Protecting the Grid Against MAD Attacks

Saleh Soltan, *Member, IEEE*, Prateek Mittal, *Senior Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—Power grids have recently been shown to be vulnerable to MAnipulation of Demand (MAD) attacks using high-wattage IoT devices. In this paper, we introduce two forms of defenses against line failures caused by these attacks: 1) we develop two algorithms named SAFE and IMMUNE for finding efficient operating points for generators during the normal operation of the grid such that no lines are overloaded instantly after any potential MAD attacks, and 2) assuming lines can temporarily tolerate overloads, we develop efficient methods to verify in advance if such overloads can quickly be cleared by changing the operating points of the generators after any attacks. We then define the novel notion of αD-robustness for a grid indicating that line overloads can either be prevented or cleared after any attacks based on the two forms of introduced defenses if an adversary can increase/decrease the demands by at most α fraction. We demonstrate that practical upper and lower bounds on the maximum α for which a grid is αD-robust can be found efficiently in polynomial time. Finally, we evaluate the performance of the developed algorithms and methods on realistic power grid test cases.**

***Index Terms*—Power grid, IoT, cyber attacks, demand manipulation, control.**

I. Introduction

POWER grids, as one of the most essential infrastructure networks, have been repeatedly shown in the past few years to be vulnerable to cyber attacks. The most infamous example of these attacks was on the Ukrainian grid that affected about 225,000 people in December 2015 [1]. However, smaller scale attacks on regional power grids have been shown in a recent report to be more common and pervasive [2]. As indicated in the report, *"Hackers are developing a penchant for attacks on energy infrastructure because of the impact the sector has on people's lives"* [2].

Because of this ever-growing threat, there has been a significant effort by researchers in recent years to find methods to protect the grid against cyber attacks. These efforts have been mainly focused on potential attacks that directly affect different components of power grids' Supervisory Control And Data Acquisition (SCADA) systems. Many system operators prefer to completely disconnect their SCADA systems from the Internet in the hope that their systems remain unreachable to hackers.

Despite these efforts, the *power demand* side of the grid operation, which is not controlled by SCADA, has been neglected as being directly susceptible to attacks in security assessments due to their predictable nature. However, as the authors [3] and Dabrowski et al. [4] have recently revealed, the universality and growth in the number of high-wattage Internet of Things (IoT) devices, such as air conditioners and water heaters, have provided a unique way for adversaries to *disrupt the normal operation of power grid, without any access to the SCADA system [5], [6].* In particular, an adversary with access to sufficiently many of such high-wattage devices (i.e., a *botnet*), can abruptly increase or decrease the total demand in the system by synchronously turning these devices on or off, respectively. We call these attacks MAnipulation of Demand (MAD) attacks (see Fig. 1).

An abrupt increase/decrease in the total demand results in abrupt drop/rise in the system's frequency. If this drop/rise is significant, generators will be automatically disconnected from the grid and a large scale blackout occurs within seconds [3], [4]. If the drop/rise in the frequency is not significant, the extra demand/generation can automatically be compensated by generators' primary controllers, and the frequency of the system will be stabilized. As a result of this automatic change in the generation–and demand by the adversary–the power flows in the transmission network change based on power flow equations. Since the power flows are not controlled by the grid operator at this stage, this change in the power flows may result in line overloads and consequent line-trippings. These initial line failures can initiate a cascading line failure and result in a large scale blackout in the grid [3]. For example, it has been demonstrated that only a 1% increase in the demands at certain scenarios may initiate a cascading failure leading to 86% power outage in the system.

The grid operator can protect the grid against initial drop/rise in the system's frequency caused by a MAD attack by ensuring that the system has enough *inertia* (mostly through rotating generators) and there is enough available *spinning reserve* (i.e., generators have enough extra generation capacity) [3]. However, protecting the grid against possible line overloads and failures after a MAD attack, which is the main focus of this paper, is more analytically and computationally challenging. Such defenses require the grid operator to analyze all possible MAD attacks and their consequences on the power flows and select operating points for the generators (i.e., their power generation output) to satisfy the power demands such that no lines are overloaded after any MAD attacks.

Manuscript received October 17, 2018; revised April 3, 2019; accepted June 4, 2019. Date of publication June 11, 2019; date of current version September 2, 2020. This work was supported in part by the Siebel Energy Institute, in part by the National Science Foundation under Grant DMS-1736417, Grant ECCS-1824710, and Grant CNS-1553437, and in part by the Office of Naval Research YIP Award. Recommended for acceptance by S. Xu. *(Corresponding author: Saleh Soltan.)*

The authors are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (e-mail: ssoltan@princeton.edu; pmittal@princeton.edu; poor@princeton.edu).

Digital Object Identifier 10.1109/TNSE.2019.2922131

2327-4697 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

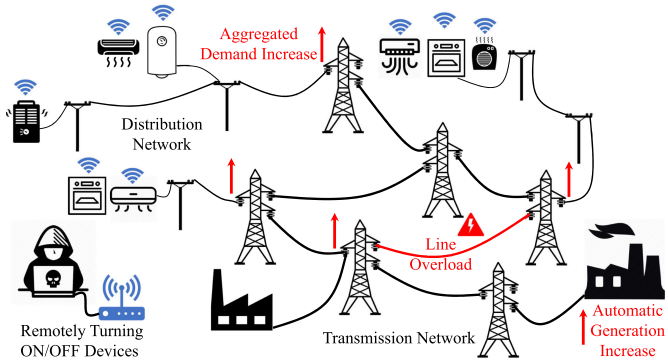

Fig. 1. The MAD attack. An adversary with access to an IoT botnet of high-wattage devices can remotely and synchronously switch on/off these devices in order to change power flows on the lines in a power transmission network and cause line overloads and failures.

We first focus on finding operating points (namely *robust operating points*) with the minimum cost for the generators such that no lines are overloaded after the automatic primary response of the generators to any MAD attacks. Since changes in power flows after a MAD attack directly depend on generators' operating points, finding the optimal operating points for the generators requires solving a nonconvex and nonlinear optimization problem which is hard in general. Despite this hardness, we develop two algorithms named the Securing Additional margin For generators in Economic dispatch (SAFE) Algorithm and the Iteratively MiniMize and boUNd Economic dispatch (IMMUNE) Algorithm for finding suboptimal yet robust operating points for the generators efficiently. The SAFE Algorithm provides robust operating points for the generators by solving a single Linear Program (LP). The IMMUNE Algorithm, on the other hand, requires a few iterations until it converges, but it provides robust operating points with lower costs than the ones obtained by the SAFE Algorithm.

In situations for which the operating cost of the grid in a robust state is costly (or no robust operating points exists due to lack of enough resources), the grid operator may decide to allow temporary line overloads–by increasing thresholds on circuit breakers–in the case of a MAD attack, and clear the overloads during the *secondary control*. During the secondary control, which comes right after the automatic primary control, the grid operator can directly change generators' operating points in order to bring back the system's frequency to its nominal value and clear any line overloads. To make sure that line overloads can be cleared during the secondary control, the grid operator needs to verify in advance whether for any potential MAD attack, there exist operating points for the generators satisfying demands such that no lines are overloaded (namely, the grid is *secondary controllable*). However, due to the extent of the attack space, checking all possible attack scenarios is computationally impractical. Hence, we develop several predetermined control policies that can be used to verify the secondary controllability of the grid in most scenarios with no false positives.

We then evaluate the *robustness* of grids against MAD attacks with different magnitudes. The magnitude of an attack can be determined by the fraction of demand (denoted by α) that the adversary can increase or decrease at each location. We call a grid αD-robust if either line overloads can be prevented (i.e., robust operating points exist for generators) or they can be cleared during the secondary control (i.e., the grid is secondary controllable) after any MAD attacks by *an adversary that can change the demands by at most a fraction* α. In general, finding the maximum α such that a given grid is αD-robust, is hard. However, by focusing on grid secondary controllability and the developed predetermined control policies, we provide efficient methods for computing practical upper and lower bounds on the maximum α in polynomial time.

Finally, we evaluate the performance of the developed algorithms and controllers numerically. For example, in the New England 39-bus system, we show that the SAFE and IMMUNE Algorithms find operating points for the generators with at most 6 and 2 percent increase in the total operating cost such that the grid is robust against MAD attacks of magnitude $\alpha = 0.08$. We also evaluate the performance of the developed methods for approximating the maximum α such that the grid is αD-robust and show that for example in the New England 39-bus system, the provided lower and upper bounds are tight and are equal to the maximum $\alpha^{\max} = 0.0962$.

To the best of our knowledge, our work is the first to study the effects of potential MAD attacks on the *power flows* in the grid and provide efficient preventive algorithms to avoid line failures after the primary control response, and also efficient methods to verify if the line overloads can be cleared during the secondary control. These algorithms and methods can be adopted by grid operators to protect their systems against MAD attacks now and in the near future.

The rest of this paper is organized as follows: Section II provides related work and Section III presents a brief introduction to the power system's operation and control. In Section IV, we introduce the MAD attacks and provide their basic properties. In Section V, we present the SAFE and IMMUNE algorithms and in Section VI, we provide efficient methods for verifying secondary controllability of a grid. Section VII provides methods to evaluate the robustness of grids against MAD attacks and Section VIII presents numerical results. Finally, Section IX provides concluding remarks and future directions. To improve the readability of the paper, some of the proofs are moved to Section X.

II. Related Work

Power systems' vulnerability to failures and attacks has been widely studied in the past few years [7]–[12]. In a recent work [13], Garcia et al. introduced Harvey malware that affects power grid control systems and can execute malicious commands. Theoretical methods for detecting cyber attacks on power grids and recovering information after such attacks have also been developed [14]–[22]. Another related type of cyber attacks called *load redistribution attacks* has been studied by Yuan et al. [23]. However, these type of attacks *change only the measurements* at the loads in order to force the grid operator into problematic corrective actions rather than actually changing the loads as have been studied in our work. Overall, most of the previous work on protecting the grid

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

against attacks have focused on attacks that directly target the power grid's physical infrastructure or its control system.

The possibility of load altering attacks on smart meters and large cloud servers has been first introduced by Mohsenian et al. [24]. Their work was mostly focused on minimizing the total cost of protecting the loads (which is not always possible, especially for distributed IoT devices) against such attacks. Amini et al. [25] have also recently studied the effects of load altering attacks on the system's dynamics and ways to use the system's frequency as feedback to improve an attack. However, until very recently, practical ways to perform such attacks on a large-scale and their consequences on power flows were not fully studied [3]. Hence, little attention has been given to protecting the grid against line failures caused by these type of attacks.

In three very recent papers, Dvorkin and Sang [26], Dabrowski et al. [4], and our work [3] revealed the possibility of exploiting compromised IoT devices to manipulate the demands and to disrupt the normal operation of the power grid. Dvorkin and Sang [26] modeled their attack as an optimization problem for the adversary—with complete knowledge of the grid—to cause circuit breakers to trip in the distribution network. Dabrowski et al. [4] studied the effect of demand increases caused by remote activation of CPUs, GPUs, hard disks, screen brightness, and printers on the frequency of the European power grid. In [3], we analyzed the effects of sudden increase and decrease in the demand via an IoT botnet of high-wattage devices from various operational perspectives and demonstrated that besides frequency instability, such attacks can also result in widespread *cascading line failures* in the transmission network leading to large-scale blackouts. Nevertheless, practical preventive defenses against possible *line failures* caused by these attacks have not been developed yet.

Finally, while there have been extensive efforts in recent years to develop efficient algorithms for solving the Optimal Power Flow (OPF) problem [27]–[29] and its different variations including *Security Constrained* OPF (SC-OPF) [30] (which considers grid robustness against possible line outages) and *Chance Constrained* OPF (CC-OPF) [31] (which considers uncertainty in the output of the renewable resources), since these works do not consider grid robustness against *adversarial changes in the demands*, our work is different from previously studied variations of the OPF problem. Moreover, the second part of this work deals with secondary controllability of the grid after an attack which is a totally different problem from OPF and its variations.

III. Model and Definitions

In this section, we provide a brief introduction to power systems' operation and control. Our focus is on the power transmission network.

Throughout this paper, we use bold uppercase characters to denote matrices (e.g., $\mathbf{A}$), italic uppercase characters to denote sets (e.g., V), and italic lowercase characters and overline arrow to denote column vectors (e.g., $\vec{\theta}$). For a matrix $\mathbf{Q}$, $\mathbf{Q}_i$ denotes its i^{th} row, q_{ij} denotes its $(i,j)^{\text{th}}$ entry, and $\mathbf{Q}^T$ denotes its transpose. For a column vector $\vec{y}$, $\vec{y}^T$ denotes its transpose, and $\|\vec{y}\|_1 := \sum_{i=1}^{n} |y_i|$ is its l_1-norm. For a variable x, $\text{sgn}(x)$ denotes its sign, and $\overline{x}$ and $\underline{x}$ denote its upper and lower limits, respectively. For a vector $\vec{y}$, for simplicity of notation, we drop the vector sign $\vec{}$ in denoting vectors of upper and lower limits on the entries of $\vec{y}$ as $\overline{y}$ and $\underline{y}$, respectively. Finally, $\vec{e}_1, \ldots, \vec{e}_n$ denote the fundamental basis of $\mathbb{R}^n$ and $\vec{1} = \sum_{i=1}^{n} \vec{e}_i$ denotes the all ones vector.

A. Power Flows

Power flows are governed by a set of differential equations. In the steady-state, using *phasors*, these differential equations can be reduced to a set of algebraic equations on complex numbers known as the *Alternating Current (AC)* power flow model. Due to the nonlinearity of AC power flow equations and the computational complexity of solving these equations, in practice and in day-ahead power grid contingency analysis and planning, the linearized version of these equations known as the *Direct Current (DC)* power flow model is widely being used [27]. Hence, in this work, we also use the DC power flow model for our analysis. This allows us to focus on the complexities of MAD attacks instead of nonlinearity of AC power flows. Nevertheless, the *main ideas* of the algorithms developed in this work can be extended to the AC power flow model as well (e.g., by combining them with the recently introduced convex relaxation methods for solving the AC Optimal Power Flow (ACOPF) problem [28]), albeit not effortlessly.

We represent the power grid by a connected directed graph $G = (V, E)$ where $V = \{1, 2, \ldots, n\}$ and $E = \{e_1, \ldots, e_m\}$ are the set of nodes and edges corresponding to the *buses* and *transmission lines*, respectively (the definition implies $|V| = n$ and $|E| = m$). Each edge e is a set of two nodes $e = (i, j)$. (Direction of the edges are arbitrary.) $\vec{p_d} \geq 0$ and $\vec{p_g} \geq 0$ denote the vector of power demand and supply values, respectively. Accordingly, $\vec{p} = \vec{p_g} - \vec{p_d}$ denotes the vector of total supply and demand values. Since the sum of supply should be equal to the sum of demand,

$$\vec{1}^T \vec{p} = 0, \tag{1}$$

in which $\vec{1}$ is an all ones vector. In the DC model, lines are also assumed to be *purely reactive*, implying that each edge $e = (i, j) \in E$ is characterized by its *reactance* $x_e = x_{ij} > 0$.

Given the power supply/demand vector $\vec{p} \in \mathbb{R}^{n\times 1}$ and the reactance values, the vector of power flows on the lines $\vec{f} \in \mathbb{R}^{m\times 1}$ can be computed by solving the following linear equations:

$$\mathbf{A}\vec{\theta} = \vec{p}, \tag{2}$$

$$\mathbf{Y}\mathbf{D}^T\vec{\theta} = \vec{f}, \tag{3}$$

where $\vec{\theta} \in \mathbb{R}^{n\times 1}$ is the vector of voltage phase angles at nodes, $\mathbf{D} \in \{-1, 0, 1\}^{n\times m}$ is the *incidence matrix* of G defined as,

$$d_{ik} = \begin{cases} 0 & \text{if } e_k \text{ is not incident to node } i, \\ 1 & \text{if } e_k \text{ is coming out of node } i, \\ -1 & \text{if } e_k \text{ is going into node } i, \end{cases}$$

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

$\mathbf{Y} := \mathrm{diag}([1/x_{e_1}, 1/x_{e_2}, \ldots, 1/x_{e_m}])$ is a diagonal matrix with diagonal entries equal to the inverse of the reactance values, and $\mathbf{A} = \mathbf{D}\mathbf{Y}\mathbf{D}^T$ is the *admittance matrix* of G.[1]

Since $\mathbf{A}$ is not a full-rank matrix, we follow [8] and use the *pseudo-inverse* of $\mathbf{A}$, denoted by $\mathbf{A}^+$ to solve (2) as $\vec{\theta} = \mathbf{A}^+\vec{p}$. Once $\vec{\theta}$ is computed, $\vec{f}$ can be computed from (3) as $\vec{f} = \mathbf{Y}\mathbf{D}^T\mathbf{A}^+\vec{p}$. For the convenience of notation, we define $\mathbf{B} := \mathbf{Y}\mathbf{D}^T\mathbf{A}^+$. Hence, $\vec{f} = \mathbf{B}\vec{p}$.

B. Power Grid Operation

Stable operation of the power grid relies on the persistent balance between the power supply and demand. In order to keep the balance between the power supply and the demand, power system operators use weather data as well as historical power consumption data to predict the power demand on a daily and hourly basis [33]. This allows the system operators to plan in advance and only deploy enough generators to meet the demand in the hours ahead without overloading any power lines. This planning ahead consists of two parts: *unit commitment* and *economic dispatch*.

In unit commitment which is mainly performed daily, the grid operator selects a set of generators to *commit* their availability during the day-ahead operation of the grid. But the actual operating points of the generators (i.e., generation outputs) are determined by the operator during the day and in the process known as *economic dispatch*. The main goal of the operator during economic dispatch is to ensure reliable operation of the grid with minimum power generation cost. When feasibility of the power flows is also considered during economic dispatch, the process is also known as *Optimal Power Flow (OPF)* problem. Since in practice feasibility of power flows is always being considered, these two terms can be used interchangeably most of the times.

In this work, we mainly focus on ensuring the robustness of the grid during the economic dispatch. Extending our methods to the unit commitment process is beyond the scope of this paper and is part of the future work. Hence, here we assume that the set of available generators are given. The main challenge is to obtain a favorable operating point for these generators.

1) Optimal Power Flow: In the OPF problem, given the vector of predicted demand values $\vec{p_d}$, the grid operator needs to find the operating point vector $\vec{p_g}$ for the generators such that supply matches the demand (i.e., $\vec{1}^T(\vec{p_g} - \vec{p_d}) = 0$), the operating and physical constraints are satisfied, and the operating cost of the generators are minimized.

In particular, each line f_{ij} has a thermal power flow limit $\overline{f_{ij}}$ limiting the amount of power that a line can *safely* carry. If the power flow on a line goes above this limit (i.e., *overloads*), in most of the cases, it will be tripped by a circuit breaker in order to keep the line from breaking due to overheating. Hence, during the normal operation of the grid

$$|f_{ij}| \leq \overline{f_{ij}}, \quad \forall (i,j) \in E. \tag{4}$$

[1] The admittance matrix $\mathbf{A}$ is also known as the *weighted Laplacian matrix* of the graph [32] in graph theory.

The amount of power that each generator p_{gi} is generating is also limited by a maximum ($\overline{p_{gi}}$) and a minimum ($\underline{p_{gi}}$) value. If there are no generators at node i, then $\overline{p_{gi}} = \underline{p_{gi}} = 0$. Hence,

$$\underline{p_g} \leq \vec{p_g} \leq \overline{p_g}. \tag{5}$$

The generation cost at each generator is a given by a cost function $c_i(x)$ in $\$/hr$. Given these cost functions, the OPF problem can be formulated as follows:

$$\begin{aligned} \min_{\vec{\theta}, \vec{f}, \vec{p_g}} \quad & \textstyle\sum_{l=1}^{n} c_l(p_{gl}), \\ \text{s.t.} \quad & (1), (2), (3), (4), (5), \\ & \vec{p} = \vec{p_g} - \vec{p_d}. \end{aligned} \tag{6}$$

Several methods for finding an optimal solution to (6) depending on the cost functions exist in the literature [27]. Here, we assume that the cost functions are convex and therefore the OPF problem can be solved optimally in polynomial time. *Our main focus in Section V is on how to add additional constraints to the OPF problem to ensure grid robustness against MAD attacks without making the problem nonconvex.*

C. Frequency Control

In power systems, the rotating speed of generators corresponds to the frequency. When demand becomes greater than supply, the rotating speeds of turbine generators' rotors decelerate, and the kinetic energy of the rotors is released into the system in response to the extra demand. Correspondingly, this causes a drop in the system's frequency. This behavior of turbine generators corresponds to Newton's first law of motion and is calculated by the *inertia* of the generators. Similarly, the supply being greater than the demand results in acceleration of the generators' rotors and a rise in the system's frequency.

This decrease/increase in the frequency of the system cannot be tolerated for a long time since frequencies lower than their nominal value severely damage the generators. If the frequency goes above or below a threshold value, protection relays turn off or disconnect the generators completely. Hence, in case of a demand increase, within seconds of the first signs of a decrease in the frequency, the *primary controllers* at generators activate and increase the mechanical input to the generators which increase the speed of the generator's rotor and correspondingly the generator's output and frequency of the system [34]. The rate of decrease/increase in the frequency of the system, before activation of the primary controllers, directly depends on the total *inertia* of the system. Systems with a higher number of rotating generators have higher inertia and therefore are more robust against sudden demand changes or generation losses.

The rate of increase in the output generation of generator i during the primary control is determined by its *governor droop characteristic* denoted by R_i [35, Chapter 9]. In particular, after a change in the total demand by $S_{\Delta p_d}$, the primary controller of each generator i increases its output with rate $1/R_i$ until the total generation is equal to the demand again. In particular, if none of the generators reach their generation limit, each generator i will increase its generation by $1/R_i \times S_{\Delta p_d}/(\sum_{l=1}^{n} 1/R_l)$. The

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

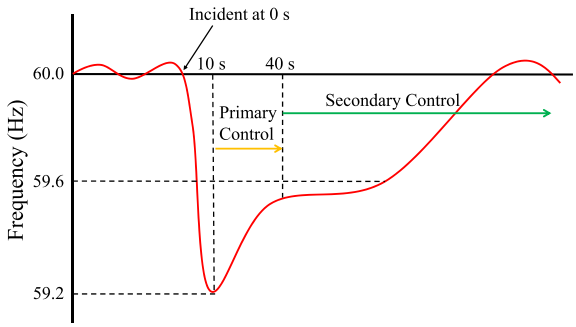

Fig. 2. A sample frequency response of the power grid to a sudden increase in the demand (or loss of generation).

amount of power that generators can provide during the primary control is called the *spinning reserve* of the generators.

Despite the stability of the system's frequency after the primary controllers' response, it may not return to its nominal value (since generators generating more than their generating set points). Hence, the *secondary controller* starts within minutes to restore the system's frequency. The secondary controller modifies the power set points and deploys available extra generators and controllable demands to restore the nominal frequency and permanently stabilizes the system.[2] Fig. 2 presents an example of the way frequency of the system changes after a sudden increase in the demand (or loss of generation) at time 0.

IV. MAD Attacks

In this work, we follow the threat model that we have initially introduced in [3]. In particular, we assume that an adversary has already gained access to an IoT botnet of many high-wattage smart appliances within a city, a country, or a continent. Such access can potentially allow the adversary to increase or decrease the demand at different locations *remotely and synchronously* at a certain time. We call the attacks under this threat model the MAnipulation of the Demand (MAD) attacks.

Since the focus of this work is to develop defenses against MAD attacks rather than dealing with complexities of performing such an attack (as extensively studied in [3]), we abstract the threat model by the adversary's power to manipulate the demands at each node. In particular, we assume the demand changes at node l by an adversary are bounded by $-\overline{\Delta p_{dl}} \leq \Delta p_{dl} \leq \overline{\Delta p_{dl}}$. Notice that from defensive point of view, there are no differences between an adversary with the total knowledge of the system (a.k.a *white-box* attacks) and an adversary with no knowledge of the system (a.k.a *black-box* attacks), since the operator needs to make sure that the grid is robust against *any possible attacks*.

The initial effect of a MAD attack, as described in Section III-C is on the frequency of the system. However, the system operator can make the system robust against frequency disturbances caused by MAD attacks by ensuring that enough generators with inertia and spinning reserve are committed to operate during the unit commitment process [3]. The minimum required inertia and spinning reserve should be computed based on the potential attack size and the properties of the grid. Devices that provide virtual inertia such as batteries, super-capacitors, and flywheels can also be integrated into the system to increase the total inertia [36].

Hence, the main challenge in protecting the grid against the initial effects of MAD attacks is at the hardware level. However, the effects of MAD attacks are not limited to frequency disturbances. Recall from Section III-A that the power flows in power grids are determined uniquely given supply and demand values. Therefore, most of the time, the grid operator does not have any control over the power flows from generators to loads. Once an adversary causes a sudden increase in the loads all around the grid, assuming that the frequency drop is not significant, the extra demand is satisfied automatically by generators through their primary controllers as described in Section III-C. Since the power flows are not controlled by the grid operator at this stage, this change in supply and demand may result in line overloads and consequent line-trippings [3].

If the primary controllers' response results in line overloads, assuming that these overloads can barely be tolerated for a short period of time, these line overloads can be cleared during the secondary control. However, the system operator needs to ensure in advance that possible line overloads can indeed be cleared during the secondary control after any MAD attacks.

In this work, we focus on the effects of MAD attacks on the power flow changes on the lines which are more challenging from the system planning perspective. Our objectives are: (i) to develop algorithms for finding efficient operating points for the generators during the economic dispatch such that no lines are overloaded after the primary control response to any potential MAD attacks, and (ii) to design methods to efficiently examine if line overloads after the primary control–if any–can be cleared during the secondary control.

Notice that we assume the system have enough inertia and reaches a steady-state after the primary controllers' response to a MAD attack (as in Fig. 2). Moreover, since power lines can normally withstand sudden but momentary power surges, in analyzing power flows after a contingency, the transient power flows are usually neglected [27]. Therefore, it is reasonable to use the steady-state power flow equations as described in Section III-A for our analysis.

V. Power Flows: Primary Control

In this section, we provide two algorithms for finding operating points for the generators during the economic dispatch process such that no lines are overloaded after the automatic response of the primary controllers to any MAD attacks. We call such operating points, *robust operating points*.

A. Power Flow Changes

In this subsection, we present a couple of examples in order to demonstrate the complexity of power flow analysis after the *primary controller's response to a MAD attack*.

First, as can be seen in Fig. 3 the relationship between the power flow changes on the lines and the demand changes is

[2] Part of these controls can be done during the *tertiary control*. However, for simplicity and without loss of generality we refer to them as the secondary control.

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

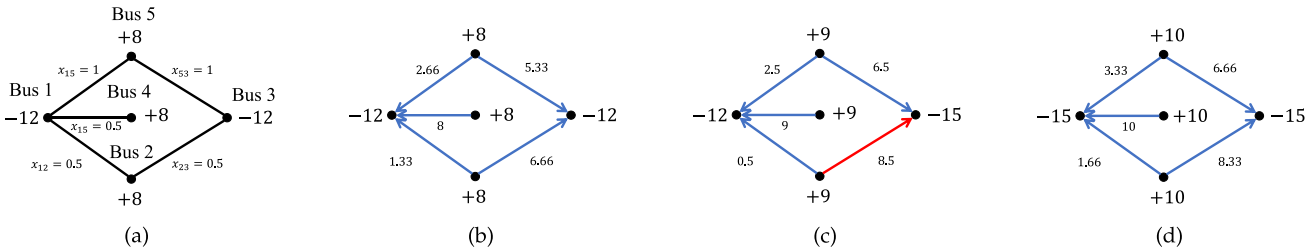

Fig. 3. An example demonstrating that increasing all demands may not necessarily result in the maximum flow on the lines. (a-b) Initial setting and power flows, (c) power flows if demand at bus 3 increases, and (d) power flows if demand at both buses 1 and 3 increases. All generators have the same droop characteristic and they all have enough spinning reserve.

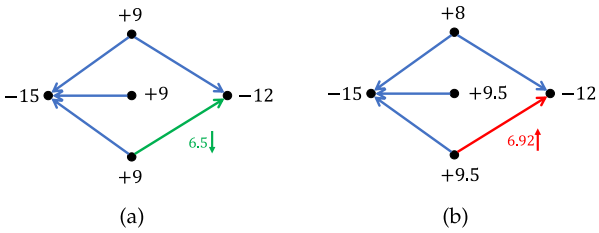

Fig. 4. Dependency of power flow changes on the location of the spinning reserves. (a) If all generators have spinning reserves, demand increase at bus 1 results in power flow decrease on line (2,3). (b) If only generators 2 and 4 have spinning reserves then demand increase at bus 1 results power flow increase on line (2,3).

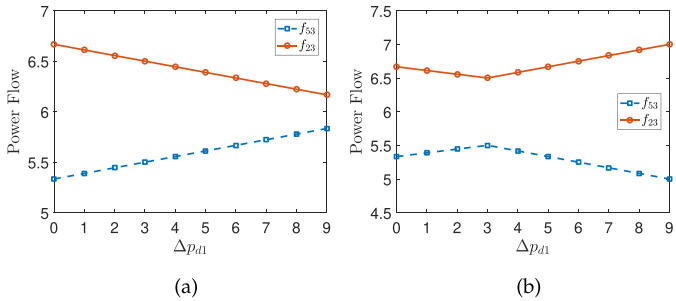

Fig. 5. Power flows on lines (5,3) and (2,3) in the grid shown in Fig. 3(a) as demand at bus 1 increases. (a) If all the generators have enough spinning reserve, and (b) if generator 5 has only 1 unit of spinning reserve.

not intuitive. For example, flow on line (2,3) is maximized when only the demand at node 3 increases (Fig. 3(c)), whereas when demands at both nodes 1 and 3 increase, flow on line (2,3) increases less (Fig. 3(d)).

Another important factor affecting the amount of power flow changes on the lines is the amount of spinning reserve at each generator. For example, as can be seen in Fig. 4, an increase in the demand at node 1 by 3 units may result in power flow *decrease* on line (2,3) if all the generators have enough spinning reserves (Fig. 4(a)). The same scenario, however, results in power flow *increase* on line (2,3), if only generators 2 and 4 have spinning reserves (Fig. 4(b)).

Fig. 5 presents the relationship between power flow changes on lines (2,3) and (5,3) versus power demand increase at node 1 during two different spinning reserve availability scenarios in the grid shown in Fig. 3(a). As can be seen in Fig. 5(a), if all generators have enough spinning reserve the power flows change monotonically with the demand change. However, as can be seen in Fig. 5(b), limited spinning reserve at generator 5 results in a nonlinear relationship between the power flows and the demand change.

Following the examples provided in this subsection, it is clear that power flow changes on the lines after a MAD attack highly depend on the initial operating point of the grid and is a nonlinear problem in most cases. Despite the difficulties, however, in the next two subsections, we provide efficient algorithms for finding efficient and robust operating points for the generators.

B. SAFE Algorithm

In order to avoid line overloads after the primary control response to a potential MAD attack, the grid operator needs to compute the maximum possible power flow changes on the lines following an attack (based on $\overline{\Delta p_{dl}}$ values) and enforce the power flows on the lines in OPF to be below their capacity minus the maximum possible changes. As shown in the previous subsection, however, the maximum power flow changes on the lines depend on the operating point of the generators and their spinning reserve. Therefore, one cannot compute the maximum power flow changes on the lines independent of the operating points to be used in the OPF problem.

One way to circumvent this problem, is to enforce all the generators to have enough spinning reserves to keep the relationship between the power flow changes and demand changes linear (as in Fig. 5(a)), and use this linear relationship to compute the maximum power flow changes on the lines based on the operating point of the generators. These values can then be added to the OPF problem without making the problem nonlinear and nonconvex. Recall that since here we use DC power flows with convex cost functions, the OPF problem is convex. Hence, when we mention the nonconvexity of the problem, it is due to additional constraints on the power flows.

For each load i, define $\vec{v}_i = [v_{i1}, v_{i2}, \ldots, v_{in}]^T$ to denote the primary controllers' response to a unit demand increase at load i. If all generators have enough spinning reserve, each generator j will increase its generation by $v_{ij} := (1/R_j)/(\sum_{l=1}^{n} 1/R_l)$ to compensate for a unit demand increase at node i (as described in Section III-C). Hence, by defining $\vec{w}_i := \vec{v}_i - \vec{e}_i$ (recall from Section III that $\vec{e}_i$ is the i^{th} fundamental basis of $\mathbb{R}^n$) one can compute the change in the flow of line $e = (i, j)$ solely in terms of changes in the demands (Δp_{di}s):

$$\Delta f_{ij} = 1/x_{ij}(\mathbf{A}_i^+ - \mathbf{A}_j^+) \sum_{l=1}^{n} \Delta p_{dl} \vec{w}_l. \tag{7}$$

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

Recall that $-\overline{\Delta p_{dl}} \leq \Delta p_{dl} \leq \overline{\Delta p_{dl}}$ based on the grid operator's estimation of the adversary's power. Hence, the maximum flow change on line (i,j) can be computed using (7) as:

$$\Delta f_{ij}^{\max} = 1/x_{ij} \sum_{l=1}^{n} \overline{\Delta p_{dl}} |(\mathbf{A}_i^+ - \mathbf{A}_j^+)\vec{w}_l|, \tag{8}$$

since for each l, Δp_{dl} can be selected by the adversary to be equal to $-\overline{\Delta p_{dl}}$, if $(\mathbf{A}_i^+ - \mathbf{A}_j^+)^T \vec{w}_l < 0$, and equal to $\overline{\Delta p_{dl}}$, if $(\mathbf{A}_i^+ - \mathbf{A}_j^+)\vec{w}_l \geq 0$. Now, to ensure that no lines are overloaded after a MAD attack, all the system operator needs to do is to replace the capacity of each line (i,j) in the OPF problem by $\overline{f_{ij}} - \Delta f_{ij}^{\max}$. The only other constraint that needs to be added to the OPF problem is to make sure that each generator i with $0 < 1/R_i$ has enough spinning reserve to increase its generation according to its governor droop. For this, define $\overline{S_{\Delta p_d}} := \sum_{l=1}^{n} \overline{\Delta p_{dl}}$. Hence, each generator's operating point should be within the following limits:

$$\begin{aligned} &\forall 1 \leq i \leq n: \\ &\underline{p_{gi}} + \frac{1/R_i}{\sum_{l=1}^{n} 1/R_l} \overline{S_{\Delta p_d}} \leq p_{gi} \leq \overline{p_{gi}} - \frac{1/R_i}{\sum_{l=1}^{n} 1/R_l} \overline{S_{\Delta p_d}}. \end{aligned} \tag{9}$$

Therefore, the robust OPF problem can be written as follows:

$$\begin{aligned} \min_{\vec{\theta},\vec{f},\vec{p_g}} \quad & \textstyle\sum_{l=1}^{n} c_l(p_{gl}), \\ \text{s.t.} \quad & (1),(2),(3),(8),(9), \\ & |f_{ij}| \leq \overline{f_{ij}} - \Delta f_{ij}^{\max}, \quad \forall (i,j) \in E \\ & \vec{p} = \vec{p_g} - \vec{p_d}. \end{aligned} \tag{10}$$

We call the algorithm for finding a robust operating point for generators by limiting their operating points—to be able to analytically compute $\Delta f_{ij}^{\max}$s—and solving (10), the Securing Additional margin For generators in Economic dispatch (SAFE) Algorithm. Since this algorithm limits the operating points of the generators by adding conditions (9) to the OPF problem, it is obvious that it may not obtain the *minimum cost* robust operating points for the generators. In the next subsection, we provide an algorithm, albeit computationally more expensive, for finding robust operating points for the generators without limiting their operating points—as in (9).

C. IMMUNE Algorithm

In (7), we assumed that none of the generators reach their maximum/minimum capacity as they increase/decrease their generation according to their droop characteristics. However, by allowing some generators to reach their maximum/minimum capacity, one may find robust operating points for the generators with a lower cost.

In this subsection, for brevity and to avoid repetition, we assume that the total demand change $S_{\Delta p_d} := \sum_{i=1}^{n} \Delta p_{di}$ can only be positive. Hence, we focus mainly on the generators' maximum capacity. However, the same set of equations can similarly be derived for the case $S_{\Delta p_d} < 0$ which should also be considered separately in computing the maximum power flow changes on the lines. In particular, whenever there is a minimization/maximization problem with $S_{\Delta p_d} \geq 0$ constraint, one should also solve a similar optimization problem with $S_{\Delta p_d} < 0$ and take the minimum/maximum of the optimal value of the two optimization problems. In Section VIII, we consider both cases for numerical evaluations.

Once a generator reaches its maximum capacity, it cannot increase its generation anymore, and therefore other generators should generate more to compensate for the extra demand. The following lemma provides the amount each generator generates based on its spinning reserve and governor droop characteristic to compensate for the extra demand after a MAD attack.

Lemma 1. Suppose generators are ordered such that if $i < j$, $R_i(\overline{p_{gi}} - p_{gi}) \leq R_j(\overline{p_{gj}} - p_{gj})$. Define $t_i := R_i(\overline{p_{gi}} - p_{gi})$ and $S_i := \sum_{l=1}^{i} t_l/R_l + \sum_{l=i+1}^{n} t_i/R_l$. If $S_i < S_{\Delta p_d} \leq S_{i+1}$, to compensate for the extra demand, generators 1 to i reach their maximum capacity and each generator $j > i$ generates $\frac{1/R_j}{\sum_{l=i+1}^{n} 1/R_l}\big(S_{\Delta p_d} - \sum_{l=1}^{i}(\overline{p_{gl}} - p_{gl})\big)$.

In general, as demonstrated in Figs. 4 and 5, due to power generation limits, power flow on a line may not change monotonically as demand changes in a specific node–as in (7). Hence, the maximum change in the power flows cannot be found in a closed form as in (8). However, one may be able to find an upper bound on the maximum power flow change on a line.

Upper bounds on the maximum power flow changes after a MAD attack can be computed by assuming the worst case initial operating points and also assuming that generators can be arbitrarily assigned to provide extra required generation. In particular, an upper bound $\widehat{\Delta f_{ij}}$ for the power flow changes on line (i,j) can be computed by finding the worst initial operating points for the generators $\vec{p_g}$ and the worst possible way to increase the power generations $\Delta\vec{p_g}$ (in oppose to the automatic primary controller's response) in response to the worst possible way to increase the demands by an adversary $\Delta\vec{p_d}$ as follows:

$$\begin{aligned} \widehat{\Delta f_{ij}} := \quad \max_{\vec{p_g},\Delta\vec{p_d},\Delta\vec{p_g}} \quad & \Big|1/x_{ij}(\mathbf{A}_i^+ - \mathbf{A}_j^+)(\Delta\vec{p_g} - \Delta\vec{p_d})\Big| \\ \text{s.t.} \quad & \vec{1}^T(\vec{p_g} - \vec{p_d}) = 0, \\ & \vec{1}^T(\Delta\vec{p_g} - \Delta\vec{p_d}) = 0, \\ & -\overline{\Delta p_{dl}} \leq \Delta p_{dl} \leq \overline{\Delta p_{dl}}, \quad 1 \leq l \leq n \\ & \underline{p_g} \leq \vec{p_g} \leq \overline{p_g}, \\ & \overline{0} \leq \Delta p_{gl} \leq \overline{p_{gl}} - p_{gl}, \quad 1 \leq l \leq n, \\ & S_{\Delta p_d} \geq 0. \end{aligned} \tag{11}$$

Optimization (11) is a Linear Program (LP) that can be solved efficiently for each line (i,j). Using these upper bounds, we can limit the power flows on the lines in the OPF problem (6) as $|f_{ij}| \leq \overline{f_{ij}} - \widehat{\Delta f_{ij}}$ to leave enough margin for the lines in case of a MAD attack. Hence, the solution to the following modified OPF problem provides robust operating points for the generators:

$$\begin{aligned} \min_{\vec{\theta},\vec{f},\vec{p_g}} \quad & \textstyle\sum_{l=1}^{n} c_l(p_{gl}), \\ \text{s.t.} \quad & (1),(2),(3),(5), \\ & |f_{ij}| \leq \overline{f_{ij}} - \widehat{\Delta f_{ij}}, \quad \forall (i,j) \in E \\ & \vec{p} = \vec{p_g} - \vec{p_d}. \end{aligned} \tag{12}$$

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

Enforcing the power flows on all the lines, such as (i,j), to be less than $\overline{f_{ij}} - \widehat{\Delta f_{ij}}$ as in (12) ensures that none of the lines will be overloaded after a potential MAD attack. However, the solution to (12) may not provide the optimal robust operating points for the generators since $\widehat{\Delta f_{ij}}$s only provide an upper bound on the maximum power flow changes on the lines. To achieve more efficient robust operating points, we introduce an iterative algorithm that solves the OPF problem and updates the lines' required safety margins to ensure that none of the lines get overloaded after a MAD attack. We will then use the upper bounds $\widehat{\Delta f_{ij}}$s to prove that the algorithm will converge to a local optimal solution.

First, given the operating points $p_{g1},\ldots,p_{gn}$ to the OPF problem, the maximum power flow change on line (i,j) (denoted by $\Delta f_{ij}^{\max}$) after an attack can be computed based on the power flow solution $\vec{f} = \mathbf{Y}\mathbf{D}^T\mathbf{A}^+\vec{p}$ by solving the following optimization problem:

$$\begin{aligned}\Delta f_{ij}^{\max} = \max_{\vec{\Delta p_d}} \quad & \operatorname{sgn}(f_{ij})\Big(1/x_{ij}\textstyle\sum_{l=1}^{n} -\Delta p_{dl}(a_{il}^{+}-a_{jl}^{+}) \\ & +1/x_{ij}\textstyle\sum_{l=1}^{n} f_l(S_{\Delta p_d})(a_{il}^{+}-a_{jl}^{+})\Big) \\ \text{s.t.} \quad & -\overline{\Delta p_{dl}} \le \Delta p_{dl} \le \overline{\Delta p_{dl}}, \quad 1 \le l \le n \\ & S_{\Delta p_d} \ge 0.\end{aligned} \tag{13}$$

in which $f_l(\cdot)$s denote piecewise linear functions that determine the extra output of the generators based on the total demand change $S_{\Delta p_d}$. Since we assumed that $p_{g1},\ldots,p_{gn}$ are given, functions $f_l(\cdot)$ can be uniquely determined using Lemma 1. $\operatorname{sgn}(f_{ij})$ in the objective of (13) is to ensure that the maximum changes are in the direction of *increase* in the power flow on line (i,j). Hence, for all lines $\Delta f_{ij}^{\max} \ge 0$.[3]

Lemma 2. Optimization (13) can be solved in polynomial time for each $(i,j) \in E$.

Proof. Without loss of generality, assume that generators are ordered such that $t_1 \le t_2 \le \ldots \le t_n$ as defined in Lemma 1. It is easy to see that by using Lemma 1 and defining $S_0 := 0$, one can solve (13) in different linear regions of $f_l(\cdot)$s by considering additional conditions for $S_{\Delta p_d}$ (for $0 \le z < n$):

$$S_z \le S_{\Delta p_d} < S_{z+1}. \tag{14}$$

Under condition (14), $f_l(\cdot)$s can be determined as follows:

$$f_l(S_{\Delta p_d}) = \begin{cases} \overline{p_l} - p_l & l \le z, \\ \dfrac{1/R_l\left(S_{\Delta p_d} - \sum_{w=1}^{z}(\overline{p_w}-p_w)\right)}{\sum_{w=z+1}^{n} 1/R_w} & l > z. \end{cases} \tag{15}$$

Hence, all the $f_l(\cdot)$ are either constant or linear functions in (13) and therefore (13) can be solved efficiently using LP. Hence, by solving (13) at most n times (once for every condition (14) for different z) $\Delta f_{ij}^{\max}$ can be found in polynomial time. ■

[3] Notice that for computing the maximum power flow changes on the lines, the $S_{\Delta p_d} < 0$ case should also be considered separately to see if it results in a larger power flow change than the one obtained from (13). However, as we mentioned at the beginning of the subsection, here we only consider $S_{\Delta p_d} \ge 0$ for the brevity of presentation.

Algorithm 1 Iteratively MiniMize and boUNd Economic dispatch (IMMUNE)

Input: G

1: flag = 1
2: Define $c_{ij} := \overline{f_{ij}}$ for all $(i,j) \in E$
3: **while** flag **do**
4: Solve the OPF problem (6) such that $\forall (i,j) \in E : |f_{ij}| \le c_{ij}$
5: **if** OPF is not feasible **then**
6: **return** none
7: Compute $\Delta f_{ij}^{\max}$ by solving (13) for all $(i,j) \in E$
8: flag = 0
9: **for** $(i,j) \in E$ **do**
10: **if** $\overline{f_{ij}} < |f_{ij}| + \Delta f_{ij}^{\max}$ **then**
11: $c_{ij} = \overline{f_{ij}} - \Delta f_{ij}^{\max}$
12: flag = 1
13: **return** $p_{g1}, p_{g2}, \ldots, p_{gn}$

After computing $\Delta f_{ij}^{\max}$ values, one can use them to verify if any of the lines will be overloaded after an attack (e.g., by checking if $\overline{f_{ij}} < |f_{ij}| + \Delta f_{ij}^{\max}$). If yes, then update the required margins for the lines that may get overloaded in the OPF problem to ensure that those lines will not be overloaded. The OPF problem can then be solved again with new power flow margins for the lines and the process continues until no additional updates for the line margins are required at the obtained operating point (which means that the obtained operating point is robust). We call this algorithm Iteratively MiniMize and boUNd Economic dispatch (IMMUNE) Algorithm (summarized in Algorithm 1).

Lemma 3. If (12) is feasible, then the IMMUNE Algorithm converges to a local optimum solution.

Lemma 3 provides a sufficient condition such that the IMMUNE Algorithm converges to a local optimum. However, even if (12) is not feasible, the system operator can still run the IMMUNE Algorithm to obtain a local optimum solution if the OPF problem remains feasible at each iteration of the algorithm.

We can also provide an upper bound on the number of iterations that IMMUNE algorithm requires to converge. For this reason, the algorithm needs to change discrete changes to the capacities at each iteration.

Lemma 4. If the IMMUNE Algorithm changes c_{ij} at each iteration by a discrete amount such as $c_{ij} = \max\{\lfloor \overline{f_{ij}} - \Delta f_{ij}^{\max} \rfloor, \overline{f_{ij}} - \widehat{\Delta f_{ij}}\}$, then it terminates in at most $O(\sum_{(i,j)\in E} \lceil \widehat{\Delta f_{ij}} \rceil)$ iterations.

Corollary 1. If generators' cost functions are linear and $\mathcal{F}(n)$ indicates the running time of the LP solver of choice with n variables (e.g., simplex or ellipsoid algorithms), the IMMUNE Algorithm terminates in $O(m\mathcal{F}(n)(\sum_{(i,j)\in E} \lceil \widehat{\Delta f_{ij}} \rceil))$.

Following a similar idea, one can decrease the running time of the IMMUNE algorithm by applying more aggressive update rules for the capacities in line 11 of the algorithm. For example, line 11 can be replaced by $c_{ij} = 0.9(\overline{f_{ij}} - \Delta f_{ij}^{\max})$ or $c_{ij} = 0.95(\overline{f_{ij}} - \Delta f_{ij}^{\max})$. We call these variations of the IMMUNE Algorithm, IMMUNE-0.9, and IMMUNE-0.95. In Section VIII-B, we numerically evaluate and compare the performance of these algorithms and demonstrate that more aggressive update rules result in faster convergence.

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

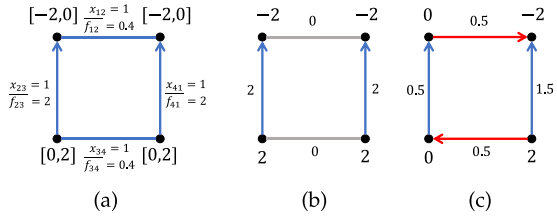

Fig. 6. Complexity of secondary controller problem. (a) Secondary controller problem setting, (b) an attack that maximizes the demand, and (c) an attack that minimizes the demand at one node and maximizes the demand at another node.

One favorable property of the IMMUNE Algorithm is that it can be easily parallelized. This parallelization can be used to simultaneously compute $\Delta f_{ij}^{\max}$ for all the lines at each iteration in order to expedite the algorithm.

If the OPF problem becomes infeasible in any iteration of the IMMUNE Algorithm, there are two ways to circumvent the issue: (i) By considering higher temporary limits for the lines (e.g., $1.1\overline{f_{ij}}$) which is a common practice in power systems operation, but the operator needs to ensure that line overloads can be cleared during the secondary control, or (ii) by returning to the unit commitment problem and change the list of committed generators to make sure (12) is feasible. We will address the first approach in the next section in detail. However, the second approach is beyond the scope of this paper and is part of our future work.

VI. Power Flows: Secondary Control

In cases that primary control cannot prevent line overloads, the system operator has to clear these overloads during the secondary control instead. In such cases, the operator needs to make sure in advance that after the primary control's response to a MAD attack, there are operating points for the generators such that the demand can be supplied with no line overloads (i.e., the secondary controller can clear the overloads). Assuming that the maximum and minimum reachable demands at node i by an adversary are $\overline{p_{di}}$ and $\underline{p_{di}}$, respectively, this problem can be defined as the *secondary controller problem*:

Secondary controller problem: For any $p_{d1}, p_{d2}, \ldots, p_{dn}$ that $\forall 1 \leq i \leq n : \underline{p_{di}} \leq p_{di} \leq \overline{p_{di}}$, are there operating points $p_{g1}, \ldots, p_{gn}$ for the generators such that $\forall 1 \leq i \leq n : \underline{p_{gi}} \leq p_{gi} \leq \overline{p_{gi}}$, $\vec{1}^T(\vec{p_g} - \vec{p_d}) = 0$, and no lines are overloaded?

Definition 1. A grid is called *secondary controllable* if the answer to the secondary controller problem is yes.

Notice that *operating cost of the generators are not important during the secondary control* since the secondary controller activates only after a potential attack and the operator needs to bring back the grid to its normal state as soon as possible at any cost. Fig. 6 provides an example of the secondary controller problem. As can be seen in Fig. 6(b), when the demands are all equal to their maximum level after a MAD attack, the demand can be supplied by generators with no line overloads. However, as presented in Fig. 6(c), when the demand is increased to its maximum level at one node and decreased to its minimum at another one, there is no possible way to supply the demand such that no lines are overloaded. This example clearly evinces that the secondary controller problem is not intuitive.

In the following subsections, we study the secondary controller problem in detail and provide efficient algorithms to verify the secondary controllability of a power system.

A. Maxmin Formulation

One way of verifying the secondary controllability of a power system is by exploiting *linear bilevel programs* [37], [38]. The secondary controller problem can be written in the form of a max-min linear problem which is a special form of *linear bilevel programs* as follows:

$$\begin{aligned} \max_{\vec{p_d}} \min_{\vec{p_g},\vec{q},\vec{f},\vec{\theta}} \quad & \vec{1}^T\vec{q} \\ \text{s.t.} \quad & (1),(2),(3),(4),(5), \\ & \vec{p} = \vec{p_g} - \vec{p_d} + \vec{q}, \\ & q_i \geq 0, \quad 1 \leq i \leq n \\ & \underline{p_{di}} \leq p_{di} \leq \overline{p_{di}}, \quad 1 \leq i \leq n. \end{aligned} \tag{16}$$

In optimization problem (16), vector $\vec{p_d}$ should be selected such that for the best possible selection of vector $\vec{p_g}$ and positive auxiliary vector $\vec{q}$, the objective value is maximized. The following proposition relates the solution of (16) to the secondary controller problem.

Proposition 1. The optimal solution of (16) is 0 if, and only if, the grid is secondary controllable.

Proof. If the optimal solution to (16) is 0, then for any demand vector $\vec{p_d}$, the vector of generation values $\vec{p_g}$ can be selected such that $\vec{1}^T(\vec{p_g} - \vec{p_d}) = 0$ and no lines are overloaded. Hence, the grid is secondary controllable. Now if the grid is secondary controllable, then for all demand vectors $\vec{p_d}$, there exists a vector of generation $\vec{p_g}$ such that $\vec{1}^T(\vec{p_d} - \vec{p_d}) = 0$ and no lines are overloaded. Hence, the auxiliary vector $\vec{q}$ can be selected to be equal to 0 by the minimization part of (16) for any vector $\vec{p_d}$. Therefore, the optimal solution to (16) would be 0. ∎

Proposition 1 clearly demonstrates that solving (16) can determine secondary controllability of a power system. Moreover, when the optimal solution of (16) is greater than 0, the nonzero entries of the optimal vector $\vec{q}$ can reveal the minimum extra generation required to ensure secondary controllability of the system.

Despite many advantages of the formulation (16), the max-min linear program is nonconvex [39] and proved to be NP-hard [40]. Therefore existing efficient algorithms for solving (16) only obtain local optimal solutions [38]. However, a local optimal solution of (16) with value 0 does not guarantee the secondary controllability of the system since the optimal solution may not be zero.

One way of solving (16) optimally, albeit in exponential running time, is through brute force search. Following lemma demonstrates that to solve the secondary controller problem, one needs to check only the extreme demand points due to the convexity of the space of all possible demand values and linearity of power flow equations.

Lemma 5. The grid is secondary controllable, if and only if for all $p_{d1}, \ldots, p_{dn}$ such that $p_{di} \in \{\overline{p_{di}}, \underline{p_{di}}\}$ there exist operating

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

points $p_{g1}, \ldots, p_{gn}$ for the generators such that $\forall 1 \leq i \leq n$: $\underline{p_{gi}} \leq p_{gi} \leq \overline{p_{gi}}$, $\vec{1}^T(\vec{p_g} - \vec{p_d}) = 0$, and no lines are overloaded.

On the other hand, for a given demand vector $\vec{p_d}$, it can be verified in polynomial time whether there exist operating points for the generators that satisfy the secondary controller problem by solving the minimization part of (16) using LP:

$$\begin{aligned} \min_{\vec{p_g},\vec{q},\vec{f},\vec{\theta}} \quad & \vec{1}^T\vec{q} \\ \text{s.t.} \quad & (1),(2),(3),(4),(5), \\ & \vec{p} = \vec{p_g} - \vec{p_d} + \vec{q} \\ & q_i \geq 0, \quad 1 \leq i \leq n. \end{aligned} \tag{17}$$

If the optimum solution to (17) is not 0, then the optimal vector $\vec{q}$ can be used by the operator to make more generators online for controllability of the grid. Hence by solving (17) for all extreme demand vectors, one can verify secondary controllability of a system in *exponential running time* and also find how to make it controllable–if it is not–based on obtained vectors $\vec{q}$.

By focusing only on nodes with the largest demands, one can approximately verify if for a subset of extreme points there exist operating points for the generators satisfying the secondary controller problem. In general, however, such an approach may not be able to guarantee the secondary controllability of a grid. Hence, in the next subsection, we provide *sufficient conditions* to ensure secondary controllability of a grid in polynomial time.

B. Predetermined Secondary Controllers

Despite the difficulty in exact determination of secondary controllability of a grid, in this subsection, we introduce and exploit suboptimal predetermined controllers to verify controllability of a grid *with no false positives* (i.e., presented methods cannot determine *uncontrollability* of a system).

In order to verify secondary controllability of the grid, one can find *the best* predetermined way to set the generation values given a demand vector $\vec{p_d}$ such that the maximum power flows over all demand vectors is minimized. In particular, we define the $\vec{\beta}$-determined controller as follows.

Definition 2 ($\vec{\beta}$-determined controller). For any demand vector $\vec{p_d}$, set $\vec{p_g} = (\sum_{i=1}^{n} p_{di}) \times \vec{\beta}$, for a vector $\vec{\beta}$ satisfying:

(i) $\vec{\beta} \geq 0$,
(ii) $\vec{1}^T\vec{\beta} = 1$,
(iii) $(\sum_{i=1}^{n} \overline{p_{di}}) \times \vec{\beta} \leq \overline{p_g}$,
(iv) $(\sum_{i=1}^{n} \underline{p_{di}}) \times \vec{\beta} \geq \underline{p_g}$.

Definition 3. A controller is called *reliable*, if for all feasible demand vectors $\vec{p_d}$, it provides a vector of operating points for the generators like $\vec{p_g}$ such that $|\vec{f}| = |\mathbf{B}(\vec{p_g} - \vec{p_d})| \leq \overline{f}$.

Proposition 2. If there exists a vector $\vec{\beta}$ such that the $\vec{\beta}$-determined controller is reliable, then the grid is secondary controllable.

For a vector $\vec{\beta}$ satisfying conditions (i-iv) in Definition 2, define vectors $\vec{w_i}^{(\beta)} := -\vec{e_i} + \vec{\beta}$ for $1 \leq i \leq n$ (as in Section V-B). The following lemma proves that maximum flow on the lines over all feasible demand vectors, given a $\vec{\beta}$-determined controller, can deterministically be computed.

Lemma 6. Given a $\vec{\beta}$-determined controller, the maximum power flow on each line e_k over all possible demand vectors is:

$$\begin{aligned} \max_{\underline{p_d} \leq \vec{p_d} \leq \overline{p_d}} |f_k| = & \left| \sum_{i=1}^{n} \frac{(\overline{p_{di}} + \underline{p_{di}})}{2} \mathbf{B}_k \vec{w_i}^{(\beta)} \right| \\ & + \sum_{i=1}^{n} \frac{(\overline{p_{di}} - \underline{p_{di}})}{2} |\mathbf{B}_k \vec{w_i}^{(\beta)}|. \end{aligned} \tag{18}$$

The main question is now whether there exists a vector $\vec{\beta}$ such that the maximum power flows as determined in (18) are less than their capacities? We prove that one can examine this efficiently and in polynomial time by solving the following optimization:

$$\begin{aligned} \min_{\eta,\vec{\beta},\vec{f}} \quad & \eta \\ \text{s.t.} \quad & \text{(i-iv) in Definition 2}, \\ & \vec{f} = |\mathbf{B}\mathbf{W}^{(\beta)}(\overline{p_d} + \underline{p_d})/2| + |\mathbf{B}\mathbf{W}^{(\beta)}|(\overline{p_d} - \underline{p_d})/2, \\ & \vec{f} \leq \eta\overline{f}, \end{aligned} \tag{19}$$

in which matrix $\mathbf{W}^{(\beta)} := [\vec{w_1}^{(\beta)}, \ldots, \vec{w_n}^{(\beta)}]$. The following proposition demonstrates that (19) can be solved using LP in polynomial time. Moreover, it indicates that the optimal solution to (19) can provide the best vector $\vec{\beta}$ for deterministically controlling the grid and its optimal value demonstrates if the corresponding $\vec{\beta}$-determined controller is reliable.

Proposition 3. Optimization (19) can be solved using LP. Moreover, if the optimal value η^* to (19) is less than or equal to 1, then the $\vec{\beta}^*$-determined controller obtained from the corresponding solution is reliable, and therefore the grid is secondary controllable.

From (18), it can be seen that the formula for computing maximum flow on the lines consists of two separate sums which can be controlled by different vectors and obtained a better controller. Hence, one can define the $(\vec{\gamma}, \vec{\beta})$-determined controller as follows.

Definition 4 ($(\vec{\gamma}, \vec{\beta})$-determined controller). For any demand vector $\vec{p_d}$, set $\vec{p_g} = (\sum_{i=1}^{n}(\overline{p_{di}} + \underline{p_{di}})/2) \times \vec{\gamma} + (\sum_{i=1}^{n}(p_{di} - \overline{p_{di}}/2 - \underline{p_{di}}/2)) \times \vec{\beta}$, for vectors $\vec{\gamma}$ and $\vec{\beta}$ satisfying:

(i) $\vec{\beta}, \vec{\gamma} \geq 0$,
(ii) $\vec{1}^T\vec{\gamma} = \vec{1}^T\vec{\beta} = 1$,
(iii) $(\sum_{i=1}^{n}(\overline{p_{di}} + \underline{p_{di}})/2) \times \vec{\gamma} + (\sum_{i=1}^{n}(\overline{p_{di}} - \underline{p_{di}})/2) \times \vec{\beta} \leq \overline{p_g}$,
(iv) $(\sum_{i=1}^{n}(\overline{p_{di}} + \underline{p_{di}})/2) \times \vec{\gamma} + (\sum_{i=1}^{n}(-\overline{p_{di}} + \underline{p_{di}})/2) \times \vec{\beta} \geq \underline{p_g}$.

The $(\vec{\gamma}, \vec{\beta})$-determined controller generalizes the $\vec{\beta}$-determined controller (just set $\vec{\gamma} = \vec{\beta}$) and it is easy to see that the maximum power flow on the lines over all demand vectors, given a $(\vec{\gamma}, \vec{\beta})$-determined controller can be computed similarly to (18) as follows:

$$\begin{aligned} \max_{\underline{p_d} \leq \vec{p_d} \leq \overline{p_d}} |f_k| = & \left| \sum_{i=1}^{n} \frac{(\overline{p_{di}} + \underline{p_{di}})}{2} \mathbf{B}_k \vec{w_i}^{(\gamma)} \right| \\ & + \sum_{i=1}^{n} \frac{(\overline{p_{di}} - \underline{p_{di}})}{2} |\mathbf{B}_k \vec{w_i}^{(\beta)}|. \end{aligned} \tag{20}$$

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

Optimal $(\vec{\gamma},\vec{\beta})$-determined controller can be found similar to the optimal $\vec{\beta}$-determined controller using an optimization similar to (19) with a few small changes:

$$\begin{aligned} \min_{\eta,\vec{\gamma},\vec{\beta},\vec{f}} \quad & \eta \\ \text{s.t.} \quad & \text{(i-iv) in Definition 4,} \\ & \vec{f} = |\mathbf{BW}^{(\gamma)}(\overline{p_d}+\underline{p_d})/2| + |\mathbf{BW}^{(\beta)}|(\overline{p_d}-\underline{p_d})/2, \\ & \vec{f} \le \eta \overline{f}. \end{aligned} \tag{21}$$

Again, as in the $\vec{\beta}$-determined controller case, the optimal value of (21) determines if the optimal $(\vec{\gamma},\vec{\beta})$-determined controller is reliable or not. Hence, the grid operator can use (21) to efficiently determine the secondary controllability of the grid, albeit obtaining false negatives in some cases.

In Section VIII, we numerically evaluate the performance of the controllers introduced in this section. Before that, however, we demonstrate that these controllers can be used to efficiently provide lower bounds on the maximum scale of a MAD attack for which the grid remains secondary controllable.

VII. αD-ROBUSTNESS

Power grids are required to withstand single equipment failures (e.g., lines, generators, and transformers) with no interruptions in their operation (a.k.a. $N-1$ standard) [27]. Following $N-1$ standard, we define a new standard for the grid operation to ensure its robustness against MAD attacks called αD standard. It requires grid operators to either prevent line overloads (as in Section V) or be able to clear them (as in Section VI) after a MAD attack by an adversary that can change the demands by at most α fraction at each node.[4] We call a grid that conforms with this standard, αD-robust.

In this section, for a given grid, we are interested in finding the maximum α such that the grid is αD-robust. We denote this value by $\alpha^{\max}$. Since ensuring that line overloads can be cleared during the secondary control is less restrictive than preventing them after the primary control, *we mainly focus on finding the maximum α such that the grid is αD-robust based on its ability to clear line overloads after the secondary control (i.e., grid's secondary controllability).*

As we described in the previous section, verifying the secondary controllability of the grid for a given upper and lower limits on the demands is hard. Hence, we cannot expect to find the $\alpha^{\max}$ efficiently. Nevertheless, in the next two subsections, we develop efficient methods for obtaining upper and lower bounds on $\alpha^{\max}$.

A. Upper Bound

Assume $\vec{p_d}^{\dagger}$ denotes the vector of predicted demand values. For a given α, the demand vector $\vec{p_d}$ resulted by a MAD attack will be bounded by $(1-\alpha)\vec{p_d}^{\dagger} \le \vec{p_d} \le (1+\alpha)\vec{p_d}^{\dagger}$. Now if a grid is αD-robust, it should particularly be robust against the maximum demand attack. Hence, finding the maximum α for which the grid can handle the maximum demand attack provides an upper bound for $\alpha^{\max}$. Such α can be found efficiently by an LP:

$$\begin{aligned} \max_{\alpha,\vec{p_d},\vec{p_g},\vec{f},\vec{\theta}} \quad & \alpha \\ \text{s.t.} \quad & (1),(2),(3),(4),(5), \\ & \vec{p_d} = (1+\alpha)p_d^{\dagger}, \\ & \vec{p} = \vec{p_g} - \vec{p_d}. \end{aligned} \tag{22}$$

Proposition 4. Assume $\hat{\alpha}$ denotes the optimal value of (22), then $\alpha^{\max} \le \hat{\alpha}$.

The optimal value of (22) provides a good upper bound for $\alpha^{\max}$ and can be computed efficiently. One can also consider $\vec{p_d} = (1-\alpha)p_d^{\dagger}$ to obtain another upper bound. However, if we set $\vec{p_d} = (1-\alpha)p_d^{\dagger}$ in (22) instead of $\vec{p_d} = (1+\alpha)p_d^{\dagger}$, it is easy to see that its optimal solution will be $\alpha = 1$. Hence, the case of $\vec{p_d} = (1-\alpha)p_d^{\dagger}$ only provides a trivial upper bound of $\alpha^{\max} \le 1$ (assuming $\underline{p_g} = 0$).

In the next subsection, we provide algorithms to find lower bounds for α based on the controllers developed in Section VI-B.

B. Lower Bound

To find a lower bound for $\alpha^{\max}$, we use the controllers in Section VI-B to limit the secondary controller's ability to change the generators' operating points. Limiting the secondary controller's ability allows us to efficiently approximate the maximum α, but because of this limitation, we only obtain lower bounds for $\alpha^{\max}$.

First, assume that we limit the secondary controller to the $\vec{\beta}$-controller for a fixed $\vec{\beta}$. We show that in this case the maximum α can be found by solving a single LP. Assume $\vec{p_g}^*$ is the optimal solution to (22) with value $\hat{\alpha}$ and set $\vec{\beta} = \vec{p_g}^*/\|\vec{p_g}^*\|_1$ (i.e., the controller only scales down the generation compared to the maximum demand case). Using (18), we show that the optimal value of the following LP gives a lower bound for $\alpha^{\max}$:

$$\begin{aligned} \max_{\alpha,\vec{f}} \quad & \alpha \\ \text{s.t.} \quad & (1+\alpha)(\textstyle\sum_{i=1}^{n} p_{di}^{\dagger}) \times \vec{\beta} \le \overline{p_g}, \\ & (1-\alpha)(\textstyle\sum_{i=1}^{n} p_{di}^{\dagger}) \times \vec{\beta} \ge \underline{p_g}, \\ & \vec{\beta} = \vec{p_g}^*/\|\vec{p_g}^*\|_1, \\ & \vec{f} = |\mathbf{BW}^{(\beta)}\vec{p_d}^{\dagger}| + |\mathbf{BW}^{(\beta)}|(\alpha\vec{p_d}^{\dagger}), \\ & |f_{ij}| \le \overline{f_{ij}}, \quad \forall (i,j) \in E. \end{aligned} \tag{23}$$

Proposition 5. The optimal solution α^* of (23) can be found in polynomial time using LP. Moreover, $\alpha^* \le \alpha^{\max}$.

Optimization (23) allows us to efficiently compute a lower bound for $\alpha^{\max}$. However, similar to Section VI-B, instead of fixing $\vec{\beta}$, we can compute a $\vec{\beta}$ that results in the largest possible lower bound. Due to the nonlinearity of the problem, however, we cannot optimize $\vec{\beta}$ and found maximum α in (23) simultaneously. The idea is to fix α, compute the optimal $\vec{\beta}$ and η using (19), then update α using η and repeat the process until α does not change by much. As in Section VI-B, we can use the $(\vec{\gamma},\vec{\beta})$-determined controller instead of the $\vec{\beta}$-determined controller to improve the obtained lower bound. The method is summarized in Module 1. When $\gamma = \beta$, Module 1 provides a lower bound on $\alpha^{\max}$ like $\alpha^{(\beta)}$ based on $\vec{\beta}$-determined controllers.

[4] This is based on the assumption that the IoT bots are uniformly distributed in an area. Therefore, an adversary's ability to change the demands is determined by the initial demand at each node.

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

TABLE I
PERFORMANCE EVALUATION OF SAFE AND IMMUNE ALGORITHMS ON THE NEW ENGLAND 39-BUS SYSTEM. COST VALUES ARE IN $\$/hr$. NUMBERS IN PARENTHESIS INDICATE THE NUMBER OF ITERATIONS TOOK THE IMMUNE ALGORITHM TO CONVERGE

α	OPF	SAFE	IMMUNE	IMMUNE-0.95	IMMUNE-0.9
0.09	41264	-	43434 (7)	43805 (4)	43859 (3)
0.08	41264	43628	42394 (8)	42431 (3)	42982 (3)
0.07	41264	42665	41773 (5)	41991 (3)	42405 (3)
0.06	41264	42050	41492 (4)	41698 (3)	41534 (2)
0.05	41264	41668	41339 (10)	41421 (3)	41419 (2)

Module 1 Lower Bound on $\alpha^{\max}$ using $(\vec{\gamma}, \vec{\beta})$-determined Controllers

Input: G, λ
1: $\alpha^{(0)} = \hat{\alpha}$
2: flag = 1
3: i = 0
4: **while** flag **do**
5: flag = 0
6: Compute the optimal value η, $\vec{\gamma}$, and $\vec{\beta}$ of (21) for $\overline{p_d} = (1+\alpha^{(i)})\vec{p_d}^{\dagger}$ and $\underline{p_d} = (1-\alpha^{(i)})\vec{p_d}^{\dagger}$
7: Set $\alpha^{(i+1)} = \alpha^{(i)} + \lambda(1-\eta)$
8: **if** $|\alpha^{(i+1)} - \alpha^{(i)}| > 0.001$ **then**
9: flag = 1
10: $i = i + 1$
11: **return** $\alpha^{(\gamma,\beta)} := \alpha^{(i)}$, $\vec{\gamma}$, and $\vec{\beta}$

Notice that λ in Module 1 should be set such that updates to α at each iteration are neither too large that the module falls into a loop, nor are too small that it takes a long time to converge.

Proposition 6. When $\gamma = \beta$, for a good λ, Module 1 converges to an $\alpha^{(\beta)}$ value such that $\alpha^{(\beta)} \leq \alpha^{\max}$. Moreover, $\alpha^* \leq \alpha^{(\beta)}$. (Recall that α^* is the optimal solution of (23).)

Proposition 7. For a good λ, Module 1 converges to an $\alpha^{(\gamma,\beta)}$ value such that $\alpha^{(\gamma,\beta)} \leq \alpha^{\max}$. Moreover, $\alpha^{(\beta)} \leq \alpha^{(\gamma,\beta)}$.

In the next section, we numerically compare the upper bound $\hat{\alpha}$, and lower bounds α^*, $\alpha^{(\beta)}$, and $\alpha^{(\gamma,\beta)}$ with $\alpha^{\max}$ in order to demonstrate the tightness of these bounds in approximating $\alpha^{\max}$.

VIII. NUMERICAL RESULTS

In this section, we first numerically evaluate the performance of SAFE and IMMUNE Algorithms developed in Section V. Then, we numerically evaluate the accuracy of the upper and lower bounds developed in Section VII in approximating the maximum α such that the grid is αD-robust (i.e., $\alpha^{\max}$).

A. Simulations Setup

For solving LP, we use *CVX*, a package for specifying and solving convex programs [41], [42]. For computing the optimal power flow part of the IMMUNE Algorithm, we use *MATPOWER* [43] which is a MATLAB based library for computing the power flows. We also exploit the power system test cases available with this library for our simulations. In particular, we use the IEEE 14-bus, 30-bus, and 57-bus test systems, and the New England 39-bus system.

TABLE II
PERFORMANCE EVALUATION OF SAFE AND IMMUNE ALGORITHMS ON THE IEEE 30-BUS SYSTEM. COST VALUES ARE IN $\$/hr$. NUMBERS IN PARENTHESIS INDICATE THE NUMBER OF ITERATIONS TOOK THE ALGORITHM TO CONVERGE

α	OPF	SAFE	IMMUNE
0.31	565.2	-	- (3)
0.3	565.2	614.8	- (4)
0.28	565.2	571.6	569.6 (3)
0.26	565.2	565.32	565.22 (2)
0.22	565.2	565.2	565.2 (1)

The line capacities are only provided for the IEEE 30-bus and New England 39-bus systems. Hence, for the other two systems, we set the capacities ourselves in two-different ways: (i) following [9] for each line we set $\overline{f_i} = \max\{1.2\,|f_i^{\dagger}|, \text{median}(|\vec{f}^{\dagger}|)\}$, and (ii) set $\overline{f_i} = 1.1\max(|\vec{f}^{\dagger}|)$, in which $\vec{f}^{\dagger}$ are the power flows given the default supply and demand values in the test systems. When the first method is used for determining the capacities, it is indicated by (f) in front of the grid name, and when the second method is used, it is indicated by (u) (e.g., see Table III).

B. Primary Control

In this subsection, we evaluate the performance of SAFE and IMMUNE Algorithms on NEW England 39-bus and IEEE 30-bus systems. We assume that $(1-\alpha)p_{di}^{\dagger} \leq p_{di} \leq (1+\alpha)p_{di}^{\dagger}$ and consider different α values to capture attacks with different magnitudes (which depends on the number of controlled bots by an adversary).

Table I compares the performance of SAFE and three variations of the IMMUNE Algorithm for different α values. Recall from Section V-B that IMMUNE-0.95 and IMMUNE-0.9 are similar to the IMMUNE Algorithm but apply more aggressive updates on the capacities in each iteration of the algorithm. This, as mentioned in Section V-B and demonstrated numerically here in Table I, results in faster convergence of the algorithm. Since the OPF problem does not consider the robustness of the grid against MAD attacks, its value is independent of the magnitude of an expected attack (α).

As can be seen in Table I and as we expected, the grid needs to be operated in a non-optimal operating point in order to be robust against MAD attacks. The required percentage increase in the operating cost of the grid obtained by the SAFE and IMMUNE Algorithms versus α are presented in Fig. 7. IMMUNE Algorithm results in the least amount of increase in the operating cost. However, since as demonstrated in Table I, IMMUNE Algorithm takes longer that IMMUNE-0.95 and IMMUNE-0.9 Algorithms to converge, the system operator may prefer to use IMMUNE-0.95 which performs approximately as well as the IMMUNE Algorithm but converges faster. Notice that due to nonconvexity of the problem, a more aggressive update rule may not necessarily result in a costlier operating point, as we see here that IMMUNE-0.9 results in a lower operating cost than IMMUNE-0.95 for $\alpha = 0.06$.

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

TABLE III
LOWER AND UPPER BOUNDS FOR $\alpha^{\max}$

Test case	α^*	$\alpha^{(\beta)}$	$\alpha^{(\gamma,\beta)}$	$\alpha^{\max}$	$\hat{\alpha}$
IEEE 14-bus(f)	0.058	0.1649	0.1906	0.2117	0.2117
IEEE 14-bus(u)	0.950	1.0243	1.1454	1.1479	1.1479
IEEE 30-bus	0.214	0.2851	0.3126	0.37	0.3717
NE 39-bus	0.039	0.0796	0.0962	0.0962	0.0962
IEEE 57-bus(f)	0.024	0.0307	0.0311	< 0.09	0.2
IEEE 57-bus(u)	0.128	0.2396	0.2864	-	0.3468

It can also be seen that SAFE Algorithm performs relatively well in finding a robust operating point of the grid much faster than all variations of IMMUNE Algorithm (recall from Section V-C that SAFE Algorithm requires only to solve a single LP). However, it may become infeasible for higher magnitude attacks (in this case for $\alpha = 0.09$).

We repeated the simulations on the IEEE 30-bus system. The results are presented in Table II. First, it can be seen that the IEEE 30-bus system can be protected against much stronger attacks ($\alpha = 0.3$) which demonstrates that different grids may have different levels of robustness against MAD attacks (we will make a similar observation in the secondary control case in the next subsection). Unlike the New England 39-bus case, here the IMMUNE Algorithm does not converge for the strongest attack ($\alpha = 0.3$) rather than the SAFE Algorithm. This demonstrates that each of these algorithms may be useful in finding a robust operating point for the grid in different scenarios–besides their running time and optimality.

As can be seen in Table II, in this case also, if the IMMUNE Algorithm converges, it converges to a lower cost operating point than the one obtained by the SAFE Algorithm. Here, the IMMUNE Algorithm converged within a few iterations. Therefore, there was no need to consider a faster variation of the IMMUNE Algorithm as in the New England 39-bus case.

Finally, it can be seen that for $\alpha = 0.31$, none of the algorithms can obtain a robust operating point for the grid. We show in the next subsection that this case can be handled by the secondary controller instead (assuming that lines can handle temporary overloads).

C. Secondary Control

In order to evaluate the performance of the controllers developed in Section VI-B, in this subsection, we focus on their performance in approximating $\alpha^{\max}$ as described in Section VII.

Table III compares the maximum α obtained by different methods in several test cases. As can be seen and proved in Section VII, in all cases, $\alpha^* \leq \alpha^{(\beta)} \leq \alpha^{(\gamma,\beta)} \leq \alpha^{\max} \leq \hat{\alpha}$. Notice that for the IEEE 57-bus system, since the brute force search algorithm needs to solve (17) about 2^{42} times for each given α to determine the secondary controllability of the grid, we could not exactly determine $\alpha^{\max}$. However, in the case of IEEE 57-bus (f), after initial iterations of the brute force search algorithm, we could determine that the grid is not secondary controllable for $0.09 \leq \alpha$ as presented in the table.

It can be seen that $\hat{\alpha}$ provides a very close upper bound for $\alpha^{\max}$ most of the time (except in IEEE 57-bus (f)). And since

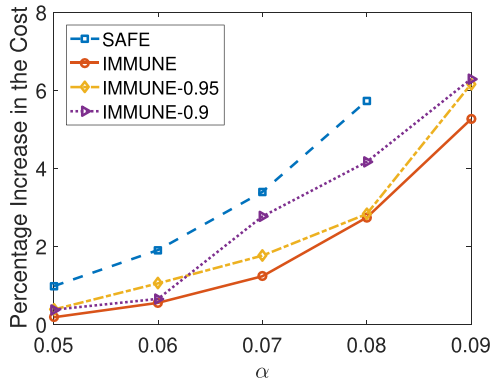

Fig. 7. Percentage increase in operating cost of the grid in order to make it robust against MAD attacks obtained by SAFE and IMMUNE Algorithms versus the magnitude of the attack (α) in New England 39-bus system.

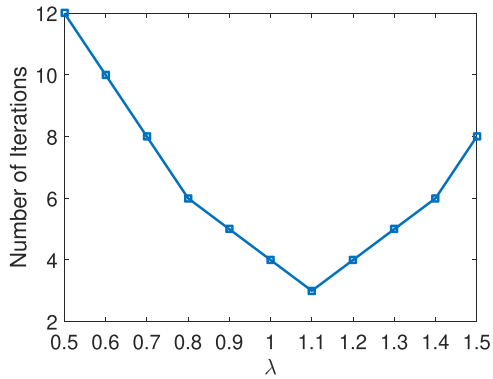

Fig. 8. Number of iterations in Module 1 before it converges versus its update step size λ in the IEEE 30-bus system.

it can be computed by a single LP, the numerical results suggest that it is an efficient and reliable way to find an upper bound for $\alpha^{\max}$. On the other hand, α^* that can also be computed efficiently by a single LP does not provide a very close lower bound in the test systems that we studied here. However, $\alpha^{(\beta)}$ and $\alpha^{(\gamma,\beta)}$ that require more time to be computed, provide much better lower bounds. In particular, in the case of New England 39-bus system $\alpha^{(\gamma,\beta)} = \hat{\alpha}$ which implies that $\alpha^{\max} = \alpha^{(\gamma,\beta)} = \hat{\alpha}$.

Although finding $\alpha^{(\beta)}$ and $\alpha^{(\gamma,\beta)}$ requires solving an LP in several iterations (as summarized in Module 1), the number of iterations can be minimized by selecting a good step size λ. For example, the number of iterations of Module 1 versus λ is presented in Fig. 8 in the IEEE 30-bus system. As can be seen, for the optimal λ (in this case $\lambda = 1.1$), the module converges in 3 iterations. Hence, it can find a good lower bound for α, as shown in Table III, very efficiently and in polynomial time (since it solves a single LP at each iteration). A good λ can be found in practice heuristically after the first few iterations and observing the rate of changes.

Finally, as mentioned in Section VI, the secondary controllability becomes more important when the primary controller cannot prevent line overloads, but the overloads can be tolerated for a short period of time. An example of such scenario happens in IEEE 30-bus system and when $\alpha = 0.31$. As can be seen in Table II, none of the SAFE and IMMUNE

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

Algorithms can find a robust operating point for the grid in this case. However, as can be seen in Table III, since this value is less that $\alpha^{\max} = 0.37$, any line overloads can be cleared by the secondary controller.

D. Open Questions

As we observed in the previous two subsections, different test systems demonstrate different levels of robustness against MAD attacks. For example, as can be seen in Table III, the $\alpha^{\max}$ for the IEEE 30-bus system is 0.37, whereas this value for the New England 39-bus system is only 0.0962. This difference in robustness can be due to the structure of the network as well as the location of the generators and loads. Analytically studying such features and developing efficient algorithms to improve grid robustness by adding extra lines to a system or build future generators at certain locations would be interesting future research directions.

Another important observation from the numerical results is that the performance of the proposed algorithms varies in different test systems. For example, in the New England 39-bus system, the IMMUNE Algorithm successfully finds robust operating points for the generators for different α values, whereas in the IEEE 30-bus system the IMMUNE Algorithm may not converge for $\alpha = 0.3$. Moreover, as can be seen in Table III, the approximation algorithms for estimating $\alpha^{\max}$ provide tight bounds for the New England 39-bus system, whereas the bounds are not tight for the IEEE 30-bus system. Hence, finding sufficient conditions on the structure and properties of a test case under which the approximation bounds are tight and the IMMUNE Algorithm is guaranteed to converge to a locally optimal solution would be important future research directions.

IX. Conclusions

In this paper, we have analyzed the effect of MAD attacks on power flows in detail and presented SAFE and IMMUNE algorithms for finding robust operating points for the generators during economic dispatch such that no lines are overloaded after automatic primary control response to any MAD attacks. Moreover, we have demonstrated that in cases for which temporary overloads can be tolerated, the system operator can approximately but efficiently verify in advance if line overloads can be cleared during the secondary control after any MAD attacks. Based on these two forms of defenses, we have defined the notion of αD-robustness and demonstrated that upper and lower bounds on the maximum α for which the grid is αD-robust can be found efficiently and in polynomial time. We finally have evaluated the performance of the developed algorithms and methods, and showed that they perform very well in practical test cases.

We believe that with universality and growth in the number of high-wattage IoT devices and smart thermostats, the probability of MAD attacks is increasing and there is an urgent need for more studies on the potential effects of these attacks and developing tools for grid protection. Our work provides the first methods for protecting the grid against potential line failures caused by newly discovered MAD attacks via IoT devices. However, our work can be extended in several directions. A natural direction is to extend the developed results to the AC power flow model. A more challenging research direction is to extend the methods to the unit commitment phase of the grid operation. Since the regular unit commitment problem is already a combinatorial problem, incorporating security constraints into that problem will be a challenging task.

In the worst-case scenario in which the scale of a MAD attack is greater than grid robustness (i.e., adversary manipulates the demands by greater than $\alpha^{\max}$ factor), the grid operator may not be able to clear the possible line overloads in a timely manner. This can consequently force the overloaded lines to trip leading to more line overloads and a cascading failure in the system [3]. To prevent cascading failures in such scenarios, the grid operator may apply common control algorithms such as *optimal load-shedding* [44] or *power grid intentional islanding* [45]. However, since an adversary can suddenly decrease the demands after an initial increase in the demands, these control algorithms may not be effective in their classical form (e.g., a sudden decrease in the demands after load-shedding may result in a critical increase in the frequency of the system). Hence, investigating ways to improve these control algorithms to protect the grid against MAD attacks in the worst-case scenarios is also a problem of considerable interest.

X. Omitted Proofs

Proof of Lemma 1: First, notice that $1/R_i$ is the rate with which generator i increases its generation to compensate for the extra demand. Hence, t_i denotes the time that generator i reaches its maximum capacity if the total supply does not meet the demand before t_i. Accordingly, generators reach their maximum capacity in the order of their t_i values from smallest to largest. Using this, it is easy to see that S_i is the total change in the generation at time t_i. Therefore, if $S_i < S_{\Delta p_d}$, then generators 1 to i will reach their maximum capacities before supply meets the total demand. Moreover, since $S_{\Delta p_d} \leq S_{i+1}$, generators $i+1, \ldots, n$ do not reach their capacities and each contribute according to their droop characteristic to compensate for the remaining $S_{\Delta p_d} - \sum_{l=1}^{i} (\overline{p_{gl}} - p_{gl})$. ■

Proof of Lemma 3: First, notice that for each line $(i,j) \in E$ and in each iteration of the IMMUNE Algorithm, c_{ij} is not increasing. To see this, assume c_{ij} changes in the l^{th} iteration, and c_{ij}^{old} and c_{ij}^{new} denote the value of c_{ij} before and after the change, respectively. Since c_{ij} is changed, it means that $\overline{f_{ij}} < |f_{ij}| + \Delta f_{ij}^{\max}$. On the other hand, $|f_{ij}| \leq c_{ij}^{\text{old}}$. Hence, $\overline{f_{ij}} < c_{ij}^{\text{old}} + \Delta f_{ij}^{\max}$ or $\overline{f_{ij}} - \Delta f_{ij}^{\max} < c_{ij}^{\text{old}}$. Since $c_{ij}^{\text{new}} = \overline{f_{ij}} - \Delta f_{ij}^{\max}$, therefore $c_{ij}^{\text{new}} < c_{ij}^{\text{old}}$.

On the other hand, from (11), it is easy to verify that after each iteration $\overline{f_{ij}} - \widehat{\Delta f_{ij}} \leq c_{ij}$. Hence, c_{ij}s cannot get smaller than the fixed values $\overline{f_{ij}} - \widehat{\Delta f_{ij}}$ and since (12) is feasible, the OPF problem remains feasible after each iteration of the IMMUNE algorithm. Now since c_{ij}s are non-increasing and

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

limited by lower bounds, the algorithm is guaranteed to remain feasible and converge to a local optimum solution. ■

Proof of Lemma 4: In each iteration of the IMMUNE algorithm, at least for a single line (i,j), the c_{ij} will be updated. Otherwise, the algorithm should terminate (either converges or become infeasible). On the other hand, since $\widehat{\Delta f_{ij}}$ is the maximum possible flow change on line (i,j), the c_{ij} cannot get smaller than $\overline{f_{ij}} - \widehat{\Delta f_{ij}}$. Hence, since the updates are discrete, in the worst case that only a single capacity is updated by a single unit at each iteration, the algorithm can take at most $\sum_{(i,j)\in E}\lceil\widehat{\Delta f_{ij}}\rceil$ iterations to terminate. ■

Proof of Lemma 5: Assume $\vec{p_d}^{(1)}, \vec{p_d}^{(2)}, \ldots, \vec{p_d}^{(2^n)}$ denote all possible extreme demand vectors. Now assume that for each extreme demand vector $\vec{p_d}^{(i)}$, there exists an operating vector $\vec{p_g}^{(i)}$ for generators that satisfies the secondary control conditions. We prove that for all demand vectors $\vec{p_d}$ within the upper and lower limits also there exists an operating vector $\vec{p_g}$ that satisfies all the secondary controller conditions. Since the space of all the demand vectors is convex, each demand vector $\vec{p_d}$ within the upper and lower limits can be written as a convex combination of the extreme points such as $\vec{p_d} = \sum_{i=1}^{2^n}\beta_i\vec{p_d}^{(i)}$ in which $\forall i: \beta_i \geq 0$ and $\sum_{i=1}^{2^n}\beta_i = 1$. We show that $\vec{p_g} = \sum_{i=1}^{2^n}\beta_i\vec{p_g}^{(i)}$ satisfies all the secondary controller conditions. First, since $\vec{p_g}$ is a convex combination of $\vec{p_g}^{(i)}$s and they are within generators upper and lower limits, so is $\vec{p_g}$. Second, it is easy to see that $\vec{1}^T(\vec{p_g} - \vec{p_d}) = \sum_{i=1}^{2^n}\beta_i\vec{1}^T(\vec{p_g}^{(i)} - \vec{p_d}^{(i)}) = \sum_{i=1}^{2^n}\beta_i 0 = 0$. Finally, based on our assumptions, for each i: $-\overline{f} \leq \mathbf{B}(\vec{p_g}^{(i)} - \vec{p_d}^{(i)}) \leq \overline{f}$. Hence, $\mathbf{B}(\vec{p_g} - \vec{p_d}) = \sum_{i=1}^{2^n}\beta_i\mathbf{B}(\vec{p_g}^{(i)} - \vec{p_d}^{(i)}) \leq \sum_{i=1}^{2^n}\beta_i\overline{f} = \overline{f}$. Similarly, $-\overline{f} \leq \mathbf{B}(\vec{p_g} - \vec{p_d})$. Therefore, $\vec{p_g}$ satisfies all the constraints of the secondary controller problem. The reverse can also be similarly proved using contradiction method. ■

Proof of Proposition 2: If there exists a vector $\vec{\beta}$ that the $\vec{\beta}$-determined controller is reliable, then for any feasible demand vector $\vec{p_d}$, vector of operating points $\vec{p_g} = (\sum_{i=1}^{n} p_{di}) \times \vec{\beta}$ satisfies the demands (i.e., $\vec{1}^T(\vec{p_g} - \vec{p_d}) = 0$) and $|\vec{f}| = |\mathbf{B}(\vec{p_g} - \vec{p_d})| \leq \overline{f}$. Therefore, the grid is secondary controllable. ■

Proof of Lemma 6: From the definition of $\vec{w_i}^{(\beta)}$ vectors, it is easy to verify that for a demand vector $\vec{p_d}$, the power flow on line e_k can be computed as $f_k = \sum_{i=1}^{n} p_{di}\mathbf{B}_k\vec{w_i}^{(\beta)}$. For $|f_k|$ to be maximized, each p_{id} should be either equal to $\underline{p_{di}}$ or $\overline{p_{di}}$ based on signs of $\mathbf{B}_k\vec{w_i}^{(\beta)}$ and f_k. On the other hand, it is easy to see that $\underline{p_{di}} = \frac{(\overline{p_{di}}+\underline{p_{di}})}{2} - \frac{(\overline{p_{di}}-\underline{p_{di}})}{2}$ and $\overline{p_{di}} = \frac{(\overline{p_{di}}+\underline{p_{di}})}{2} + \frac{(\overline{p_{di}}-\underline{p_{di}})}{2}$. So by considering only $p_{di} \in \{\overline{p_{di}}, \underline{p_{di}}\}$, f_k can be computed as follows:

$$f_k = \sum_{i=1}^{n} p_{di}\mathbf{B}_k\vec{w_i}^{(\beta)} = \sum_{i=1}^{n}\Big(\frac{(\overline{p_{di}}+\underline{p_{di}})}{2} \pm \frac{(\overline{p_{di}}-\underline{p_{di}})}{2}\Big)\mathbf{B}_k\vec{w_i}^{(\beta)}$$
$$= \sum_{i=1}^{n}\frac{(\overline{p_{di}}+\underline{p_{di}})}{2}\mathbf{B}_k\vec{w_i}^{(\beta)} + \sum_{i=1}^{n}\Big(\pm\frac{(\overline{p_{di}}-\underline{p_{di}})}{2}\Big)\mathbf{B}_k\vec{w_i}^{(\beta)}.$$

From the equation above, it can be seen that the first part is fixed but the second part can be selected based on the sign of the first part in order to maximize $|f_k|$. Hence, it is easy to see that maximum value of $|f_k|$ is:

$$\max_{\underline{p_d}\leq\vec{p_d}\leq\overline{p_d}}|f_k| = \left|\sum_{i=1}^{n}\frac{(\overline{p_{di}}+\underline{p_{di}})}{2}\mathbf{B}_k\vec{w_i}^{(\gamma)}\right| + \sum_{i=1}^{n}\frac{(\overline{p_{di}}-\underline{p_{di}})}{2}|\mathbf{B}_k\vec{w_i}^{(\beta)}|.$$

■

Proof of Proposition 3: In order to solve (19) using LP, one can define auxiliary vector $\vec{u}$ and matrix $\mathbf{Q}$ and replace the constraint $\vec{f} = |\mathbf{BW}^{(\beta)}(\overline{p_d}+\underline{p_d})/2| + |\mathbf{BW}^{(\beta)}|(\overline{p_d}-\underline{p_d})/2$ in (19) with following set of inequalities:

$$\vec{f} = \vec{u} + \mathbf{Q}(\overline{p_d}-\underline{p_d})/2,$$
$$\vec{u} \geq \mathbf{BW}^{(\beta)}(\overline{p_d}+\underline{p_d})/2,$$
$$\vec{u} \geq -\mathbf{BW}^{(\beta)}(\overline{p_d}+\underline{p_d})/2,$$
$$\mathbf{Q} \geq \mathbf{BW}^{(\beta)}, \quad \mathbf{Q} \geq -\mathbf{BW}^{(\beta)},$$

in which the matrix inequalities are entry by entry. Now it is easy to verify that since the optimization minimize η and $\vec{f} \leq \eta\overline{f}$, in the optimal solution $\vec{f}$ will be minimized and therefore $\vec{u}$ and $\mathbf{Q}$ will be equal to $|\mathbf{BW}^{(\beta)}(\overline{p_d}+\underline{p_d})/2|$ and $|\mathbf{BW}^{(\beta)}|$, respectively. Hence using the above transformation, (19) can be solved using LP. It can be seen that if the optimal solution η^* to (19) is less than or equal to 1, then since $\vec{f}$ is equal to the maximum power flow on the lines over all possible demand vectors (and corresponding generation operating points obtained by the $\vec{\beta}^*$-determined controller) and $\vec{f} \leq \eta^*\overline{f} \leq \overline{f}$, the $\vec{\beta}^*$-controller is reliable. Hence, the grid is secondary controllable. ■

Proof of Proposition 4: Since in optimization (22) only the maximum demand case (i.e., $\vec{p_d} = (1+\alpha)\vec{p_d}^{\dagger}$) is being verified to be satisfiable by the generators with no line overloads, the optimal solution of (22) only provides an upper bound for $\alpha^{\max}$. ■

Proof of Proposition 5: Using (18), it can be verified that the maximum power flow on a line (i,j) over all the demand vectors and corresponding generation vector determined by the $\vec{\beta}$-determined controller is equal to $|\mathbf{BW}^{(\beta)}\vec{p_d}^{\dagger}| + |\mathbf{BW}^{(\beta)}|(\alpha\vec{p_d}^{\dagger})$. Hence, optimization (23) maximizes α such that the grid is αD-robust using the specified $\vec{\beta}$-determined controller. On the other hand, since the operating points of the generators are limited to the operating points obtained by the specified $\vec{\beta}$-determined controller, it is obvious that demand vectors that are controllable by this controller are a subset of all controllable vectors. Hence, α^* only provides a lower bound for $\alpha^{\max}$. Finally, it is also easy to see that similar to the technique presented in the proof of Proposition 3, optimization (23) can be solved using LP and therefore α^* can be computed in polynomial time. ■

Proof of Proposition 6: At each iteration, if $\alpha^{(i)} > \alpha^{\max}$, then the solution η to (19) would be greater than 1. Hence, if λ is small enough, $0 \leq \alpha^{(i+1)} = \alpha^{(i)} + \lambda(1-\eta) \leq \alpha^{(i)}$. Similarly, it can be shown that if $\alpha^{(i)} < \alpha^{\max}$, then $\alpha^{(i+1)} > \alpha^{(i)}$. On the other hand, for $\alpha^{(i)} = \alpha^{\max}$, the solution η to (19) would be zero and $\alpha^{(i)} = \alpha^{(i+1)} = \alpha^{\max}$. Hence, $\alpha^{\max}$ is the only absorbing point for this algorithm which it converges to (if λ is small enough). ■

Proof of Proposition 7: The convergence proof is similar to the proof of Proposition 6. It is also easy to see that

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

since $\vec{\beta}$-determined controllers are a special case of $(\vec{\gamma}, \vec{\beta})$-determined controllers, $\alpha^{(\beta)} \leq \alpha^{(\gamma,\beta)}$. ■

REFERENCES

[1] NERC, "Analysis of the cyber attack on the Ukrainian power grid," 2016, [Online]. Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf. Accessed: Jan. 2018.

[2] N. S. Malik and R. Collins, "The cyberattack that crippled gas pipelines is now hitting another industry," 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay. Accessed: Jun. 2018.

[3] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. USENIX Secur.*, Aug. 2018.

[4] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *Proc. ACM 33rd Annu. Comput. Secur. Appl. Conf.*, Dec. 2017, pp. 303–314.

[5] "How hacked water heaters could trigger mass blackouts," *Wired Mag.*, Aug. 2018, [Online]. Available: https://www.wired.com/story/water-heaters-power-grid-hack-blackout/

[6] "Your smart air conditioner could help bring down the power grid," *CNET*, Aug. 2018, [Online]. Available: https://www.wired.com/story/water-heaters-power-grid-hack-blackout/

[7] I. Dobson, "Cascading network failure in power grid blackouts," *Encyclopedia Syst. Control*, pp. 105–108, 2015. [Online]. Available: https://link.springer.com/referenceworkentry/10.1007/978-1-4471-5058-9_264#howtocite

[8] S. Soltan, D. Mazauric, and G. Zussman, "Analysis of failures in power grids," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 3, pp. 288–300, Jun. 2017.

[9] H. Cetinay, S. Soltan, F. A. Kuipers, G. Zussman, and P. Van Mieghem, "Analyzing cascading failures in power grids under the AC and DC power flow models," in *Proc. IFIP Perform. Eval. Rev.*, vol. 45, pp. 198–203 Nov. 2017.

[10] D. Bienstock, *Electrical Transmission System Cascades and Vulnerability: An Operations Research Viewpoint*. Philadelphia, PA, USA: SIAM, 2016.

[11] B. Carreras, V. Lynch, I. Dobson, and D. Newman, "Critical points and transitions in an electric power transmission model for cascading failure blackouts," *Chaos*, vol. 12, no. 4, pp. 985–994, 2002.

[12] J. Song, E. Cotilla-Sanchez, G. Ghanavati, and P. D. Hines, "Dynamic modeling of cascading failure in power systems," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2085–2095, May 2016.

[13] L. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. Mohammed, and S. A. Zonouz, "Hey, my malware knows physics! attacking plcs with physical model aware rootkit," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2017.

[14] 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, 2011, Art. no. 13.

[15] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 214–219.

[16] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

[17] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Trans. Signal Process.*, vol. 63, no. 5, pp. 1102–1114, Mar. 2015.

[18] S. Soltan, M. Yannakakis, and G. Zussman, "Joint cyber and physical attacks on power grids: Graph theoretical approaches for information recovery," in *Proc. ACM SIGMETRICS Int. Conf. Meas. Model. Comput. Syst.*, Jun. 2015, pp. 361–374.

[19] D. Bienstock and M. Escobar, "Computing undetectable attacks on power grids," *ACM PER*, vol. 45, no. 2, pp. 115–118, 2017.

[20] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.

[21] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.

[22] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2016–2025, Jul. 2016.

[23] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[24] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.

[25] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2862–2872, Jul. 2018.

[26] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," in *Proc. North Amer. Power Symp.*, Sep. 2017.

[27] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control*. Hoboken, NJ, USA: Wiley, 2012.

[28] S. H. Low, "Convex relaxation of optimal power flow-part I: Formulations and equivalence," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 1, pp. 15–27, Mar. 2014.

[29] A. Castillo and R. P. ONeill, "Survey of approaches to solving the ACOPF," US Federal Energy Regulatory Commission, Washington, DC, USA, Tech. Rep, 2013. [Online]. Available: https://www.ferc.gov/industries/electric/indus-act/market-planning/opf-papers/acopf-4-solution-techniques-survey.pdf

[30] A. Monticelli, M. Pereira, and S. Granville, "Security-constrained optimal power flow with post-contingency corrective rescheduling," *IEEE Trans. Power Syst.*, vol. 2, no. 1, pp. 175–180, Feb. 1987.

[31] D. Bienstock, M. Chertkov, and S. Harnett, "Chance-constrained optimal power flow: Risk-aware network control under uncertainty," *SIAM Rev.*, vol. 56, no. 3, pp. 461–495, 2014.

[32] R. Bapat, *Graphs and Matrices*. New York, NY, USA: Springer, 2010.

[33] *Energy Primer, a Handbook of Energy Market Basics*. Washington, DC, USA: Federal Energy Regulatory Commission, 2012.

[34] European Network of Transmission System Operators for Electricity (ENTSOE), "Continental europe operation handbook," 2004. [Online]. Available: https://www.entsoe.eu/publications/system-operations-reports/operation-handbook/Pages/default.aspx. Accessed: Jan. 2018.

[35] J. Machowski, J. Bialek, and J. R. Bumby, *Power System Dynamics and Stability*. Hoboken, NJ, USA: Wiley, 1997.

[36] R. Hebner, J. Beno, and A. Walls, "Flywheel batteries come around again," *IEEE Spectr.*, vol. 39, no. 4, pp. 46–51, May 2002.

[37] J. E. Falk, "A linear max-min problem," *Math. Program.*, vol. 5, no. 1, pp. 169–188, 1973.

[38] J. F. Bard, *Practical Bilevel Optimization: Algorithms and Applications*. New York, NY, USA: Springer, 1998.

[39] W. F. Bialas and M. H. Karwan, "Two-level linear programming," *Manage. Sci.*, vol. 30, no. 8, pp. 1004–1020, 1984.

[40] P. Hansen, B. Jaumard, and G. Savard, "New branch-and-bound rules for linear bilevel programming," *SIAM J. Sci. Comput.*, vol. 13, no. 5, pp. 1194–1217, 1992.

[41] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," Mar. 2014. [Online]. Available: http://cvxr.com/cvx,

[42] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds. New York, NY, USA: Springer-Verlag, 2008, pp. 95–110. [Online]. Available: http://stanford.edu/ boyd/graph_dcp.html.

[43] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[44] D. Bienstock, "Optimal control of cascading power grid failures," in *Proc. IEEE 50th IEEE Conf. Decis. Control Eur. Control Conf.*, Dec. 2011, pp. 2166–2173.

[45] S. Soltan, M. Yannakakis, and G. Zussman, "Doubly balanced connected graph partitioning," in *Proc. 28th Annu. ACM-SIAM Symp. Discrete Algorithms*, Jan. 2017.

Saleh Soltan (M'15) is a Postdoctoral Research Associate with the Department of Electrical Engineering, Princeton University, Princeton, NJ, USA. He received the Ph.D. degree in electrical engineering from Columbia University. He received the B.S. degrees in electrical engineering and mathematics (double major) from Sharif University of Technology, Iran, in 2011 and the M.S. degree in electrical engineering from Columbia University in 2012. He is the Gold Medalist of the 23rd National Mathematics Olympiad in Iran in 2005 and the recipient of Columbia University Electrical Engineering Armstrong Memorial Award in 2012 and Jury Award in 2018.

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.

Prateek Mittal is currently an Associate Professor with the Department of Electrical Engineering, Princeton University. He received the Ph.D. degree from University of Illinois at Urbana-Champaign in 2012. He is the recipient of the NSF CAREER award (2016), ARO YIP Award (2018), ONR YIP award (2018), M.E. Van Valkenburg award, Google Faculty Research Award (2016, 2017), Cisco Faculty research award (2016), Intel Faculty research award (2016, 2017), and IBM Faculty award (2017). He was awarded Princeton University's E. Lawrence Keyes Award for outstanding research and teaching, and is the recipient of multiple outstanding paper awards including ACM CCS and ACM ASIACCS.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in EECS from Princeton University, Princeton, NJ, USA, in 1977. From 1977 to 1990, he was with the faculty of the University of Illinois at Urbana-Champaign. Since 1990, he has been with the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering. From 2006 to 2016, he also served as the Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. His research interests include the areas of information theory and signal processing, and their applications in wireless networks, energy systems, and related fields. Among his publications in these areas is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, the 2019 ASEE Benjamin Garver Lamme Award, a D.Sc. *honoris causa* from Syracuse University, awarded in 2017, and a D.Eng. *honoris causa* from the University of Waterloo, awarded in 2019.

Authorized licensed use limited to: The University of British Columbia Library. Downloaded on September 26,2020 at 23:24:42 UTC from IEEE Xplore. Restrictions apply.