2021 American Control Conference (ACC)
New Orleans, USA, May 25-28, 2021

Optimal Dynamic Load-Altering Attacks Against Power Systems

Vaibhav Katewa and Fabio Pasqualetti

Abstract— **In this paper we study dynamical load-altering attacks in power networks, where an attacker aims to destabilize the network by modifying a portion of the loads present in it, and provide a provable method to design such attacks. From a practical standpoint, dynamic load-altering attacks are easily implemented by tampering with demand response and demand side management services, and can greatly compromise the efficiency and reliability of the grid. From a technical standpoint, dynamic load-altering attacks act as sparse perturbations to the network matrices that alter key dynamical properties, thus constituting a form of distributed or sparse controller for network systems. We cast the problem of designing minimally-invasive destabilizing load-altering attacks as a sparse stability radius optimization problem, and present a numerical algorithm to efficiently compute optimal destabilizing load-altering attacks. This analysis provides a vulnerability map that identifies secure and vulnerable loads in the power network. We illustrate our results using the IEEE-39 bus system.**

I. Introduction

Security concerns arise in all sectors of power systems, from generation to distribution, control, and consumption [1]–[3]. In the consumption sector, demand response and demand side services, which are used by utilities to control flexible loads in response to changes in grid conditions [4], [5], can be the target of inexpensive, yet impactful, load-altering attacks [6]. In this paper, we address the outstanding question of characterizing and computing minimally-invasive destabilizing load-altering attacks, which allow the operator to identify the most vulnerable loads in the grid and, ultimately, design preventive actions against these attacks.

From a system-theoretic perspective, dynamic load-altering attacks can be modeled as perturbations to a subset of parameters of the power system. The attacker's objective is to design such minimal perturbations to induce dynamic instabilities. Then, the problem of understanding optimal destabilizing load-altering attacks is effectively one of *sparse stability radius* [7], which, in a linear setting, asks for the smallest perturbation of the system matrix that satisfies a desired sparsity pattern and renders the system unstable. In this paper we extend the sparse stability radius results of [7] to account for the singular dynamics arising in power systems, and validate their utility using the IEEE-39 bus system.

Related work. The literature on cyber-physical attacks is particularly rich of theoretical studies and practical cases [1], [8]. The case of (single-point) dynamic load-altering attacks against power systems was first presented in [6], which discusses the implementation details and the destabilizing impact of this type of attacks. Subsequent works have analyzed the ability to detect such attacks [9], as well as the design of optimal attack inputs [10]–[13] and defense mechanisms [14]–[16], among others. This paper complements this line of work by providing the theoretical and algorithmic basis to design minimally-invasive, multi-point, dynamic load-altering attacks, which destabilize the grid by minimally modifying only a predefined subset of loads.

The literature on the stability radius of linear systems is also relevant to this paper. The notion of 2-norm stability radius was introduced formally in [17], [18]. Various bounds and characterizations of unstructured, complex, and real stability radius were given in [17], [19]. Characterizations and algorithms for the complex stability radius were presented in [20]–[24]. The real stability radius problem is considerably more difficult than its complex counterpart [17]. Several bounds for the unstructured case are presented in [25], [26], and a complete algebraic characterization of the structured case is contained in [27].

Differently from the above works, we focus here on the Frobenius-norm stability radius problem, which has received substantially less attention. Notable exceptions are [7], [28], which study explicitly the Frobenius-norm sparse stability radius. In this paper, we build on the approach developed in [7], and extend the framework to include the case of singular linear dynamics, as they naturally arise in the study of multi-point dynamic load altering attacks against power systems.

Contribution. The main contribution of this paper is twofold. First, we formulate the problem of computing minimally-invasive (as measured by the Frobenius norm), multi-point, destabilizing dynamic load-altering attacks as a sparse stability radius problem. Then, following the approach in [7], we derive a theoretical and computational framework to compute the sparse stability radius of singular linear systems, as they naturally arise in the study of power systems. Second, we demonstrate our results numerically on a model of the IEEE 39-bus power network, and we show how our analysis allows the operator to identify the loads that are most vulnerable to load-altering attacks, and to quantify the effects of minimally-invasive attacks on different buses.

Mathematical notation. We use $\mathrm{diag}(A, B, C)$ to denote a block diagonal matrix with A, B and C as the diagonal blocks. We let $\circ$ denote the Hadamard (element-wise) product, $\mathrm{vec}(\cdot)$ the vectorization operator, and $\|\cdot\|_F$ the Frobenius norm. $\lambda(A, B)$ denotes a generalized eigenvalue

This material is based upon work supported in part by awards SG/MHRD-20-0003, UCOP-LFR-18-548175, ARO-71603NSYIP, and AFOSR-FA9550-19-1-0235. Vaibhav Katewa is with the department of Electrical Communication Engineering, Indian Institute of Science, Bangalore (Email: vkatewa@iisc.ac.in). Fabio Pasqualetti is with the Department of Mechanical Engineering, University of California at Riverside (Email: fabiopas@engr.ucr.edu).

of the pair (A, B). The spectral abscissa of (A, B) is defined as $\alpha(A, B) = \max\{\text{real}\{\lambda(A, B) : \lambda(A, B) \text{ is finite}\}\}$.

II. Problem Setup

A. Power System Model

We consider a power transmission network consisting of $n_g > 0$ generator buses, $n_l > 0$ load buses, and transmission lines connecting these buses. Let $n_b = n_g + n_l$ denote the total number of buses. Without loss on generality, we assume that $\mathcal{G} \triangleq \{1, 2, \cdots, n_g\}$ are generator buses and $\mathcal{L} \triangleq \{n_g+1, \cdots, n_b\}$ are load buses. We make the following assumptions about the power network:

Assumption 1: The transmission lines are lossless and reactive power in the buses and transmission lines is absent. Further, no loads are connected to the generator buses. □

Let θ_i and ω_i denote the voltage phase angle deviation and the frequency deviation at bus i. Further, let $M_i > 0$ and $D_i^g > 0$ denote the moment of inertia and the damping coefficient of generator i, respectively. The generator dynamics is modeled by the following linear swing equation [29]:

$$M_i\dot{\omega}_i = P_i^m - D_i^g\omega_i - P_i^g, \qquad i \in \mathcal{G} \tag{1}$$

where P_i^m and P_i^g are the mechanical power input and the power injection of the generator at bus i, respectively. We assume that P_i^m is controlled using a combination of a turbine-governor controller and a load-frequency controller. We model the two controllers together as a proportional-integral (PI) controller [30]:

$$P_i^m = -(K_i^p\omega_i + K_i^i\int_0^t \omega_i\, dt) = -(K_i^p\omega_i + K_i^i\theta_i), \tag{2}$$

where $K_i^p > 0$ and $K_i^i > 0$ are the proportional and integral controller gains, respectively.

The linear power flow equations of the power network are:

$$\begin{aligned} P_i^g &= \sum_{i=1}^{n} L_{ij}(\theta_i - \theta_j), && \text{with } i \in \mathcal{G}, \\ -P_i^l &= \sum_{i=1}^{n} L_{ij}(\theta_i - \theta_j), && \text{with } i \in \mathcal{L}, \end{aligned} \tag{3}$$

where P_i^l is the power consumption of the load at bus i, and $L_{ij} \geq 0$ is the admittance of the transmission line between buses i and j, with $L_{ij} = L_{ji}$. Note that $L_{ij} = 0$ if there is no line between buses i and j.

We consider two types of loads connected to load bus i [31]. The first type is a frequency-sensitive load (ex. motor) that changes with the bus frequency and is modeled by $D_i^l\omega_i$, with $D_i^l > 0$. The second type of load is frequency-insensitive (ex. heating and lighting) and controllable, which can be adapted freely in response to the network conditions. This is denoted by P_i^{lc}. Thus, we have:

$$P_i^l = P_i^{lc} + D_i^l\omega_i, \qquad \text{with } i \in \mathcal{L}. \tag{4}$$

Combining equations (1)-(4) yields a dynamic model for the whole power system:

$$\begin{bmatrix} I & 0 \\ 0 & \bar{M} \end{bmatrix} \begin{bmatrix} \dot{\theta} \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} 0 & I \\ \bar{L} & \bar{D} \end{bmatrix} \begin{bmatrix} \theta \\ \omega \end{bmatrix} + \begin{bmatrix} 0 \\ \bar{I}_1 \end{bmatrix} P^{lc}, \tag{5}$$

$$\bar{M} = \text{diag}(-M, 0), \qquad \bar{L} = -L + \text{diag}(K^i, 0),$$
$$\bar{D} = \text{diag}(D^g + K^p, D^l), \quad \bar{I}_1 = \begin{bmatrix} 0 \\ I \end{bmatrix},$$

and M, K^i, K^p, D^g are diagonal matrices containing $\{M_i, K_i^i, K_i^p, D_i^g\}$ for $i \in \mathcal{G}$, respectively. Further D^l and P^{lc} are a diagonal matrix and a vector, respectively, containing $\{D_i^l\}$ and $\{P_i^{lc}\}$ for $i \in \mathcal{L}$. θ and ω are vectors containing $\{\theta_i\}$ and $\{\omega_i\}$ for all the buses. Finally, $L = [L_{ij}]$ is the network Laplacian matrix with $L_{ii} = -\sum_{k=1,k\neq i}^{n_b} L_{ik}$. Modeling the power system dynamics as a singular linear system via linearization around the operating point is standard in literature [6], [12], [16].

B. Threat Model

We assume that an attacker is capable of changing the controllable loads P^{lc} connected to the load buses and it has access to the frequency measurements ω_i of the generator and load buses. The attacker uses these frequency measurements to vary the loads appropriately to make the power system dynamics unstable. We consider that the attacker uses the following proportional feedback law[1]:

$$P_i^{lc} = \sum_{j=1}^{n_b} K_{i,j}^a\omega_j, \qquad \text{with } i \in \mathcal{L}, \tag{6}$$

where $K_{i,j}^a$ is the proportional gain (in Joules) corresponding to the attack on i^{th} load based using the frequency of j^{th} bus. Note that, if ω_j is not used (or not available) for the attack on the i^{th} load, then $K_{i,j}^a = 0$. We define a binary structure matrix $\mathsf{S} \in \{0, 1\}^{n_l \times n_b}$ that specifies which frequency measurement is available for performing an attack:

$$K_{i,j}^a = \begin{cases} 0 & \text{if } \mathsf{S}_{i,j} = 0, \\ \in \mathbb{R} & \text{if } \mathsf{S}_{i,j} = 1. \end{cases} \tag{7}$$

The matrix S defines all possible structures for the measurement availability and load attacks. For instance, if the i^{th} row of S is zero, then there is no attack on the i^{th} load. Further, if the i^{th} column is zero, then the i^{th} frequency measurement is not available to the attacker. Typically, S would be a sparse matrix if there are only a few attack locations. Further, we can vary S to analyze the effect of attacks on different locations (see Section IV) The collective load control equations (6) and sparsity constraints (7), respectively, yield:

$$P^{lc} = K^a\omega = K^a \begin{bmatrix} 0 & I \end{bmatrix} \begin{bmatrix} \delta \\ \omega \end{bmatrix}, \tag{8}$$

$$\mathsf{S}^c \circ K^a = 0, \tag{9}$$

where $K^a = [K_{ij}^a]$, and S^c denotes the complement of S.

[1]The attacker can use other complex laws as well. However, for simplicity, we focus on the proportional law in the paper.

The power system dynamics (5) with the dynamic load-altering attacks (8) reads as

$$\underbrace{\begin{bmatrix} I & 0 \\ 0 & \bar{M} \end{bmatrix}}_{E} \begin{bmatrix} \dot{\theta} \\ \dot{\omega} \end{bmatrix} = \left(\underbrace{\begin{bmatrix} 0 & I \\ \bar{L} & \bar{D} \end{bmatrix}}_{A} + \underbrace{\begin{bmatrix} 0 \\ \bar{I}_1 \end{bmatrix}}_{B} \underbrace{K^a}_{\Delta} \underbrace{\begin{bmatrix} 0 & I \end{bmatrix}}_{C} \right) \underbrace{\begin{bmatrix} \theta \\ \omega \end{bmatrix}}_{x}$$
$$\triangleq \quad E\dot{x} = (A + B\Delta C)x. \tag{10}$$

For convenience, we use the notations (E, A, B, C, Δ) henceforth, and let $A \in \mathbb{R}^{n\times n}, B \in \mathbb{R}^{n\times m}$ and $C \in \mathbb{R}^{p\times n}$. Since E is singular, 10 represents a singular linear system. The load-altering attacks perturb the dynamics matrix of the power system from A to $A(\Delta) \triangleq A + B\Delta C$, and the perturbation Δ satisfies the sparsity constraints $\mathsf{S}^c \circ \Delta = 0$ (c.f. (9)). The dynamical system (10) is stable if and only if the finite[2] generalized eigenvalues of $(A(\Delta), E)$ lie strictly in the left-half complex plane. Therefore, the attacker's goal is to destabilize the power system by moving these generalized eigenvalue(s) to the right-half complex plane.

Remark 1: ***(Uncontrollable and Secure Loads)*** It might be possible that a portion of the loads at the load buses are uncontrollable or secure and cannot be changed by the attacker. We ignore such loads since they appear as additional additive terms in (10), and do not play a role in the destabilization of the network. Thus, P^{lc} in (5) are treated as load alterations by the attacker. □

III. Optimal Load-Altering Attacks

The attacker's goal is to find a perturbation Δ such that the system (10) becomes unstable. Besides this, it also desires that such destabilization occurs by altering a minimum amount of load [3]. From (8), we observe that $\|P^{lc}\| \leq \|\Delta\|\|\omega\|$. Intuitively, the attacked loads is small if $\|\Delta\|$ is small. Thus, the objective of the attacker is to find a minimum-norm Δ that destabilizes (10). This is also known as the stability radius problem in literature [7]. We use the Frobenius norm (instead of 2-norm, for instance) since it captures the element-wise perturbation of Δ (each element corresponds to a attack on a particular bus using a particular measurement) and also leads to a tractable analysis. We make the following assumptions:

Assumption 2: The system (A, E) is stable, that is, $\alpha(A, E) < 0$, where $\alpha(\cdot)$ denotes the spectral abscissa. □

Assumption 3: The matrix pencil $A - \lambda E$ is regular. □

Assumptions 2 and 3 are typically satisfied by the power system (10). Since the generalized eigenvalues of $(A(\Delta), E)$ are continuous with respect to Δ, the minimum-norm Δ that destabilizes the system (10) corresponds to the condition $\alpha(A(\Delta), E) = 0$. This condition implies that: (i) atleast one generalized eigenvalue lies on the imaginary axis of the complex plane, and (ii) the remaining generalized eigenvalues lie strictly inside the left-half complex plane. We reformulate the first condition as $A(\Delta)x = j\beta Ex$, where $j\beta$, with $\beta \in \mathbb{R}$, is a generalized eigenvalue and x is the corresponding generalized eigenvector.[4] We assume that the generalized eigenvalue corresponding to the minimum-norm solution is imaginary. The case when such eigenvalue is real can be handled analogously. We ignore the second condition since it is automatically satisfied by the minimum-norm solution due to Assumption 2 and the continuity property of the generalized eigenvalues. Based on the above discussion, we formulate the following attack optimization problem:

$$\Delta^* = \underset{\Delta,\, x,\, \beta}{\arg\min} \quad \frac{1}{2}\|\Delta\|_F^2 \tag{11}$$
$$\text{s.t.} \quad (A + B\Delta C)x = j\beta Ex, \tag{11a}$$
$$\mathsf{S}^c \circ \Delta = 0, \tag{11b}$$

where (11b) follows from (9). Since the constraint (11a) is not convex, the optimization problem (11) is also not convex and can have multiple local minima. At a local minimum, the condition $\alpha(A(\Delta), E) = 0$ may be violated since there may be some generalized eigenvalues of $(A(\Delta), E)$ in the right-half complex plane. Irrespective of whether $\alpha(A(\Delta), E) = 0$ holds or not, a local minimum always provides an upper bound to $\|\Delta^*\|_F$. Further, it may be possible that the constraints (11a)-(11b) are not feasible. In such cases, the system cannot be destabilized by load-altering attacks. Finally, let Δ_1^* and Δ_2^* correspond to the solutions of (11) for sparsity patterns S_1 and S_2, respectively. If S_2 is a subset of S_1 in the sense that $\mathsf{S}_2 \circ \mathsf{S}_1 = \mathsf{S}_2$, then $\|\Delta_1^*\|_F \leq \|\Delta_2^*\|_F$.

Next, we develop a gradient based algorithm to obtain local solutions of (11). We proceed in the following steps:

Step 1: To avoid computations in the complex domain, we convert the constraint (11a) into the following real constraint:

$$(A + B\Delta C)X = \beta EX\bar{I}, \tag{12}$$

where $X = \begin{bmatrix} \mathrm{Re}(x) & \mathrm{Im}(x) \end{bmatrix}$ and $\bar{I} \triangleq \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$.

Step 2: We use the Sylvester equation based parametrization (see [32]) to reformulate (12) as:

$$AX - \beta EX\bar{I} = -BG, \tag{13a}$$
$$G = \Delta CX. \tag{13b}$$

Step 3: We handle the sparsity constraints (11b) by using the penalty based optimization approach [33]. We relax the optimization problem by dropping the sparsity constraints and modifying the cost function in (11) to include a penalty when these sparsity constraints are violated. The penalty is imposed by weighing individual entries of Δ using a weighing matrix W given by

$$W_{ij} = \begin{cases} 1, & \text{if } \mathsf{S}_{ij} = 1, \\ \mathbf{w} \gg 1, & \text{if } \mathsf{S}_{ij} = 0. \end{cases}$$

Using W, the penalized cost becomes $J_W = \frac{1}{2}\|W \circ \Delta\|_F^2$.

[2]Since E is singular, $(A(\Delta), E)$ has generalized eigenvalue(s) at infinity.

[3]Other objectives could be to destabilize the system by (i) attacking the minimum number of loads, or, (ii) attacking least costly loads, where each load cost captures the difficulty of attacking the load. We defer such formulations for future research.

[4]With a slight abuse of notation, we use x to denote both the state of (10) and a generalized eigenvector of $(A(\Delta), E)$.

Based on the above steps, we reformulate (11) as:

$$\min_{G,\,\beta} \quad J_W = \frac{1}{2}\left\|W \circ \Delta\right\|_F^2 \qquad (14)$$
$$\text{s.t.} \qquad \text{(13a), and (13b) hold.}$$

Next, we show that (14) is an unconstrained optimization problem in (G, β). Since (i) $A - \lambda E$ is assumed to be regular (c.f. Assumption 3), (ii) $\beta\bar{I} - \lambda I$ is always regular, and (iii) the spectrum of (A, E) and $(\beta\bar{I}, I)$ are disjoint (c.f. Assumption 2), the Sylvester equation (13a) has a unique solution X for any (G, β) [34]. Further, for any (G, β), (13b) has a solution if CX has rank two. We make the following assumption which holds generically for almost all (G, β):

Assumption 4: CX has full column rank, where X is the unique solution of (13a). □

For a given (G, β) and under Assumption 4, we can solve (13b) to obtain Δ, which, in general, may not be unique. Since we aim to minimize $\frac{1}{2}\left\|W \circ \Delta\right\|_F^2$, we choose Δ as the solution of the following quadratic optimization problem:

$$\min_{\Delta} \quad J_W = \frac{1}{2}\left\|W \circ \Delta\right\|_F^2 \qquad (15)$$
$$\text{s.t.} \qquad \text{(13b) holds.}$$

Since $W_{ij} > 0$, the optimization problem (15) is strictly convex (under Assumption 4) and its unique global minimum is obtained by solving the following Lagrange conditions:

$$W \circ W \circ \Delta + \Phi(CX)^{\mathsf{T}} = 0, \qquad (16a)$$
$$\Delta CX = G, \qquad (16b)$$

where the matrix Φ is the Lagrange multiplier of (15).

To summarize, using the Sylvester equation based parametrization, we can freely vary (G, β) (under Assumption 4) and compute the corresponding unique X using (13a) and the unique Δ using (16a)-(16b). This renders (14) as an unconstrained optimization problem is variables (G, β).

Next, we compute the analytical expressions for the gradient and Hessian of the cost in (14), which will be used to solve numerically the optimization problem. Let $g \triangleq \text{vec}(G), x_v = \text{vec}(X)$, $\phi = \text{vec}(\Phi)$, $\delta = \text{vec}(\Delta)$, and let the free variables of (14) be denoted by $\bar{z} \triangleq [g^{\mathsf{T}}, \beta]^{\mathsf{T}}$. Further, let $e = [0, \cdots, 0, 1]^{\mathsf{T}} \in \mathbb{R}^{2m+1}$ and $\bar{W} = \text{diag}(\text{vec}(W \circ W))$.

Theorem 3.1: **(Gradient and Hessian)** Define the following Kronecker products:

$$\tilde{B} = I_2 \otimes B, \qquad \tilde{I} = \bar{I} \otimes E, \qquad \tilde{A}(\beta) = I_2 \otimes A + \beta\tilde{I},$$
$$\tilde{\Delta} = I_2 \otimes (\Delta C), \quad \tilde{X} = (CX)^{\mathsf{T}} \otimes I_m, \quad \bar{X} = \begin{bmatrix} \bar{W} & \tilde{X}^{\mathsf{T}} \\ \tilde{X} & 0 \end{bmatrix},$$

and $F = \begin{bmatrix} (C \otimes \Phi)T_{n,2} \\ \tilde{\Delta} \end{bmatrix}$.

Let $U = \begin{bmatrix} U_1 & U_2 \end{bmatrix}$ and V be the unique solutions of

$$U\bar{X} = \begin{bmatrix} I_{mp} & 0 \end{bmatrix}, \quad \text{and} \quad \tilde{A}(\beta)V = \begin{bmatrix} \tilde{B} & \tilde{I}x_v \end{bmatrix},$$

and let $\bar{U}_1$ and $\bar{U}_2$ be such that $\text{vec}(\bar{U}_1) = U_1^{\mathsf{T}}\bar{W}\delta$ and $\text{vec}(\bar{U}_2) = U_2^{\mathsf{T}}\bar{W}\delta$. Define $Y = \left[\begin{smallmatrix} 0 & 0 \\ I_{2m} & 0 \end{smallmatrix}\right] + FV$, $Z = (UY)^{\mathsf{T}}$,

Algorithm 1: Damped Newton descent for (14)

Input: $E, A, B, C, W, g_0, \beta_0$.
Output: Local minimum (Δ, X, ω) of (14).
Initialize: $\bar{z}_0 = \begin{bmatrix} g_0, \beta_0 \end{bmatrix}^{\mathsf{T}}$, $(x_{v0}, \delta_0) \leftarrow$ See line 3-4
repeat
1 $\quad \beta \leftarrow$ Update step size (see below);
2 $\quad \bar{z} \leftarrow \bar{z} - \beta d$, where $(H + K)d = Z\bar{W}\delta$;
3 $\quad x_v \leftarrow$ Vectorization of solution of (13a) ;
4 $\quad \delta \leftarrow$ Vectorization of solution of (16a)-(16b) ;
until convergence;
return (Δ, X, ω)

and

$$M = V^{\mathsf{T}}\begin{bmatrix}(\bar{U}_2^{\mathsf{T}} \otimes C^{\mathsf{T}})T_{m,p} & T_{2,n}(C^{\mathsf{T}}\bar{U}_1^{\mathsf{T}} \otimes I_2)T_{m,2}\end{bmatrix}\bar{X}^{-1}Y - V^{\mathsf{T}}\tilde{I}^{\mathsf{T}}\tilde{A}(\beta)^{-\mathsf{T}}F^{\mathsf{T}}U^{\mathsf{T}}\bar{W}\delta e^{\mathsf{T}}.$$

Then, the gradient and Hessian of J_W in (14) satisfy

$$\frac{dJ_W}{d\bar{z}} = Z\bar{W}\,\delta, \text{ and} \qquad (17)$$
$$\frac{d^2J_W}{d^2\bar{z}} \triangleq H = Z\bar{W}Z^{\mathsf{T}} + M + M^{\mathsf{T}}. \qquad (18)$$

Proof: See the proof of Lemma 4.1 in [7]. ■

Based on the above result, in Algorithm 1 we present a damped Newton descent method to compute local solutions of the optimization problem (14). Step 2 of Algorithm 1 represents the damped Newton descent step. In this step, the Hessian H is required to be positive-definite. To satisfy this property, we add the term $K = \epsilon I - M - M^{\mathsf{T}}$ to the Hessian, with $0 < \epsilon \ll 1$ [33]. Further, the step size β can be updated using backtracking line search or Armijo's rule [33]. If Assumption 4 is not satisfied in any iteration of Algorithm 1 (i.e., CX does not have full column rank), then we slightly modify (g, β) randomly to ensure that it is satisfied, and continue the iterations. Finally, we run Algorithm 1 multiple times with different random initial conditions in order to capture the global minimum of (14). However, notice that finding the global minimum is not guaranteed.

IV. Simulation Results

We study load-altering attacks on the IEEE 39-bus New England benchmark system shown in Fig. 1. This network consists of 10 generators and 29 load buses. The generator inertia data (H_i) is taken from Table 5, Column 2, in [35], and we use $M_i = \frac{2H_i}{120\pi}$ to compute the moments of inertia. The transmission line reactance data is taken from Table 7, Column 4, in [36]. Since the lines are assumed to be lossless, we compute the admittance as $L_{ij} = \frac{1}{X_{ij}}$, where X_{ij} is the reactance of the line between buses i and j. We choose the generator damping coefficients as $D_1^g = 3$, $D_2^g = \cdots = D_{10}^g = 0.15$, the proportional gains as $K_1^p = 100, K_2^p = K_3^p = 45, K_4^p = 10, K_5^p = K_{10}^p = 50, K_6^p = K_9^p = 40, K_7^p = 30, K_8^p = 20$, the integral gains as $K_1^i = \cdots = K_{10}^i = 60$ and the load coefficients as $D_1^l = \cdots = D_{10}^l = 0.1$. For all simulations, the weight

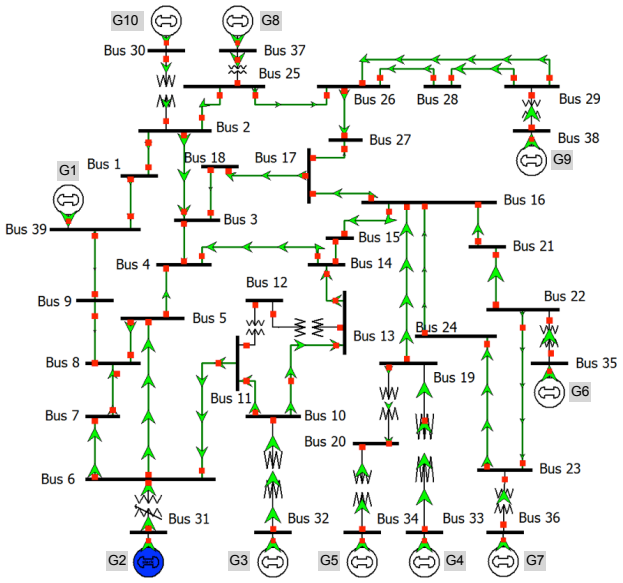


Fig. 1. The IEEE 39-bus power network with 10 generators and 29 loads. $G1 - G10$ denote the generator numbers. (Image courtesy of https://icseg.iti.illinois.edu/ieee-39-bus-system)

for constructing the matrix W is $\mathbf{w} = 10^4$, and the stopping criteria of Algorithm 1 is $\|\frac{dJ_W}{d\bar{z}}\|_F = \|Z\bar{W}\delta\|_F < 10^{-5}$.

Single-point attacks: We consider attacks on a single load based on the frequency measurements from generators $\{1, 2, 3\}$. We compute the optimal attacks for all loads by solving the optimization problem (14) individually for each load by choosing appropriate weighing matrix W. Fig. 2 shows the 10 lowest (in terms of Frobenius norm) optimal solutions among the ones corresponding to the 29 loads. Intuitively, these loads are the most vulnerable towards a single-point attack since they represent the lowest load-change required to make the power system unstable.[5] This analysis allows us to find a vulnerability map of the whole system.

Next, we show the time response of the power system as the attacker increases the compromised load. We consider an attack on load 11 based on the measurement from generator 1. The optimal attack value is $\Delta^*_{1,1} = -153.55$, and the remaining entries of Δ are constrained to be zero. Fig. 3 shows the frequencies of generators 1 and 2 for three values of $\Delta_{1,1} = \{-152, \Delta^*_{1,1}, -154.5\}$. The spectral abscissa for these cases are $\alpha(A(\Delta), E) = \{-0.18, 0, 0.11\}$, respectively. As the system moves from the stable to the unstable domain, the frequencies in the system become unbounded, confirming that our solution is indeed the minimum-norm destabilizing attack for the considered scenario.

Multi-point attacks: We now consider the case when the attacker is capable of compromising the loads $\{11, 12, 13\}$ simultaneously. We assume that measurements from only one generator are available, and compute the optimal attacks for all the generators. The results are shown in Fig. 4. We notice that the measurements from generator 8 are most effective

[5]Note that this ranking of the nodes according to their vulnerability may change if the measurements are obtained from a different set of generators.

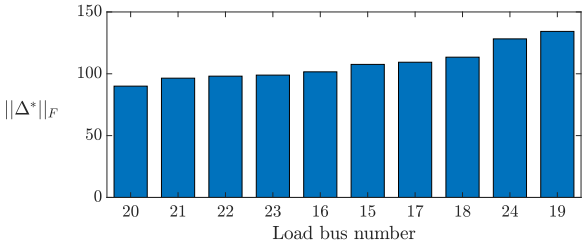
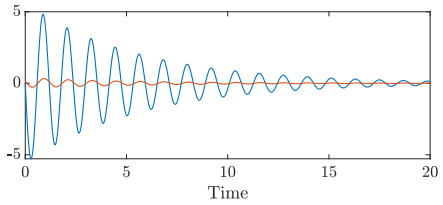
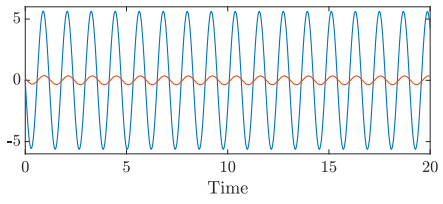


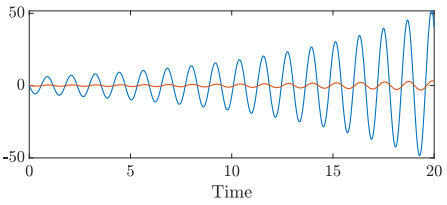
Fig. 2. The minimum load-change $\|\Delta^*\|_F$ required for instability corresponding to the 10 most vulnerable loads. A lower value of $\|\Delta^*\|_F$ indicates more vulnerability.



(a) $\Delta_{1,1} = -152$



(b) $\Delta_{1,1} = -153.55$



(c) $\Delta_{1,1} = -154.5$

Fig. 3. Impulse response of the power system for three different values of $\Delta_{1,1}$. The plots contain the frequencies of generators 1 (blue) and 2 (red).

for the multi-point attack, since it corresponds to the lowest load-change required for instability. The analysis can also be used for multi-attack case that use measurements from multiple generator/load buses. We omit an illustration of such case due to space limitations.

Finally, we focus on the case when measurements from generator 8 are used in the multi-point attack. In this case, Algorithm 1 obtains the global solution $(\Delta^*_{1,8}, \Delta^*_{2,8}, \Delta^*_{3,8}) = (-23.75, -62.34, -39.04)$. Fig. 5 shows an iteration of Algorithm 1: as the iterations progress, the cost decreases monotonically until the minimum is achieved.

V. Conclusion

We derive a theoretical and computational framework to characterize and design minimally-invasive, multi-point, dynamic load-altering attacks against power systems. Our

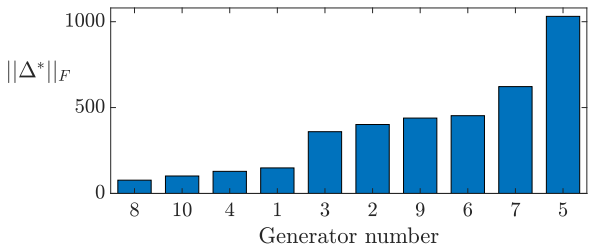


Fig. 4. The minimum load-change $\|\Delta^*\|_F$ required for instability corresponding to attacks on loads $\{11, 12, 13\}$ and measurements from one generator. A lower value of $\|\Delta^*\|_F$ indicates more vulnerability.

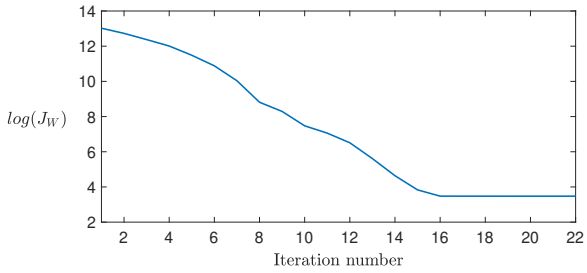


Fig. 5. The cost J_W as the iterations of Algorithm 1 progress. The algorithm converges in 22 iterations.

results allow the operator to identify the most vulnerable loads in the network, and to ultimately design targeted protection mechanisms. From a technical perspective, this paper extends the results in [7] to quantify the real, sparse stability radius of singular linear systems, which arise in the study of power and other mass distribution systems. Future work includes using this analysis for developing a threat mitigation strategy.

REFERENCES

[1] Y. Z. Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto. State of the art of cyber-physical systems security: An automatic control perspective. *The Journal of Systems and Software*, 149(2019):174–216, 2019.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. *Communications Surveys & Tutorials*, 14(4):998–1010, 2012.

[3] K. Moslehi and R. Kumar. A reliability perspective of the smart grid. *IEEE Transactions on Smart Grid*, 1(1):57–64, 2010.

[4] S. Shao, M. Pipattanasomporn, and S. Rahman. Demand response as a load shaping tool in an intelligent grid with electric vehicles. *IEEE Transactions on Smart Grid*, 2(4):624–631, December 2011.

[5] A. Molina-Garciá, F. Bouffard, and D. S. Kirschen. Decentralized demand-side contribution to primary frequency control. *IEEE Transactions on Power Systems*, 26(1):411–419, February 2011.

[6] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad. Dynamic load altering attacks against power system stability: Attack models and protection schemes. *IEEE Transactions on Smart Grid*, 9(4):2862 – 2872, 2016.

[7] V. Katewa and F. Pasqualetti. On the real stability radius of sparse systems. *Automatica*, 113:108685, 2020.

[8] S. Mehrdad, S. Mousavian, G. Madraki, and Y. Dvorkin. Cyber-physical resilience of electrical power systems against malicious attacks: A review. *Current Sustainable/Renewable Energy Reports*, 5(1):14–22, 2018.

[9] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad. Detecting dynamic load altering attacks: A data-driven time-frequency analysis. In *IEEE Int. Conf. on Smart Grid Communications*, pages 503–508, Miami, FL, November 2015.

[10] Z. Wang, H. He, Z. Wan, and Y. Sun. Detection of false data injection attacks in ac state estimation using phasor measurements. *IEEE Transactions on Smart Grid*, 2020. In press.

[11] G. Wu, J. Sun, and J. Chen. Optimal data injection attacks in cyber-physical systems. *IEEE transactions on cybernetics*, 48(12):3302–3312, 2018.

[12] X. Luo, X. Wang, X. Pan, and X. Guan. Detection and isolation of false data injection attack for smart grids via unknown input observers. *IET Generation, Transmission & Distribution*, 13(8):1277–1286, 2019.

[13] F. Pasqualetti, F. Dörfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, 2013.

[14] E. Baron-Prada, E. Osorio, and E. Mojica-Nava. Resilient transactive control in microgrids under dynamic load altering attacks. In *Colombian Conference on Automatic Control*, pages 1–5. IEEE, 2017.

[15] A. Gusrialdi and Z. Qu. Smart grid security: Attacks and defenses. In *Smart grid control*, pages 199–223. Springer, 2019.

[16] R. Germanà, A. Giuseppi, and A. Di Giorgio. Ensuring the stability of power systems against dynamic load altering attacks: A robust control scheme using energy storage systems. In *European Control Conference*, pages 1330–1335. IEEE, 2020.

[17] D. Hinrichsen and A. J. Pritchard. Stability radii of linear systems. *Systems & Control Letters*, 7(1):1–10, 1986.

[18] D. Hinrichsen and A. J. Pritchard. Stability radius for structured perturbations and the algebraic Riccati equation. *Systems & Control Letters*, 8(2):105–113, 1986.

[19] C. Van Loan. How near is a stable matrix to an unstable matrix? *Contemporary Mathematics*, 47:465–478, 1985.

[20] R. Byers. A bisection method for measuring the distance of a stable matrix to the unstable matrices. *SIAM Journal on Scientific and Statistical Computing*, 9(5):875–881, 1988.

[21] D. Hinrichsen, B. Kelb, and A. Linnemann. An algorithm for the computation of the structured complex stability radius. *Automatica*, 25(5):771–775, 1989.

[22] S. Boyd, V. Balakrishnan, and P. Kabamba. A bisection method for computing the H_∞-norm of a transfer matrix and related problems. *Mathematics of Control, Signals and Systems*, 2(3):207–219, 1989.

[23] S. Boyd and V. Balakrishnan. A regularity result for the singular values of a transfer matrix and a quadratically convergent algorithm for computing its H_∞-norm. *Systems & Control Letters*, 15(1):1–7, 1990.

[24] N. A. Bruinsma and M. Steinbucha. A fast algorithm to compute the H_∞-norm of a transfer function matrix. *Systems & Control Letters*, 14(4):287–293, 1990.

[25] L. Qiu and E. J. Davison. The stability robustness determination of state space models with real unstructured perturbations. *Mathematics of Control, Signals and Systems*, 4(3):447–267, 1991.

[26] L. Qiu and E. J. Davison. Bounds on the real stability radius. In *Robustness of Dynamic Systems with Parameter Uncertainties*, pages 139–145, 1992.

[27] L. Qiu, B. Bernhardsson, A. Rantzer, E. J. Davison, P. M. Young, and J. C. Doyle. A formula for computation of the real stability radius. *Automatica*, 31(6):879–890, 1995.

[28] S. C. Johnson, M. Wicks, M. Zefran, and R. A. DeCarlo. The structured distance to the nearest system without property $\mathcal{P}$. *IEEE Transactions on Automatic Control*, 63(9):2960–2975, 2018.

[29] P. Kundur. *Power System Stability and Control*. McGraw-Hill, 1994.

[30] J. D. Glover, M. S. Sarma, and T. J. Overbye. *Power System Analysis and Design*. Cengage Learning, 5th edition, 2009.

[31] C. Zhao, U. Topcu, N. Li, and S. Low. Design and stability of load-side primary frequency control in power systems. *IEEE Transactions on Automatic Control*, 59(5):1177–1189, 2014.

[32] S. P. Bhattacharyya and E. De Souza. Pole assignment via Sylvester's equation. *Systems & Control Letters*, 1(4):261—263, 1982.

[33] D. G. Luenberger and Y Ye. *Linear and Nonlinear Programming*. Springer, 3 edition, 2008.

[34] K. E Chu. On the solutions of the matrix equations $AXB - CXD = E$ AND $(YA - DZ, YC - BZ) = (E, F)$. *Linear Algebra and its Applications*, 93:93–105, 1987.

[35] T. Athay, R. Podmore, and S. Virmani. A practical method for the direct analysis of transient stability. *IEEE Transactions on Power Apparatus and Systems*, 98(2):573–584, 1979.

[36] I. Hiskens. IEEE PES task force on benchmark systems for stability controls. Technical report, 2013.