Dynamic Load Altering Attacks in Smart Grid

Sajjad Amini†, Hamed Mohsenian-Rad†, and Fabio Pasqualetti‡
†Department of Electrical and Computer Engineering, University of California, Riverside, CA, USA
‡Department of Mechanical Engineering, University of California, Riverside, CA, USA
E-mails: {saamini, hamed}@ece.ucr.edu and fabiopas@engr.ucr.edu

***Abstract*—A load altering attack (LAA) is a cyber-physical attack against demand response and demand side management programs. It attempts to control and change certain *unsecured controllable loads* in order to damage the grid through circuit overflow or other adverse effects. So far, the focus in the LAA literature has been only on *static* load altering attacks, where the attack is mainly concerned in changing the volume of the load. In contrast, in this paper, we address *dynamic* load altering attacks (DLAAs), where we are concerned with not only the amount of the change in the load, but also the *trajectory over time* at which we change the load. Interestingly, we can prove that if a DLAA is *closed-loop* in a way that the load is changed in response to changes in power grid frequency, then we can introduce DLAA trajectories that make the power system unstable. This can be achieved without the need for increasing the scope or volume of the attack, compared to a static LAA scenario. We present simulation results based on an example six bus test system.**

***Keywords*: Load altering attacks, power system dynamics, demand response, smart grid cyber security, closed-loop control.**

I. Introduction

The use of information technology (IT) in power systems has introduced new opportunities to enhance efficiency and reliability of the power infrastructure [1]. However, IT and communications systems may also create new vulnerabilities in power networks if they are not accompanied with appropriate security enforcements. For example, recent studies have shown that adversaries may compromise the readings of power sensors and phasor measure units and affect the monitoring and control tasks in interconnected power networks [2]–[4]

In this paper, our focus is on attacks against 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 [5]. In a related field, DSM techniques also seek to exploit the load flexibility in different load sectors, e.g., by using automated energy consumption management systems [6]. Examples of DR and DSM studies include [7]–[9] for charging electric-vehicles, [10], [11] for industrial loads, [12], [13] for buildings and commercial loads, and [14]–[16] for residential loads.

An important class of cyber-physical attacks against DR an DSM systems are load altering attacks (LAA) [17]. LAA attempts to control and change a group of 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., controllable loads that automatically respond to price signals [14], [15], loads in direct load control (DLC) programs [18], and data centers and other computation loads [17], [19].

This work was supported in part by National Science Foundation grants ECCS 1405330 and ECCS 1253516 and California Energy Commission grant EISG 57757A. H. Mohsenian-Rad is the corresponding author.

The analysis in [17] was mainly on *static* load altering attacks, where the attack is concerned in changing the volume of certain loads, in particular in an *abrupt* fashion. In contrast, in this paper, we address *dynamic* load altering attacks (DLAAs), where we are not only concerned with the amount of the change in the load but also the *trajectory over time* at which we change the load. Accordingly, our analysis is based on power system dynamics and we use feedback control theory as the main tool to design the attack. The contributions in this paper can be summarized as follows:

- We introduce dynamic load altering attacks as a new class of cyber-physical attacks against smart grid. To the best of our knowledge, no prior study has addressed DLAAs.
- We formulate a closed-loop DLAA against power system stability, where the attacker controls the victim load based on a feedback from the power system frequency.
- We test the proposed closed-loop DLAA design against power system stability in a six bus case study and show some basic properties of the attack, such as the impact of attack controller gain and the impact of attack location.

This study complements and merges two generally independent lines of research in the literature. First, it can benefit the recent efforts in designing efficient and practical demand response and demand side management programs [5]–[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].

II. System Model

Consider a power system with $\mathcal{N}$ as the set of buses. Assume that the set of generators and load buses are denoted by $\mathcal{G} \subseteq \mathcal{N}$ and $\mathcal{L} \subseteq \mathcal{N}$, respectively. An example is shown in Fig. 1, where $\mathcal{L} = \mathcal{N} = \{1, 2, \ldots, 6\}$, $\mathcal{G} = \{1, 2, 3\}$. We can write the linear power flow equations for this network as [24]:

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

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

where P_i^G denotes the power injection of the generator at bus i, P_i^L denotes the power consumption of the load at bus i, δ_i denotes the voltage phase angle at generator bus i, θ_i denotes

the voltage phase angle at non-generator bus $i \in \mathcal{N}\backslash\mathcal{G}$, and b_{ij} denotes the admittance of the transmission line between buses i and j. Note that, if there is no transmission line between buses i and j, then we have $b_{ij} = 0$. We also have $b_{ii} = 0$.

Next, we model the generators. We can write the linear swing equations for the generator at each bus $i \in \mathcal{G}$ as [25]:

$$\dot{\delta}_i = \omega_i, \tag{3}$$

$$m_i\dot{\omega}_i = P_i^M - d_i\omega_i - P_i^G, \tag{4}$$

where ω_i is the rotor angular frequency deviation from nominal angular frequency, m_i is the inertia of the rotor, d_i is the damping coefficient, and P_i^M is the mechanical power input. In practice, there are two controllers that affect the mechanical power input: turbine-governor controller and load-frequency controller [24]. The turbine-governor controller senses the rotor frequency and compares it with the base frequency, e.g. 377 rad/s, to specify the amount of mechanical power that is needed in order to match the injected electrical power at steady state. Then, the load-frequency controller, which has a slower dynamic, seeks to keep frequency at its nominal level, i.e., it tries to push the frequency deviation ω_i back to zero.

Ideally, i.e., if we ignore the delays and internal dynamics of the generator, we can jointly model the above two controllers in form of the following proportional-integral (PI) controller:

$$P_i^M = K_i^P\omega_i + K_i^I\int_0^t \omega_i, \tag{5}$$

where K_i^I and K_i^P are the proportional and integral controller coefficients, respectively. From (3), we can rewrite (5) as

$$P_i^M = K_i^P\omega_i + K_i^I\delta_i. \tag{6}$$

By replacing (1) and (6) in (4), we can rewrite (4) as

$$\begin{aligned} m_i\dot{\omega}_i = &\left(K_i^P - d_i\right)\omega_i + K_i^I\delta_i - \sum_{j\in\mathcal{G}} b_{ij}\left(\delta_i - \delta_j\right) \\ &- \sum_{j\in\mathcal{N}\backslash\mathcal{G}} b_{ij}\left(\delta_i - \theta_j\right). \end{aligned} \tag{7}$$

We are now ready to present the power system dynamics in form of the following state-space descriptor model:

$$\begin{aligned} &\begin{bmatrix} I & 0 & 0 \\ 0 & M & 0 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} \dot{\delta} \\ \dot{\omega} \\ \dot{\theta} \end{bmatrix} = \\ &\begin{bmatrix} 0 & I & 0 \\ K^I - B^{GG} & K^P - D & -B^{GL} \\ B^{LG} & 0 & B^{LL} \end{bmatrix}\begin{bmatrix} \delta \\ \omega \\ \theta \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ P^L \end{bmatrix}, \end{aligned} \tag{8}$$

where δ is the vector of phase angles at all generation buses, ω is the vector of rotor angular frequency deviation at all generation buses, θ is the vector of phase angles at all non-generation buses, and P^L is the vector of power consumptions at all load buses. Also, I is the identity matrix and M and D are diagonal matrices with diagonal entries equal to the inertia and damping coefficients of the generators, respectively. Similarly, K^I and K^P are diagonal matrices with diagonal entries equal to the integral controller coefficients and proportional controller coefficients of the generators at all generation buses, respectively. Finally, we have

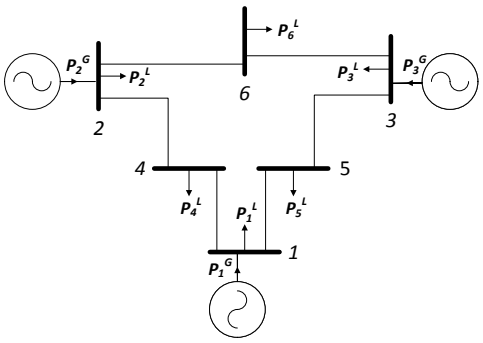

Fig. 1. A power grid with 6 buses, 6 load buses, and 3 generator buses.

$$B = \begin{bmatrix} B^{GG} & B^{GL} \\ B^{LG} & B^{LL} \end{bmatrix}, \tag{9}$$

where B is the imaginary part of the Y-Bus matrix of the power system [24]. For the example six-bus power network in Fig. 1, I, M, D, K^I, and K^P are 3×3 diagonal matrices, Y is a 9×9 matrix, and P^L is a 6×1 vector. Note that, compared to the state-space models that are commonly used in the control theory literature, e.g., in [20]–[22], our model is more complete as it includes also the model for the turbine-governor and load-frequency controllers of generators.

III. Dynamic Load Altering Attacks

Recall from Section II that the inputs to the power system dynamics is the amount of power consumption at each load bus. Traditionally, the power consumption vector P^L is treated as an uncontrollable stochastic process, which depends on the power consumption behavior of the end consumers at different industrial, commercial and residential sectors. However, as we explained in Section I, there have been growing efforts in demand response and demand side management fields to exploit the load flexibility potentials of various consumers so that we can control a portion of the load to make the power system more efficient and reliable. In particular, different automated energy consumption scheduling systems and two-way communications infrastructures are used to change the load in response to changes in grid conditions, c.f. [26], [27].

While the use of advanced demand response and demand side management techniques are promising to improve power grid efficiency, we also face a critical question to answer: *what if an adversary hacks into these automated and IT-enabled energy consumption scheduling devices and price-based and direct load control systems?* The first step towards answering this question was taken in [17], where the authors introduced the concept of *static* load altering attacks. In this section, we aim to understand and model *dynamic* load altering attacks.

A dynamic load altering attack is a LAA over a period of time. Once the load at a load bus $i \in \mathcal{L}$ is hacked, the adversary seeks to control the trajectory of P_i^L over the time period $[0, T]$, where T denotes the ultimate moment that the DLAA causes the *intended damage* to the power grid. In general, we can think of two different types of dynamic load altering

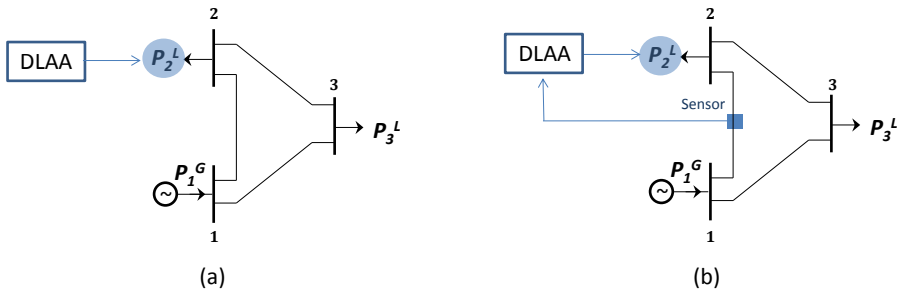

Fig. 2. Two types of dynamic load altering attacks: a) open-loop, b) closed-loop. The closed-loop attack can be designed using feedback control theory.

attacks: *open-loop* and *closed-loop*. An open-loop attack is shown in Fig. 2(a). Here, the attacker does not monitor the grid conditions. Instead, it uses some historical data to impose a pre-programmed trajectory to the victim load. However, in a closed-loop attack, which is shown in Fig. 2(b), the attack constantly monitors the grid conditions through the attacker's installed sensors so that it can adjust the attack trajectory based on the current conditions in the power grid. Clearly, a closed-loop DLAA is a more advanced cyber-physical attack than a blind open-loop DLAA. Therefore, in this paper, our focus is solely on closed-loop dynamic load altering attacks.

An informative quantity that an attacker can monitor is the grid frequency. Note that, in practice, an entire interconnected power grid operates at or around a nominal frequency. For example, the nominal frequency in North America is 60 Hz. As we explained in Section II, it is the responsibility of various generators to control their operation so that they can maintain frequency at such nominal level at all times and in response to fluctuations in load. Accordingly, in this paper, we assume that the closed-loop dynamic load altering attack works by taking the grid frequency as its feedback quantity. In general, the DLAA frequency sensor can be either co-located with the victim load, or placed anywhere else on the same interconnected network, e.g., at a particular generation bus. Note that, measuring frequency is generally an easy task as it can be done at any power outlet using inexpensive commercial sensors. In fact, it is already done in *frequency responsive* loads that control usage to assist frequency regulation [28].

Without loss of generality, we assume that the dynamic load altering attack is implemented in form of a simple proportional controller. If the load at bus $v \in \mathcal{L}$ is the victim load, then we model the *compromised* power consumption level at bus v as

$$\bar{P}_v^L = P_v^L + \epsilon_v^L - K_{vs}^L \omega_s, \tag{10}$$

where K_{vs}^L is the proportional gain for the attack controller, ω_s is the deviation in the angular frequency from its nominal value at sensor bus s, and ϵ_v^L is a small power consumption level that we may need to create at the victim bus in order create a slight deviation in the frequency from its nominal value before we can apply the attack. Note that, in practice, there is likely no need to include ϵ_v^L in the attack model. This is because the natural fluctuations on the demand side always creates the slight frequency deviations $\omega_s \neq 0$ that is needed for the proportional controller term $K_{vs}^L \omega_s$ to work. Furthermore, we note that $K_{vs}^L \geq 0$ in order to exacerbate frequency deviation.

Once we plug-in (10) into the state-space model in (8), the *system dynamics under attack* are modeled as

$$\begin{bmatrix} I & 0 & 0 \\ 0 & M & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\omega} \\ \dot{\theta} \end{bmatrix} = \begin{bmatrix} 0 & I & 0 \\ K^I - B^{GG} & K^P - D & -B^{GL} \\ B^{LG} & -K^L & B^{LL} \end{bmatrix} \begin{bmatrix} \delta \\ \omega \\ \theta \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ P^L + \epsilon^L \end{bmatrix}, \tag{11}$$

where ϵ^L has the same size as P^L, with all entries equal to zero, except for its entry for bus v which is ϵ_v^L. Note that, besides the appearance of ϵ^L in the input vector, the more important difference between (11) and (8) is the appearance of the attack control parameter K^L inside the state matrix. Here, K^L is the matrix of all attack controller gains.

From (11), the attacker is capable of changing the poles of the system by changing the entries of matrix K^L. In particular, the attacker might be able to make the system *unstable*. That is, it can fight back the turbine-governor and load-frequency controllers of the generators and push the frequency at bus s or other buses away from the nominal frequency.

Since the generators are designed for operation at nominal frequency, they are equipped with protection systems and circuit breakers to disconnect the generator from the grid, if the frequency deviation goes beyond a certain threshold $\omega_i^{\max}$. As a result, a DLAA attack may set its ultimate goal to push a particular generator offline and disconnected from the grid, putting the system at risk of equipment damage or blackout. Next, we analyze such scenario in details in a case study.

IV. Case Study

A. System Setup

Consider the network in Fig. 1 with the following parameters in per unit: $m_1 = 0.125$, $m_2 = 0.034$, $m_3 = 0.016$, $d_1 = 0.125$, $d_2 = 0.068$, $d_3 = 0.032$, $K_1^P = -2$, $K_2^P = -9$, $K_3^P = -3$, $K_1^I = -35$, $K_2^I = -40$, $K_3^I = -35$, $b_{11} = -17.4$, $b_{14} = 17.4$, $b_{22} = -16$, $b_{25} = 16$, $b_{33} = -17.1$, $b_{36} = 17.1$, $b_{41} = 17.4$, $b_{44} = -24.3$, $b_{47} = 3.5$, $b_{48} = 3.4$, $b_{52} = 16$, $b_{55} = -46.3$, $b_{57} = 16.4$, $b_{59} = 13.9$, $b_{63} = 17.1$, $b_{66} = -53.8$, $b_{68} = 16.7$, $b_{69} = 20$, $b_{74} = 3.5$, $b_{75} = 16.4$, $b_{77} = -19.9$, $b_{84} = 3.4$, $b_{86} = 16.7$, $b_{88} = -20.1$, $b_{95} = 13.9$,

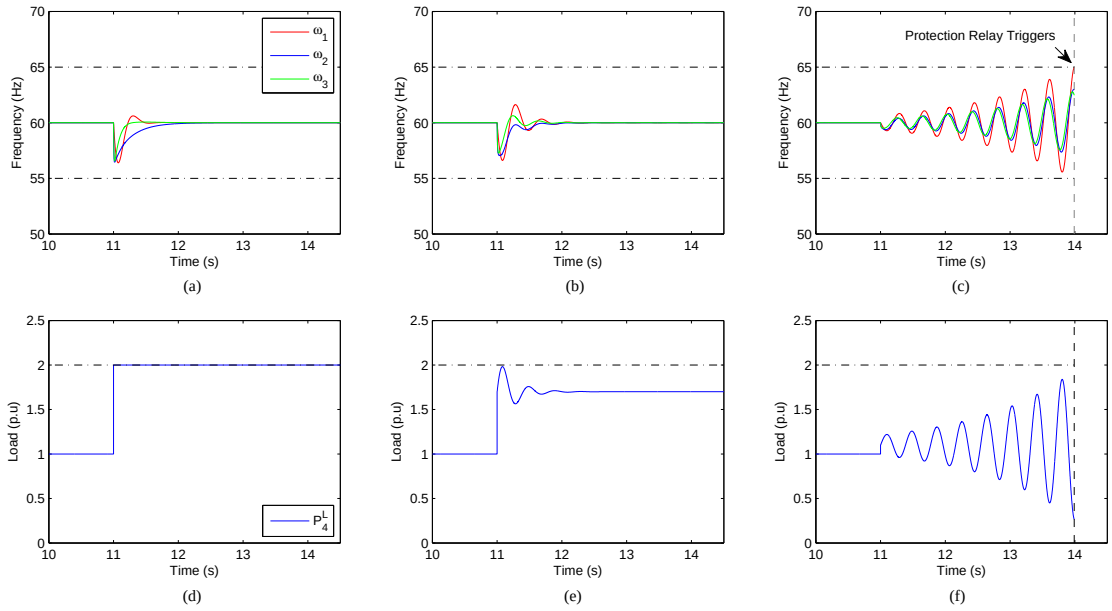

Fig. 3. Simulation results under various attack conditions. The figures in the first row show the system frequencies over time. The figures in the second row show the victim load changes. The figures in the first column are for the case when the attack causes an abrupt increase in the load. The figures in the second column are for the case when the attack is dynamic with gain 5. The figures in the third column are for the case when the attack is dynamic with gain 10.

$b_{96} = 20$, $b_{99} = -33.9$. All other entries of matrix B are zero. For all load buses $i = 1, \ldots, 6$, we have $P_i^L = 1$ p.u. The poles of this dynamic system are obtained as

$$-262.8, -180.2, -10.3, -8.5 \pm 13.3i, -3.8. \qquad (12)$$

We can see that all system poles are stable. That is, if there is no DLAA, then the power system operates properly.

B. Attack examples and Their Impacts

In this section, we examine three attack scenarios. The results are shown in Fig. 3. Here, the victim load is located at bus $v = 4$. The frequency sensor is assumed to be placed at bus $s = 1$. First, assume that the attack causes an abrupt change in the victim load, as in Fig. 3(d). The poles of the system remain as in (12). We can see in Fig. 3(a) that the system can easily absorb such one-time abrupt change. Second, assume that the attack follows the structure in (5) with $K_{41}^L = 5$ and $\epsilon_4^L = 0.7$. The poles of the system move to -262.9, -180.3, -10.0, $-4.0 \pm 15.6i$, and -3.7. The attack causes an overshoot at P_4^L at 2 per unit and some relatively major over- and under-shoots in frequency deviations. Nevertheless, the system can still push the frequency back to zero to continue with normal operation. Finally, assume that the attack follows the structure in (5) with $K_{41}^L = 10$ and $\epsilon_4^L = 0.1$. The new poles of the system are -262.9, -180.3, -10.0, -3.7, and $0.8 \pm 16.3i$. In this case, the system becomes *unstable* due to the poles at 0.8 ± 16.3. The attack forces the frequency deviation of the first generator to reach the frequency deviation threshold $\omega_1^{\max} = 5$ Hz $= 0.083$ per unit, causing the generator's circuit breaker to trigger at around time $t = 14$. Note that, at this point, the generator at bus 1 goes offline, concluding the attack. Interestingly, the DLAA attack under this last scenario did not even need to increase the volume of the victim load to its feasible maximum $P_4^{L,\max} = 2$ p.u. All it did was following the right trajectory in response to changes in system frequency.

C. Minimum Required Attack Controller Gain

From the results in Section IV-B, we can see that the choice of the attack controller gain K_{41}^L has direct impact both on the poles of the system and also on the outcome of the attack. To gain insights, we plot the root-locus curve [29] for the system poles under attack in Fig. 4. We can see that, as we increase the gain the two complex poles move towards the imaginary axis. The system becomes unstable once the gain reaches 9.3. Of course, higher values of K_{41}^L can also cause instability and push the frequency deviation towards its limits even faster, but at the cost of making more significant changes in the victim load, i.e., at the cost of requiring more loads to be hacked.

D. Impact of Attack Location

Finally, it is interesting to also assess the impact of attack location. The results for different choices of victim load bus v and frequency sensor bus s are shown in Table I. Here, we have calculated the minimum attack controller gain K_{vs}^L that can make the system unstable, based on a root-locus analysis. We can see that both the location of the victim load and the location of the frequency sensor have impact on the choice of the attack controller gain. Recall from Section IV-C that a lower gain means requiring less loads to be hacked for the attack to work. In this regard, we can conclude that if we aim to push generator 1 off-line, then it is best if we hack the controllable loads at bus $v = 1$. However, if this is not feasible, e.g., due to the type and security level of the loads at

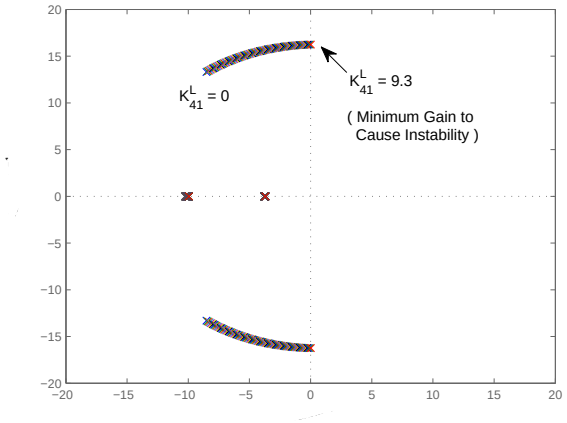

Fig. 4. The root-locus diagram to show the relocation of the closed-loop system poles when we change the attack controller gain K^L_{41}.

TABLE I
MINIMUM REQUIRED ATTACK CONTROLLER GAIN

		Victim Load Bus		
		$s = 1$	$s = 2$	$s = 3$
Frequency Sensor Bus	$v = 1$	2.8	79.0	26.1
	$v = 4$	9.3	16.0	15.2
	$v = 6$	20.0	23.1	6.2

bus 1, then we can still implement a successful dynamic load altering attack by hacking more loads in other buses.

V. CONCLUSIONS

In this paper, we introduced and formulated dynamic load altering attacks as a new class of cyber-physical attacks against smart grid. To the best of our knowledge, no prior study has addressed DLAAs. First, we presented two types of dynamic load altering attacks as open-loop and closed-loop attacks. Then, we designed a closed-loop dynamic load altering attack that aims to make the power system unstable. The feedback loop was based on measuring power system frequency. We demonstrated the proposed closed-loop DLAA against power system stability in a six bus case study and showed some basic properties of the attack, such as method to choose the attack controller gain and the impact of the attack location.

The analysis and results in this paper can be extended in various directions. First, while the attack controller design in this paper was based on a proportional control concept, more advanced controller design options can be taken into consideration. Second, the analysis can be extended to identify the most critical attack location based on the topology and dynamics of the power grid. Third, it is interesting to examine attacks that involve multiple victim loads and also look at larger networks with more complex dynamics and topologies.

REFERENCES

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power & Energy Magazine*, vol. 7, no. 2, pp. 52–62, Mar. 2009.

[2] 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.

[3] 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.

[4] 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.

[5] J. Medina, N. Muller, and I. Roytelman, "Demand response and distribution grid operations: Opportunities and challenges," *IEEE Trans. on Smart Grid*, vol. 1, no. 2, pp. 193–198, 2010.

[6] G. Strbac, "Demand side management: Benefits and challenges," *Energy Policy*, vol. 36, no. 12, pp. 4419–4426, Dec. 2008.

[7] 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.

[8] M. Mallette and G. Venkataramanan, "The role of plug-in hybrid electric vehicles in demand response and beyond," in *Proc of the IEEE PES Transmission and Distribution Conference and Exposition*, New Orleans, LA, Apr. 2010.

[9] C. Wu, H. Mohsenian-Rad, and J. Huang, "Vehicle-to-Aggregator Interaction Game," *IEEE Trans. on Smart Grid*, vol. 4, no. 1, pp. 434–442, Mar. 2012.

[10] A. Gholian, H. Mohsenian-Rad, Y. Hua, and J. Qin, "Optimal industrial load control in smart grid: A case study for oil refineries," in *Proc. of IEEE PES General Meeting*, Vancouver, Canada, Jul. 2013.

[11] P. Yang, G. Tang, and A. Nehorai, "A game-theoretic approach for optimal time-of-use electricity pricing," *IEEE Trans. on Power Systems*, vol. 28, no. 2, pp. 884–892, May 2013.

[12] J. L. Mathieu, P. N. Price, S. Kiliccote, and M. A. Piette, "Quantifying changes in building electricity use, with application to demand response," *IEEE Trans. on Smart Grid*, vol. 2, no. 3, pp. 507–518, 2011.

[13] C. Ninagawa, S. Kondo, S. Isozumi, and H. Yoshida, "Fine-time-granularity fast demand control of building HVAC facilities for future smart grid," in *Proc. of IEEE PES ISGT*, Beril, Germany, Oct. 2012.

[14] 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.

[15] 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.

[16] C. Adika and L. Wang, "Autonomous appliance scheduling for household energy management," *IEEE Trans. on Smart Grid*, vol. 5, 2014.

[17] 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.

[18] 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.

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

[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] H. Fawzi, P. Tabuada, and S. Diggav, "Security for control systems under sensor and actuator attacks," in *Proc. of IEEE Conference on Decision and Control*, Maui, HI, Dec. 2012.

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

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

[26] 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.

[27] J. A. Short, D. G. Infield, and L. L. Freris, "Stabilization of grid frequency through dynamic demand control," *IEEE Trans. on Power Systems*, vol. 22, no. 3, pp. 1284–1293, Aug. 2007.

[28] 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.

[29] R. C. Dorf, *Modern control systems*. Addison-Wesley Longman Publishing Co., Inc., 1995.