This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes

Sajjad Amini, *Student Member, IEEE*, Fabio Pasqualetti, *Member, IEEE*, and Hamed Mohsenian-Rad, *Senior Member, IEEE*

***Abstract*—Dynamic Load Altering Attacks (D-LAA) are introduced as a new class of cyber-physical attacks against smart grid demand response programs. The fundamental characteristics of D-LAAs are explained. Accordingly, D-LAAs are classified in terms of open-loop versus closed-loop attacks, single-point versus multi-point attacks, the type of feedback, and the type of attack controller. A specific closed-loop D-LAA against power system stability is formulated and analyzed, where the attacker controls the changes in the victim load based on a feedback from the power system frequency. A protection system is designed against D-LAAs by formulating and solving a non-convex pole-placement optimization problem. Uncertainty with respect to attack sensor location is addressed. Case studies are presented to assess system vulnerabilities, impacts of single-point and multi-point attacks, and optimal load protection in an IEEE 39 bus test system.**

***Keywords*: Cyber-physical security, load altering attacks, protection, demand response, power system dynamics, optimization.**

NOMENCLATURE

$\mathcal{N}$	Set of buses
$\mathcal{G}, \mathcal{L}$	Set of generator and load buses
$\mathcal{V}, \mathcal{S}$	Set of victim and sensor buses
i, j	Index of buses
v, s	Index of victim and sensor buses
H	Imaginary part of admittance matrix
δ	Voltage phase angle at generator buses
θ	Voltage phase angle at load buses
ω	Frequency deviation at generator buses
φ	Frequency deviation at load buses
ω^{max}	Frequency relay threshold for generators
P^G	Power injection at generator buses
P^L	Power consumption at load buses
P^M	Mechanical power input to generators
P^{LS}, P^{LV}	Secured and vulnerable portion of the load
M	Inertia matrix for generators
D^G, D^L	Damping coefficient matrices
K^P, K^I	Generator controller gain matrices
K^{LG}, K^{LL}	Attack controller gain matrices
A, B	State-space matrices of open-loop system
X	Lyapunov symmetric matrix

I. INTRODUCTION

The development of distributed intelligence technologies have introduced new opportunities to enhance efficiency and reliability of power grid. However, if these technologies are not accompanied with appropriate security enforcements, they may also create new vulnerabilities in power networks, leaving them open to a wide range of cyber-physical attacks [1]–[3].

Cyber security concerns arise at all sectors of power systems: generation, distribution and control, and consumption. In cyber attacks that target generation sector, the adversary may attempt to hack into major power plants, trying to disrupt or take control over the operation of generation units, c.f. [4], [5]. In cyber attacks that target distribution and control sector, the adversary may attempt to compromise the power sensors that are deployed across the power grid. Alternatively, they may attempt to break into the routers that relay the measured data from such sensors to the control and operation centers. The goal is often to inject false data into the wide area monitoring system, e.g., to affect power system state estimation [6], [7].

Unlike in [4]–[7], in this paper, the focus is on cyber attacks that target the *consumption* sector. Specifically, we are concerned with attacks that seek to compromise the demand response (DR) and demand side management (DSM) programs. DR programs are used by utilities to control the load at the user side of the meter in response to changes in grid conditions [8]. In a related field, DSM techniques seek to exploit the load flexibility in different load sectors, e.g., by using automated energy consumption scheduling [9].

An important class of cyber-physical attacks against DR and DSM systems is load altering attack (LAA) [10]. LAA attempts to control and change a group of remotely accessible but unsecured controllable loads in order to damage the grid through circuit overflow or other mechanisms. There is a variety of load types that are potentially vulnerable to LAAs, e.g., remotely controllable loads [11], loads that automatically respond to price or Direct Load Control (DLC) command signals [12]–[14], and frequency-responsive loads [15], [16]. Some of the recent studies that address modeling, detection, and prevention of LAAs include [17]–[19].

So far, the focus in the LAA literature has been mainly on *static* load altering attacks, where the attack is concerned with changing the volume of certain vulnerable loads, in particular in an *abrupt* fashion. In contrast, in this paper, we address *dynamic* load altering attacks, where we are concerned with not only the amount of the change in the compromised load but also the *trajectory over time* at which the load is changed. Unlike in [10], [17]–[19], the analysis in this paper is based on power system dynamics. Accordingly, we use feedback control theory as the main analytical tool to model or prevent the attack. In this regard, we take into account not only the cyber security challenges but also the physics of the power system. The contributions in this paper can be summarized as follows:

S. Amini and H. Mohsenian-Rad are with the Department of Electrical and Computer Engineering, University of California, Riverside, CA, USA, e-mail: {saamini, hamed}@ece.ucr.edu. F. Pasqualetti is with the Department of Mechanical Engineering, University of California, Riverside, CA, USA, e-mail: fabiopas@engr.ucr.edu. This work was supported by the National Science Foundation through grants ECCS 1253516, ECCS 1462530, and ECCS 1405330. The corresponding author is H. Mohsenian-Rad.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

1) Dynamic Load Altering Attacks (D-LAA) are introduced, characterized, and classified as a new form of cyber-physical attacks against smart grid.
2) A closed-loop D-LAA against power system stability is formulated and analyzed, where the attacker controls the changes in the victim load based on a feedback from the power system frequency. System vulnerabilities and the impacts of single-point and coordinated multi-point attacks are assessed on the IEEE 39 bus test system.
3) A protection scheme is designed against both single-point and multi-point D-LAAs by formulating and solving a non-convex pole placement optimization problem. It seeks to minimize the total vulnerable load that must be protected to assure power system stability under D-LAAs against the remaining unprotected vulnerable loads. Designing under uncertainty with respect to the exact attack location is also taken into consideration. The protection system design is assessed on the IEEE 39 bus test system.

This study complements and merges two generally independent lines of research in the literature. First, it benefits the recent efforts in designing efficient and practical demand response and demand side management programs [8]–[16] by increasing awareness about potential vulnerabilities in these programs, not only to consumers, but also to grid as a whole. Second, it also adds to the existing results on control-theoretic study of cyber-physical attacks, c.f. [20]–[23].

Compared to the conference paper in [24], the following aspects are new in this journal submission. First, the analysis in [24] is limited to single-point attacks. Here, we investigate both single-point and coordinated multi-point D-LAAs. In the latter case, the attacker seeks to simultaneously compromise vulnerable loads at several victim load buses in order to maximize the attack impact. Second, the analysis in [24] does not provide any protection mechanism of any kind against D-LAAs. In contrast, a key concern in this journal version is to design a protection scheme by formulating and solving a non-convex pole-placement optimization problem. Third, the case studies in [24] were limited to a nine bus network, while the case studies here are based on a 39 bus IEEE test system.

II. Dynamic Load Altering Attack

The central idea in a load altering attack is to change a group of unsecured loads in order to damage the grid. While Static Load Altering Attack (S-LAA) is concerned mainly with the *volume* of the vulnerable load that is intended to change [10], [17], [18], in this paper, we introduce and characterize *Dynamic* Load Altering Attack (D-LAA), where the attack is concerned with not only the volume but also the *trajectory* of the changes that are made in the vulnerable load.

A. Attack Classification

A D-LAA can be *open-loop* or *closed-loop*. In an open-loop D-LAA, see Fig. 1(a), the attacker tends to manipulate some vulnerable load *without* monitoring the grid conditions in real-time or monitoring the impact that its load manipulation may cause on the power grid while the attack is being implemented.

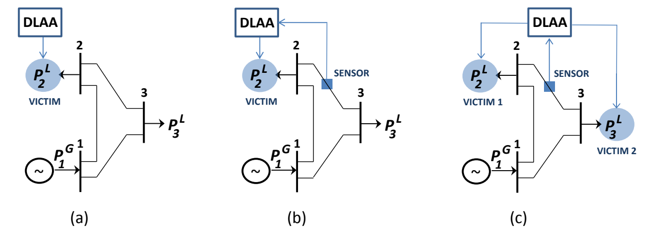

Fig. 1. Three examples of dynamic load altering attacks: a) open-loop D-LAA, b) single-point closed-loop D-LAA, c) multi-point closed-loop D-LAA.

Accordingly, an open-loop D-LAA relies on some historical data that it may collect prior the attack to impose a *pre-programmed* trajectory to the compromised load. In contrast, in a closed-loop D-LAA, the attacker constantly monitors the grid conditions, e.g., through the attacker's installed sensors or via hacking into an existing power system monitoring infrastructure, such that it can control the load trajectory at the victim load bus(es) based on the grid operating conditions. An adversary can conduct a successful D-LAA only if it compromises sufficient amount of vulnerable loads. That is, D-LAA is meaningful only if there is enough flexible and vulnerable (not secured) load to potentially compromise.

The feedback in a closed-loop D-LAA can be based on different types of power grid measurements. For example, the grid conditions can be monitored by measuring voltage magnitude or frequency, aiming for various malicious goals.

The D-LAAs can be classified also based on their scope. Specifically, D-LAAs can be *single-point* or *multi-point*. In a single-point D-LAA, the attacker seeks to compromise the vulnerable load at *one* victim load bus. In a multi-point D-LAA, the attacker seeks to compromise a group of vulnerable loads at *several* victim load buses. The vulnerable loads at different load buses are compromised in a *coordinated* fashion. Examples of single-point and multi-point closed-loop D-LAAs are shown in Figs. 1(b) and (c), respectively.

Finally, one can classify D-LAAs also based on the type of controller being used in order to manipulate the control variable which is load consumption of victim bus(es), whether through a feed-forward controller in case of an open-loop attack or a feedback controller in case of a closed-loop attack. For example, if the D-LAA is closed-loop, then the attacker may use a bang-bang, P, PI, or PID controller [25], or any other more complex feedback control system mechanism.

B. Attack Adverse Impacts

Load altering attacks may seek to cause different adverse impacts. For example, a static load altering attack may involve abruptly increasing the load at the most crucial locations in the grid in order to cause *circuit overflow* on distribution or transmission lines that can cause significant damage to the utility company and/or user equipment. Such attacks may also seek to disturb the balance between power supply and demand during peak-load hours. Please refer to [10] for more details about the possible impacts of static load altering attacks.

As for dynamic load altering attacks, the attack objective depends on the type of attack. For example, for a closed-loop D-LAA where the feedback is based on power grid frequency,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

the attack may seek to deviate the frequency from its nominal value. Note that, an entire interconnected power grid operates at or around a nominal frequency. For example, the nominal frequency in North America is 60 Hz and regional transmission system operators are required to maintain and stabilize frequency at or very closely around this level. Accordingly, a D-LAA may try to damage the grid by *destabilizing* the frequency away from its nominal value.

For a D-LAA against power system stability, an attack may be considered *successful* once it trips one or more over/under frequency relays, c.f. [26], e.g., to force at least one generator go offline, causing a major disturbance to the normal operation of power grid. Such disturbance can potentially trigger *ripple-effects* across the interconnected power system. In fact, due to the connectivity of the grid, small localized perturbations can reach far away regions, and in a disruptive fashion. See for instance the *Nature* paper in [27] for a characterization of certain cascading effects across interconnected networks. Alternatively, if the size of the compromised load is small, it is also possible that triggering the relays and protection systems rather confines the compromised load area, avoiding the attack to spread out to other regions of the power grid, c.f. [28]. But even in that case, the attack is considered successful because it cuts off service for a subset of loads, even though the impact is not catastrophic as in case of an attack with cascade effects.

C. Closed-loop Attack Implementation

In this paper, we are interested in closed-loop D-LAAs because they can potentially affect power system *stability*. We assume that the attack feedback based on measuring power grid *frequency*. This setup is of practical importance also due to its link to the concept of frequency-responsive loads [15], [16]. Note that, if a frequency-responsive load is compromised, then power system frequency is already available to the attacker through local measurements. The frequency sensor can be either co-located with the victim load bus, or it can be placed at some other bus but on the same interconnected network. Throughout this paper, we refer to the bus where the frequency sensor is located as the *sensor bus* s. While D-LAAs take place at the customer and distribution level, their impact is understood only when the system dynamics are studied at the transmission level. Because it is at the transmission level where the area frequency is affected due to an aggregate impact of compromised loads. Nevertheless, the adversary does *not* need access to the transmission-level SCADA/EMS system to implement the attack. All that he/she needs is to hack into the remote load control systems that often exist in demand response programs to adjust the power consumption trajectory.

To implement a D-LAA, the adversary must undergo two major tasks: 1) changing load, and 2) sensing feedback.

1) Changing Load: The adversary must alter the energy consumption of target vulnerable loads by breaking into the smart grid communications, monitoring, or control infrastructure. This can be done in different ways depending on the type of attack, type of load, or type of the communications infrastructure. In particular, an attack may target compromising *price signals* in price-based demand response programs

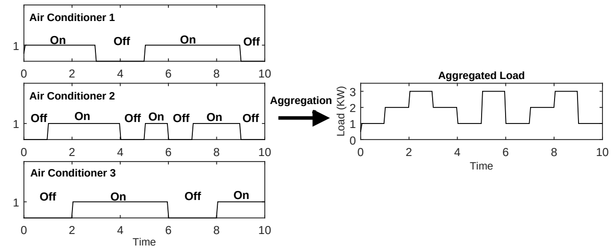

Fig. 2. An example on how an adversary may achieve its desired aggregated load by sending proper DLC command signals to individual vulnerable loads.

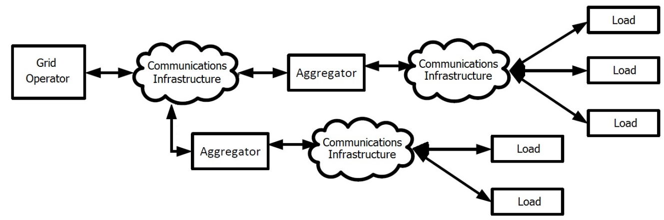

Fig. 3. A demand response program may involve two-way communications between grid operator and aggregators and between aggregators and loads. An intrusion may occur in any of these communications infrastructures.

or *command signals* in Direct Load Control (DLC) programs [13], [29], [30]. For example, the communications infrastructure vulnerability in price-based demand response is discussed in details in [31], [32]. Compromising the command signals in DLC programs is also directly related to D-LAAs, because DLC programs allow remote and direct access to and control over the load without the need to bypass an intermediate or local load control mechanism. Fig. 2 shows how an adversary may generate its desired aggregated load profile by sending a carefully selected sequence of DLC signals - in form of simple on/off commands - to three air conditioners.

In [11], the authors proposed a remote load control mechanism that works over the Internet. Hacking into this Internet-based system may allow taking simultaneous control over several small controllable loads, see Fig. 3. Other communications infrastructures, such as cellular or other wireless networks that are used in advanced metering infrastructures (AMIs) [33], may also be vulnerable to various intrusion attempts.

Some load types that could potentially be vulnerable to load altering attacks due to their major role in demand response and DLC include: vacuum cleaners, e.g., Roomba, smart washing machines, e.g., Miele, smart ovens, e.g., LG Thinq, [34], air conditioners [13], water heaters [35], irrigation pumps [36], electric vehicles [37], and computation equipment [38].

2) Sensing Feedback: In a closed-loop D-LAA, the energy consumption of vulnerable loads is changed according to a feedback signal, such as power system frequency. While a single-point attack requires installing one frequency sensor, a multi-point attack may need one or multiple frequency sensors, depending on how the attack is designed and implemented.

In general, measuring frequency of power grid is not difficult as it can be done at any power outlet using an inexpensive commercial sensor [39]. In fact, such sensing mechanism is already embedded in *frequency responsive* loads that control power usage to contribute, e.g., to frequency regulation [16].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

3) Attack Steps: In summary, an adversary may undergo the following three main steps to implement a D-LAA:

1) Monitor frequency at sensor bus(es) and constantly send measurements to the D-LAA controller. For the special case where the D-LAA controller measures frequency locally, i.e., when the sensor bus and the victim bus are the same, frequency can be measured without the need to intrude into any cyber or physical system.
2) Calculate the amount of vulnerable load P^{LV} that needs to be compromised at victim bus(es) according to the feedback signal and based on the attack control mechanism. This step is done inside the D-LAA controller; therefore, no intrusion is needed in this step.
3) Remotely control the victim load at the amount that is calculated in Step 2. This is the only step which requires an intrusion mechanism in order to remotely control the load, please see Section II-C.1 for more details.

Assessing the vulnerability of Supervisory Control and Data Acquisition (SCADA) systems in smart grids, i.e., the focus of Step 3 above, is also discussed in [33], [40].

III. System Model

Consider a power system with $\mathcal{N} = \mathcal{G} \cup \mathcal{L}$ as the set of buses, where $\mathcal{G}$ and $\mathcal{L}$ are the sets of generator and load buses, respectively. An example is shown in Fig.4. The linear power flow equations at each bus $i \in \mathcal{N}$ can be written as [41]:

$$P_i^G = \sum_{j\in\mathcal{G}} H_{ij}(\delta_i - \delta_j) + \sum_{j\in\mathcal{L}} H_{ij}(\delta_i - \theta_j), \forall i \in \mathcal{G}, \quad (1)$$

$$-P_i^L = \sum_{j\in\mathcal{G}} H_{ij}(\theta_i - \delta_j) + \sum_{j\in\mathcal{L}} H_{ij}(\theta_i - \theta_j), \forall i \in \mathcal{L}, \quad (2)$$

where P_i^G is the power injection of the generator at bus i, P_i^L is the power consumption of the load at bus i, δ_i is the voltage phase angle at generator bus i, θ_i is the voltage phase angle at load bus i, and H_{ij} is the admittance of the transmission line between buses i and j. If there is no transmission line between buses i and j, then we have $H_{ij} = 0$.

We adopt the linear swing equations, c.f., [42], to model the generator dynamics at each generator bus $i \in \mathcal{G}$, that is,

$$\dot{\delta}_i = \omega_i, \quad (3)$$

$$M_i\dot{\omega}_i = P_i^M - D_i^G\omega_i - P_i^G, \quad (4)$$

where ω_i is the rotor frequency deviation at the generator bus i, $M_i > 0$ is the inertia of the rotor, $D_i^G > 0$ is the damping coefficient, and P_i^M is the mechanical power input. We assume two controllers that affect the mechanical power input: turbine-governor controller and load-frequency controller [41]. The turbine-governor controller compares the rotor frequency with a base frequency, for instance 377 rad/s, to determine the amount of mechanical power that is needed to compensate the generated electrical power at steady state. The load-frequency controller, which has a slower dynamic, aims to maintain the rotor frequency at its nominal level by pushing the frequency deviation ω_i back to zero. The two controllers can together be modeled as a proportional-integral (PI) controller, that is,

$$P_i^M = -\left(K_i^P\omega_i + K_i^I\int_0^t \omega_i\right), \quad (5)$$

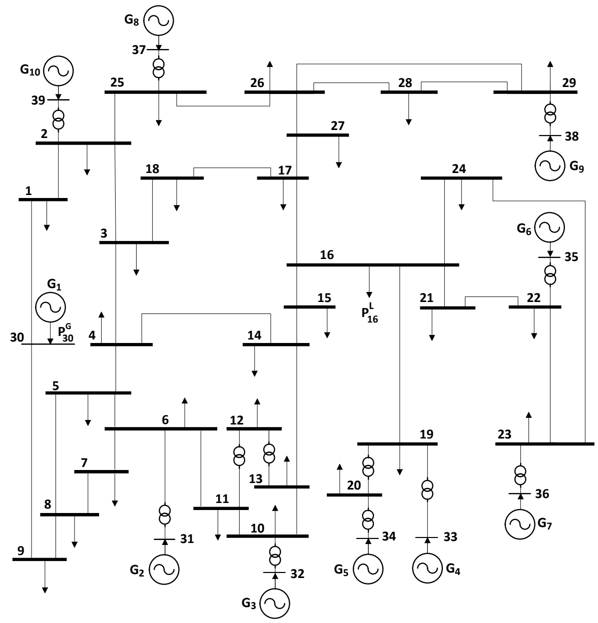

Fig. 4. The IEEE 39 bus test system based on the 10-machine New-England power network, where $\mathcal{L} = \{1, \ldots, 29\}$ and $\mathcal{G} = \{30, \ldots, 39\}$.

where $K_i^I > 0$ and $K_i^P > 0$ are the proportional and integral controller coefficients, respectively. Equation (4) can be rewritten by combining (1) and (5) as

$$-M_i\dot{\omega}_i = \left(K_i^P + D_i^G\right)\omega_i + K_i^I\delta_i + \sum_{j\in\mathcal{G}} H_{ij}\left(\delta_i - \delta_j\right) + \sum_{j\in\mathcal{L}} H_{ij}\left(\delta_i - \theta_j\right), \qquad \forall i \in \mathcal{G}. \quad (6)$$

Three load types are considered in this system [43]: (i) uncontrollable, (ii) controllable but frequency-insensitive, and (iii) controllable and frequency-sensitive. For notational convenience, at each load bus i, we represent the type (i) and type (ii) loads with term P_i^L in (2), and represent the type (iii) loads with term $D_i^L\varphi_i$, where $\varphi_i = -\dot{\theta}_i$ is the frequency deviation at load bus i. The power flow equation in (2) becomes

$$-D_i^L\varphi_i - P_i^L = \sum_{j\in\mathcal{G}} H_{ij}(\theta_i - \delta_j) + \sum_{j\in\mathcal{L}} H_{ij}(\theta_i - \theta_j), \quad (7)$$

and the overall power system dynamics can be conveniently written as the following linear state-space descriptor system:

$$\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -M & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \\ \dot{\varphi} \end{bmatrix} = \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & -I \\ K^I + H^{GG} & H^{GL} & K^P + D^G & 0 \\ H^{LG} & H^{LL} & 0 & D^L \end{bmatrix} \begin{bmatrix} \delta \\ \theta \\ \omega \\ \varphi \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ I \end{bmatrix} P^L. \quad (8)$$

In (8), δ is the vector of voltage phase angles at all generator buses, ω is the vector of rotor angular frequency deviations at all generator buses, θ is the vector of voltage phase angles at all load buses, φ is the vector of frequency deviations at all

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

load buses, and P^L is the vector of power consumption at all load buses. Additionally, I is the identity matrix of appropriate dimension, and M, D^G, and D^L are diagonal matrices with diagonal entries equal to the inertia, damping coefficients of the generators, and damping coefficients of the loads, respectively. Similarly, K^I and K^P are diagonal matrices with diagonal entries equal to the integral and proportional controller coefficients of the generators at all generator buses. We denote the imaginary part of the admittance matrix as

$$H_{bus} = \begin{bmatrix} H^{GG} & H^{GL} \\ H^{LG} & H^{LL} \end{bmatrix}.$$

IV. Analysis of the Attack

In this section, we provide a mathematically representation of the D-LAA and study the attack impact on grid performance and stability. Various case studies are presented.

A. Power System Dynamics Under Attack

Based on the system model in Section III, a load altering attack can be characterized based on how it affects the *vulnerable* portion of the load vector P^L, i.e., the input signal in (8). Accordingly, at each load bus i, we define

$$P_i^L = P_i^{LS} + P_i^{LV}, \tag{9}$$

where P_i^{LS} denotes the *secure* and P_i^{LV} denotes the *vulnerable* portion of the load at bus i, respectively. An attack may compromise only the vulnerable part of a victim load bus.

Now, consider a single-point closed-loop D-LAA that is implemented at victim load buses $\mathcal{V} \subseteq \mathcal{L}$. Suppose a proportional controller is used by the attacker. Let $K_{vs}^{LG} \geq 0$ denote the attack controller's gain at bus $v \in \mathcal{V}$ if the sensor bus s is a generator bus. Similarly, let $K_{vs}^{LL} \geq 0$ denote the attack controller's gain at bus v if the sensor bus s is a load bus. Note that, for each victim load bus v, only one of the two parameters K_{vs}^{LG} and K_{vs}^{LL} can be non-zero, depending on the choice of sensor bus. We can write

$$P_v^{LV} = -K_{vs}^{LG}\omega_s - K_{vs}^{LL}\varphi_s. \tag{10}$$

Note that, since K_{vs}^{LG} and K_{vs}^{LL} are positive valued, P_v^{LV} is updated in opposition to the values of ω_s and φ_s. For example, if ω_s decreases, i.e., the frequency drops from its nominal value, then the attack controller increases the load at bus v. This is exactly the opposite of how a frequency-responsive load would react to frequency lag in a DR program, c.f. [16].

The system dynamics subject to the above D-LAA becomes

$$\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -M & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \\ \dot{\varphi} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ I \end{bmatrix} P^{LS} +$$
$$\begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & -I \\ K^I + H^{GG} & H^{GL} & K^P + D^G & 0 \\ H^{LG} & H^{LL} & -K^{LG} & -K^{LL} + D^L \end{bmatrix} \begin{bmatrix} \delta \\ \theta \\ \omega \\ \varphi \end{bmatrix}. \tag{11}$$

From (11), the attacker is capable of affecting the system dynamics. Specifically, the attacker can affect the system matrix and the system poles by adjusting its controller matrices K^{LG} and K^{LL}. If the size of the vulnerable load is large enough, then the attacker can render the system dynamics unstable by moving the system poles to the right-half complex plane [25]. Of course, in practice, since the generators are equipped with over- and under-frequency relays as part of their protection systems, c.f. [26], a D-LAA may ultimately force certain generators to disconnect from the main grid, possibly triggering cascading effects or blackouts.

Next, we investigate sufficient conditions for making (11) unstable. To do so, we modify the system model in (11) into a regular, i.e., non-descriptor state-space model. This is done by eliminating the power flow equations and integrating them into the swing equations. Suppose the sensor bus s is a generator bus, i.e., $s \in \mathcal{G}$. Accordingly, we have $K_{vs}^{LL} = 0$ for all victim load buses v. From this, and the last row in (11), we have:

$$\varphi = -\left(D^L\right)^{-1} \left(\begin{bmatrix} H^{LG} \\ H^{LL} \\ -K^{LG} \end{bmatrix}^T \begin{bmatrix} \delta \\ \theta \\ \omega \end{bmatrix} + P^{LS} \right). \tag{12}$$

If we substitute (12) with φ in (11), the equivalent non-descriptor / regular state-space model under attack becomes:

$$\begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \end{bmatrix} = A \begin{bmatrix} \delta \\ \theta \\ \omega \end{bmatrix} + B \left(- \begin{bmatrix} 0 \\ 0 \\ K^{LG} \end{bmatrix}^T \begin{bmatrix} \delta \\ \theta \\ \omega \end{bmatrix} + P^{LS} \right), \tag{13}$$

where

$$A = \begin{bmatrix} I & 0 & 0 \\ 0 & (D^L)^{-1} & 0 \\ 0 & 0 & -M^{-1} \end{bmatrix} \times \begin{bmatrix} 0 & 0 & I \\ H^{LG} & H^{LL} & 0 \\ K^I + H^{GG} & H^{GL} & K^P + D^G \end{bmatrix}$$

and

$$B = \begin{bmatrix} 0 \\ (D^L)^{-1} \\ 0 \end{bmatrix}.$$

Note that, we have $K_{ij}^{LG} = 0$ for any $i \notin \mathcal{V}$ and any $j \neq s$.

The state-space model in (13) represents the system dynamics in *presence* of a closed-loop D-LAA, where A and B are the system and input matrices in the corresponding open-loop system in *absence* of the D-LAA. The instability of this linear system can be analyzed using the Linear Quadratic Lyapunov Theory that is overviewed in the Appendix A. Specifically, the closed-loop system in (13) is unstable if there exists a *symmetric negative definite* matrix X such that

$$\left(A - B \begin{bmatrix} 0 \\ 0 \\ K^{LG} \end{bmatrix}^T \right)^T X + X \left(A - B \begin{bmatrix} 0 \\ 0 \\ K^{LG} \end{bmatrix}^T \right) < 0. \tag{14}$$

This Nonlinear Matrix Inequality (NLMI) can be changed to Linear Matrix Inequality (LMI) by applying linear fractional transformation [44]. Specifically, if we define $Y \triangleq X^{-1}$ and $W \triangleq [0 \quad 0 \quad K^{LG}]X^{-1}$, we can rewrite (14) as

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

TABLE I
TOTAL LOADS AND VULNERABLE LOADS

Load Bus	P^{LS} (p.u)	P^{LV} (p.u)	Load Bus	P^{LS} (p.u)	P^{LV} (p.u)
1	4	0	**16**	7.8	3.1
2	4	0	**17**	4	0
3	7.2	0	**18**	5.6	0
4	9	0	**19**	4	1.6
5	4	0	**20**	10.3	0
6	5	2	**21**	6.7	0
7	6.3	0	**22**	4	0
8	9.2	0	**23**	7	2.8
9	4	0	**24**	7	0
10	4	0	**25**	6.2	0
11	4	0	**26**	5.4	0
12	4.1	0	**27**	6.8	0
13	4	0	**28**	6.1	0
14	4	0	**29**	10.8	4.3
15	7.2	0	—	—	—

$$(A - BWY^{-1})^T Y^{-1} + Y^{-1}(A - BWY^{-1}) < 0. \quad (15)$$

If we multiply both sides by Y, we obtain [44]:

$$YA^T - W^T B^T + AY - BW < 0, \quad (16)$$

which is an LMI in Y and W . If this LMI has a solution over $Y < 0$, then the Lyapunov function $V(z) = z^T Y^{-1} z$ proves the *instability* of the closed loop system under attack.

B. Case Studies

Consider the IEEE 39 bus power system in Fig. 4. Suppose the parameters of the transmission lines and the inertia and damping coefficients of generators are as in [45]. Secure loads and vulnerable loads at each load bus are as in Table I. Generator controller parameters are $K_1^P = 100$, $K_2^P = K_3^P = 45$, $K_4^P = 10$, $K_5^P = K_{10}^P = 50$, $K_6^P = K_9^P = 40$, $K_7^P = 30$, $K_8^P = 20$, and $K_1^I = \ldots = K_{10}^I = 60$. The damping coefficient for each fixed dynamic load is 10. Controller parameters are set so as to keep the system stable during normal operations, i.e., in absence of an attack. The system is initiated to run with P^L being equal to $P^{LS} + P^{LV}/2$.

We assume that only five load buses have vulnerable loads. They can potentially become victim buses, i.e., we can have $\mathcal{V} = \{6, 16, 19, 23, 29\}$. These victim load buses are highlighted using color gray in Table I. Sensor buses are assumed to be placed only at $\mathcal{S} = \{31, 33, 36, 38\}$. The nominal system frequency is 60 Hz. The generator's over-frequency relays trip at 62 Hz and the under-frequency relays trip at 58 Hz.

1) Assessing System Vulnerabilities: The attacker can assess the vulnerability of the loads at each load bus to see the possibility of conducting D-LAA in the power system, also the type of attack. Fig. 5 shows how the root locus [25] analysis helps the attacker to find the minimum attack gain $K_{19,33}^{LG} = 15$ to conduct a single-point D-LAA when $v = 19$ and $s = 33$. If we multiply the minimum attack gain by two times the frequency deviation threshold $\omega_s^{\max} = 2/60$ at which the generators frequency relays trip, then we can conclude that at least $2K_{19,33}^{LG}\omega_s^{\max} = 15 \times 2 \times 2/60 = 1$ p.u. of the total 1.6 p.u. vulnerable load at victim bus 19 must be compromised when the frequency sensor is at bus $s = 33$ in order to have a successful single-point D-LAA. Note that the compromised load consumption must follow the frequency signal by a proportional controller. Also, the frequency signal deviates around its nominal value. Hence, the multiplication by two in $2K\omega_s$ is due to the fact that the compromised load must provide enough room to allow both over and under frequency fluctuations before the attack makes the frequency relays tripped. Similarly, we can calculate the minimum portion of vulnerable load that must be compromised for having successful single-point D-LAAs for all victim and sensor bus scenarios to find the vulnerabilities of the power system. The results are shown in Table II. We can see that only two successful single-point attacks are feasible: a single-point attack at victim bus $v = 19$ with sensor bus $s = 33$, and a single-point attack at victim bus $v = 29$ and sensor bus $s = 38$. No other single-point attack is feasible due to lack of sufficient vulnerable load. Another implication of the results in Table II is with respect to the coordinated multi-point attacks. For example, based on the column with $s = 33$, although hacking the loads individually at victim buses 16 and 23 cannot lead to successful single-point attacks, it might be possible to hack some loads at both buses and conduct a successful *coordinated multi-point* D-LAA.

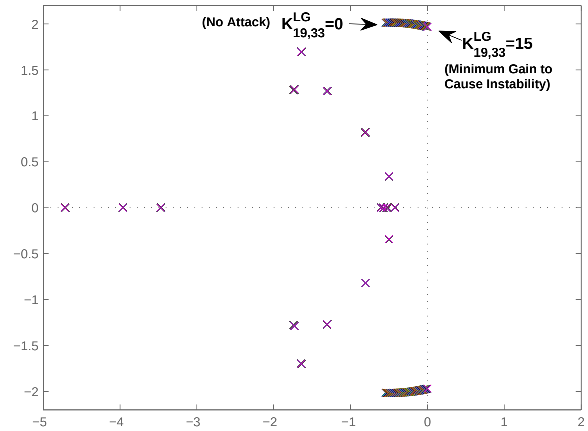

Fig. 5. Power system poles versus the attack gain $K_{19,33}^{LG}$.

TABLE II
MINIMUM PORTION OF VULNERABLE LOAD THAT MUST BE COMPROMISED TO ASSURE A SUCCESSFUL D-LAA

Sensor Bus / Victim Bus	31	33	36	38
6	4.9	18.4	81.2	128.1
16	24.7	1.2	6.5	23.3
19	69.2	0.6	15.2	48.8
23	79.1	3.2	1.9	66.8
29	92.2	8.9	46.5	0.7

2) Single-point Attack: Next, we examine three single-point attack scenarios for the case where $v = 19$ and $s = 33$. The results are shown in Fig. 6. First, assume that the attack is *static*, causing an abrupt change in victim load as shown in Fig. 6(d). The poles of the system are *not* changed under this

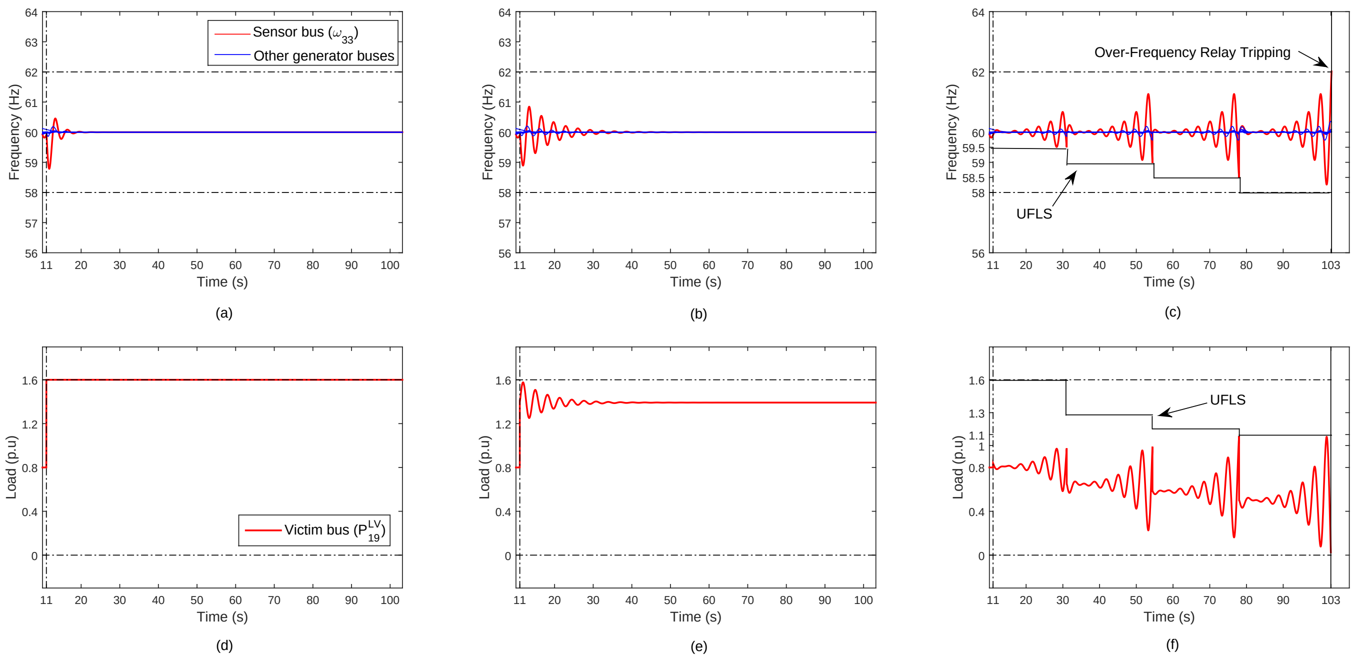

Fig. 6. Simulation results under various attack conditions. First row: system frequencies over time. Second row: vulnerable load changes. First column: S-LAA causing an abrupt load increase. Second column: an unsuccessful D-LAA with $K^{LG}_{19,33} = 10$. Third column: a successful D-LAA with $K^{LG}_{19,33} = 20$.

TABLE III
FREQUENCY SETTINGS OF THE UFLS RELAY

Step Number	Frequency Setting (Hz)	Amount of P^{LV}_{19} to be shed (p.u)
1	**59.5**	$20\% = 0.32$
2	**59**	$10\% = 0.13$
3	**58.5**	$5\% = 0.06$

attack. We can see in Fig. 6(a) that the system can easily absorb such one-time abrupt change. Second, assume that the attack is *dynamic* and $K^{LG}_{19,33} = 10$. We can see in Fig. 6(b) that the attack causes some relatively major over- and under-shoots in frequency. Nevertheless, the system remains stable and the frequency deviation is forced back to zero.

Finally, suppose the attack is dynamic and $K^{LG}_{19,33} = 20$. Under this third attack, two of the system poles are pushed to the right half-plane, making the system *unstable*. What is different in this case is that load Bus 19 is assumed to be equipped with a three-step UFLS protection relay [46]. This UFLS sheds only the vulnerable (but protected) portion of the load in response to frequency drop in its three sequential steps as listed in Table III. Fig. 6(c) shows that even after the three load shedding steps by the UFLS relay, the attack can still force the frequency deviation at generator bus $s = 33$ to reach the threshold $\omega_1^{\max} = 2/60$ p.u., causing the over-frequency relay of the generator at bus 33 to trip at time $t = 103s$, pushing this generator offline, thus, concluding the attack. Interestingly, the D-LAA under this last scenario did not need to hack the entire available vulnerable load at bus $v = 19$. Instead, it only followed the *right* trajectory in response to the changes in frequency in order to be successful.

Note that, implementing a D-LAA does not require all loads to be equipped with smart meters. In fact, according to Table I, only less than *one-third* of the loads at each bus are assumed to be vulnerable. That means, at each bus, over *two-third* of the loads are traditional loads and may not even have smart meters or any demand response equipment. Also, only a portion of the vulnerable loads needs to be compromised to conduct a successful attack. For example, according to Table II, the adversary can plan a single-point D-LAA by compromising only 60% of the total vulnerable loads at bus 19. Hence, only 60 % of smart meters at bus 19 need to be compromised.

3) Coordinated Multi-point Attack: Recall from Section IV-B1 that a coordinated multi-point attack at victim buses $v = 16$ and $v = 23$ might lead to a successful D-LAA. The amount of vulnerable load that needs to be hacked at each of the two victim buses to make the system unstable can be obtained using a two-dimensional root locus analysis in form of an exhaustive search. The results are shown in Fig. 7. This figure shows the *attack success time*, i.e., the time that takes from the moment the attack is launched until the moment the target generator goes offline, for all possible combinations of hacking vulnerable loads at buses $v = 16$ and $v = 23$. Note that, for those combinations where a successful attack is not feasible, no point is plotted in the curve. We can conclude that, while increasing the amount of compromised loads may not always be necessary to make the system unstable, it can still be beneficial to decrease the attack success time.

V. PROTECTION SCHEME

In the previous sections, we introduced, classified, and analyzed D-LAAs with focus on attacks against power system stability. In this section, we assume that each vulnerable load can be protected, e.g., by implementing reinforced security measures, but at some cost. The cost is due to adding hardware and software security components, whether at device level

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

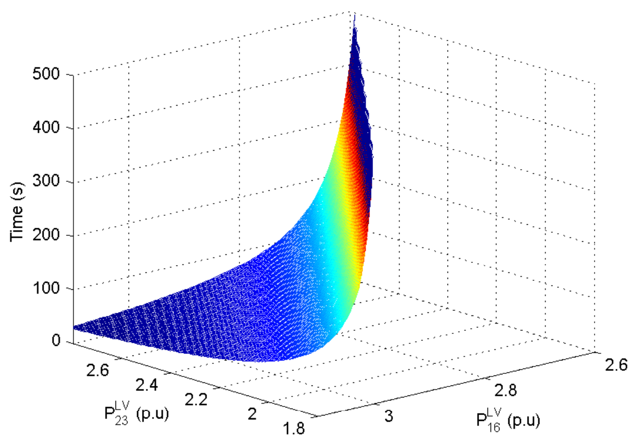

Fig. 7. Attack success time versus the amount of compromised load at each victim load bus in a coordinated multi-point closed-loop D-LAA.

[47, Section 6.2] or at communication level [1], [48]. Such cost is incurred directly to utility companies and indirectly to end consumers. Accordingly, we propose an algorithm to determine the *minimum* amount of load that must be protected at each load bus in order to assure power system stability under D-LAAs against the remaining unprotected vulnerable loads.

Note that, besides protecting the load, there might also exist some compensators to counter-attack D-LAAs to keep the power system stable. This may include frequency-responsive loads (see Section II-C) or load protection mechanisms such as UFLS protection relays (see Section IV-B), as well as ancillary generation mechanisms that respond to under- or over-frequencies. All such compensators can be integrated into our analysis by adding their corresponding system dynamics to the state-space system model in (11). Once such state-space model is updated, the rest of the attack analysis in Section IV as well as the protection scheme design approaches in this Section can still be applied similarly to the new system model.

A. Optimization Problem Formulation

The foundation of the proposed protection mechanism is to protect enough vulnerable loads such that we can maintain the system in (11) stable. Specifically, we want to keep the poles of the system on the left-half complex plane even if all unprotected vulnerable loads are compromised. This requires formulating and solving a *non-convex pole placement optimization problem*, as we will explain in details next.

The stability of the closed-loop system (13) can be analyzed using the Linear Quadratic Lyapunov Theory that is overviewed in Appendix A. Specifically, the closed-loop system in (13) is stable if there exists a *symmetric positive semi-definite* matrix X such that

$$\left(A - B\begin{bmatrix} 0 \\ 0 \\ K^{LG} \end{bmatrix}^T\right)^T X + X\left(A - B\begin{bmatrix} 0 \\ 0 \\ K^{LG} \end{bmatrix}^T\right) < 0. \tag{17}$$

For each victim load bus v, let P_v^{LP} denote the potentially vulnerable but *protected* load. Note that, we have $0 \le P_v^{LP} \le P_v^{LV}$. Accordingly, the amount of unprotected vulnerable load at bus v is calculated as $P_v^{LV} - P_v^{LP}$. This puts an upper bound on the attack controller gain K_{vs}^{LG}. Specifically, we have

$$K_{vs}^{LG}\omega_s^{\max} \le \left(P_v^{LV} - P_v^{LP}\right)/2, \tag{18}$$

where $\omega_s^{\max}$ denotes the maximum admissible frequency deviation for generator s before its over or under frequency relays trip. The division by two on the right hand side is due to the fact that the compromised load $P_v^{LV} - P_v^{LP}$ must provide enough room to allow both over or under frequency fluctuations, e.g., see Fig. 6(c) and (f), before the attack can trip the frequency relays at generator s, e.g., see Fig. 6(f).

To design an efficient load protection plan against D-LAAs, we need to solve the following optimization problem:

$$\begin{aligned} \textbf{minimize} \quad & \sum_{v\in\mathcal{V}} P_v^{LP} \\ \textbf{subject to} \quad & 0 \le P^{LP} \le P^{LV}, \\ & X \succeq 0, \\ & X = X^T, \\ & \text{Eqs. (17) and (18)}, \quad \forall v \in \mathcal{V}, \end{aligned} \tag{19}$$

where the variables are P^{LP}, K^{LG}, and X. Notation $\succeq$ indicates matrix positive semi-definiteness. Here, we seek to deploy the minimum total load protection that guarantees power system stability under D-LAA attacks against any unprotected vulnerable load when the frequency sensor is located at generator bus s. Problem (19) is a non-convex optimization problem due to the non-convex quadratic constraint in (17).

B. Solution Method

First, we note that the inequality constraint in (18) must hold as equality for any optimal solution of problem (19). This can be proved by contradiction. Note that, if at optimality, the constraint in (18) holds as strict inequality at a victim load bus v, then one can reduce P_v^{LP} and lower the objective function, thus, contradicting the optimality status. Therefore, K_{vs}^{LG} acts as a slack variable as far solving optimization problem (19) is concerned. Once P_v^{LP} is known, we have

$$K_{vs}^{LG} = \left(P_v^{LV} - P_v^{LP}\right)/\left(2\omega_s^{\max}\right). \tag{20}$$

Therefore, there are only two sets of variables in the optimization problem in (19), P^{LP} and X. They are *coupled* through the non-convex inequality constraint in (18). To tackle this non-convexity, we propose to solve problem (19) using the *coordinate descent method* [49, pp. 207]. The idea is to first take P^{LP} as a constant and solve problem (19) over X only:

$$\begin{aligned} \textbf{Minimize} \quad & \sum_{v\in\mathcal{V}} P_v^{LP} \\ \textbf{Subject to} \quad & X \succeq 0, \\ & X = X^T, \\ & \text{Eqs. (17) and (20)}, \quad \forall v \in \mathcal{V}, \end{aligned} \tag{21}$$

where the variables are the entries of matrix X. Here, the objective function could be *anything* because problem (21) is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

essentially a *feasibility* problem, c.f. [50, pp. 129]. Problem (21) can also be classified as a *semi-definite program* [50, pp. 168]. Next, we take X as a constant based on the solution of problem (21) and solve problem (19) over P^{LP} only:

$$\begin{aligned} &\textbf{Minimize} \quad \sum_{v\in\mathcal{V}} P_v^{LP} \\ &\textbf{Subject to} \quad 0 \le P^{LP} \le P^{LV}, \\ &\qquad\qquad\quad \text{Eqs. (17) and (20)}, \quad \forall v \in \mathcal{V}, \end{aligned} \tag{22}$$

where the variables are the entries of vector P^{LP}. This procedure is repeated, leading to an iterative algorithm. As for the initial condition, we start with full protection, i.e., we initially set $P_v^{LP} = P_v^{LV}$ for all potential victim load buses v. Next, we continue improving the protection system by lowering the amount of protected load while maintaining the stability of the system using the Lyapunov criteria in (17). The convergence of the coordinated descent algorithm is guaranteed, c.f. [49, Proposition 2.5]. Note that, at each iteration, the total protected load either reduces or remains unchanged. Therefore, the iterations continue until either we find the exact optimal solution for (19) or we reach a stationary point that is sub-optimal. As we will see in Section V-D, the optimality gap for the above algorithm is typically very small.

C. Protection System Design Under Uncertainty

For the analysis in Sections V-A and V-B, it was implicitly assumed that the power system operator knows where the frequency sensor is deployed. That is, it knows the location of sensor bus s. However, this assumption may not always hold in practice. This creates uncertainty when designing the protection system. The key to tackle uncertainty is to design the protection system in a way that it is robust to any scenario for the location of the sensor bus. This can be done by solving the following optimization problem which is an extension of problem (19) across various sensor bus location scenarios:

$$\begin{aligned} &\textbf{minimize} \quad \sum_{v\in\mathcal{V}} P_v^{LP} \\ &\textbf{subject to} \quad 0 \le P^{LP} \le P^{LV}, \\ &\qquad X_s \succeq 0, \qquad \forall s \in \mathcal{S}, \\ &\qquad X_s = X_s^T, \quad \forall s \in \mathcal{S}, \\ &\qquad \text{Eqs. (17) and (20)}, \quad \forall v \in \mathcal{V},\ \forall s \in \mathcal{S}, \end{aligned} \tag{23}$$

where the variables are P^{LP}, K^{LG}, and X_s for any $s \in \mathcal{S}$. Here, $\mathcal{S} \subseteq \mathcal{G}$ denotes the set of all potential locations for the sensor bus. Problem (23) can be solved similar to problem (19) using the coordinated descent method, see Section V-B.

D. Case Studies

Again consider the power system in Section IV-B. We would like to protect this system against closed-loop D-LAAs.

1) Known Sensor Bus Location: Suppose the sensor bus is located at bus $s = 33$ and this is known to the grid operator. The results for solving the protection system optimization problem in (19) in this case are shown in Fig. 8. We can see that as long as we fully protect the vulnerable load at bus 19 and protect 30.4% of the vulnerable load at bus 16, then no D-LAA with $s = 33$ can make the power system unstable. Note that, the total optimal load protection in this case is only 18.4% of the total vulnerable load in the system.

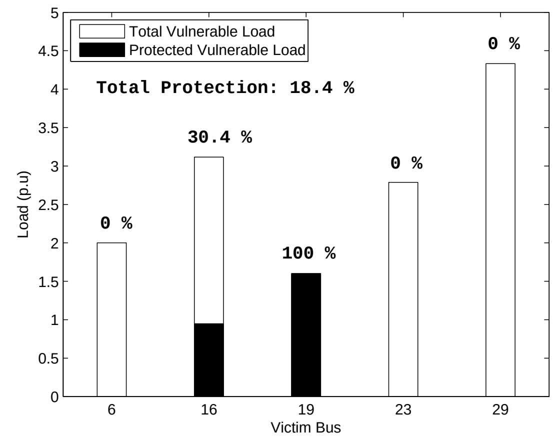

Fig. 8. The optimal load protection scheme when the sensor location is known.

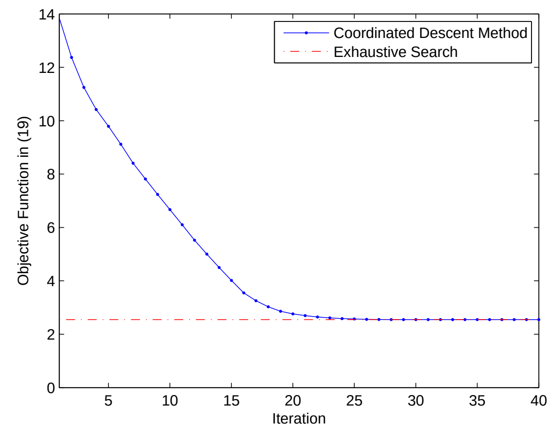

Fig. 9. The iterative approach to solve the optimization problem in (19).

The operation of our proposed iterative algorithm to solve problem (19) is illustrated in Fig. 9. Recall from Section V-B that the algorithm starts from full protection and iterates until it reaches a stationary point at a much lower protection level. We can see that, the algorithm has indeed converged to the global optimal solution in this case after less than 45 iterations. Here, the global optimal solution is verified by conducting an exhaustive search based on an extensive root locus analysis.

2) Unknown Sensor Bus Location: Next, consider the more practical scenario where the operator does *not* know where the attack frequency sensor is located. Accordingly, it needs to solve the extended optimization problem in (23). The results are shown in Fig. 10. As expected, the amount of vulnerable loads that need to be protected is higher in this case. However, such amount is still not too high and only at 26.8% of the total vulnerable load in the system. We can see that the uncertainty about the attack sensor location can be tackled by slightly adjusting the load protection plan, where we also protect 29.3% of the vulnerable load at bus 29. Interestingly, such

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

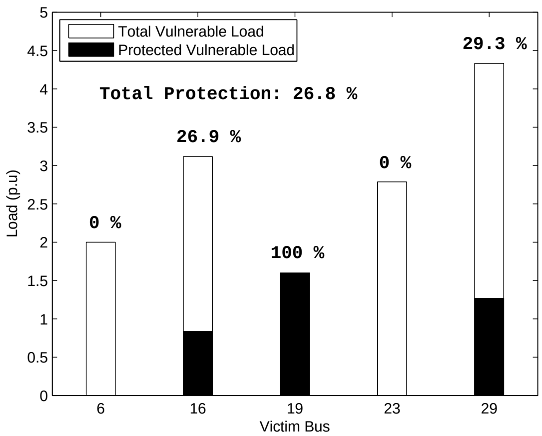

Fig. 10. The optimal load protection scheme when the sensor location is unknown.

protection allows some decrease, from 30.4% to 26.9%, in the level of vulnerable load that must be protected at bus 16.

VI. Conclusions

Dynamic load altering attacks were introduced, characterized, and classified. Of particular interest was a closed-loop D-LAA against power system stability with feedback from power system frequency. Both single-point and coordinated multi-point attacks were investigated. A protection scheme was designed against closed-loop D-LAA attacks by formulating and solving a non-convex pole placement optimization problem. The non-convexity was tackled by using an iterative algorithm which solves a sequence of semi-definite optimization and convex feasibility optimization problems. Uncertainty with respect to the attack sensor location was addressed. Various case studies were presented to assess system vulnerabilities, the impacts of single-point and multi-point attacks, and the optimal load protection scheme in an IEEE 39 bus test system.

Appendix A
Linear Quadratic Lyapunov Theory

Consider the linear time-invariant system $\dot{x} = Ax$. Using Lyapunov function $V(x) = x^T X x$, one can show that:

1) The system is stable if there exists a real, symmetric, and positive definite matrix X such that $C = A^T X + XA$ and C is negative definite [51, Theorem 7.3]; and
2) The system is unstable if $C = A^T X + XA$ is negative definite, and X is real, symmetric, and either negative definite or indefinite [51, Theorem 7.3].

References

[1] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 4, pp. 998–1010, 2012.
[2] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *Smart Grid, IEEE Transactions on*, vol. 1, no. 1, pp. 57–64, 2010.
[3] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Innovative Smart Grid Technologies (ISGT), 2010*. IEEE, 2010, pp. 1–7.
[4] W. F. Boyer and S. A. McBride, "Study of security attributes of smart grid systems–current cyber security issues," *Idaho National Laboratory, USDOE, Under Contract DE-AC07-05ID14517*, 2009.
[5] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," in *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES*. IEEE, 2009, pp. 1–8.
[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, May 2011.
[7] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *IEEE International Conference on Smart Grid Communications*, Brussels, Belgium, Oct. 2011.
[8] S. Shao, M. Pipattanasomporn, and S. Rahman, "Demand response as a load shaping tool in an intelligent grid with electric vehicles," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 624–631, Dec. 2011.
[9] G. Strbac, "Demand side management: Benefits and challenges," *Energy Policy*, vol. 36, no. 12, pp. 4419–4426, Dec. 2008.
[10] H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.
[11] S. Kiliccote, S. Lanzisera, A. Liao, O. Schetrit, and M. A. Piette, "Fast dr: Controlling small loads over the internet," *Forthcoming Proceedings of the ACEEE Summer Study on Energy Efficiency in Buildings*, 2014.
[12] H. Mohsenian-Rad, V. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous Demand Side Management Based on Game-Theoretic Energy Consumption Scheduling for the Future Smart Grid," *IEEE Trans. on Smart Grid*, vol. 1, no. 3, pp. 320–331, Dec. 2010.
[13] L. Yao and L. Hau-Ren, "A Two-Way Direct Control of Central Air-Conditioning Load Via the Internet," *IEEE Trans. on Power Delivery*, vol. 24, no. 1, pp. 240–248, Jan. 2009.
[14] H. Mohsenian-Rad and A. Leon-Garcia, "Optimal Residential Load Control with Price Prediction in Real-Time Electricity Pricing Environments," *IEEE Trans. on Smart Grid*, vol. 1, pp. 120–133, Sep. 2010.
[15] A. Molina-Garcia, F. Bouffard, and D. S. Kirschen, "Decentralized demand-side contribution to primary frequency control," *IEEE Trans. on Power Systems*, vol. 26, no. 1, pp. 411–419, Feb. 2011.
[16] C. Zhao, U. Topcu, and S. H. Low, "Optimal load control via frequency measurement and neighborhood area communication," *IEEE Trans. on Power Systems*, vol. 28, no. 4, pp. 3576–3587, Nov. 2013.
[17] A. K. Marnerides, P. Smith, A. Schaeffer-Filho, and A. Mauthe, "Power consumption profiling using energy time-frequency distributions in smart grids," *IEEE Communications Letters*, vol. 19, no. 1, pp. 46–49, 2015.
[18] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38–45, 2012.
[19] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.
[20] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.
[21] F. Pasqualetti, A. Bicchi, and F. Bullo, "A graph-theoretical characterization of power network vulnerabilities," in *Proc. of IEEE American Control Conference*, San Francisco, CA, Jun. 2011.
[22] J. W. V. der Woude, "A graph-theoretic characterization for the rank of the transfer matrix of a structured system," *Signals and Systems Mathematics of Control*, vol. 4, no. 1, pp. 33–40, 1991.
[23] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Proc. of Workshop on Secure Control Sys.*, Stockholm, Sweden, 2010.
[24] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *IEEE PES Conference on Innovative Smat Grid Technologies (ISGT)*, Washington, D.C, Feb. 2015.
[25] R. C. Dorf, *Modern control systems*. Addison-Wesley Longman Publishing Co., Inc., 1995.
[26] J. C. Vieira, W. Freitas, W. Xu, and A. Morelato, "Performance of frequency relays for distributed generation protection," *Power Delivery, IEEE Transactions on*, vol. 21, no. 3, pp. 1120–1127, 2006.
[27] S. V. Buldyrev and R. Parshani and G. Paul and H. E. Stanley and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.
[28] Y. Tomita, C. Fukui, H. Kudo, J. Koda, and K. Yabe, "A cooperative protection system with an agent model," *Power Delivery, IEEE Transactions on*, vol. 13, no. 4, pp. 1060–1066, 1998.
[29] P. Du and N. Lu, "Appliance Commitment for Household Load Scheduling," *IEEE Trans. on Smart Grid*, vol. 2, no. 2, pp. 411–419, Jun. 2011.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2622686, IEEE Transactions on Smart Grid

[30] P. Kadurek, C. Ioakimidis, and P. Ferrao, "Electric vehicles and their impact to the electric grid in isolated systems," in *Proc. of International Conference on Power Engineering, Energy and Electrical Drives*, Lisbon, Portugal, Mar. 2009.

[31] L. Yang, S. Hu, and T. Ho, "Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks," in *Proc. of the IEEE/ACM International Conference on Computer-Aided Design*, San Jose, CA, Nov. 2014.

[32] L. Husheng and Z. Han, "Manipulating the electricity power market via jamming the price signaling in smart grid," in *Proc. of the IEEE GLOBECOM Workshops*, Houston, TX, Dec. 2011.

[33] C. W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *Power Systems, IEEE Transactions on*, vol. 23, no. 4, pp. 1836–1846, 2008.

[34] S. Mishra, X. Li, T. Pan, A. Kuhnle, M. T. Thai, and J. Seo, "Price modification attack and protection scheme in smart grid," *IEEE Trans. on Smart Grid*, 2016.

[35] K. Vanthournout, R. D'hulst, D. Geysen, and G. Jacobs, "A smart domestic hot water buffer," *Smart Grid, IEEE Transactions on*, vol. 3, no. 4, pp. 2121–2127, 2012.

[36] G. Marks, "Opportunities for demand response in california agricultural irrigation: A scoping study," 2014.

[37] S. Shao, T. Zhang, M. Pipattanasomporn, and S. Rahman, "Impact of tou rates on distribution load shapes in a smart grid with phev penetration," in *Proc. of IEEE PES Transmission and Distribution Conference and Exposition*, 2010.

[38] M. Ghamkhari and H. Mohsenian-Rad, "Energy and performance management of green data centers: A profit maximization approach," *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 1017–1025, 2013.

[39] http://www.mainsfrequency.com/meter.htm.

[40] J. D. Fernandez and A. E. Fernandez, "Scada systems: vulnerabilities and remediation," *Journal of Computing Sciences in Colleges*, vol. 20, no. 4, pp. 160–168, 2005.

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

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

[43] C. Zhao, U. Topcu, N. Li, and S. Low, "Design and stability of load-side primary frequency control in power systems," *Automatic Control, IEEE Transactions on*, vol. 59, no. 5, pp. 1177–1189, 2014.

[44] S. P. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear matrix inequalities in system and control theory*. SIAM, 1994, vol. 15.

[45] http://sys.elec.kitami-it.ac.jp/ueda/demo/WebPF/39-New-England.pdf.

[46] R. Hassan, M. Abdallah, G. Radman, F. Marco, S. Hammer, J. Wigington, J. Givens, D. Hislop, J. Short, and S. Carroll., "Under-frequency load shedding: towards a smarter smart house with a consumer level controller," in *Proc. of the IEEE SoutheastCon*, Nashville, TN, Mar. 2011.

[47] M. Mahmoud, J. Misic, X. Shen *et al.*, "Investigating public-key certificate revocation in smart grid," *IEEE Internet of Things Journal*, Mar. 2015.

[48] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 36–46, 2013.

[49] D. P. Bertsekas and J. N. Tsitsiklis, *Parallel and distributed computation: numerical methods*. Prentice hall Englewood Cliffs, NJ, 1989, vol. 23.

[50] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[51] P. J. Antsaklis and A. N. Michel, *Linear systems*. Springer Science & Business Media, 2006.

Sajjad Amini (S'14) received the M.Sc. degree in electrical engineering - control systems from Amirkabir University of Technology, Tehran, Iran, in 2012. He is currently working toward his Ph.D. degree in electrical engineering - smart grid at the University of California, Riverside, CA, USA. His research interests include power system dynamics, cyber-physical security, demand response, Wide Area Monitoring Systems (WAMS), and large scale control systems.

Fabio Pasqualetti (S'07-M'13) is an Assistant Professor in the Department of Mechanical Engineering, University of California, Riverside. He completed a Doctor of Philosophy degree in Mechanical Engineering at the University of California, Santa Barbara, in 2012, a Laurea Magistrale degree (M.Sc. equivalent) in Automation Engineering at the University of Pisa, Italy, in 2007, and a Laurea degree (B.Sc. equivalent) in Computer Engineering at the University of Pisa, Italy, in 2004.

His main research interest is in secure control systems, with application to multi-agent networks, distributed computing, and power networks. Other interests include vehicle routing and combinatorial optimization, with application to distributed area patrolling and persistent surveillance, and computational neuroscience.

Hamed Mohsenian-Rad (S'04-M'09-SM'14) received the Ph.D. degree in electrical and computer engineering from the University of British Columbia Vancouver, BC, Canada, in 2008. He is currently an Associate Professor of electrical engineering at the University of California, Riverside, CA, USA. His research interests include modeling, analysis, and optimization of power systems and smart grids with focus on large-scale power data analysis. He received the National Science Foundation CAREER Award 2012, the Best Paper Award from the IEEE Power and Energy Society General Meeting 2013, and the Best Paper Award from the IEEE International Conference on Smart Grid Communications 2012. He serves as an Editor for the IEEE TRANSACTIONS ON SMART GRID and the IEEE COMMUNICATIONS LETTERS.