Detecting Dynamic Load Altering Attacks: A Data-Driven Time-Frequency Analysis

Sajjad Amini[†], Fabio Pasqualetti[‡], and Hamed Mohsenian-Rad[†]
[†]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*—In this paper, we focus on the problem of detecting Dynamic Load Altering Attacks (D-LAAs) in power systems from raw data of smart meters and without knowledge of the power system dynamics. The detection of D-LAA solely based on the smart meter readings is addressed in the frequency domain. We show that a D-LAA is detectable through a frequency domain analysis, and that the attack signature corresponds to the system poles that are relocated by the D-LAA feedback. We provide conditions on the time resolution of the smart meters to ensure attack detection, and we highlight the potential for interference from instrumentation and communication devices. For the case when smart meter readings and frequency measurements are both available, we show that a cross-correlation analysis allows to detect D-LAA, and to distinguish between D-LAAs and the effect of benign frequency responsive loads. We conclude that depending on the attack implementation and the type of data available, both time-domain and frequency-domain detection analysis may be needed to ensure accurate attack detection.**

I. Introduction

Load Altering Attacks (LAAs) constitute an important class of cyber-physical attacks against Demand Response (DR) and Demand Side Management (DSM) programs [1]–[4]. LAAs attempt to control and change a group of unsecured controllable loads to damage the grid through circuit overflow or other mechanisms. There are different load types that could be vulnerable to LAAs, e.g., remotely controllable loads [5], loads that automatically respond to price or direct load control command signals [6]–[8], and frequency-responsive loads [9].

So far, the focus in the LAA literature has been mainly on *Static* Load Altering Attacks (S-LAAs), where the attacker is concerned with changing the volume of certain vulnerable loads, possibly in an *abrupt* fashion. However, if loads can be controlled dynamically, then *Dynamic* Load Altering Attacks (D-LAAs) are also possible [10], [11]. D-LAAs have the ability to render the power system unstable by controlling certain loads in a malicious way. In particular, D-LAAs are concerned with not only the amount of change in the compromised load, but also the *trajectory over time* of the load signal.

Unlike in the analysis of S-LAAs, where the focus is on the steady-state behavior of power systems, the analysis of D-LAAs is concerned with the dynamics and transient behavior of power systems. D-LAAs are classified in terms of open-loop versus closed-loop attacks, single-point versus coordinated multi-point attacks, the type of feedback signal, and the type of attack strategy [11]. For example, in a closed-loop D-LAA with grid frequency as feedback signal, the compromised load may react to a frequency lag in the *opposite* way of frequency-responsive loads under demand response problems, c.f. [12], [13], in order to maximize system frequency fluctuations.

The problem of *detecting* attacks in cyber-physical systems is a well-studied problem; see [14] and the references therein. While most approaches use model-based techniques, in this paper we focus on the problem of detecting D-LAAs in power systems from raw data of *smart meters* and without knowledge of the power system dynamics. Smart meters are advanced measuring equipment that are used to measure electrical energy consumption at much higher time-resolutions than conventional meters [15]. They are also capable of two-way communications with utility companies. Currently, there are over 45 million smart meters installed in the U.S. that generate more than one billion data points every day [16].

The contributions of this paper are summarized as follows:

- *Data-driven attack detection problems*: This paper introduces the problem of detecting D-LAAs from measurement data only, and without knowledge of the power system dynamics. The data-driven D-LAA detection problem is addressed for smart meters readings only, and for smart meter readings together with frequency measurements. To the best of our knowledge, no prior work has discussed either of these attack detection problems.
- *Frequency domain analysis of D-LAA*: The detection of D-LAA with smart meter readings only is addressed in the frequency domain. We show that a D-LAA is detectable through a frequency domain analysis, and that the attack signature corresponds to the system poles that are relocated by the D-LAA feedback. We provide conditions on the time resolution of the smart meters to ensure attack detection, and we highlight the potential interference from instrumentation and communication devices.
- *Time domain analysis of D-LAA*: For the case when smart meter readings and frequency measurements are both available, we show that a cross-correlation analysis allows to detect D-LAA, and to distinguish between D-LAAs and the effect of benign frequency responsive loads.

Our results in this paper show that it is indeed possible to detect D-LAAs via purely data-driven approaches. Moreover, depending on the attack implementation and the type of data available, both time-domain and frequency-domain detection analysis may be needed to ensure accurate attack detection.

This work was supported by NSF grants ECCS 1253516, ECCS 1462530, and ECCS 1405330. The corresponding author is H. Mohsenian-Rad.

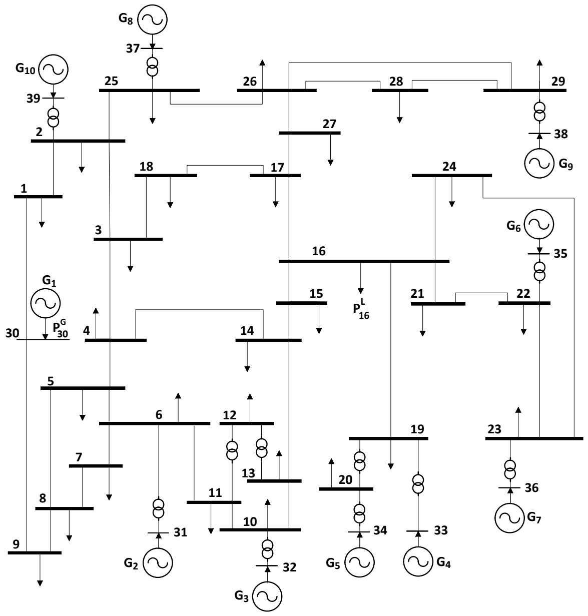


Fig. 1. The IEEE 39 bus test system based on the 10-machine New-England power network, where $\mathcal{L} = \{1, \ldots, 29\}$ and $\mathcal{G} = \{30, \ldots, 39\}$.

II. Background

A. Dynamic Load Altering Attack in Power Systems

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 buses and load buses, respectively. An example is shown in Fig. 1. By combining the power flow equations with the swing equations at generator buses, turbine-governor and load frequency controller equations of generators, and the D-LAA proportional controller equations, a linear state-space descriptor model of the power system under D-LAA can be obtained as [10], [11]:

$$\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & -M & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \dot{\delta} \\ \dot{\theta} \\ \dot{\omega} \\ \dot{\varphi} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ I \end{bmatrix} P^L + \begin{bmatrix} 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \\ K^I + H^{GG} & H^{GL} & K^P + D^G & 0 \\ H^{LG} & H^{LL} & -K^{LG} & -K^{LL} - D^L \end{bmatrix} \begin{bmatrix} \delta \\ \theta \\ \omega \\ \varphi \end{bmatrix}, \tag{1}$$

where δ is the vector of phase angles at all generator buses, ω is the vector of rotor angular frequency deviations at all generator buses, θ is the vector of phase angles at all load buses, and φ is the vector of frequency deviations at all load buses, I is the identity matrix, H^{GG}, H^{GL}, H^{LG}, and H^{LL} are the sub-matrices of the imaginary part of power system admittance matrix, 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. Finally, K^{LG} and K^{LL} are the attack controller gain matrices, and P^L is the vector of power consumption at all load buses.

Consider a single-point closed-loop D-LAA that uses frequency measurements at the sensor bus $s \in \mathcal{N}$ and accordingly alters the load P^L at the victim bus $v \in \mathcal{L}$. From [11], if $s \in \mathcal{G}$, then the compromised load is modeled as

TABLE I
Power consumption at load buses in per unit.

Bus	P^L	Bus	P^L	Bus	P^L	Bus	P^L	Bus	P^L
1	4	**7**	6.3	**13**	4	**19**	B	**25**	6.2
2	4	**8**	9.2	**14**	4	**20**	10.3	**26**	5.4
3	7.2	**9**	4	**15**	7.2	**21**	6.7	**27**	6.8
4	9	**10**	4	**16**	A	**22**	4	**28**	6.1
5	4	**11**	4	**17**	4	**23**	C	**29**	10.8
6	5	**12**	4	**18**	5.6	**24**	7	**-**	-

$$P^L_v = -K^{LG}_{vs}\,\omega_s. \tag{2}$$

Otherwise, if $s \in \mathcal{L}$, then the compromised load reads as

$$P^L_v = -K^{LL}_{vs}\,\varphi_s. \tag{3}$$

Note that, $K^{LG}_{vs} \geq 0$ and $K^{LL}_{vs} \geq 0$ are the attack controller's gains. See [10], [11] for more details about D-LAAs.

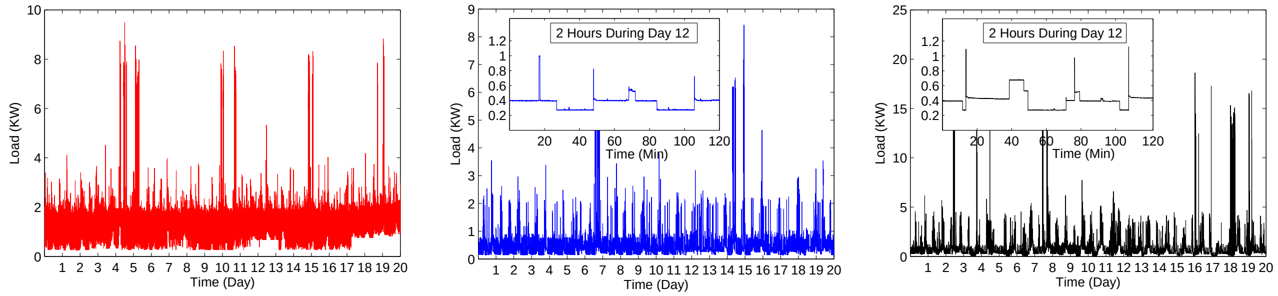
From a system-theoretic perspective, the attack gain matrices K^{LG} and K^{LL} modify the *poles* of system (1). In fact, if the attack matrices are selected properly, then the attack can force the system poles to the right half-plane, rendering the power system *unstable*. Loosely speaking, a D-LAA can fight back the turbine-governor and load-frequency controllers of the generators and push the frequency of certain buses away from their nominal values. If the frequency deviation goes beyond a certain threshold, protection relays will be activated.

B. Smart Meter Data and a Case Study

The focus in this paper is on data-driven D-LAA detection. In this regard, we use the experimental data in [17], which includes the smart meter data of three different homes (A, B, and C) in Western Massachusetts; see Fig. 2. The time-resolution for all smart meters is *one second*. All three homes have typical household appliances such as refrigerator, washing machine, etc. Home A is further instrumented with appliance-level submeters that monitor the loads for all appliances separately. For example, about 30 of 35 wall switches have been replaced with units that transmit on-off-dim events for the switches to a gateway server at about every 2.5 seconds (on average) by using Power Line Communication (PLC) data transmissions.

To utilize the above smart meter data in a study on D-LAA detection, we integrated the three available smart meter data sets into the 39-bus IEEE test system in Fig. 1. The parameters of the transmission lines and the inertia and damping coefficients of generators are as in [18]. The generator controller parameters are chosen as $K^P_1 = 100$, $K^P_2 = K^P_3 = 45$, $K^P_4 = 10$, $K^P_5 = K^P_{10} = 50$, $K^P_6 = K^P_9 = 40$, $K^P_7 = 30$, $K^P_8 = 20$, and $K^I_1 = \ldots = K^I_{10} = 60$. The damping coefficient for each fixed dynamic load is 10. Note that, the generator controller parameters are set so as to keep the system stable during normal operations and in the absence of attacks. Throughout this paper, the simulations are done in MATLAB.

The system is initiated to run with constant amount of P^L for all load buses as in Table I, for the load buses 16, 19, and 23, the load changes according to the smart meter data in Fig.

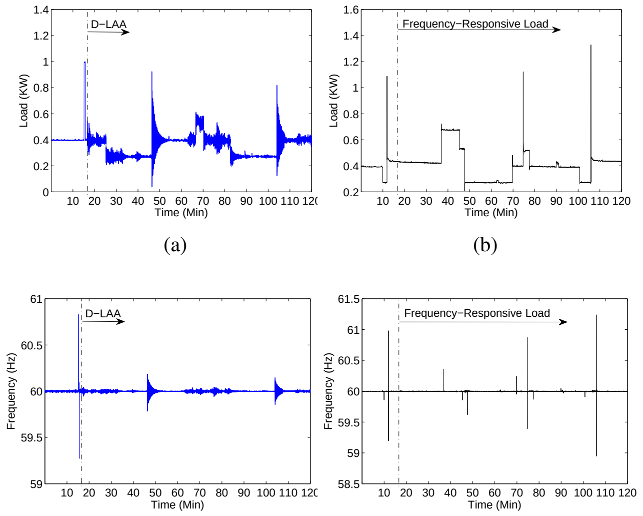


(a)

(b)

(c)

Fig. 2. Smart meter data at second-by-second resolution over 20 days from May 1, 2012 to May 20, 2012: a) Home A, b) Home B, c) Home C.



(a)

(b)

(c)

(d)

Fig. 3. The measurements corresponding to the case study in Section II-B: a) load signal for a home at bus 19, b) load signal for a home at bus 23, c) frequency signal a home at bus 19, d) frequency signal for a home at bus 23.

2. Specifically, we assume that there are 10,000 homes at bus 16 whose load profile equals that of Home A, 30,000 homes at bus 19 whose load profile equals that of Home B, and 20,000 homes at bus 23 whose load profile equals that of Home C. A single-point closed-loop D-LAA with $K_{vs}^{LL} = 43$ is attempted at bus 19 which is both victim and sensor bus. There is also a frequency-responsive load with gain -2 at bus 23. Fig. 3 shows load and frequency at buses 19 and 23 for two hours on day 12. The D-LAA at bus 19 and the frequency-responsive load at bus 23 are activated at $t = 16.6$ min.

III. Detection Solely Based on Load Signal

In this section we characterize the possibility of detecting D-LAAs through the knowledge of the load data only.

A. Frequency Domain Analysis

Consider the typical smart meter data in Fig. 2. Notice that the load signal has major fluctuations during the day. Suppose that a portion of the load at a victim bus is compromised, e.g., in form of the load in Fig. 3(a). If the volume of the compromised load is high, then it can be detected by looking at the smart meter data in time domain, because the frequency-responsive behavior of the compromised load under D-LAA in this case significantly changes the shape of the total metered load. Such detection can be done automatically, e.g., by using appropriate pattern recognition algorithms, c.f. [19]. However, if the volume of the compromised load under D-LAA is low, then the attack may be difficult to detect through time-domain analysis, and a frequency-domain analysis may be preferable.

We first compute the Fast Fourier Transform (FFT), c.f., [20], of the original load signals of Fig. 2, i.e., the second-by-second load profile in the absence of D-LAAs. Fig. 4 shows the frequency spectrum of the load signals. Here, the DC portion of the signal has been omitted before applying the FFT algorithm. We can see that, except for some noticeable non-zero coefficients around 0.47 Hz for the case of Home A, the FFT coefficients are negligible at frequencies above 0.05 Hz. Note that, for the non-zero coefficients around 0.47 Hz, they do not represent any residential load. Instead, they are created due to extensive instrumentation of Home A and the fact that about 30 wall switches make PLC-based transmissions of the submeter data to a gateway once roughly every 2.5 seconds, see Section II-B and Remark 3. From the results in Fig. 2, the FFT of a typical load signal of a residential customer has non-zero coefficients only at very low frequencies.

***Remark** 1:* The spectrum analysis of the smart meter data in this paper is very different from the well-studied analysis of *harmonics* for nonlinear loads in power systems and power electronics, c.f., [21], [22]. Let $p(t)$ denote the instantaneous power draw for a load. Note that, $p(t)$ is a continuous-time signal. In order to analyze the harmonics for nonlinear loads, one would take the following continuous Fourier transform:

$$\mathcal{F}_C\left\{p(t)\right\}. \tag{4}$$

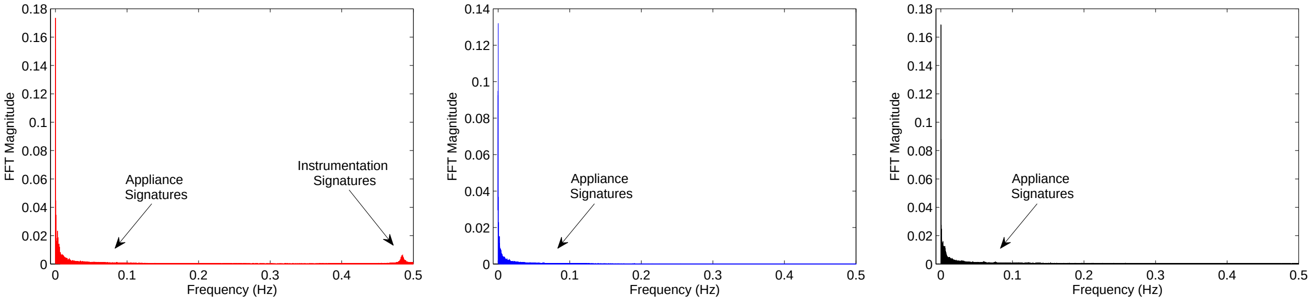
Now, consider a smart meter that reports the average power usage every T seconds. The k^{th} meter reading is calculated as

$$\bar{p}[k] = \frac{1}{T}\int_{t=(k-1)T}^{kT} p(t)dt. \tag{5}$$

In this paper, for the purpose of dynamic load altering attack detection, we take the following discrete Fourier transform:

$$\mathcal{F}_D\left\{\bar{p}[k]\right\}. \tag{6}$$

Thus, our spectral analysis is focused on much lower frequencies than in a typical harmonics analysis of nonlinear loads.



(a) (b) (c)

Fig. 4. The spectral analysis of the residential load signals in Fig. 2 over the entire 20 days period using (5) and (6): a) Home A, b) Home B, c) Home C.

Next, consider the two-hour zoomed-in time frame in Fig. 2(b). The frequency spectrum for the load signal of each home at bus 19 without and with attack is shown in Figs. 5(a) and (b), respectively. We see that the presence of D-LAA has created a *new signature* to the frequency spectrum at about 0.26 Hz; see Remark 2. This new signature is away from the load signatures. Hence, it can be used to detect the attack; see Section III-B. The magnitude of attack signature depends on factors such as amount and location of the compromised load.

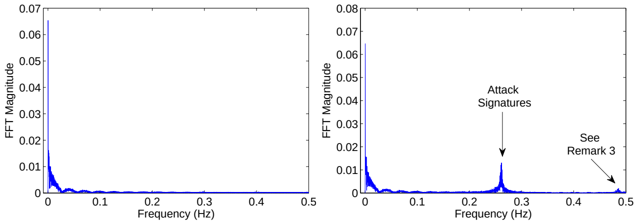
***Remark** 2:* The D-LAA has moved a pair of system poles from $-0.55 \pm 2.01i$ to $-0.0095 \pm 1.64i$. Since the *real* part of these poles has increased, the poles are now much closer to the imaginary axis, making the system (almost) only marginally stable. The new poles induce slowly decaying oscillations with larger magnitudes compared to other oscillations in the system, creating a noticeable attack signature in frequency domain. As for the *imaginary* part of relocated poles, it highly affects the frequency at which we should see the attack frequency signature. Specifically, the attack signature in Fig. 5(b) has appeared at the *natural frequency* of the relocated poles [23]:

$$\omega_n = \sqrt{-0.0095^2 + 1.64^2} = 1.64. \tag{7}$$

Note that, $f_n = \omega_n/(2\pi) = 0.26\,\text{Hz}$, which equals the central frequency of the attack signature in Fig. 5(b).

The above remark may also give some basic hints on how an attacker may conduct an optimal pole placement - subject to the available load vulnerabilities - in order to maximize the attack impact on the power grid while minimizing the chance of being detected through frequency-domain analysis.

***Remark** 3:* Besides the main attack signature at 0.26 Hz, the attack has also created a small signature at 0.47 Hz in Fig. 5(b). Interestingly, this signature is *indirectly* related to the instrumentation signature that we previously identified for the load at bus 16. Note that, since the grid is an *interconnected* system, the dynamics of loads/genertors at any bus may have impact on the frequency at another bus. Accordingly, since the instrumentation signature at 0.47 Hz at bus 19 has some impact on the frequency fluctuations at bus 19, and also because the compromised loads at bus 19 respond to the frequency fluctuations at bus 19, the instrumentation signature at bus 16 has now appeared, although with attenuations, at bus 19. This suggests that the communications activities of instrumentation devices can potentially *interfere* with attack detection. However, such interference is likely negligible in practice, as we do not expect instrumentation with high power usage compared to the actual load of a home in practice.



(a) (b)

Fig. 5. Spectral analysis of the original and compromised load signals of each home at bus 19 over a two-hour period: a) original, b) compromised.

One may ask: *is it possible to see the attack signature if the meter data is minute-by-minute instead of second-by-second?* The answer is 'no', as it is explained in the next remark.

***Remark** 4:* Based on the Nyquist-Shannon sampling theorem [24], the sampling frequency must be twice the highest frequency of the signal in order to avoid aliasing in the signal spectrum. Of course, the integral nature of energy metering operation in (5) is different from standard sampling. Nevertheless, the above theorem may still provide a good practical approximation for the minimum required time resolution of smart meters. Loosely speaking, for the attack signature to be observable in a frequency-domain analysis, it is required that

$$T \leq \frac{1}{2f_n} = \frac{\pi}{\omega_n}, \tag{8}$$

where T is the smart meter pulse interval; see (5). For example, to detect the attack signature in Fig. 5(b), the reading interval of the smart meter needs to be roughly two seconds or less.

B. Real-time Detection in Frequency Domain

In the previous section, we studied the detectability of D-LAA via spectral analysis. In order to detect an attack in a prompt and efficient manner, in this section we employ the Windowed FFT (W-FFT) method [22]. The performance of W-FFT is affected by the choices of three parameters: *window size*, *sampling rate*, and *detection threshold*. The window size indicates the length of time series signal in each FFT window. The sampling rate indicates the time between two consecutive

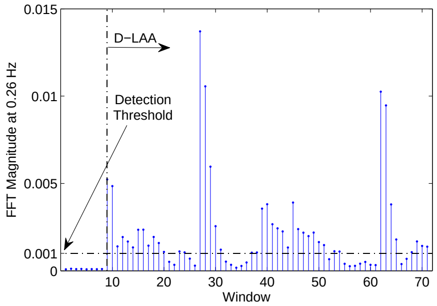


Fig. 6. The W-FFT coefficient of a compromised load at attack frequency 0.26 Hz versus the W-FFT sliding windows for each home at bus 19.

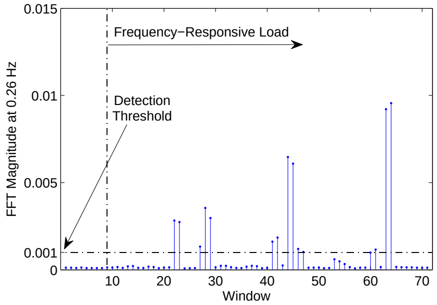


Fig. 7.The W-FFT coefficient of a frequency-responsive load at attack frequency 0.26 Hz versus the W-FFT sliding windows for each home at bus 23.

FFT window samples. The detection threshold indicates the smallest magnitude for the FFT or W-FFT coefficients around the natural frequency of a relocated system pole that triggers the detection of an attack frequency signature.

Suppose we set the sampling rate to 100 sec, window size to 200 sec, and detection threshold to 0.001. To assess the efficiency of W-FFT in detecting D-LAAs, we calculate the W-FFT coefficient at attack frequency 0.26 Hz for each sliding window. The results are shown in Fig. 6. We can see that the W-FFT coefficient at attack frequency 0.26 Hz exceeds the detection threshold right after the attack is launched. This allows an immediate detection of the attack. However, there are also certain windows, e.g., windows number 21 and 22, where the W-FFT coefficient is below the detection threshold.

Finally, we must also point out a key limitation of detecting D-LAA solely based on load signals. Consider the W-FFT coefficients for a benign frequency-responsive load of a home at bus 23 in Fig. 7. We can see that there are still quite a few W-FFT coefficients that exceed the detection threshold, even though a frequency-responsive load is helping the grid.

***Remark** 5:* The frequency-domain analysis in this section is effective in detecting *load activities* around the natural frequencies of the system poles. However, it cannot distinguish between a compromised load (with adverse activity) and a frequency-responsive load (with benign activity), because such distinction is not possible by solely looking at the load signal and without considering frequency measurements.

IV. Detection Based on Both Load and Frequency Signals

In this section, we examine the possibility of detecting D-LAAs when there is access to both load and frequency signals. We show that the additional information that is provided by the frequency signal can particularly help in distinguishing between a D-LAA and a frequency-responsive load.

The analysis in this section is in time-domain; and Cross-Correlation (CC) is the main mathematical tool [25]. Since we are interested in detecting D-LAAs in real-time, we use the Windowed Cross-Correlation (W-CC) method. Analogously to Section III-B, three parameters of sampling rate, window size, and detection threshold can affect the analysis performance.

Suppose we set the sampling rate to 100 sec, window size to 200 sec, and detection threshold to 0.05. The results for the W-CC analysis of the load and frequency signals are shown in Figs. 8 and 9. For each W-CC sliding window, only the zero-lag cross-correlation coefficient is shown. Unlike in Figs. 6 and 7, where compromised loads and frequency-responsive loads create similar coefficients, here, one can easily distinguish D-LAAs from frequency-responsive loads. Specifically, the zero-lag coefficients are *negative* for a compromised load under D-LAA and *positive* for a frequency-response load.

Recall from Remark 4 that the frequency-domain analysis in Section III-A requires the reading interval of the smart meter to be two seconds or less. Next, we examine the impact of smart meter time-resolution on detecting the correlations between the load and frequency signals. The results are shown in Fig. 10 for the zero-lag W-CC coefficient between a compromised load signal and the frequency signal of a home at bus 19. We can see that the magnitude of the correlation coefficients attenuate quickly as we lower the smart meter time-resolution.

***Remark** 6:* It appears that the need for high resolution smart meters does not depend on the method of detection, whether it is in time or frequency domain. This is an important observation because in practice most smart meters do not support high resolution readings. In fact, the need for such frequent meter readings has not been raised yet. In this regard, the problem of detecting D-LAAs in this paper appears to be one of the first smart meter data applications that can justify second-by-second or higher time-resolutions for smart meters.

***Remark** 7:* For the analysis in this section, it was implicitly assumed that the D-LAA sensor bus is the same as the D-LAA victim bus, i.e., $v = s$. In other words, the feedback on system frequency is measured at the same bus that the potential compromised load is located. However, in general, the sensor bus and the victim bus may not be the same in a D-LAA, see [10], [11]. Accordingly, if the location of the sensor bus is *unknown*, selecting the right frequency signal to be used as the base for cross-correlation analysis could be challenging. Another challenge in this case is to select the detection threshold for the CC and W-CC algorithms for each specific sensor bus location, even if such location is known.

The challenges highlighted in Remark 7 suggest that, even if the frequency signals are available, one may not rely only on a time-domain cross-correlation analysis. Instead, it is more desirable if a frequency-domain analysis of the load signal is combined with a time-domain analysis of the load and frequency signals. In fact, in addition to the concerns in Remark 7, since the performance of both the frequency-domain and time-domain detection methods are highly sensi-

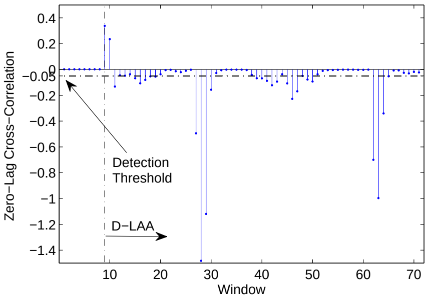


Fig. 8. The zero-lag W-CC coefficient between the compromised load and frequency signals versus the W-CC sliding windows of a home at bus 19.

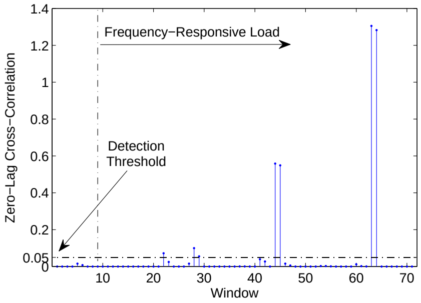


Fig. 9. The zero-lag W-CC coefficient between the frequency-responsive load and frequency signals versus the W-CC sliding windows of a home at bus 23.

tive to the choice of various parameters such as the detection threshold, a proper combination of the two methods might help in obtaining a more accurate and robust detection method.

V. Conclusions

This paper, for the first time, addresses the problem of detecting D-LAAs in power systems from raw data of smart meters and without knowledge of the power system dynamics. Two scenarios are addressed: detecting D-LAAs solely based on load signal using a frequency domain analysis and detecting D-LAAs based on both load and frequency signals using a time domain analysis. Several detailed remarks are made in each case to gain analytical and practical insights. It is shown that depending on the type of attack and available data, both time-domain and frequency-domain detection analysis could be needed in order to ensure accurate attack detection.

This paper can be extended in several directions. First, the sampling rates, window sizes, and detection thresholds can be selected in an optimal or adaptive fashion. Second, the analysis can be extended to detect coordinated multi-point D-LAAs, c.f. [11]. Experimental load signals from other load sectors, such as commercial and industrial, or at other aggregation levels, such as feeder and substation, may also be analyzed.

References

[1] 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.

[2] 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.

[3] 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.

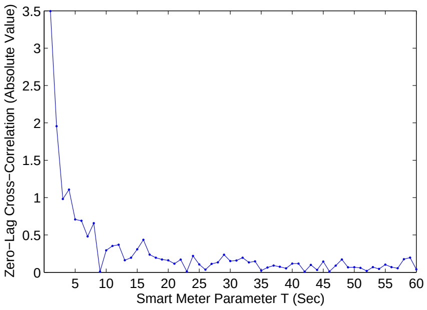


Fig. 10. The zero-lag CC coefficient between the compromised load and frequency signals versus smart meter time-resolution for a home at bus 19.

[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] S. Kiliccote, S. Lanzisera, A. L. O. Schetrit, and M. Piette, “Fast DR: Controlling small loads over the internet,” *Proc. of the ACEEE Summer Study on Energy Efficiency in Buildings*, Aug. 2014.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, “Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Designs,” *Submitted to IEEE Trans. on Smart Grid.*

[12] 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.

[13] 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.

[14] 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, 2013.

[15] C. Efthymiou and G. Kalogridis, “Smart grid privacy via anonymization of smart metering data,” in *Proc. of the IEEE SmartGridComm*, Gaithersburg, MD, Oct. 2010.

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

[17] S. Barker, A. Mishra, D. Irwin, E. Cecchet, P. Shenoy, and J. Albrecht, “Smart: An open data set and tools for enabling research in sustainable homes,” in *Proc. of the SustKDD*, Beijing, China, Aug. 2012.

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

[19] J. Liang, S. K. Ng, G. Kendall, and J. W. Cheng, “Load signature studypart i: Basic concept, structure, and methodology,” *IEEE Trans. on Power Delivery*, vol. 25, no. 2, pp. 551–560, 2010.

[20] P. Duhamel and M. Vetterli, “Fast fourier transforms: a tutorial review and a state of the art,” *Signal processing*, vol. 19, pp. 259–299, 1990.

[21] A. Medina, J. Segundo, P. Ribeiro, W. Xu, K. Lian, G. Chang, V. Dinavahi, and N. Watson, “Harmonic analysis in frequency and time domain,” *IEEE Trans. on Power Delivery*, vol. 28, no. 3, Jul. 2013.

[22] F. Zhang, Z. Geng, and W. Yuan, “The algorithm of interpolating windowed FFT for harmonic analysis of electric power system,” *IEEE Trans. on Power Delivery*, vol. 16, no. 2, pp. 160–164, Apr. 2001.

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

[24] U. Grenander, *Probability and Statistics: The Harald Cram r Volume*. Alqvist & Wiksell, 1959.

[25] J. R. Buck, M. M. Daniel, and A. C. Singer, *Computer explorations in signals and systems using MATLAB*. Prentice Hall, 2002.