Analysis of IoT-Based Load Altering Attacks Against Power Grids Using the Theory of Second-Order Dynamical Systems

Subhash Lakshminarayana, *Senior Member, IEEE*, Sondipon Adhikari, and Carsten Maple

***Abstract*—Recent research has shown that large-scale Internet of Things (IoT)-based load altering attacks can have a serious impact on power grid operations such as causing unsafe frequency excursions and destabilizing the grid's control loops. In this work, we present an analytical framework to investigate the impact of IoT-based static/dynamic load altering attacks (S/DLAAs) on the power grid's dynamic response. Existing work on this topic has mainly relied on numerical simulations and, to date, there is no analytical framework to identify the victim nodes from which that attacker can launch the most impactful attacks. To address these shortcomings, we use results from second-order dynamical systems to analyze the power grid frequency control loop under S/DLAAs. We use parametric sensitivity of the system's eigensolutions to identify victim nodes that correspond to the *least-effort* destabilizing DLAAs. Further, to analyze the SLAAs, we present closed-form expression for the system's frequency response in terms of the attacker's inputs, helping us characterize the minimum load change required to cause unsafe frequency excursions. Using these results, we formulate the defense against S/DLAAs as a linear programming problem in which we determine the minimum amount of load that needs to be secured at the victim nodes to ensure system safety/stability. Extensive simulations conducted using benchmark IEEE-bus systems validate the accuracy and efficacy of our approach.**

***Index Terms*—IoT-based load altering attacks, second-order dynamical systems, eigenvalue sensitivity, attack impact.**

I. Introduction

THE ELECTRIC grid is undergoing a fundamental transformation from a centralized, producer-controlled network to one that integrates distributed players in its operations. Programs such as demand response seek the active involvement of end-users in reducing the grid's peak demand. Moreover, there is also a growing integration of Internet-of-Things (IoT) enabled devices at the consumer side, such as Wi-Fi-enabled air conditioners and residential battery energy storage systems [1], which can be remotely controlled using personal computers or mobile phones such as smartphones, PC/tablets. These intelligent devices provide convenience, efficiency and monitoring capabilities, enabling consumers to better manage their usage.

However, IoT-enabled consumer appliances are often poorly engineered from a security point of view [2], [3]. As such, they may become convenient entry points for malicious parties to gain access to the system and disrupt important grid operations by abruptly changing the demand. Cyber attacks targeting bulk power grid operations and state estimation problems have received significant attention [4], [5], [6], [7], [8]. In contrast, research on cyber attacks that target the end-user consumer devices is relatively new. Although Internet-based load altering attacks were first introduced in [9], which identified various load devices that are vulnerable to such attacks and proposed defense strategies, it was only recently that large-scale load altering attacks were studied considering a IoT-Botnet type attack [10], [11], [12]. These works showed sudden and abrupt manipulation of the power grid demand due to such attacks can increase the grid's operational cost, and in some cases, cause unsafe frequency excursions. While power grid protection mechanisms such as under frequency load shedding (UFLS) can prevent large-scale blackouts, nevertheless, load-altering attacks remain capable of causing a partition in bulk power systems and/or a controlled load shedding event [13]. The aforementioned works are representatives of the so-called *static load altering attacks* (SLAAs), which involves a one-time manipulation of the demand.

More severe attacks are the so-called *dynamic load altering attacks* (DLAAs), in which the attacker changes the amount of compromised load over time to follow a certain trajectory [14], [15]. In contrast to SLAAs, DLAAs require the attacker to monitor certain power grid signals (e.g., frequency) and alter the load in response to the fluctuations of the signal. This is feasible due to the availability of inexpensive commercial sensors to monitor the grid frequency (e.g., see [16]), and they can be installed at any power outlet of the grid. These devices are already installed in existing frequency-sensitive loads that participate in the grid frequency regulation [17]. While DLAAs require enhanced capabilities on the part of the attacker, they can have a much more severe impact on grid operations than SLAAs, such as destabilizing the power grid control loops [14], leading to generator trips and cascading failures.

Manuscript received September 21, 2020; revised February 12, 2021; accepted March 26, 2021. Date of publication April 1, 2021; date of current version August 23, 2021. This work was supported in part by the Startup Grant from the University of Warwick. The work of Carsten Maple was supported by the Alan Turing Institute and PETRAS, UK's National Centre of Excellence for IoT Systems Cyber Security. Paper no. TSG-01429-2020. *(Corresponding author: Subhash Lakshminarayana.)*

Subhash Lakshminarayana is with the School of Engineering, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: subhash.lakshminarayana@warwick.ac.uk).

Sondipon Adhikari is with the College of Engineering, Swansea University, Swansea SA2 8PP, U.K. (e-mail: s.adhikari@swansea.ac.uk).

Carsten Maple is with the Warwick Manufacturing Group, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: cm@warwick.ac.uk).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2021.3070313.

Digital Object Identifier 10.1109/TSG.2021.3070313

A major shortcoming of existing work on load altering attacks is that they either adopt a simulation-based approach (e.g., [12] to assess the impact of SLAAs) or employ methods such as root locus analysis (e.g., [14] to assess the impact of DLAAs). However, these approaches can be computationally expensive as they require exhaustive simulations or eigenvalue computations under all possible combinations of nodes that could be targeted by the attacker (in a coordinated multi-point attack). They do not provide any physical insights into the system under DLAAs and SLAAs. Moreover, to date, there is no analytical method to identify the nodes that are most vulnerable to DLAAs and SLAAs. Amini *et al.* [14] also propose a defense against DLAAs based on securing a portion of the vulnerable loads. However, finding the locations and the amount of the loads which must be secured requires solving a non-convex pole placement optimization problem that is computationally complex. A concurrent work [18] presents an alternative defense by the use of energy storage systems to compensate for the destabilizing effects of DLAAs. However, the design requires further research on tuning the control parameters to ensure system stability under DLAAs.

To address these shortcomings, in this work, we present an analytical and low-complexity approach to assess the system's vulnerabilities and identify the victim nodes that correspond to the "least-effort" DLAAs that will destabilize the system or SLAAs that will cause unsafe frequency excursions. Here "least effort" is in terms of the amount vulnerable load that needs to be compromised at the victim buses to achieve the aforementioned objectives. As in prior work on this topic [14], [15], [19], we use linear swing equations in our analysis. Our approach is based on the theory of second-order dynamical systems [20].

We make two important contributions. First, to analyze DLAAs, we compute the system's *parametric eigenvalue sensitivities*. The sensitivity factors are a linear approximation that predict how much the system's eigenvalues change due to an incremental change in the attack parameters. The sensitivities can then be used to predict the attack impact on the system's stability. A major advantage of this approach is that the parametric sensitivity factors need to be computed considering single-point attacks only (i.e., considering DLAA at only one node of the grid at a time). Since the sensitivities are a linear approximation, the eigenvalues of the system under a coordinated multi-point attack can be approximated using the sum of eigenvalue sensitivities of multiple single-point attacks. Thus, the impact of multi-point attacks can be predicted using results from the single-point attacks. Moreover, the computation of the parametric sensitivity factors itself is computationally cheap. Using the sensitivity approach, we propose a defense strategy against DLAAs in which we compute the least-amount of load that needs to be secured at each of the victim nodes to ensure system stability. The defense problem requires solving a simple linear programming problem, which is also computationally cheap.

Second, to analyze SLAAs, we present a closed-form expression of the system's dynamic response due to a sudden change in the system load, in terms of its eigensolutions. Using these expressions, we can compute the maximum fluctuation in the system's frequency response due to a unit change in the load at a particular victim node, which helps us identify the victim node corresponding to the least-effort SLAAs. The closed-form expression also enables us to formulate the defense against SLAAs as a linear programming problem, in which we compute the least-amount of load that needs to be secured at each of the victim nodes to ensure no unsafe frequency excursions due to SLAAs.

Our results show that the eigenvalues obtained by the parametric sensitivity approach can accurately predict the true eigenvalues of the system under DLAAs over a wide range of attacker's parameters. Moreover, they also accurately characterize the nodes corresponding to the least-effort DLAAs. Our results also provide closed-form expressions to characterize the minimum values of attack control parameters that will destabilize the system (for DLAAs) and minimum change in the system load that will cause unsafe frequency excursions (for SLAAs) in terms of the system's eigensolutions. Further, the proposed defense can efficiently secure the system against destabilizing DLAAs or SLAAs.

To the best of our knowledge, this work is the first to apply results from the theory of second-order dynamical systems to analyze load altering attacks against power grids. The theory has been provably applied extensively in vibration problems in civil, mechanical, and aerospace engineering [21]. While eigenvalue sensitivities have been applied in the past in power systems research for planning and analysis purposes (see, e.g., [22], [23]), they have not been utilized in a power grid security context. In particular, the application of parametric sensitivity analysis of second-order systems to analyze DLAAs and SLAAs is novel; this is one of the important contributions of our work.

The rest of the article is organized as follows. We present the system model in Section II. We provide a brief overview of the theory of second-order systems in Section III. Using this theory, we analyze DLAAs and SLAAs in Section IV and Section V respectively. We present the simulation results in Section VI and conclude in Section VII.

Notations: We use bold font lower case and upper case to denote vectors and matrices respectively. We denote the i^{th} entry of vector $\mathbf{x}$ by x_i and the $(i,j)^{\text{th}}$ entry of a matrix $\mathbf{X}$ by $\mathbf{X}_{i,j}$. The real and imaginary parts of a complex number X are denoted by $\text{Re}(X)$ and $\text{Im}(X)$ respectively. We use $\mathbf{O}$ to denote a matrix of all zeros, $\underline{0}$ to denote a vector of zeros, and $\mathbf{I}$ to denote the identity matrix. We use $[\mathbf{x}; \mathbf{y}]$ to denote the concatenation of vectors $\mathbf{x}$ and $\mathbf{y}$.

II. System Model

Power Grid Model: We consider a power grid consisting of a set of $\mathcal{N} = \{1, \ldots, N\}$ buses. The set of buses are divided into generator buses $\mathcal{G} = \{g_1, \ldots, g_{N_G}\}$ and load buses $\mathcal{L} = \{l_1, \ldots, l_{N_L}\}$, where N_G and N_L represent the number of generator and load buses respectively and $\mathcal{N} = \mathcal{G} \cup \mathcal{L}$. Here in, g_i and l_i represent the index of the i^{th} generator and load bus respectively. We let $\mathbf{p}^L \in \mathbb{R}^{N_L}$ denote the vector of demands at the load buses $\mathcal{L}$. The linearized version of the power grid

dynamic model is given by the differential equations [24]:

$$\begin{bmatrix} \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & -\mathbf{M} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \end{bmatrix} \begin{bmatrix} \dot{\boldsymbol{\delta}} \\ \dot{\boldsymbol{\theta}} \\ \dot{\boldsymbol{\omega}} \\ \dot{\varphi} \end{bmatrix} = \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{p}^L \end{bmatrix} + \begin{bmatrix} \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} \\ \mathbf{K}^I + \mathbf{B}^{GG} & \mathbf{B}^{GL} & \mathbf{K}^P + \mathbf{D}^G & \mathbf{O} \\ \mathbf{B}^{LG} & \mathbf{B}^{LL} & \mathbf{O} & \mathbf{D}^L \end{bmatrix} \begin{bmatrix} \boldsymbol{\delta} \\ \boldsymbol{\theta} \\ \boldsymbol{\omega} \\ \varphi \end{bmatrix}, \quad (1)$$

where $\boldsymbol{\delta}, \boldsymbol{\omega} \in \mathbb{R}^{N_G}$ comprise the phase angles and rotor frequency deviations at the generator buses respectively, $\boldsymbol{\theta}, \varphi \in \mathbb{R}^{N_L}$ comprise the phase angles and the frequency deviations of the load buses respectively. $\mathbf{M}, \mathbf{D}^G \in \mathbb{R}^{N_G \times N_G}$ and $\mathbf{D}^L \in \mathbb{R}^{N_L \times N_L}$ are diagonal matrices with their diagonal entries given by the generator inertia and generator damping coefficients and load damping coefficients respectively. $\mathbf{K}^I, \mathbf{K}^P \in \mathbb{R}^{N_G \times N_G}$ are diagonal matrices with their diagonal entries given by the integral and proportional control coefficients of the generators respectively. Matrices $\mathbf{B}^{GG} \in \mathbb{R}^{N_G \times N_G}$, $\mathbf{B}^{LL} \in \mathbb{R}^{N_L \times N_L}$, $\mathbf{B}^{GL} \in \mathbb{R}^{N_G \times N_L}$ are sub-matrices of the admittance matrix, derived as $\mathbf{B}_{bus} = \begin{bmatrix} \mathbf{B}^{GG} & \mathbf{B}^{GL} \\ \mathbf{B}^{LG} & \mathbf{B}^{LL} \end{bmatrix}$. We denote ω_{nom} as the grid's nominal frequency, e.g., 50 Hz in Europe or 60 Hz in North America. For safe operations, the frequency must be maintained within the safety limits. We denote $\omega_{\max}$ as the maximum permissible frequency deviation for system safety. Thus, $|\omega_{\text{nom}} - \omega_i| \leq \omega_{\max}, \forall i \in \mathcal{G}$. We note that in steady state, $\dot{\omega}_i = 0, \forall i \in \mathcal{G}$.

Load Altering Attacks: Under IoT-based load-altering attacks, the attacker manipulates the system load by synchronously switching on or off a large number of high-wattage devices. Assume that the demand at the load buses consists of two components $\mathbf{p}^L = \mathbf{p}^{LS} + \mathbf{p}^{LV}$, where $\mathbf{p}^{LS}$ denotes the secure part of the load (i.e., load that cannot be altered) and $\mathbf{p}^{LV}$ denotes the vulnerable part of the load. We denote the set of victim nodes by $\mathcal{V}(\subseteq \mathcal{L})$, and $N_v = |\mathcal{V}|$, which are the subset of load buses at which the attacker can manipulate the load. The system load under load-altering attacks, which we denote by $\mathbf{p}_a^L$, is given by

$$\mathbf{p}_a^L = \mathbf{p}^{LS} + \boldsymbol{\epsilon}^L - \mathbf{K}^{LG}\boldsymbol{\omega} - \mathbf{K}^{LL}\varphi. \quad (2)$$

Herein, $\boldsymbol{\epsilon}^L$ is a step-change in the load introduced by the attacker. Note $\epsilon_i^L = 0$ if $i \notin \mathcal{V}$. The components $\mathbf{K}^{LG}\boldsymbol{\omega}$ and $\mathbf{K}^{LL}\varphi$ are time-varying load altering attacks that follows the frequency fluctuations of the generator buses and load buses respectively (note that these are a series of load alterations whose magnitude is varying with time). We assume that the attacker can monitor the frequency at a subset of the generator buses $\mathcal{S}_G(\subseteq \mathcal{N}_G)$, and/or a subset of load buses $\mathcal{S}_L(\subseteq \mathcal{N}_L)$, by accessing the frequency measuring devices at these nodes. We denote $\mathcal{S} = \mathcal{S}_G \cup \mathcal{S}_L$. $\mathbf{K}^{LG} \in \mathbb{R}^{N_L \times N_G}$ and $\mathbf{K}^{LL} \in \mathbb{R}^{N_L \times N_L}$ denote matrices consisting of attack controller gain values, where the elements $\mathbf{K}_{i,j}^{LG}$ are the gains corresponding to the attack at load bus $i \in \mathcal{N}_L$ that follows the frequency at generator bus $j \in \mathcal{N}_G$. Similarly, $\mathbf{K}_{i,j}^{LL}$ are the gains that follows the frequency at the load bus $j \in \mathcal{N}_L$. Note that $\mathbf{K}_{i,j}^{LG} = 0$ or $\mathbf{K}_{i,j}^{LL} = 0$ either if $i \notin \mathcal{V}$ or $j \notin \mathcal{S}$. The power grid dynamics (1) with the load altering attack in (2) becomes

$$\begin{bmatrix} \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & -\mathbf{M} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \end{bmatrix} \begin{bmatrix} \dot{\boldsymbol{\delta}} \\ \dot{\boldsymbol{\theta}} \\ \dot{\boldsymbol{\omega}} \\ \dot{\varphi} \end{bmatrix} = \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \\ \mathbf{p}^{LS} + \boldsymbol{\epsilon}^L \end{bmatrix} + \begin{bmatrix} \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} \\ \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} \\ \mathbf{K}^I + \mathbf{B}^{GG} & \mathbf{B}^{GL} & \mathbf{K}^P + \mathbf{D}^G & \mathbf{O} \\ \mathbf{B}^{LG} & \mathbf{B}^{LL} & -\mathbf{K}^{LG} & -\mathbf{K}^{LL} + \mathbf{D}^L \end{bmatrix} \begin{bmatrix} \boldsymbol{\delta} \\ \boldsymbol{\theta} \\ \boldsymbol{\omega} \\ \varphi \end{bmatrix}. \quad (3)$$

The limits on the attack components are given as follows. $\boldsymbol{\epsilon}^L \leq \mathbf{p}^{LV}, K_{v,s}^L \geq 0$ and

$$\sum_{s \in \mathcal{S}} K_{v,s}^L \omega_s^{\max} \leq (P_v^{LV} - \epsilon_v^L)/2, \forall v \in \mathcal{V}. \quad (4)$$

The limit in (4) can be explained as follows. First note that $\sum_{s \in \mathcal{S}} K_{v,s}^L \omega_s^{\max}$ is the maximum value of the load to be altered by the attacker at victim bus v before the frequency at any sensor bus s exceeds the safety limit $\omega_s^{\max}$. (Herein, we have used $\mathbf{K}^L$ as a short-hand notation to denote either $\mathbf{K}^{LG}$ or $\mathbf{K}^{LL}$.) This must be less than the amount of vulnerable load, i.e., $P_v^{LV} - \epsilon_v$ (after removing the step change). Finally, the factor of 2 in the denominator of the RHS represents the fact that the amount of load that can be compromised must allow for both over and under frequency fluctuations before the system frequency exceeds $\omega_s^{\max}$ (see [14]).

Problem Formulation: Within the framework of (2), we consider two types of load-altering attacks: (i) SLAAs, which consist of an abrupt one-time increase/decrease in power demand. In this case $\boldsymbol{\epsilon}^L \neq \mathbf{0}$ and $\mathbf{K}^{LG} = \mathbf{K}^{LL} = \mathbf{O}$. As shown in [12], if the value of $\boldsymbol{\epsilon}^L$ is large, this will result in unsafe frequency excursions. (ii) DLAAs, in which $\mathbf{K}^{LG}, \mathbf{K}^{LL} \neq \mathbf{O}$. Under DLAAs, the attacker can alter the eigenvalues of the system indirectly by changing the elements of the matrix $\mathbf{K}^{LG}$ or $\mathbf{K}^{LL}$. Thus, DLAAs can potentially destabilize the power grid frequency control loop [14].

The objectives of this work are two-fold: (1) identify the victim nodes that correspond to the least-effort SLAAs and DLAAs, i.e., buses from which an unsafe excursion or destabilizing attack can be launched by altering the least amount of load, and (2) find a low-computational defense strategy that computes the least amount of load to be secured at the victim nodes such that the attacker cannot launch a successful SLAAs or DLAAs. The results give us fundamental insights into identifying vulnerable nodes in the grid that are susceptible to DLAAs and SLAAs, and reinforce them to enhance the grid's resilience.

In the following section, we first provide a brief overview of general second-order systems and describe results from parametric sensitivities of its eigensolutions and dynamic response. Then, in Sections IV and V, we apply these results to analyze DLAAs and SLAAs respectively.

III. Brief Review of General Second-Order Systems

Second-order matrix differential equations form the essential basis for the linear dynamic analysis of mechanical systems since their introduction by Rayleigh [25] in 1877. The standard second-order system is given by the following dynamic equation:

$$\boldsymbol{\mathcal{M}}\ddot{\mathbf{u}}(t) + \boldsymbol{\mathcal{C}}\dot{\mathbf{u}}(t) + \boldsymbol{\mathcal{G}}\mathbf{u}(t) = \mathbf{f}(\mathbf{t}). \tag{5}$$

Here $\mathbf{u}(t) \in \mathbb{R}^N$ and $\mathbf{f}(t) \in \mathbb{R}^N$ are the response vector and the forcing vector respectively. The system matrices in equation (5), namely $\boldsymbol{\mathcal{M}}$, $\boldsymbol{\mathcal{C}}$ and $\boldsymbol{\mathcal{G}} \in \mathbb{R}^{N\times N}$, are the so-called inertia, damping and stiffness matrices. In general they are real and non-symmetric matrices. However, for many mechanical systems these matrices become symmetric matrices. In that case a simplified approach, known as the modal analysis [21], is available. Under certain conditions, a general non-symmetric system can be transformed into an equivalent symmetric system [26]. For such symmetric linear systems, dynamic response in the frequency domain can be obtained efficiently [27] using the eigenvalues and eigenvectors of the system.

A. Eigenvalues and Eigenvectors of Second-Order System

The eigenvalues and the eigenvectors are important descriptors of the system and they together determine the system's dynamic response. The *right* eigenvalue problem associated with the second-order system in(5) can be represented by the $\lambda-$matrix problem as

$$\lambda_j^2\boldsymbol{\mathcal{M}}\mathbf{u}_j + \lambda_j\boldsymbol{\mathcal{C}}\mathbf{u}_j + \boldsymbol{\mathcal{G}}\mathbf{u}_j = \underline{0}, \quad \forall j = 1, \ldots, N$$

where $\lambda_j \in \mathbb{C}$ is the j-th latent root (eigenvalue) and $\mathbf{u}_j \in \mathbb{C}^N$ is the j-th right latent vector (right eigenvector). The *left* eigenvalue problem can be represented by

$$\lambda_j^2\mathbf{b}_j^\top\boldsymbol{\mathcal{M}} + \lambda_j\mathbf{b}_j^\top\boldsymbol{\mathcal{C}} + \mathbf{b}_j^\top\boldsymbol{\mathcal{G}} = \underline{0}^\top, \quad \forall j = 1, \ldots, N$$

where $\mathbf{b}_j \in \mathbb{C}^N$ is the j-th left latent vector (left eigenvector) and $(\bullet)^\top$ denotes the matrix transpose. When **M, C** and **G** are general asymmetric matrices the right and left eigenvectors can easily be obtained from the first-order formulations, for example, the state-space method or Duncan forms [28]. Equation (5) is transformed into the first-order (Duncan) form as

$$\boldsymbol{\mathcal{A}}\dot{\mathfrak{z}}(t) + \boldsymbol{\mathcal{B}}\mathfrak{z}(t) = \mathfrak{f}(t) \tag{6}$$

where $\boldsymbol{\mathcal{A}}$, $\boldsymbol{\mathcal{B}} \in \mathbb{R}^{2N\times 2N}$ are the system matrices, $\mathfrak{f}(t) \in \mathbb{R}^{2N}$ is the forcing vector and $\mathfrak{z}(t) \in \mathbb{R}^{2N}$ is the state vector given by

$$\boldsymbol{\mathcal{A}} = \begin{bmatrix} \boldsymbol{\mathcal{C}} & \boldsymbol{\mathcal{M}} \\ \boldsymbol{\mathcal{M}} & \mathbf{O} \end{bmatrix}, \boldsymbol{\mathcal{B}} = \begin{bmatrix} \boldsymbol{\mathcal{G}} & \mathbf{O} \\ \mathbf{O} & -\boldsymbol{\mathcal{M}} \end{bmatrix} \tag{7}$$

$$\mathfrak{f}(t) = \begin{Bmatrix} \mathbf{f}(t) \\ \mathbf{0} \end{Bmatrix}, \mathfrak{z}(t) = \begin{Bmatrix} \mathfrak{u}(t) \\ \dot{\mathfrak{u}}(t) \end{Bmatrix}. \tag{8}$$

Taking the Laplace transform of equation (6) we obtain

$$s\boldsymbol{\mathcal{A}}\bar{\mathbf{z}}(s) + \boldsymbol{\mathcal{B}}\bar{\mathbf{z}}(s) = \bar{\mathbf{f}}(s) + \boldsymbol{\mathcal{A}}\mathbf{z}_0 \tag{9}$$

Here, $\bar{\mathbf{z}}(s)$ is the Laplace transform of $\mathfrak{z}(t)$ and $\bar{\mathbf{f}}(s)$ is the Laplace transform of $\mathfrak{f}(t)$ and the initial condition vector in the state-space $\mathfrak{z}(0) = \mathbf{z}_0$. The vector $\mathbf{p}(s) = \bar{\mathbf{f}}(s) + \boldsymbol{\mathcal{A}}\mathbf{z}_0$ is the effective state-space forcing function in the Laplace domain.

The *right* and *left* eigenvalue problem associated with equation (6) can be expressed as

$$\lambda_j\boldsymbol{\mathcal{A}}\mathbf{z}_j + \boldsymbol{\mathcal{B}}\mathbf{z}_j = \underline{0}, \forall j = 1, \ldots, 2N,$$
$$\lambda_j\mathbf{y}_j^\top\boldsymbol{\mathcal{A}} + \mathbf{y}_j^\top\boldsymbol{\mathcal{B}} = \underline{0}, \forall j = 1, \ldots, 2N,$$

where $\lambda_j \in \mathbb{C}$ is the j-th eigenvalue and $\mathbf{z}_j, \mathbf{y}_j \in \mathbb{C}^{2N_G}$ is the j-th right/left eigenvector which is related to the j-th right/left eigenvector of the second-order system as $\mathbf{z}_j = [\mathbf{u}_j; \lambda_j\mathbf{u}_j]$ and $\mathbf{y}_j = [\mathbf{b}_j; \lambda_j\mathbf{b}_j]$.

B. Dynamic Response of the Second-Order System

The eigenvalues along with the right and left eigenvectors of the first-order system can be used to obtain the dynamic response of the system in an efficient manner under general forcing and initial conditions. The transfer function matrix of the system in the Laplace domain can be expressed in terms of the eigensolutions (see for example [29]) as $\mathbf{H}(s) = \sum_{j=1}^{2N_G} \frac{\mathbf{z}_j\mathbf{y}_j^\top}{(s-\lambda_j)}$. Using this, the response vector can be obtained from equation (9) as

$$\bar{\mathbf{z}}(s) = \mathbf{H}(s)\mathbf{p}(s) = \sum_{j=1}^{2N_G} \frac{\mathbf{y}_j^\top\mathbf{p}(s)}{(s-\lambda_j)}\mathbf{z}_j. \tag{10}$$

This is the most general expression of the response vector as a function of the total forcing function $\mathbf{p}(s)$ includes both the initial conditions and applied forcing. We consider a special case when the applied forcing function is a step function of the form $\mathfrak{f}(t) = U(t)\mathbf{f}_0$, where $\mathbf{f}_0$ is a vector containing amplitudes of the forcing at different degrees of freedom and $U(\bullet)$ is a unit step function. Using this we obtain $\mathbf{p}(s) = \frac{1}{s}\mathbf{f}_0 + \boldsymbol{\mathcal{A}}\mathbf{z}_0$. Substituting this expression of $\mathbf{p}(s)$ in equation (10) and taking the inverse Laplace transform of equation (10), we obtain

$$\mathfrak{z}(t) = \sum_{j=1}^{2N_G} a_j(t)\mathbf{z}_j, \tag{11}$$

$$\text{where } a_j(t) = \left(\frac{e^{\lambda_j t} - 1}{\lambda_j}\right)\mathbf{y}_j^\top\mathbf{f}_0 + e^{\lambda_j t}\left(\mathbf{y}_j^\top\boldsymbol{\mathcal{A}}\mathbf{z}_0\right). \tag{12}$$

Equations (11) and (12) give the general closed-form expression of the response vector of non-symmetric second-order dynamic systems in terms of the eigensolutions.

C. Parametric Sensitivity of the Eigensolutions

A key interest in this article is to quantify the change in the system characteristics and the response when elements of the system matrices change. To include all possible changes in the system matrices in a generic manner, we assume that the system matrices $\boldsymbol{\mathcal{M}}$, $\boldsymbol{\mathcal{C}}$ and $\boldsymbol{\mathcal{G}}$ are functions of a parameter vector $\boldsymbol{\alpha} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}^\top \in \mathbb{R}^m$. As a result, the mass, damping and stiffness matrices become functions of $\boldsymbol{\alpha}$, that is $\boldsymbol{\mathcal{M}} \equiv \boldsymbol{\mathcal{M}}(\boldsymbol{\alpha}), \boldsymbol{\mathcal{C}} \equiv \boldsymbol{\mathcal{C}}(\boldsymbol{\alpha})$ and $\boldsymbol{\mathcal{G}} \equiv \boldsymbol{\mathcal{G}}(\boldsymbol{\alpha})$. We consider these functions to be smooth, continuous and differentiable. There are several publication which discuss the parametric sensitivity of the eigensolutions of symmetric second-order systems (see

for example [20]). Below we follow the derivations in [30] for non-symmetric second-order systems.

1) Sensitivity of Eigenvalues: We consider a generic element in the parameter vector $\alpha_m \in \boldsymbol{\alpha}$. The sensitivity of the eigenvalue of a second-order system with respect to the parameter α_m is given by [30]:

$$\frac{\partial \lambda_j}{\partial \alpha_m} = -\mathbf{y}_j^\top \left[\lambda_j \frac{\partial \boldsymbol{\mathcal{A}}}{\partial \alpha_m} + \frac{\partial \boldsymbol{\mathcal{B}}}{\partial \alpha_m} \right] \mathbf{z}_j. \tag{13}$$

Note that the derivative of a given eigenvalue requires the knowledge of only the corresponding eigenvalue and right and left eigenvectors under consideration, and thus a complete solution of the eigenproblem is not required.

2) Sensitivity of Eigenvectors: The sensitivity of the eigenvector of a second-order system with respect to the parameter α_m is given by [30]:

$$\frac{\partial \mathbf{z}_j}{\partial \alpha_m} = \sum_{l=1}^{2N_G} a_{jl}^{(\alpha)} \mathbf{z}_l \text{ and } \frac{\partial \mathbf{y}_j}{\partial \alpha_m} = \sum_{l=1}^{2N_G} b_{jl}^{(\alpha)} \mathbf{y}_l. \tag{14}$$

Here $a_{jl}^{(\alpha)}$ and $b_{jl}^{(\alpha)}$, $\forall\, l = 1, \ldots, 2N$ are sets of complex constants defined as

$$a_{jl}^{(\alpha)} = -\mathbf{y}_l^\top \left[\lambda_j \frac{\partial \boldsymbol{\mathcal{A}}}{\partial \alpha_m} + \frac{\partial \boldsymbol{\mathcal{B}}}{\partial \alpha_m} \right] \mathbf{z}_j, l = 1, \ldots, 2N; l \neq j,$$

$$b_{jl}^{(\alpha)} = -\mathbf{y}_j^\top \left[\lambda_j \frac{\partial \boldsymbol{\mathcal{A}}}{\partial \alpha_m} + \frac{\partial \boldsymbol{\mathcal{B}}}{\partial \alpha_m} \right] \mathbf{z}_l, l = 1, \ldots, 2N; l \neq j,$$

$$\text{and } a_{jj}^{(\alpha)} = b_{jj}^{(\alpha)} = -\frac{1}{2} \mathbf{b}_j^\top \left[2\lambda_j \frac{\partial \mathbf{M}}{\partial \alpha_m} + \frac{\partial \mathbf{C}}{\partial \alpha_m} \right] \mathbf{u}_j.$$

3) Sensitivity of the Step-Response: Using the results above, we derive the sensitivity of the step response with respect to the change in the parameter α_m. The result is summarized in the following proposition.

Proposition 1: The parametric sensitivity of the step response with respect to α can be computed as

$$\frac{\partial \mathfrak{z}(t)}{\partial \alpha_m} = \sum_{j=1}^{2N_G} \left(\frac{\partial a_j(t)}{\partial \alpha_m} \mathbf{z}_j + a_j(t) \frac{\partial \mathbf{z}_j}{\partial \alpha_m} \right), \tag{15}$$

where $\frac{\partial a_j(t)}{\partial \alpha_m}$ is a function of the eigenvalues and the eigenvectors and their derivatives.

The expression of $\frac{\partial a_j(t)}{\partial \alpha_m}$ and the derivation of Proposition 1 is presented in a technical report [31].

IV. Analysis of Dynamic Load Altering Attacks Based on Second-Order System Theory

We now employ the results presented in Section III to analyze DLAAs. Using some straightforward manipulations, the power grid dynamic equations in (3) can be converted into the second-order system as

$$\underbrace{\begin{bmatrix} \mathbf{M} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} \end{bmatrix}}_{\boldsymbol{\mathcal{M}}} \begin{bmatrix} \ddot{\boldsymbol{\omega}} \\ \ddot{\varphi} \end{bmatrix} + \underbrace{\begin{bmatrix} \mathbf{K}^P + \mathbf{D}^G & \mathbf{O} \\ -\mathbf{K}^{LG} & \mathbf{K}^{LL} \end{bmatrix}}_{\boldsymbol{\mathcal{C}}} \begin{bmatrix} \dot{\boldsymbol{\omega}} \\ \dot{\varphi} \end{bmatrix} + \underbrace{\begin{bmatrix} \mathbf{K}^I + \mathbf{B}^{GG} & \mathbf{B}^{GL} \\ \mathbf{B}^{LG} & \mathbf{B}^{LL} \end{bmatrix}}_{\boldsymbol{\mathcal{G}}} \begin{bmatrix} \boldsymbol{\omega} \\ \varphi \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{0} \\ -(\mathbf{p}^{LS} + \boldsymbol{\epsilon}^L) \end{bmatrix}}_{\mathbf{f}_0}. \tag{16}$$

Let $\{\lambda_i\}_{i=1}^{2N}$ denote the eigenvalues of the system without DLAAs (i.e., with $\mathbf{K}^{LG} = \mathbf{K}^{LL} = \mathbf{O}$). Since the system is stable without attacks, we must have $\Re(\lambda_i) < 0$, $i = 1, \ldots, 2N$.

In DLAAs, the attacker can indirectly control the system matrices by changing the elements of $\mathbf{K}^{LG}$ or $\mathbf{K}^{LL}$. Let us denote the eigenvalues of the system with DLAAs by $\{\nu_i(\mathbf{K}^L)\}_{i=1}^{2N}$, where (with a slight abuse of notation) we have used $\mathbf{K}^L$ as a short-hand notation to denote either $\mathbf{K}^{LG}$ or $\mathbf{K}^{LL}$. The system will be rendered unstable if there exists at least one $\nu_i(\mathbf{K}^L)$ such that $\Re(\nu_i(\mathbf{K}^L)) > 0$. Thus, in order to understand the impact of DLAAs on system stability, we must understand how the eigenvalues of the system change with respect an incremental change in the elements of the matrix $\mathbf{K}^L$.

Our approach is to treat the elements of $\mathbf{K}^{LG}$ and $\mathbf{K}^{LL}$ as parameters of the system matrices and use the parametric sensitivity results to analyze DLAAs. First note that the matrices $\boldsymbol{\mathcal{M}}$ and $\boldsymbol{\mathcal{G}}$ are independent of the elements of $\mathbf{K}^L$, so they need not be consider them in the sensitivity analysis. The matrix $\boldsymbol{\mathcal{C}}$ however is a smooth continuous, and differentiable function of the elements of $\mathbf{K}^L$. Hence, the method of sensitivity of second-order systems is directly applicable to the analysis of DLAAs. It can be shown that for the power grid model in (16), using (13), the parametric sensitivity of the eigenvalues with respect to elements of $\mathbf{K}^L$ can be computed as

$$\frac{\partial \lambda_i}{\partial K_{v,s}^L} = -\lambda_i \mathbf{y}_i^\top \begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \frac{\partial \boldsymbol{\mathcal{C}}}{\partial K_{v,s}^L} & \mathbf{O} \end{bmatrix} \mathbf{z}_i, \tag{17}$$

where,

$$\frac{\partial \boldsymbol{\mathcal{C}}}{\partial K_{v,s}^L} = \begin{cases} \begin{bmatrix} \mathbf{O} & \mathbf{O} \\ -\mathbf{I}_{v,s} & \mathbf{O}, \end{bmatrix}, & \text{if } \; s \in \mathcal{S}_G, \\ \begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{I}_{v,s}, \end{bmatrix} & \text{if } \; s \in \mathcal{S}_L. \end{cases}$$

Here in, $\mathbf{I}_{v,s}$ is a matrix whose $(v,s)^{\text{th}}$ entry is 1, and all other entries are zero. Note that $\frac{\partial \lambda_i}{\partial K_{v,s}^L} = 0$ if $v \notin \mathcal{V}$ and $s \notin \mathcal{S}$. Using sensitivity analysis, the estimate $\widehat{\nu}_i(\mathbf{K}^L)$ of $\nu_i(\mathbf{K}^L)$ can be computed as:

$$\widehat{\nu}_i(\mathbf{K}^L) = \lambda_i + \sum_{v \in \mathcal{V}} \sum_{s \in \mathcal{S}} \frac{\partial \lambda_i}{\partial K_{v,s}^L} K_{v,s}^L, \;\; i = 1, \ldots, 2N. \tag{18}$$

A. Least-Effort DLAAs Using Parametric Sensitivity

The node corresponding to the least-effort destabilizing single-point DLAA can be located using sensitivity analysis in the following manner. First note that if there exists at least one $\nu_i(\mathbf{K}^L) > 0$ the system becomes unstable. Also, we assume that $\widehat{\nu}_i(\mathbf{K}^L)$ closely approximates $\nu_i(\mathbf{K}^L)$. Then, using (18) under single-point DLAA, it follows that a feedback gain greater than $\frac{-\lambda_i}{\frac{\partial \lambda_i}{\partial K_{v,s}^L}}$ renders the eigenvalue $\widehat{\nu}_i(\mathbf{K}^L)$ to be positive. We denote the minimum value of the feedback gain at which the system becomes unstable by $K_{v,s}^{L^*}$ and its estimate by $\widehat{K}_{v,s}^{L^*}$. Since only one eigenvalue is required to be positive for the system to be unstable, it follows that

$$\widehat{K}_{v,s}^{L^*} = \min_{i=1,\ldots,2N_G} \frac{-\lambda_i}{\frac{\partial \lambda_i}{\partial K_{v,s}^L}} \tag{19}$$

is the minimum value of feedback gain that makes the system unstable. Using (19), the node that corresponds to the least-effort destabilizing attack can be found as

$$\left\{v^*, s^*\right\} = \arg\min_{v\in\mathcal{V}, s\in\mathcal{S}} \widehat{K}^{L^*}_{v,s}. \tag{20}$$

A similar analysis can be performed for a coordinated multipoint DLAA. In particular, the set of feedback gain values that destabilize the system can be characterized as follows. Let $\mathbf{k}^L \in \mathbb{R}^{N_v N_s}$ denote a vector whose elements are given by $K^L_{v,s}$, $v \in \mathcal{V}$, $s \in \mathcal{S}$. If we define a polyhedron $\mathcal{P}$ as

$$\mathcal{P} = \left\{ \mathbf{k}^L | \lambda_i + \sum_{v\in\mathcal{V}}\sum_{s\in\mathcal{S}} \frac{\partial \lambda_i}{\partial K^L_{v,s}} K^L_{v,s} < 0,\ \ i = 1, \ldots, 2N_G \right\},$$

then all feedback gain vectors $\mathbf{k}^L$ that lie outside $\mathcal{P}$ render the system unstable.

Finally, note that the system dynamics under DLAAs can also be evaluated by using results from the parametric sensitivity of the step response presented in Proposition 1.

B. Defending Against DLAAs Based on Parametric Sensitivity Results

Next, we illustrate the utility of the parametric sensitivity approach to defend against DLAAs. We adopt a similar approach to that of [14]. The main idea to find the minimum amount of load that must be protected to ensure system stability in the face of DLAAs. In practical terms, protecting the load implies enhancing security measures such as enabling encryption at a device level or in the communication links. Minimizing the total amount of protected load will in turn minimize the cost of deploying such security measures. The defense problem can be formulated as a linear program (LP) as follows:

$$\begin{aligned} \min_{P^{LP}_v, K^L_{v,s}} \ & \sum_{v\in\mathcal{V}} P^{LP}_v \\ s.t.\ \ & 0 \le P^{LP}_v \le P^{LV}_v,\ \ \forall v \in \mathcal{V}, \\ & \lambda^r_i + \sum_{v\in\mathcal{V}}\sum_{s\in\mathcal{S}} \left(\frac{\partial \lambda_i}{\partial K^L_{v,s}}\right)^r K^L_{v,s} < 0,\ \ \forall \{\lambda_i\}_{i=1}^{2N_G}, \\ & \sum_s K^L_{v,s}\omega^{\max}_s = (P^{LV}_v - P^{LP}_v)/2, \forall v \in \mathcal{V}, \end{aligned} \tag{21}$$

where X^r represents $\Re(X)$. In (21), P^{LP}_v denotes the amount of load (from the vulnerable portion of the load) that must be protected at victim node $v \in \mathcal{V}$. Naturally, this must be less than the total vulnerable load (first constraint of (21)). The second constraint of (21) ensures that the eigenvalues are negative, and hence, the system cannot be made unstable by the DLAA. The final constraint represents the limit on the attack controller's gain, which follows from (4). In this constraint, we use equality to ensure that the system remains stable even if the attacker uses the maximum permissible value of the attack controller gain. This is because the defender does not have prior knowledge of the actual parameters that the attacker intends to use. Without such knowledge, the defender must design a defense that is capable of ensuring system stability against all possible attack parameters.

We note that although the main idea behind the defense (i.e., protecting the vulnerable load) is similar to [14], a key advantage of our approach is that it only requires solving an LP rather than solving a non-convex pole placement optimization problem. LPs can be solved exactly and efficiently, demonstrating the effectiveness of the proposed approach of analyzing DLAAs using the parametric sensitivity analysis of the eigensolutions.

Computational Complexity: The main advantage of the parametric sensitivity approach is the reduction in computational complexity. We note that the sensitivity parameters only need to be computed for single-point attacks only (i.e., one victim node at a time). This amounts to computing $N_v N_s$ sensitivity factors for each eigenvalue of the system. Moreover, the computations (17) are cheap, since λ_i, $\mathbf{y}_i$ and $\mathbf{z}_i$ need to only be computed once. Only the factor $\mathbf{B}^M\mathbf{I}_{v,s}$ must be recomputed for every combination of victim and sensor nodes. For a coordinated multipoint attack, the net effect of attacking multiple nodes can be computed using the superposition principle as in (18). In contrast, directly assessing the impact of DLAAs would require recomputing the eigenvalues for each combination of victim/sensor nodes (there are $2^{N_v N_s}$ such combinations) and each value of the feedback gain. This method soon becomes computationally infeasible.

V. Analysis of Static Load Altering Attacks

In this section, we analyze SLAAs using results from the theory of second-order systems. From (16), note that under SLAAs, the attacker cannot modify the system matrices. As such, it is not possible to change the eigenvalues of the system. Thus the parametric sensitivity analysis of eigensolutions cannot be used to assess the attack impact directly.

Although SLAAs cannot destabilize the system, a sudden and abrupt change in the system load can result in unsafe frequency excursions [12]. It is thus of interest to identify nodes that correspond to the least-effort SLAAs (in terms of the amount of altered load) and defend the system against such attacks. To this end, we use the analytical expression for the step response presented in (11) and (12). Without loss of generality, we assume initial conditions $\mathbf{z}_0 = \mathbf{0}$. Thus, the step response in the time domain is given by

$$\mathfrak{z}(t) = \left(\sum_{j=1}^{2N_G} \frac{e^{\lambda_j t} - 1}{\lambda_j}\right)\left(\mathbf{y}_j^\top \mathbf{f}_0\right)\mathbf{z}_j. \tag{22}$$

In the above equation, note that $\mathfrak{z}(t) = [\boldsymbol{\delta}(t); \boldsymbol{\omega}(t)]$. Using (22), we can express the power grid response to a change in the system load $\boldsymbol{\epsilon}^L$. First note from (16), the forcing function $\mathbf{f}_0$ and the change in the load $\boldsymbol{\epsilon}^L$ are related as $\mathbf{f}_0 = [\mathbf{0}; -(\mathbf{p}^{LS} + \boldsymbol{\epsilon}^L)]$. Using this in (22), and rearranging, we obtain,

$$\mathfrak{z}(t) = \sum_{i=1}^{N_L} \epsilon^L_{l_i} \sum_{j=1}^{2N_G} \left(\frac{e^{\lambda_j t} - 1}{\lambda_j}\right) k_{ji}\mathbf{z}_j, \tag{23}$$

where $\mathbf{k}_j$ is a row vector given by $\mathbf{k}_j = \mathbf{y}_j^\top \in \mathbb{R}^{1\times N_L}$ and $\mathbf{k}_{ji}$ is the i^{th} element of $\mathbf{k}_j$. For convenience, let us denote

$$\mathbf{f}_i(t) = \sum_{j=1}^{2N_G} \left(\frac{e^{\lambda_j t} - 1}{\lambda_j}\right) k_{ji}\mathbf{z}_j. \tag{24}$$

Note that $\mathbf{f}_i(t) = [f_{i,1}(t), \ldots, f_{i,2N_G}(t)]^\top$ at each time t is a $2N_G$ dimensional vector, where each element of $\mathbf{f}_i(t)$ corresponds to the fluctuation of the components of $\mathfrak{z}(t)$.

Equation (23) gives us a closed-form expression of the system's response in terms of the change in the load. A salient observation is that the response is a linear function of the load perturbation $\boldsymbol{\epsilon}^L$. Assume we are interested in the fluctuation of the frequency at the n^{th} generator bus. Let us define

$$l_{i^*,n} = \underset{i=1,\ldots,N_L}{\arg\max} f_{i,n}\big(t^*_{i,n}\big),\ n = N_G+1, \ldots, 2N_G, \qquad (25)$$

where $t^*_{i,n} = \arg\max_t f_{i,n}(t)$. Since (23) is a linear function of the system load, under a single-point SLAA, the node $l_{i^*_n}$ is the node that corresponds to least-effort attack. In (25), $t^*_{i,n}$ can be found by simply taking the derivative of $f_{i,n}(t)$ with respect to time and finding the time at which the derivative function is zero. Note that there may be multiple times at which the derivative function becomes zero. For a stable system, we must have $\Re(\lambda_i) < 0$. Thus, each function $f_{i,n}(t)$ is a decaying function of time (note the component $e^{\Re(\lambda_j)}$) in the numerator of (23)). It thus follows that the peak fluctuation of $f_{i,n}(t)$ occurs at time t at which the derivative function becomes zero for the first time.

The function $f_{i,n}(t)$ represents the fluctuation of the n^{th} frequency component for a per unit change in the system load. Thus, the minimum load change at load bus i under SLAA that can cause an unsafe frequency excursion in the n^{th} generator bus frequency can be computed as

$$\epsilon^L_{l_i,n} = \frac{\omega_n^{max}}{f_{i,n}\big(t^*_{i,n}\big)},\ i = 1, \ldots, N_L. \qquad (26)$$

As in the case of DLAAs, the closed-form expression of the step response in (23) can also be used to formulate the defense optimization problem against SLAAs as follows:

$$\begin{aligned} \min\ & \sum_{v\in\mathcal{V}} P^{LP}_v \\ s.t.\ & 0 \le P^{LP}_v \le P^{LV}_v,\ \forall v \in \mathcal{V}, \\ & \left| \sum_{i=1}^{N_L} \epsilon^L_i \sum_{j=1}^{2N_G} \left(\frac{e^{\lambda_j t^*_{i,n}} - 1}{\lambda_j} \right) k_{ji} \mathbf{z}_{jn} \right| \le \omega_n^{\max} \\ & n = 1, \ldots, 2N_G, \\ & \epsilon^L_v = P^{LV}_v - P^{LP}_v, \forall v \in \mathcal{V}. \end{aligned} \qquad (27)$$

In (27), the objective function and the first constraint equation is similar to (21). The second constraint represents the fact that the peak of the system's response due to the SLAA must not exceed the safety limit. The last constraint ensures that the compromised load does not exceed the vulnerable portion of the load after protection. As in (21), we consider equality constraint to ensure no unsafe frequency excursions even if the attacker alters the maximum permissible load.

Once again, we note that optimization (27) is a linear programming problem, which can be solved exactly and efficiently. This again illustrates the merit of the proposed technique. Finally, note that combined defense against DLAAs and SLAAs can be solved in a straightforward manner by combining the constraints of (21) and (27). We omit the details due to the lack of space.

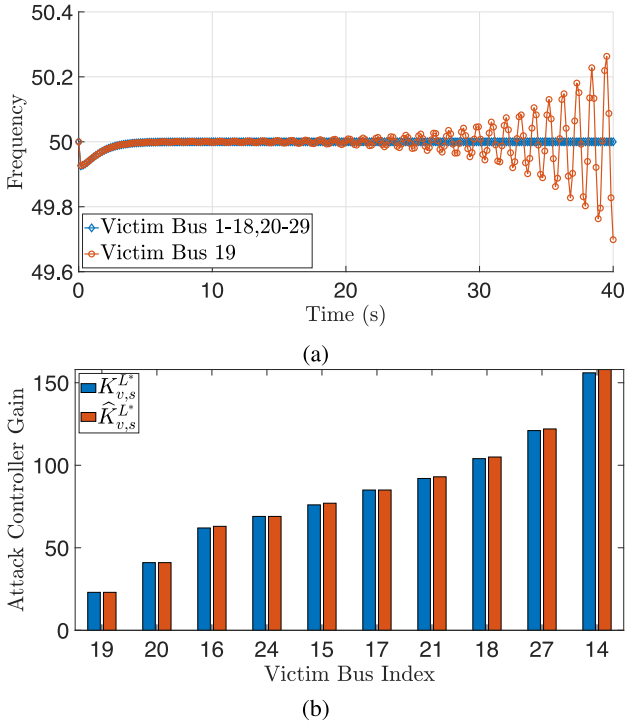

Fig. 1. (a) Frequency dynamics under single-point DLAAs for different victim buses in the IEEE-39 bus system, $K^L_{v,s} = 25$ with $s = 33$ (sensing bus). Maximum compromised load = 2 p.u. (b) Values of $K^{L^*}_{v,s}$ and $\widehat{K}^{L^*}_{v,s}$ for different victim buses.

VI. Simulation Results

In this section, we present simulation results to illustrate the effectiveness of the proposed approach. All simulations are conducted using MATLAB and the power grid topological data obtained from the MATPOWER simulator. We use IEEE-6, 14, and 39 bus systems to illustrate our results. The power grid dynamics are obtained by solving the differential equations (1) in MATLAB.

Single-Point DLAAs: First we consider single-point DLAAs using the IEEE 39-bus system. We set bus 33 as the sensing bus, and inject DLAAs at the load buses 1-29 (one bus at a time). At victim bus $v \in \mathcal{V}$, we set the attack controller gain $K^L(v, 33) = 25$, $(v \in \{1-29\})$, which corresponds to a maximum compromised load of $2K^L_{v,s}\omega_{\max} = 2\times25\times2/50 = 2$ p.u. We plot the frequency dynamics under DLAAs in Fig. 1 (a). For clarity, we only plot the frequency dynamics of one of the first generator buses, i.e., bus 30. We observe that the DLAA at victim bus 19 is able to destabilize the system, whereas the DLAA rest of the victim buses do not. Thus, bus 19 corresponds to the least-effort destabilizing attack. We also plot the values of $K^{L^*}_{v,s}$ and $\widehat{K}^{L^*}_{v,s}$ for 10 different victim nodes in Fig. 1 (b) (the buses are chosen in terms of the increasing values of $K^{L^*}_{v,s}$). Recall that $K^{L^*}_{v,s}$ is the true value of the attack controller gain at which the system becomes unstable and $\widehat{K}^{L^*}_{v,s}$ is the prediction based on the sensitivity analysis. We observe that bus 19 has the least value of $K^{L^*}_{v,s}$, and thus $v^* = 19$. Moreover, the values of $K^{L^*}_{v,s}$ and $\widehat{K}^{L^*}_{v,s}$ match closely. This result shows that the parametric sensitivity approach can accurately predict the critical vulnerable nodes of the system.

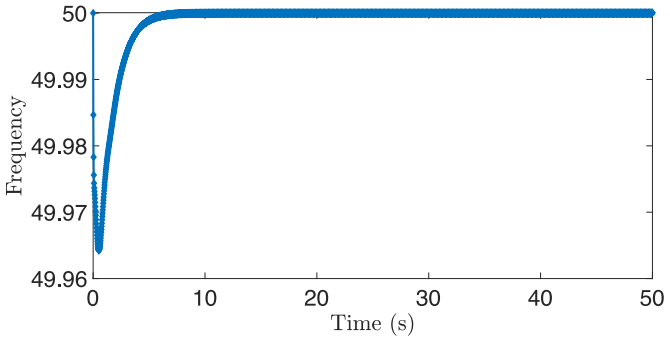

Fig. 2. Frequency dynamics of generator bus 30 under SLAA. $\epsilon_v = 2$ p.u. with $v = 19$ for the IEEE-39 bus system.

To compare the impact of DLAAs and SLAAs, we compromise an identical amount of load of 2 p.u. as an SLAA (one-time step change) at victim bus 19 and plot of frequency dynamics in Fig. 2. It can be observed that in contrast to DLAAs, SLAA only leads to a minor deviation and the frequency gets restored to the nominal value relatively quickly. Thus, DLAA is clearly advantageous for the attacker.

Further, we verify the accuracy of the sensitivity approach in approximating the true eigenvalues of the system under DLAAs. Without the loss of generality, assume that eigenvalues $\{\nu_i(\mathbf{K}^L)\}_{i=1}^{2N_g}$ are sorted according to the decreasing value of their real parts. We plot the real part of $\nu_1(\mathbf{K}^L)$ (i.e., eigenvalue which has the maximum real part) and $\widehat{\nu}_1((\mathbf{K}^L))$ for IEEE-6 bus and IEEE-39 bus systems by varying $K^L_{v,s}$ in Fig. 3. For the IEEE-6 bus system, $s = 1$ and $v = \{4\}, \{5\}, \{6\}$. For the IEEE-39 bus system, $s = 33$ and $v = \{19\}, \{20\}, \{16\}, \{24\}, \{15\}$ (we choose the 5 victim buses that correspond to the 5 least-effort DLAAs in this case). We observe that for both the bus systems, the two quantities match closely, thus validating the parametric sensitivity approach. Further, we also observe that the accuracy degrades slightly for large values of attack controller gains $K^L_{v,s}$, which is expected since the sensitivity approach is a linear approximation. However, for a reasonable range of $K^L_{v,s}$, the approximation remains accurate. E.g., in Fig. 3 (bottom figure), we observe a good match for $K^L_{v,s}$, values up to 50 p.u., which corresponds to $p^L_v = 2K^L_{v,s}\omega_{\max} = 2 \times 50 \times 2/50 = 4$p.u. $= 400$ MWs of compromised load (assuming base load of 100 MWs).

We enlist the parameter $\eta = (K^{L^*}_{v^*,s} - \widehat{K}^{L^*}_{v^*,s})/K^{L^*}_{v^*,s}$ for different IEEE bus systems in Table I. Recall that $\{v^*\} = \arg\min_{v\in\mathcal{V}} \widehat{K}^{L^*}_{v,s}$, and thus, we are identifying the attack parameters that correspond to the least-effort destabilizing attacks for different bus systems. We see that the sensitivity approach can closely approximate the value of attack controller gain at which the system becomes unstable. Further, we observe that the accuracy of the sensitivity approach is independent of the size of the bus system under consideration, but however, depends on the value of $K^L_{v,s}$. This is evident from the values of $K^{L^*}_{v^*,s}$ noted in Table I, where we observe that the accuracy slightly degrades for higher values of $\widehat{K}^{L^*}_{v,s}$, which is consistent with the observation in Fig. 3 (b).

Multi-Point DLAAs: Next, we investigate multi-point DLAAs. We vary the attack controller gain values of two victim nodes simultaneously in the IEEE-39 bus system,

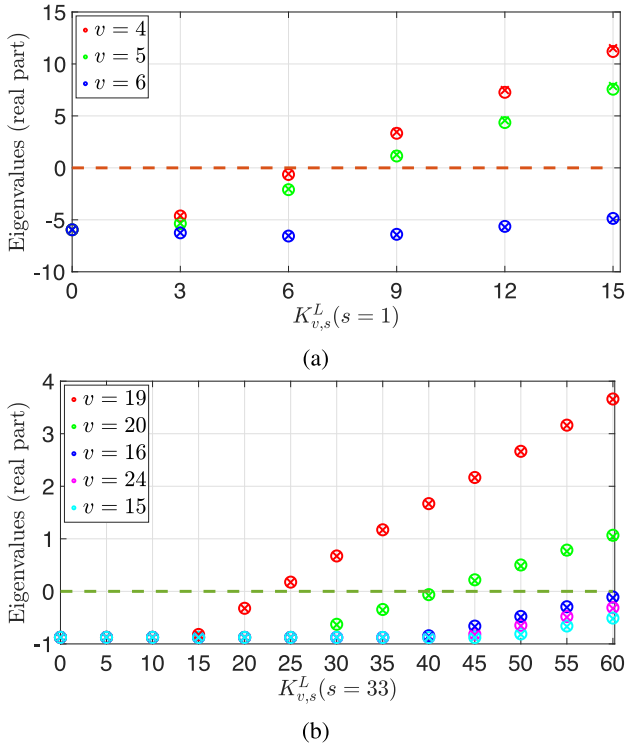

Fig. 3. Real part of $\nu_1(\mathbf{K}^L)$ under single-point DLAAs for different values of $K^L_{v,s}$. (a) IEEE-6 bus, $s = 1$ and $v = \{4\}, \{5\}, \{6\}$. (b) IEEE-39 bus, $s = 33$ and $v = \{19\}, \{20\}, \{16\}, \{24\}, \{15\}$. Circles: $\nu_i(\mathbf{K}^L)$), Crosses: $\widehat{\nu}_i(\mathbf{K}^L)$.

TABLE I
VALUE OF $\eta = |(K^{L^*}_{v^*,s} - \widehat{K}^{L^*}_{v^*,s})/K^{L^*}_{v^*,s}|$ FOR DIFFERENT IEEE BUS SYSTEMS. BUS 1 IS ASSUMED TO BE SENSOR BUS

Bus system	Sensing bus	η	$K^{L^*}_{v^*,s}$
IEEE 6-bus system	1	0	6.1
IEEE 14-bus system	1	0.009	11
IEEE 39-bus system	30	0.0385	249
IEEE 39-bus system	33	0.0043	23.4
IEEE 39-bus system	37	0.0059	58.3

namely buses 19 and 20 (note these two victim bus correspond to the locations of the least-effort load-altering attack). We plot the true eigenvalues of the system $\nu_1(\mathbf{K}^L)$ and those predicted by the sensitivity approach $\widehat{\nu}_1(\mathbf{K}^L)$ in Fig. 4. Once again, we observe a close match between the two, showing that the proposed approach is effective in approximating the true eigenvalues under multi-point DLAAs.

We also implement the defense against DLAAs by solving the optimization problem (21). We plot the amount of load to be protected according to the solution of (21) for the IEEE-6 bus system in Fig. 5 (a). To verify its correctness, we plot the frequency dynamics considering the maximum permissible values of attack feedback again, i.e., by setting $K^L_{v,s} = (P^{LV}_v - P^{LP*}_v)/2\omega^{\max}_s$, where ($P^{LP*}_v$ is the solution of (21)) in Fig. 5 (b). We observe that the oscillations are damping and will eventually go to 0, thus verifying that the proposed defense can make the system resilient to DLAAs.

Static Load Altering Attacks: We also perform simulations for the results derived from SLAA in Section V. To this end, we plot the functions $f_{i,n}(t)$ for different generator and load

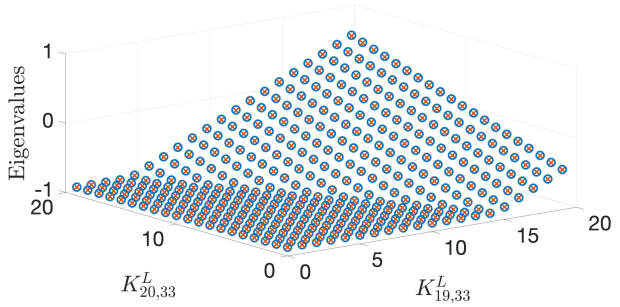

Fig. 4. Real part of $\nu_1(\mathbf{K}^L)$ under multipoint DLAAs for different values of $K^L_{19,33}$ and $K^L_{20,33}$ for IEEE-39 Bus system. Circles: $\nu_1(\mathbf{K}^L)$, Crosses: $\widehat{\nu}_1(\mathbf{K}^L)$.

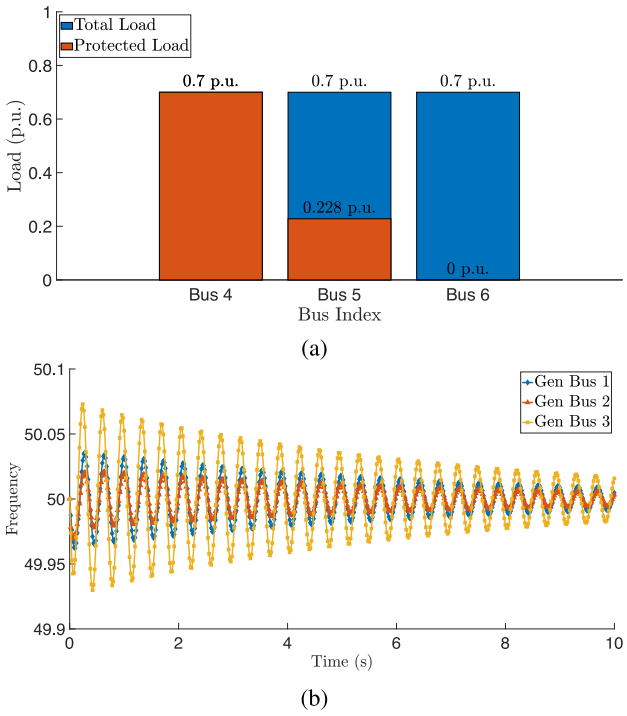

Fig. 5. (a) Protected load to defend against DLAAs. (b) Dynamics under multi-point DLAAs with the unprotected load. Both plots consider the IEEE 6-bus system.

buses considering IEEE-39 bus system in Fig. 6. These functions represent the fluctuation of the frequency for per unit change in the load. For the ease of illustration, we only plot the curves corresponding to three generator buses, i.e., bus 29,30 and 31. The victim bus corresponding to the least-effort SLAA is marked in the figure. Using the curves above and the result in (26), a grid operator can determine the minimum amount of load altering required to cause unsafe frequency fluctuation.

Comparison with Non-linear Model: We also compare the effectiveness of the proposed sensitivity approach in predicting the least-effort DLAA under a non-linear model of the power grid. To this end, we simulate a simplified version of the non-linear model given by

$$\begin{aligned}\dot{\delta}_i &= \omega_i, i \in \mathcal{N}_G \\ M_i\dot{\omega}_i &= -D_i\omega_i - K^P_i\omega_i - K^I_i\delta_i, \qquad i \in \mathcal{N}_G \\ &\quad - \sum_{j\in\mathcal{N}_G} B_{i,j}\sin(\delta_i - \delta_j) - \sum_{j\in\mathcal{N}_L} B_{i,j}\sin(\delta_i - \theta_j),\end{aligned}$$

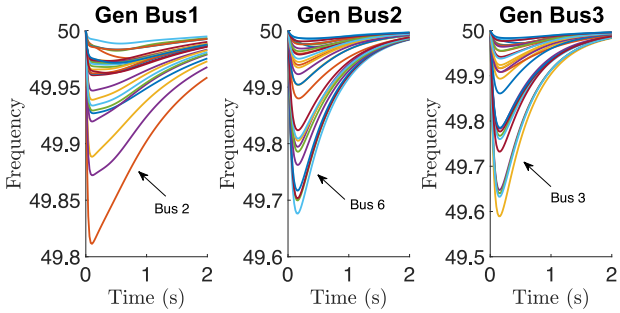

Fig. 6. Function $f_{i,n}(t)$ for different generator and load buses in IEEE-39 bus system. Each curve corresponds to a victim bus. The victim bus corresponding to the least-effort SLAA is marked.

TABLE II
COMPARISON OF THE NON-LINEAR MODEL WITH THE SENSITIVITY APPROACH (BASED ON THE LINEAR MODEL) FOR DIFFERENT IEEE BUS SYSTEMS

Bus system	$\{v, s\}$	$K^{L^*}_{v^*,s}$ (Non-linear)	$\widehat{\nu}_i(K^{L^*}_{v,s})$ (Sensitivity)
IEEE 6-bus system	$\{4, 1\}$	6.7	6.8
IEEE 14-bus system	$\{5, 1\}$	11.3	11
IEEE 39-bus system	$\{19, 33\}$	25.2	24.9

$$\begin{aligned}D_i\dot{\theta}_i &= \sum_{s\in\mathcal{S}} K^{LG}_{i,s}\omega_s - P^{LS}_i \qquad i \in \mathcal{N}_L \\ &\quad - \sum_{j\in\mathcal{N}_G} B_{i,j}\sin(\theta_i - \delta_j) - \sum_{j\in\mathcal{N}_L} B_{i,j}\sin(\theta_i - \theta_j).\end{aligned}$$

By varying the attack controller gain values $K^L_{i,s}$ in the equations above, we find the minimum value of $K^{L^*}_{i,s}$ at which the system becomes unstable. We compare this with $\widehat{\nu}_i(K^{L^*}_{v,s})$ obtained by the sensitivity approach (formulated based on the linear model). The results are listed in Table II for different IEEE bus systems. We note that the sensitivity approach based on the linear model is able to predict the attack controller gain at which the non-linear system becomes unstable reasonably accurately. Thus, we believe that our analysis is a good initial step towards analyzing the system under more generalized system models.

VII. CONCLUSION AND FUTURE WORK

In this work, we have shown how results from second-order dynamical systems can be used to analyze IoT-based load altering attacks against power grids. Our results offer a low-complexity analytical approach to identify nodes corresponding to the least-effort destabilizing DLAAs and least-effort SLAAs that cause unsafe frequency excursions. Using these results, we also proposed defense against DLAAs and SLAAs. Our results show the analyses of DLAAs and SLAAs depend critically on the eigensolutions of the system and their sensitivity to changes in the attack parameters. Our analysis provides insights into how a grid operator can enhance the grid's resilience to such attacks. To the best of our knowledge, this is the first work to apply concepts for second-order dynamical systems to analyze DLAAs and SLAAs.

There are several interesting future research directions. First, large-scale load-altering attacks might potentially result in major shifts in the dynamic/algebraic state of the power network, requiring analysis under generalized non-linear grid models rather than the linearized small-signal model used in this article as well as prior works on this topic [14], [15], [19]. The preliminary simulation results presented in Section VI suggest that the proposed sensitivity based approach could be a good starting point for this generalization. Moreover, this approach has been extended in the past to advanced systems involving general higher-order eigenvalue problems, see, e.g., [32]. Recent works [33], [34] also show that eigen-sensitivity analysis plays a significant role in the response analysis of general complex systems involving non-linear eigenproblems. Further research will be required in this direction to adapt the results for generalized models. Finally, analysis of the system that incorporates multiple control areas and potential safety mechanisms such as under frequency load shedding is important.

REFERENCES

[1] *Bosch Home Connect*. Accessed: May 2020. [Online]. Available: https://www.bosch-home.co.uk/bosch-innovations/homeconnect/

[2] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. IEEE Symp. Security Privacy (S&P)*, May 2016, pp. 636–654.

[3] C. Maple, "Security and privacy in the Internet of Things," *J. Cyber Policy*, vol. 2, no. 2, pp. 155–184, 2017.

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, 2009, pp. 21–32.

[5] 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.

[6] S. Lakshminarayana, T. Z. Teng, D. K. Y. Yau, and R. Tan, "Optimal attack against cyber-physical control systems with reactive attack mitigation," in *Proc. ACM Int. Conf. Future Energy Syst. (e-Energy)*, 2017, pp. 179–190.

[7] S. Lakshminarayana, A. Kammoun, M. Debbah, and H. V. Poor, "Data-driven false data injection attacks against power grids: A random matrix approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 635–646, Jan. 2021, doi: 10.1109/TSG.2020.3011391.

[8] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense for detecting coordinated cyber-physical attacks in power grids," in *Proc. IEEE SmartGridComm*, Oct. 2019, pp. 1–7.

[9] A. 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.

[10] 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. ACSAC*, 2017, pp. 303–314.

[11] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," in *Proc. North Amer. Power Symp. (NAPS)*, 2017, pp. 1–6.

[12] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. USENIX Security Symp.*, Baltimore, MD, USA, Aug. 2018, pp. 15–32.

[13] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks," in *Proc. USENIX Security Symp.*, Aug. 2019, pp. 1115–1132.

[14] 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.

[15] S. Amini, F. Pasqualetti, M. Abbaszadeh, and H. Mohsenian-Rad, "Hierarchical location identification of destabilizing faults and attacks in power systems: A frequency-domain approach," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2036–2045, Mar. 2019.

[16] *Measuring Devices for Frequency Measurement*. Accessed: Jan. 2021. [Online]. Available: https://www.mainsfrequency.com/meter.htm

[17] C. Zhao, U. Topcu, and S. H. Low, "Optimal load control via frequency measurement and neighborhood area communication," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 3576–3587, Nov. 2013.

[18] R. Germanà, A. Giuseppi, and A. D. Giorgio, "Ensuring the stability of power systems against dynamic load altering attacks: A robust control scheme using energy storage systems," in *Proc. Eur. Control Conf. (ECC)*, 2020, pp. 1330–1335.

[19] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?" *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5099–5113, Nov. 2020.

[20] S. Adhikari, *Structural Dynamic Analysis With Generalized Damping Models: Identification*. London, U.K.: Wiley ISTE, 2013, p. 272. [Online]. Available: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-184821670X.html

[21] L. Meirovitch, *Principles and Techniques of Vibrations*. Upper Saddle River, NJ, USA: Prentice-Hall Int., Inc., 1997.

[22] T. Smed, "Feasible eigenvalue sensitivity for large power systems," *IEEE Trans. Power Syst.*, vol. 8, no. 2, pp. 555–563, May 1993.

[23] H.-K. Nam, Y.-K. Kim, K.-S. Shim, and K. Y. Lee, "A new eigen-sensitivity theory of augmented matrix and its applications to power system stability analysis," *IEEE Trans. Power Syst.*, vol. 15, no. 1, pp. 363–369, Feb. 2000.

[24] P. Kundur, N. Balu, and M. Lauby, *Power System Stability and Control*. New York, NY, USA: McGraw-Hill Educ., 1994.

[25] J. W. Rayleigh, *Theory of Sound (Two Volumes)*, 1945th ed. New York, NY, USA: Dover Publ., 1877.

[26] S. Adhikari, "On symmetrizable systems of second kind," *J. Appl. Mech.*, vol. 67, no. 4, pp. 797–802, Dec. 2000.

[27] L. Li, Y. Hu, X. Wang, and L. Lü, "A hybrid expansion method for frequency response functions of non-proportionally damped systems," *Mech. Syst. Signal Process.*, vol. 42, nos. 1–2, pp. 31–41, 2014.

[28] L. Meirovitch, *Computational Methods in Structural Dynamics*. Alphen aan den Rijn, The Netherlands: Sijthoff & Noordohoff, 1980.

[29] S. Adhikari, "Modal analysis of linear asymmetric non-conservative systems," *J. Eng. Mech.*, vol. 125, no. 12, pp. 1372–1379, Dec. 1999.

[30] S. Adhikari and M. I. Friswell, "Eigenderivative analysis of asymmetric non-conservative systems," *Int. J. Numer. Methods Eng.*, vol. 51, no. 6, pp. 709–733, Jun. 2001.

[31] S. Lakshminarayana, S. Adhikari, and C. Maple. *Technical Report: Analysis of IoT-Based Load Altering Attacks Against Power Grids Using the Theory of Second-Order Dynamical Systems—Supplementart Material*. Accessed: Mar. 2021. [Online]. Available: https://bit.ly/3ryt0zA

[32] S. Adhikari, "Derivative of eigensolutions of non-viscously damped linear systems," *AIAA J.*, vol. 40, no. 10, pp. 2061–2069, Oct. 2002.

[33] L. Li, Y. Hu, and X. Wang, "Design sensitivity and hessian matrix of generalized eigenproblems," *Mech. Syst. Signal Process.*, vol. 43, nos. 1–2, pp. 272–294, 2014.

[34] L. Li, Y. Hu, and X. Wang, "A study on design sensitivity analysis for general nonlinear eigenproblems," *Mech. Syst. Signal Process.*, vol. 34, nos. 1–2, pp. 88–105, 2013.

Subhash Lakshminarayana (Senior Member, IEEE) received the B.S. degree from Bangalore University, India, the M.S. degree in electrical and computer engineering from The Ohio State University in 2009, and the Ph.D. degree from the Alcatel Lucent Chair on Flexible Radio and the Department of Telecommunications, SUPELEC, France, in 2012.

He is an Assistant Professor with the School of Engineering, University of Warwick, U.K. He was worked as a Researcher with the Advanced Digital Sciences Center, Singapore, from 2015 to 2018, and a Joint Postdoctoral Researcher with Princeton University and the Singapore University of Technology and Design from 2013 to 2015. His research interests include cyber-physical system security (power grids and urban transportation) and wireless communications. His works have been selected among the best conference papers on integration of renewable and intermittent resources at the IEEE PESGM 2015 Conference, and the "Best 50 papers" of IEEE Globecom 2014 conference. He serves as an Associate Editor of the *IET Smart Grid* and *Frontiers in Communications and Networks Journal* (Smart Grid Communications section), and regularly serves in the technical program committees of IEEE conferences.

Sondipon Adhikari received the Ph.D. degree from the Trinity College, University of Cambridge in 2001.

He was a Lecturer with the Bristol University and a Junior Research Fellow with Fitzwilliam College, Cambridge. He was a Visiting Professor with the Ecole Centrale Lyon, Rice University, University of Paris, UT Austin, and IIT Kanpur, and a Visiting Scientist with the Los Alamos National Laboratory. He is the Chair of Aerospace Engineering with the College of Engineering, Swansea University. His research areas are multidisciplinary in nature and include uncertainty quantification in dynamic systems, computational nanomechanics, dynamics of complex systems, inverse problems for linear and non-linear dynamics, and vibration energy harvesting. He was a Wolfson Research Merit Award holder from the Royal Society. He was an Engineering and Physical Science Research Council Advanced Research Fellow and a winner of the Philip Leverhulme Prize in 2007. He is a Member of the editorial board of several journals, such as *Advances in Aircraft and Spacecraft Science*, *Probabilistic Engineering Mechanics*, *Computer and Structures*, and *Journal of Sound and Vibration*. He is a Fellow of the Royal Aeronautical Society, an Associate Fellow of the American Institute of Aeronautics and Astronautics (AIAA) and a member of the AIAA Non-Deterministic Approaches Technical Committee.

Carsten Maple is the Principal Investigator of the NCSC–EPSRC Academic Centre of Excellence in Cyber Security Research, University of Warwick, where he is a Professor of Cyber Systems Engineering with Warwick Manufacturing Group. He is also a Fellow of the Alan Turing Institute, the National Institute for Data Science, and AI in the U.K., where he is a Principal Investigator on a $5 million project developing trustworthy national identity to enable financial inclusion. He is a Co-Investigator of PETRAS, the National Centre of Excellence for IoT Systems Cyber Security and works with numerous banking organizations advising on security, privacy, and use of artificial intelligence. He has an international research reputation and extensive experience of institutional strategy development and interacting with external agencies. He has published over 250 peer-reviewed papers and has coauthored the U.K. Security Breach Investigations Report 2010, supported by the Serious Organized Crime Agency and the Police Central e-crime Unit.