{P}_{n,k}^{\text{pv}}$, such that the dispatched solar active power should satisfy

$$0 \leq P_{n,k}^{\text{pv}} \leq \hat{P}_{n,k}^{\text{pv}}. \quad (7)$$

Any available solar not dispatched is henceforth referred to as the solar curtailment:

$$P_{n,k}^{\text{pv,curt}} := \hat{P}_{n,k}^{\text{pv}} - P_{n,k}^{\text{pv}}. \quad (8)$$

- *Load curtailment*: We assume that each load bus, the *desired*, $P_{n,k}^{\text{load,des}}$, and *minimum (critically necessary)*, $P_{n,k}^{\text{load,min}}$, load values are specified/available. Therefore the dispatched load value should follow certain limits:

$$P_{n,k}^{\text{load,min}} \leq P_{n,k}^{\text{load}} \leq P_{n,k}^{\text{load,des}}. \quad (9)$$

Typically, the range of specified flexibility is narrower for critical loads for which the specified minimum value would be close to (or, same as) the desired value. Any unmet load is referred to as load curtailment:

$$P_{n,k}^{\text{load,curt}} := P_{n,k}^{\text{load,des}} - P_{n,k}^{\text{load}}. \quad (10)$$

Remark 1: Additional constraints can also be included in the formulation. For example, constraining the power factor could be important to alleviate power quality concerns. As such, we can place constraints such as:

$$\left| Q_{n,k}^{\text{pv}} \right| \leq \gamma^* \left| P_{n,k}^{\text{pv}} \right| \quad \text{and} \quad \left| Q_{n,k}^{\text{es}} \right| \leq \gamma^* \left| P_{n,k}^{\text{es}} \right|,$$

where $\gamma^* > 0$ is some suitably chosen values.

The objective function of the optimization problem consists of costs of generating from the DG unit, and penalties on the solar and load curtailment. In this paper, we adopt a multi-period linear cost function defined as follows:

$$f(u) := \sum_k \sum_n \left(c_1 P_{n,k}^{\text{dg}} + c_2 P_{n,k}^{\text{pv,curt}} + c_3 P_{n,k}^{\text{load,curt}} \right) \quad (11)$$

where the parameters $c_{1,2,3}$ are chosen appropriately to reflect the cost (or, penalty) on each term. Several works in the literature, such as [21], [22], have shown that using a linear cost function in microgrids is a reasonable assumption. The baseline optimization is then given as below:

$$(\text{BASELINE}) \quad \min f(u), \text{ s.t. constraints (2)-(10).} \quad (12)$$

III. ROBUST OPTIMIZATION PROBLEM

We adapt the optimization problem (12) to robustify it against a specified set of adversarial events. The main idea behind robustifying the optimization dispatch is to ensure *sufficient reserves* in the dispatched resources (DG, PV, storage, and interruptible load) so that these can adjust their output in response to adversarial events. While we omit the detailed description of the robust formulation due to space limitations, and refer the interested readers to [7] (and the references therein), we present here the essential deviations from the baseline formulation (12). The adversarial events are grouped into the *event* (or, perturbation) vector w , which may represent various cyber-physical attacks and/or physical disruptions. For example, an outage in DG could be represented by an uncertainty in the parameter $\bar{S}_{n,k}^{\text{dg}}$. Likewise, a load-masking attack could be represented by an uncertainty in $P_{n,k}^{\text{load,des}}$, while a sudden loss in solar generation could be represented by an uncertainty in $\hat{P}_{n,k}^{\text{pv}}$. In this paper, we consider a bounded set of uncertainties:

$$w \in \Omega_W. \quad (13)$$

In the most general form, the robust optimization problem for a system can be expressed in the following form:

$$\min_u \max_w f(u, w) \quad (14a)$$

$$\text{s.t. } g(u, w) \leq 0 \quad \forall w \in \Omega_W \quad (14b)$$

where $g(u, w)$ are the constraints (2)-(10). The above optimization problem (14) can be converted to a robust formulation using the *explicit maximization method* (see [23]) in the following form:

$$\min_u \hat{f}(u), \quad \text{s.t. } \hat{g}(u) \leq 0 \quad (15)$$

where $\hat{f}(u) = \max_w f(u, w)$ and $\hat{g}(u) = \max_w g(u, w)$. The new model does not contain any disturbance terms and if the functions $\hat{f}(u)$ and $\hat{g}(u)$ are convex, then the optimization problem is convex, which can be solved efficiently.

The additional decision variables we consider in our robust formulation include:

- *Solar reserves*: These are the up ($R_{n,k}^{\text{pv}+} > 0$) and down ($R_{n,k}^{\text{pv}-} > 0$) reserves set aside on the solar generation dispatch, so that the solar output has flexibility to increase or decrease from the optimally dispatched amount ($P_{n,k}^{\text{pv}}$) in response to an adversarial event:

$$R_{n,k}^{\text{pv}-} \leq P_{n,k}^{\text{pv}} \leq \hat{P}_{n,k}^{\text{pv}} - R_{n,k}^{\text{pv}+} \quad (16)$$

- *DG reserves*: These are the up ($R_{n,k}^{\text{dg}+} > 0$) and down ($R_{n,k}^{\text{dg}-} > 0$) reserves set aside on the DG dispatch:

$$R_{n,k}^{\text{dg}-} \leq P_{n,k}^{\text{dg}} \leq \bar{S}_{n,k}^{\text{dg}} - R_{n,k}^{\text{dg}+} \quad (17)$$

- *Storage reserves*: These are the up ($R_{n,k}^{\text{es}+} > 0$) and down ($R_{n,k}^{\text{es}-} > 0$) reserves set aside on the storage dispatch, allocated in such a way that there is flexibility on both the charging/discharging rates, as well as the SoC limits (assuming a look-ahead period of Δt):

$$-\bar{P}_{n,k}^{\text{es}} + R_{n,k}^{\text{es}-} \leq P_{n,k}^{\text{es}} \leq \bar{P}_{n,k}^{\text{es}} - R_{n,k}^{\text{es}+} \quad (18a)$$

$$\underline{E}_n + R_{n,k}^{\text{es}+} \Delta t \leq E_{n,k}^{\text{es}} \leq \bar{E}_n - R_{n,k}^{\text{es}-} \Delta t. \quad (18b)$$

- *Load reserves*: These are the up ($R_{n,k}^{\text{load}+} > 0$) and down ($R_{n,k}^{\text{load}-} > 0$) reserves set aside on the load dispatch (note the reverse convention on direction):

$$P_{n,k}^{\text{load,min}} + R_{n,k}^{\text{load}+} \leq P_{n,k}^{\text{load}} \leq P_{n,k}^{\text{load,des}} - R_{n,k}^{\text{load}-} \quad (19)$$

The goal of the robust microgrid optimization is then to minimize the cost of dispatched generation and reserves while satisfying the device and network constraints for all the disturbances in the selected disturbance set Ω_W . Combining the additional reserves cost and the additional constraints (16)-(19), we develop the following robust formulation:

$$(\text{ROBUST}) \quad \min_u \hat{f}(u) + f^R(\mathbf{R}_{n,k}^{\text{pv}}, \mathbf{R}_{n,k}^{\text{dg}}, \mathbf{R}_{n,k}^{\text{es}}, \mathbf{R}_{n,k}^{\text{load}}) \quad (20a)$$

$$\text{s.t. } \hat{g}(u) \leq 0, \text{ constraints (16)-(19)} \quad (20b)$$

where the bold-faced $\mathbf{R}_{n,k}^{pv} = (R_{n,k}^{pv+}, R_{n,k}^{pv-})$ and likewise, while f^R is a linear cost function of the allocated reserves, defined similarly as f .

Finally, we implement a simple measurement based control algorithm that dispatches reserves in response to disturbance events. In microgrids, the amount of flexible generation is increased/decreased based on real-time frequency measurements. In our quasi-static analysis, we consider the supply-demand power imbalance to be the measure of frequency and utilize that to dispatch the microgrid reserves in order to meet the demand under disturbance events. While works such as [24] has explored such feedback control methods, in this work, we employ a simple proportional controller that dispatches reserves in proportion to their available capacity:

$$Reserve Dispatch = \frac{Reserve Capacity}{Total Reserves} * Imbalance.$$

IV. ADVERSARIAL SET CHARACTERIZATION

While the robust formulation (20) can be solved for a given uncertainty set Ω_w , it is not known *a priori* what all adversarial events (as specified by the set) the system could be resilient against. In other words, it could be possible that, for a specified adversarial set Ω_w , the problem (20) returns infeasible. In this paper, we attempt to address this fact directly by proposing an algorithmic method to characterize the (maximal) adversarial set that the system can tolerate without violation of any critical constraint.

The optimal dispatch \mathbf{u}^* obtained by solving the optimization problem (2)-(10) are the set-points associated with the diesel generators, dispatchable loads and solar generation. The goal of the adversarial set characterization is to gain an understanding of the set of adversarial events that can be mitigated by the reserves associated with the optimal dispatch. For brevity, we will denote the *robust* version of the constraints (2)-(10) which jointly considers the decision variables $u \in \mathbb{R}^n$ and the adversarial event $w \in \Omega_w \subset \mathbb{R}^m$ as a convex constraint $g(u, w) \leq 0$.

A polytopic inner approximation $\bar{\Omega}_w$ of Ω_w that captures the set of adversarial events which can be mitigated by the reserves associated with the optimal dispatch \mathbf{u}^* can be constructed by solving m optimization problems as follows:

$$\mathbf{P}_i : \max_{w_i} \alpha_i \quad (21a)$$

$$g(\mathbf{u}^*, w_i) \leq 0 \quad (21b)$$

$$w_i \in \Omega_w \quad (21c)$$

$$w_i = w^{nom} + \alpha_i e_i \quad (21d)$$

where $i \in \{1, \dots, m\}$, $e_i \in \mathbb{R}^m$ is the i 'th basis vector and w^{nom} is the nominal value of the adversarial disturbance. The nominal value is simply the best estimate of the adversarial disturbance. In the absence of any information, we can assume that w^{nom} to correspond to the event where there has been no adversarial interference. The optimal solution to \mathbf{P}_i is the vector w_i^* which maximizes the magnitude of the i 'th component of the adversarial vector w . We will denote

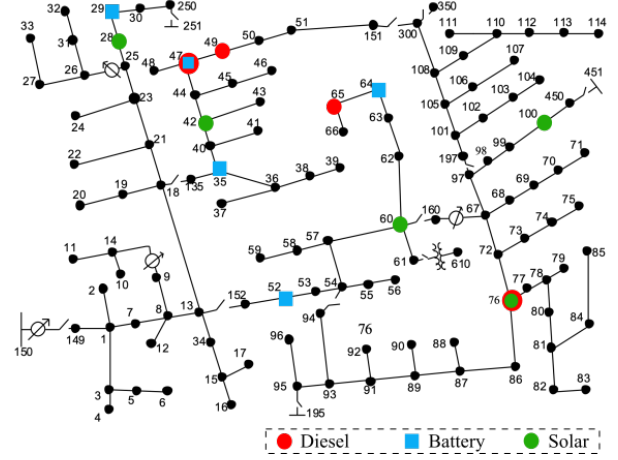


Fig. 1: Modified IEEE-123 node system with added solar PV, diesel generators and battery units. Note that the bus 76 has collocated diesel and solar generator, while bus 47 has collocated diesel generator and battery.

$w_0^* = w^{nom}$. Since g is convex, it follows that for any convex combination $\sum_{i=1}^m \alpha_i w_i^*$ of the optimal solutions, $g(\mathbf{u}^*, \sum_{i=1}^m \alpha_i w_i^*) \leq 0$. Then, we can define:

$$\bar{\Omega}_w = \{w \mid w = \sum_{i=0}^m \alpha_i w_i^*, \sum_{i=0}^m \alpha_i = 1, \alpha_i \geq 0\}.$$

The set $\bar{\Omega}_w$ represents an inner approximation of the set of adversarial events which can be mitigated by the available reserves given that the optimal dispatch is *fixed* to \mathbf{u}^* .

V. SIMULATION RESULTS

A. Baseline Optimization: Example

We illustrate the baseline optimization problem (12) on a modified three-phase IEEE-123 node system [25], shown in Fig. 1, which is converted into an islanded microgrid by disconnecting the substation from the utility. The figure shows the location of the solar PV units, diesel generator (DG) units and battery units in the network. The peak load value in the network is 3.5 MW (active) and 1.9 MVAR (reactive). The cumulative maximum generation limit of the DGs is kept at 2.5 MW, while the cumulative maximum PV generation is 1.77 MW. The aggregated (charging/discharging) power limit of the batteries is 1.5 MW, with an aggregated energy capacity of 6 MWh. The network model is hosted in GridLAB-D [26] and interacts with the baseline optimization (implemented in Julia) via FNCS which is a co-simulation platform [27]. To showcase the baseline optimization problem, we simulate the model under two scenarios: 1) *low solar high load*, and 2) *high solar low load*.

1) *Low solar high load case*: This scenario represents the solar and load profiles typically observed during the morning hours, with a low but increasing amount of solar and a high load. The generation and load dispatch for this case is shown in Fig. 2 which shows how with increasing solar generation over time, the DG generation is reduced in order to reduce the cost of operation. Furthermore, Fig. 3

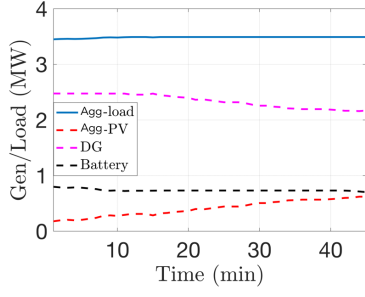


Fig. 2: Generation and load in the low solar high load case.

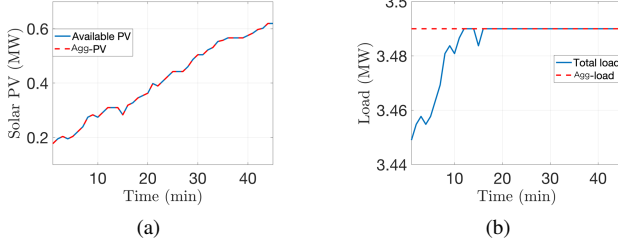


Fig. 3: Low solar high load case: (a) Solar curtailment (b) Load curtailment

shows the curtailment in solar and load, highlighting that initially there a small amount of load curtailment which is required due to inadequate solar PV available, but as the solar PV generation increases, the load curtailment becomes zero. The effect of the generation and load dispatches on the system constraints is depicted in Fig. 4 which shows that the voltages are within their operational limits and the state of charge (SoC) of each battery in the system is also within the SoC limits. In these simulation results, we assume that the initial SoC of the batteries is randomly chosen.

2) *High solar low load case:* This scenario represents the solar and load profiles typically observed during the noon/midday hours, with high solar generation but low load. The generation and load dispatch for this case is depicted in Fig. 5, which shows how the battery generation reduces and the solar generation increases (since reducing solar curtailment is part of the objective). Also, it can be seen that the DG output is zero as there is sufficient output available from the solar generation and batteries to meet the load. The effect on the system constraints of this generation dispatch is shown in Fig. 6, which depicts that the voltages are within their nodal limits and that the state of charge (SoC) for all the batteries is within their respective limits (in per unit).

These case studies show that the baseline optimization satisfies supply-demand balance and is able to satisfy the voltage and state of charge constraints. Furthermore, the amount of load curtailment is minimum and supply is maintained to critical loads in the system.

B. Robust optimization simulation results

In the following set of simulation results, we will illustrate the effectiveness of the robust formulation (in Sec. III). We consider a disturbance event consisting of a cyber-physical

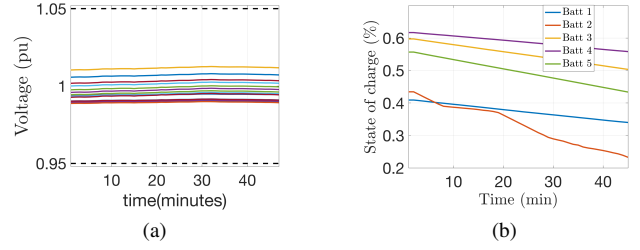


Fig. 4: Low solar high load case: (a) Nodal voltages (b) Battery state of charge evolution.

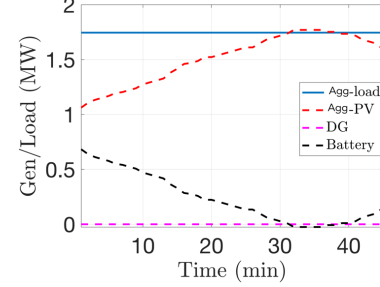


Fig. 5: Generation and load in the high solar low load case.

event as depicted in Fig. 7a, wherein the largest DG in the microgrid (DG 65) trips at time 20 min and become offline and soon after, at 30 min, there is a cyber attack which masks the increase in load from the system operator. The DG is made operational and comes back online at 40 min, whereas the cyber attack is finally over at 50 min. We solve the robust optimization problem to maintain sufficient reserves in order to meet the increased demand and also maintain system constraints under this cyber-physical event, i.e., the robust optimization problem should have enough reserves to dispatch in case such a cyber-physical event happens on the microgrid. It is assumed that the disturbance can be measured through the imbalance in supply and demand which manifests itself in the form of frequency deviation in the system. This frequency measurement is utilized by the flexible resources to dispatch their reserves when an adversarial event occurs. The results for the robust optimization dispatch are shown in Fig. 7b. The results show that as the DG trips at 20 min, the solar PV and the battery increase their output in order to meet the load. Furthermore, when the cyber-attack at 30 min masks the increased load, the battery and PV generation is further increased to meet this load. As the DG unit comes back online and the cyber-attack ends, the battery and solar PV also reduce their output. These simulation results illustrate the effectiveness of the robust formulation to deal with this cyber-physical event. Furthermore, Fig. 8 shows that the robust formulation allocates enough total reserves to deal with this cyber-physical event, i.e., to counter the loss of the largest DG and the load masking cyber-attack. The results in Fig. 9 demonstrate the effect of this robust dispatch on the system constraints, i.e., the SoC of all the batteries is within their limits and the nodal voltages are

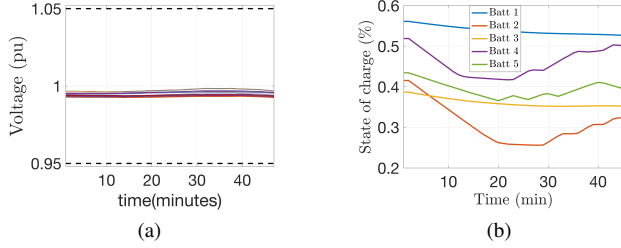


Fig. 6: High solar low load case: (a) Nodal voltages (b) Battery state of charge evolution

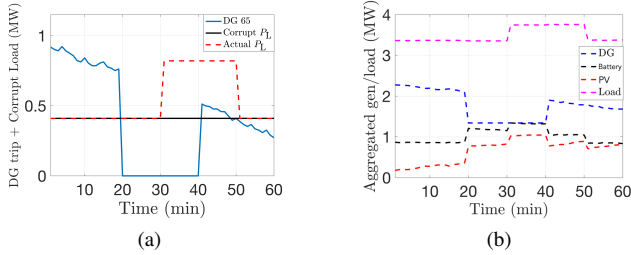


Fig. 7: Cyber-physical event case: (a) DG-trip followed by cyber-attack that masks the increase in load (b) Response of the flexible generation and curtailment to deal with this event

within the specified bounds.

C. Adversarial set simulation results

In order to showcase the adversarial set characterization (presented in Sec. IV), we determine the set of largest disturbances which the system can handle. In this scenario we consider losing the largest DG unit, load increase at certain buses, and error in the solar forecast. The baseline optimization problem is solved for each time instant, and given the baseline dispatch, the set $\bar{\Omega}_w$ is computed for each time step by solving \mathbf{P}_i for each potential adversarial event. The maximum component-wise perturbation that can be tolerated and a 2-dimensional projection of $\bar{\Omega}_w$ for specific time instants is shown in Fig 10a and Fig 10b. Furthermore, the shape of the set $\bar{\Omega}_w$ changes over time and depends on the amount of flexibility that is available in the system (see Fig 11a and Fig 11b). Then sampling from the set $\bar{\Omega}_w$ showcases that these disturbances can be handled by the available flexibility. This is shown in Fig. 12 which shows the response of the generators to the loss of DG unit and increase in load and also shows that in this response the SoC constraints are still satisfied. Figure 12a shows that at time $T = 20$ minutes there is a loss of DG (chosen randomly between zero and maximum DG loss calculated for the adversarial set). Based on the above analysis, we are guaranteed to have enough reserves available in the system to deal with this disturbance, which can be seen from the increase in battery output and solar PV generation. Furthermore, at $T = 30$ minutes, we experience a load increase at certain buses (again chosen randomly at each step between zero and the maximum calculated based on the adversarial set). To deal with this load

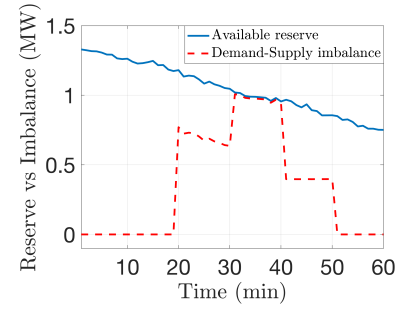


Fig. 8: Supply demand imbalance created by the cyber-physical event and the reserves available to deal with such an event. The figure shows that enough reserves are available to the system operator to effectively deal with this event.

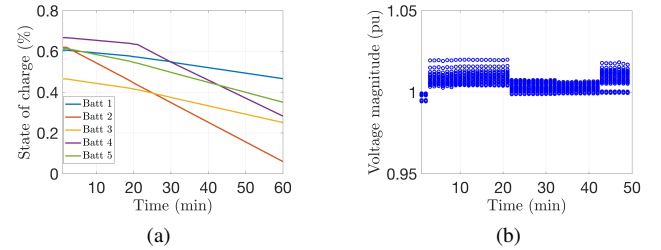


Fig. 9: Network constraint under cyber-physical event: (a) Battery state of charge (SoC) (b) Network voltages

increase, we dispatch additional flexibility from the battery and the DG units. These simulation results illustrate that the maximum adversarial set calculated in the previous analysis can be managed feasibly by the available flexibility in the microgrid, while maintaining the supply-demand balance and other constraints such as SoC as depicted in Fig. 12b.

VI. CONCLUSIONS

This paper presented a method to determine the adversarial set of a three-phase microgrid system. We formulate the robust optimization problem and from that we formulate the adversarial set characterization problem. We illustrate the inner approximation of the adversarial set through simulation results on IEEE-123 node distribution system. Future work will develop methods to incorporate the determined adversarial sets in microgrid planning and operation. Future work will also focus on probabilistic uncertainties (in the form of chance-constrained and risk based optimization), and compare the conservativeness of the characterized adversarial set between the deterministic and probabilistic approaches. Moreover, we will also investigate the applicability of this approach to larger systems (e.g., networked microgrids).

ACKNOWLEDGMENT

This research was supported by the “Resilience through Data-driven Intelligently-Designed Control” Initiative, under the Laboratory Directed Research and Development Program at Pacific Northwest National Laboratory (PNNL). PNNL is a multi-program national laboratory operated for the U.S.

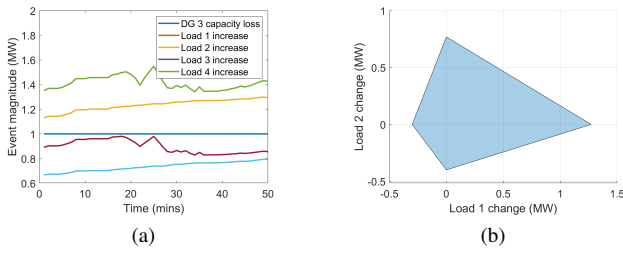


Fig. 10: Adversarial set characterization: (a) The maximum component-wise perturbation α_i^* that is supported by the available reserves (b) A 2-dimensional subset of $\bar{\Omega}_w$ for a specific time instant that illustrates the convex region of the tolerable variations in load 1 and 2.

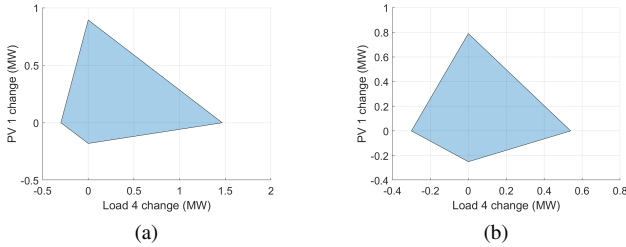


Fig. 11: 2-dimensional subset of the time-varying adversarial set $\bar{\Omega}_w$ capturing the allowable variations in solar PV output and load 4, at a) T = 1 minute b) T= 25 min.

Department of Energy by Battelle Memorial Institute under Contract No. DE-AC05-76RL01830.

REFERENCES

- [1] M. L. Di Silvestre, S. Favuzza, E. R. Sanseverino, and G. Zizzo, "How decarbonization, digitalization and decentralization are changing key power infrastructures," *Renewable and Sustainable Energy Reviews*, vol. 93, pp. 483–498, 2018.
- [2] M. Farrokhhabadi, C. A. Cañizares, J. W. Simpson-Porco, E. Nasr, L. Fan, P. A. Mendoza-Araya, R. Tonkoski, U. Tamrakar, N. Hatziaziyriou, D. Lagos *et al.*, "Microgrid stability definitions, analysis, and examples," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 13–29, 2019.
- [3] S. Parhizi, H. Lotfi, A. Khodaei, and S. Bahramirad, "State of the art in research on microgrids: A review," *IEEE Access*, vol. 3, pp. 890–925, 2015.
- [4] K. H. Anderson, N. A. DiOrio, D. S. Cutler, and R. S. Butt, "Increasing resiliency through renewable energy microgrids," *International Journal of Energy Sector Management*, vol. 2, 2017.
- [5] A. Hussain, A. O. Rousis, I. Konstantelos, G. Strbac, J. Jeon, and H.-M. Kim, "Impact of uncertainties on resilient operation of microgrids: A data-driven approach," *IEEE Access*, vol. 7, pp. 14924–14937, 2019.
- [6] X. Wu, Z. Wang, T. Ding, X. Wang, Z. Li, and F. Li, "Microgrid planning considering the resilience against contingencies," *IET Generation, Transmission & Distribution*, vol. 13, no. 16, pp. 3534–3548, 2019.
- [7] G. Liu, M. Starke, B. Xiao, and K. Tomsovic, "Robust optimisation-based microgrid scheduling with islanding constraints," *IET Generation, Transmission & Distribution*, vol. 11, no. 7, pp. 1820–1828, 2017.
- [8] M. Dehghani, T. Niknam, M. Ghiasi, N. Bayati, and M. Savaghebi, "Cyber-attack detection in dc microgrids based on deep machine learning and wavelet singular values approach," *Electronics*, vol. 10, no. 16, p. 1914, 2021.

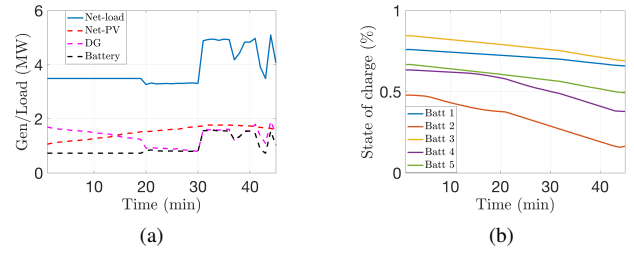


Fig. 12: Network constraint under cyber-physical event:(a) Response of the flexible generation under cyber-physical event (b) Battery state of charge (SoC)

- [9] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, and G. Cao, "Deep learning aided interval state prediction for improving cyber security in energy internet," *Energy*, vol. 174, pp. 1292–1304, 2019.
- [10] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, M. Shasadeghi, N. Ghadimi, and F. Taghizadeh-Hesary, "Blockchain-based securing of data exchange in a power transmission system considering congestion management and social welfare," *Sustainability*, vol. 13, no. 1, p. 90, 2021.
- [11] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.
- [12] L. Che, X. Liu, Z. Shuai, and J. Zhao, "The impact of ramp-induced data attacks on power system operational security," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 5064–5075, 2019.
- [13] M. R. Habibi, H. R. Baghaee, T. Dragičević, F. Blaabjerg *et al.*, "Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020.
- [14] T. R. B. Kushal, K. Lai, and M. S. Illindala, "Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4741–4750, 2018.
- [15] S. Banerjee and A. Chatterjee, "Online fast detection and diagnosis of power grid security attacks using state checksums," in *2021 IEEE 27th International Symposium on On-Line Testing and Robust System Design (IOLTS)*. IEEE, 2021, pp. 1–7.
- [16] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.
- [17] H. He, S. Huang, Y. Liu, and T. Zhang, "A tri-level optimization model for power grid defense with the consideration of post-allocated dgs against coordinated cyber-physical attacks," *International Journal of Electrical Power & Energy Systems*, vol. 130, p. 106903, 2021.
- [18] L. Gan and S. H. Low, "Convex relaxations and linear approximation for optimal power flow in multiphase radial networks," in *2014 Power Systems Computation Conference*. IEEE, 2014, pp. 1–9.
- [19] N. Nazir, P. Racherla, and M. Almassalkhi, "Optimal multi-period dispatch of distributed energy resources in unbalanced distribution feeders," *IEEE Transactions on Power Systems*, vol. 35, no. 4, pp. 2683–2692, 2020.
- [20] S. Bolognani and F. Dörfler, "Fast power system analysis via implicit linearization of the power flow manifold," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2015, pp. 402–409.
- [21] A. Parisio, E. Rikos, and L. Glielmo, "A model predictive control approach to microgrid operation optimization," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 5, pp. 1813–1827, 2014.
- [22] Y. Zhang, N. Gatsis, and G. B. Giannakis, "Robust energy management for microgrids with high-penetration renewables," *IEEE transactions on sustainable energy*, vol. 4, no. 4, pp. 944–953, 2013.
- [23] X. Bai, L. Qu, and W. Qiao, "Robust AC optimal power flow for power networks with wind power generation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 4163–4164, 2015.
- [24] S. Brahma, N. Nazir, H. Ossareh, and M. Almassalkhi, "Optimal and resilient coordination of virtual batteries in distribution feeders," *IEEE Transactions on Power Systems*, 2020.

- [25] W. H. Kersting, *Distribution system modeling and analysis*. CRC press, 2006.
- [26] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, “GridLAB-D: An open-source power systems modeling and simulation environment,” in *Transmission and distribution conference and exposition, 2008. t&d. IEEE/PES*. IEEE, 2008, pp. 1–5.
- [27] S. Ciraci, J. Daily, J. Fuller, A. Fisher, L. Marinovici, and K. Agarwal, “FNCS: A framework for power system and communication networks co-simulation,” in *Proceedings of the symposium on theory of modeling & simulation-DEVS integrative*, 2014, pp. 1–8.