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

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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N$</td>
<td>Set of buses</td>
</tr>
<tr>
<td>$G$, $L$</td>
<td>Set of generator and load buses</td>
</tr>
<tr>
<td>$V$, $S$</td>
<td>Set of victim and sensor buses</td>
</tr>
<tr>
<td>$i$, $j$</td>
<td>Index of buses</td>
</tr>
<tr>
<td>$v$, $s$</td>
<td>Index of victim and sensor buses</td>
</tr>
<tr>
<td>$H$</td>
<td>Admittance matrix</td>
</tr>
<tr>
<td>$\delta$</td>
<td>Voltage phase angle at generator buses</td>
</tr>
<tr>
<td>$\theta$</td>
<td>Voltage phase angle at load buses</td>
</tr>
<tr>
<td>$\omega$</td>
<td>Frequency deviation at generator buses</td>
</tr>
<tr>
<td>$\varphi$</td>
<td>Frequency deviation at load buses</td>
</tr>
<tr>
<td>$\omega_{\max}$</td>
<td>Frequency relay threshold for generators</td>
</tr>
<tr>
<td>$p^G$</td>
<td>Power injection at generator buses</td>
</tr>
<tr>
<td>$p^L$</td>
<td>Power consumption at load buses</td>
</tr>
<tr>
<td>$p^M$</td>
<td>Mechanical power input to generators</td>
</tr>
<tr>
<td>$M^G$</td>
<td>Inertia matrix for generators</td>
</tr>
<tr>
<td>$P^{LV}$, $P^{LS}$</td>
<td>Secured and vulnerable portion of the load</td>
</tr>
<tr>
<td>$D^G$, $D^L$</td>
<td>Damping coefficient matrices</td>
</tr>
<tr>
<td>$K^P$, $K^I$</td>
<td>Generator controller gain matrices</td>
</tr>
<tr>
<td>$K^{LG}$, $K^{LL}$</td>
<td>Attack controller gain matrices</td>
</tr>
<tr>
<td>$A$, $B$</td>
<td>State-space matrices of open-loop system</td>
</tr>
<tr>
<td>$X$</td>
<td>Lyapunov positive semi-definite matrix</td>
</tr>
</tbody>
</table>

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 load altering attacks, e.g., remotely controllable loads [11], loads that automatically respond to price or direct load control 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:
Dynamic load altering attacks (D-LAA) are introduced and characterized as a new form of cyber-physical attacks against smart grid. D-LAAs are then classified in terms of open-loop versus closed-loop attacks, single-point versus coordinated multi-point attacks, the type of feedback measurement, and the type of the attack controller.

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 in an IEEE 39 bus test system.

A protection system 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 in the system to assure power system stability under D-LAAs against the remaining unprotected vulnerable loads. Design uncertainty with respect to the exact attack location is taken into consideration. The protection system design is assessed in an 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 can also add 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 system by formulating and solving a non-convex pole placement optimization problem. Third, the case studies in [24] were limited to a six bus network, while the case studies here are based on a 39 bus IEEE test system.

II. SYSTEM MODEL

Consider a power system with $N = G \cup \mathcal{L}$ as the set of buses, where $G$ and $\mathcal{L}$ are the sets of generator and load buses, respectively. An example is shown in Fig. 1. The linear power flow equations at each bus $i \in N$ can be written as [25]:

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

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

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 $i$, $\delta_i$ is the voltage phase angle at generator bus $i$, $\theta_i$ 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., [26], to model the generator dynamics at each generator bus $i \in G$, 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 $\omega_i$ 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 [25]. 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 $\omega_i$ back to zero. The two controllers can together be modeled as a proportional-integral (PI) controller, that is,

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

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

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

Three load types are considered in this system [27]: (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

Fig. 1. The IEEE 39 bus test system based on the 10-machine New-England power network, where $\mathcal{L} = \{1, \ldots, 29\}$ and $G = \{30, \ldots, 39\}$.
We denote the imaginary part of the admittance matrix as
\[ \text{with diagonal entries equal to the integral and proportional \, dimension, and} \]
\[ D^L \varphi_i - P^L_i = \sum_{j \in G} H_{ij}(\theta_i - \delta_j) + \sum_{j \in L} H_{ij}(\theta_i - \delta_j), \]
and the overall power system dynamics can be conveniently written as the following linear state-space descriptor system:
\[
\begin{bmatrix}
I & 0 & 0 & 0 \\
0 & I & 0 & 0 \\
0 & 0 & -M & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\begin{bmatrix}
\dot{\delta} \\
\dot{\theta} \\
\dot{\omega}_L \\
\dot{\omega}_G
\end{bmatrix} = \begin{bmatrix}
0 & 0 & I & 0 \\
0 & 0 & 0 & I \\
K^I + B^{GG} & H^{GL} & K^P + D^G & 0 \\
H^{LG} & H^{LL} & 0 & -D^L
\end{bmatrix}
\begin{bmatrix}
\dot{\delta} \\
\dot{\theta} \\
\dot{\omega}_L \\
\dot{\omega}_G
\end{bmatrix} + \begin{bmatrix}
0 \\
0 \\
0 \\
0
\end{bmatrix} P^L_i.
\] (8)

In (8), \( \delta \) is the vector of phase angles at all generator buses, \( \omega \) is the vector of rotor angular frequency deviations at all generator buses, \( \theta \) is the vector of phase angles at all load buses, \( \varphi \) is the vector of frequency deviations at all 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
\[ H_{bus} = \begin{bmatrix}
H^{GG} & H^{GL} \\
H^{LG} & H^{LL}
\end{bmatrix} \]
III. DYNAMIC LOAD ALTERING ATTACK

In this section, we formally introduce dynamic load altering attacks, their classifications, and their impact on the grid performance and stability. Various case studies are presented.

A. Basic Concepts and D-LAA Classifications

Based on the system model in Section II, 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
\[ P^L_i = P^{LS}_i + P^{LV}_i, \]
where \( P^{LS}_i \) denotes the secure and \( P^{LV}_i \) denotes the vulnerable portion of the load at bus \( i \), respectively. An attack may compromise only the vulnerable part of a victim load bus.

So far, the focus on load altering attacks in the literature has been limited to static attacks, e.g., see [10], [17], [18]. A Static Load Altering Attacks (S-LAA) is concerned mainly with the volume of the vulnerable load that has to change in order to damage the grid. For example, in [10], the focus is on calculating the minimum load volume that must be switched on simultaneously in order to create a load spike that is large enough to cause circuit overflow on a target transmission line.

In contrast, in this paper, we define and characterize Dynamic Load Altering Attacks (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 at the victim load bus. Next, we explain different classes of D-LAAs.

A D-LAA can be open-loop or closed-loop. In an open-loop D-LAA, see Fig. 2(a), the attacker does not monitor the grid conditions in real-time. Instead, it 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 based on the grid operating conditions.

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. 2(b) and (c), respectively.

In this paper, we are particularly interested in closed-loop D-LAAs as they can potentially affect power system stability. In general, 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. Since our focus is on attacks against power system stability, we assume that the attack feedback loop is based on measuring power grid frequency. This setup is also of practical importance 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 on the same interconnected network. We refer to the bus where the frequency sensor is located as the sensor bus \( s \).

Finally, one can classify D-LAAs also based on the type of controller being used in order to adjust the victim loads, 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 [28], or
any other more complex feedback control system mechanism.

B. Power System Dynamics Under Attack

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

$$P_v^{LV} = -K_{LG} \omega_s - K_{LL} \varphi_s. \quad (10)$$

Note that, since $K_{LG}$ and $K_{LL}$ are positive valued, $P_v^{LV}$ is updated in opposition to the values of $\omega_s$ and $\varphi_s$. For example, if $\omega_s$ 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

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

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 unstable by moving the system poles to the right-half complex plane [28]. Of course, in practice, since the generators are equipped with over- and under-frequency relays as part of their protection systems, c.f. [29], a D-LAA attack may ultimately force certain generators to disconnect from the main grid, possibly triggering cascading effects or blackouts.

Power system dynamics under a multi-point closed-loop D-LAA can be analyzed similarly. Next, we assess the system vulnerabilities and the attack outcome under both single-point and multi-point D-LAA through some case studies.

C. Case Studies

Consider the IEEE 39 bus power system in Fig. 1. Suppose the parameters of the transmission lines and the inertia and damping coefficients of generators are as in [30]. Total loads and vulnerable loads at each load bus are as in Table I. Generator controller parameters are $K^P = 100$, $K^L = 45$, $K_p = 10$, $K_p^L = K_p^G = 50$, $K_p^L = 40$, $K_p^G = 30$, $K^L = 20$, and $K^L_1 = \ldots = K^L_{10} = 60$. 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 $V = \{6, 16, 19, 23, 29\}$. These victim load buses are highlighted using color gray in Table I. Sensor buses are assumed to be placed only at $S = \{31, 33, 36, 38\}$. 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. 3 shows how the root locus [28] 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. Similarly, we can calculate the minimum portion of vulnerable

### Table I

<table>
<thead>
<tr>
<th>Bus</th>
<th>$P^L$ (p.u)</th>
<th>$P^{LV}$ (p.u)</th>
<th>Bus</th>
<th>$P^L$ (p.u)</th>
<th>$P^{LV}$ (p.u)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>0</td>
<td>16</td>
<td>7.8</td>
<td>3.1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>0</td>
<td>17</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>7.2</td>
<td>0</td>
<td>18</td>
<td>5.6</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>0</td>
<td>19</td>
<td>4</td>
<td>1.6</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>0</td>
<td>20</td>
<td>10.3</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>2</td>
<td>21</td>
<td>6.7</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>6.5</td>
<td>0</td>
<td>22</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>9.2</td>
<td>0</td>
<td>23</td>
<td>7</td>
<td>2.8</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>0</td>
<td>24</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>0</td>
<td>25</td>
<td>6.2</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>0</td>
<td>26</td>
<td>5.4</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>4.1</td>
<td>0</td>
<td>27</td>
<td>6.8</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>0</td>
<td>28</td>
<td>6.1</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
<td>0</td>
<td>29</td>
<td>10.8</td>
<td>4.3</td>
</tr>
<tr>
<td>15</td>
<td>7.2</td>
<td>0</td>
<td>30</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

![Power system poles versus the attack gain $K_{19,33}^{LG}$](image-url)
TABLE II
MINIMUM PORTION OF VULNERABLE LOAD THAT MUST BE COMPROMISED TO ASSURE A SUCCESSFUL D-LAA

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

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.

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. 4. First, assume that the attack is static, causing an abrupt change in victim load as shown in Fig. 4(d). The poles of the system are not changed under this attack. We can see in Fig. 4(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. 4(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, assume that 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. We can see in Fig. 4(c) that the attack forces the frequency deviation at generator bus \(s = 33\) to reach the threshold \(\omega_{max}^{19} = 2/60 \text{ p.u.}\), causing the over-frequency relay of the generator at bus 33 to trip at time \(t = 36\text{s}\), pushing this generator offline, thus, concluding the attack. Interestingly, the D-LAA under this last scenario did not need to hack the entire 1.6 p.u. vulnerable load at bus \(v = 19\). Instead, it only followed the right trajectory in response to changes in frequency in order to be successful.

3) Coordinated Multi-point Attack: Recall from Section III.A.1 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. 5. 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.

IV. PROTECTION DESIGN

In the previous section, 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. Accordingly, we propose an algorithm to determine the minimum amount of load that must
be protected at each bus to assure power system stability under D-LAAs against the remaining unprotected vulnerable loads.

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.

First, 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., $s \in G$. Accordingly, we have $K_{v}^{LG}$ = 0 for all victim load buses $v$. From this, and the last row in (11), we have:

$$\varphi = (D^{L})^{-1} \left[ \begin{array}{c} (H^{LL})^{T} \delta \\ -K^{LG} \end{array} \right] + P^{LS}.$$

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

$$\begin{bmatrix} \delta \\ \dot{\theta} \\ \dot{\omega} \end{bmatrix} = A \begin{bmatrix} \delta \\ \theta \\ \omega \end{bmatrix} + B \begin{bmatrix} 0 \\ 0 \\ K^{LG} \end{bmatrix}^{T} \begin{bmatrix} \delta \\ \theta \\ \omega \end{bmatrix} + P^{LS},$$

where

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

and

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

Note that, we have $K_{s}^{LG}$ = 0 for any $i \notin V$ 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 matrixes in the corresponding open-loop system in absence of the D-LAA. The stability of this closed-loop system can be analyzed using the Lyapunov theorem [31]. Specifically, the closed-loop system in (13) is stable if there exists a symmetric positive semi-definite matrix $X$ such that

$$\begin{bmatrix} A - B & 0 \\ 0 & K^{LG} \end{bmatrix}^{T} X + X \begin{bmatrix} A - B & 0 \\ 0 & K^{LG} \end{bmatrix} < 0.$$  

(14)

For each victim load bus $v$, let $P_{v}^{LP}$ denote the potentially vulnerable but protected load. Note that, we have $0 \leq P_{v}^{LP} \leq P_{v}^{LV}$. 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 $K_{v}^{LG}$. Specifically, we have

$$K_{v}^{LG} \omega_{s}^{\text{max}} \leq (P_{v}^{LV} - P_{v}^{LP}) / 2,$$

(15)

where $\omega_{s}^{\text{max}}$ 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. 4(c) and (f), before the attack can trip the frequency relays at generator $s$, e.g., see Fig. 4(f).

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

$$\text{minimize} \sum_{v \in V} P_{v}^{LP}$$

subject to

$$0 \leq P_{v}^{LP} \leq P_{v}^{LV},$$

$$X \succeq 0,$$

$$X = X^{T},$$

Eqs. (14) and (15), $\forall v \in V,$

where the variables are $P_{v}^{LP}$, $K_{v}^{LG}$, 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 (16) is a non-convex optimization problem due to the non-convex quadratic constraint in (14).

B. Solution Method

First, we note that the inequality constraint in (15) must hold as equality for any optimal solution of problem (16). This can be proved by contradiction. Note that, if at optimality, the constraint in (15) 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, $K_{v}^{LG}$ acts as a slack variable as far solving optimization problem (16) is concerned. Once $P_{v}^{LP}$ is known, we have

$$K_{v}^{LG} = (P_{v}^{LV} - P_{v}^{LP}) / (2\omega_{s}^{\text{max}}).$$

(17)

Therefore, there are only two sets of variables in the optimization problem in (16), $P^{LP}$ and $X$. They are coupled through...
the non-convex inequality constraint in (15). To tackle this non-convexity, we propose to solve problem (16) using the coordinate descent method [32, pp. 207]. The idea is to first take $P_{LP}$ as a constant and solve problem (16) over $X$ only:

$$\text{Minimize} \sum_{v \in V} P_{v}^{LP}$$

$$\text{Subject to } X \succeq 0,$$

$$X = X^T,$$

Eqs. (14) and (17), $\forall v \in V$,

where the variables are the entries of matrix $X$. Here, the objective function could be anything because problem (18) is essentially a feasibility problem, c.f. [33, pp. 129]. Problem (18) can also be classified as a semi-definite program [33, pp. 168]. Next, we take $X$ as a constant based on the solution of problem (18) and solve problem (16) over $P_{LP}$ only:

$$\text{Minimize} \sum_{v \in V} P_{v}^{LP}$$

$$\text{Subject to } 0 \leq P_{LP} \leq P_{LV},$$

Eqs. (14) and (17), $\forall v \in V$,

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 (14). The convergence of the coordinated descent algorithm is guaranteed, c.f. [32, 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 (16) or we reach a stationary point that is sub-optimal. As we will see in Section IV-D, the optimality gap for the above algorithm is typically very small.

C. Protection System Design Under Uncertainty

For the analysis in Sections IV-A and IV-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 (16) across various sensor bus location scenarios:

$$\text{minimize} \sum_{v \in V} P_{v}^{LP}$$

$$\text{subject to } 0 \leq P_{LP} \leq P_{LV},$$

$$X_s \succeq 0, \quad \forall s \in S,$$

$$X_s = X_s^T, \quad \forall s \in S,$$

Eqs. (14) and (17), $\forall v \in V, \forall s \in S$,

where the variables are $P_{LP}$, $K_{LG}$, and $X_s$ for any $s \in S$. Here, $S \subseteq G$ denotes the set of all potential locations for the sensor bus. Problem (20) can be solved similar to problem (16) using the coordinated descent method, see Section IV-B.

D. Case Studies

Again consider the power system in Section III-C. 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 (16) in this case are shown in Fig. 6. 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.

The operation of our proposed iterative algorithm to solve problem (16) is illustrated in Fig. 7. Recall from Section IV-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.
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 system 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 plan in an IEEE 39 bus test system.

V. 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 system 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 plan in an IEEE 39 bus test system.

REFERENCES


