

Transactive Energy to Guard against a Zero-Day Load Altering Attack on Power Distribution Systems

Samuel Yankson¹ and Mahdi Ghamkhari²

Department of Electrical and Computer Engineering

University of Louisiana at Lafayette

Lafayette, LA, USA

Emails: samuel.yankson1@louisiana.edu¹ and mahdi.ghamkhari@louisiana.edu²

Abstract—Zero-day cyber attacks against a system are novel attacks that exploit vulnerabilities in the system not known to the developers of the system. Accordingly, zero-day attacks can cause severe damages to the target system since they are not defended against. In this paper a zero-day load altering attack against power distribution systems is introduced. The zero-day attack exploits the mutual dependency of the price of electricity and the power consumption of the flexible loads in demand response programs. Through numerical simulations, it is shown that the zero-day attack amplifies the negative impact of the compromised electric loads on the power distribution systems by a factor of 86, making a much more devastating impact on the distribution systems. The extreme danger of the zero-day attack is demonstrated by bolding the shortcomings of the conventional attack prevention technique in forestalling the zero-day attack. To avert such dangers, a novel approach is proposed to guard against the zero-day attack in a transactive energy framework. Numerical Simulations on IEEE 33-bus standard system validate the effectiveness of the transactive energy framework in safeguarding power distribution systems.

Keywords: Cyber security, load altering attacks, power distribution systems, transactive energy, demand response, zero-day exploits, wholesale electricity market.

I. INTRODUCTION

The Global Risks Report prepared by World Economics Forum bolds the use of cyberattacks as a growing trend in targeting critical infrastructures and jeopardizing functioning of societies [1, page 14]. This is attested to by a recent survey undertaken by Black Hat, where 60% of security professionals in the Information Technology area have foreseen a successful cyber attack on US critical infrastructures to be made in the next following years [2, page 4]. Energy utilities are believed to be at heart of these cyber attacks [2, page 14]. Such a supposition is supported by at least two facts. First, a successful attack on energy utilities will assist the cyber attackers to also disrupt operation of other infrastructures that heavily rely on the electricity from energy utilities, e.g. water and gas infrastructures. Second, growing deployment of smart grid technologies with their inherent cyber vulnerabilities has expanded the attack surface area for cyber attackers to infiltrate to energy utilities' control and communication systems [3, page ii].

Various ways can be looked at by cyber attackers to harm an energy utility. The cyber attackers may attempt to

penetrate into the substations' networks and access special tools that give them an ability to disrupt, desynchronize or destabilize the utility operation [3, page 11]. However, gaining an unauthorized access to the substations is a difficult task requiring advanced skills of the cyber attackers [3, page 11]. A more subtle way of harming energy utilities is to target Programmable Logic Controllers or Remote Terminal Units with insecure and vulnerable implementation of industrial communication protocols. In this way, the attacker can gain access to the utility's substations by penetrating into non-critical field equipments [3, page 13]. A third way to harm an energy utility is to impact the operation of the utility through the electric loads that are equipped with Internet-of-Things technology [4, page 2], e.g. electric vehicles [5], [6] and computers [7, page 27], [8]. This third way is specially the most convenient way, corroborated by the fact that in the recent years Internet-of-Things objects have been target of massive cyber attacks [9].

Once being compromised by the cyber attackers, the electric loads can be employed to cause damages to the energy utility. Specially, the compromised loads can be used in launching a load altering attack against the power distribution system that is operated by the energy utility. In a load altering attack, compromised loads are remotely commanded by the cyber attackers to behave abnormally and disturb the balance between power supply and power demand in the power distribution system [7, page 27]. There are various types of load altering attacks each one targeting one of the mechanisms incorporated in power grids to maintain a balance between power supply and power demand. For instance, load altering attacks can target the Automatic Generation Control [10]–[14] or demand response programs [15]–[17].

In this paper a zero-day load altering attack against power distribution systems is introduced. Zero-day cyber attacks against a system are novel attacks that exploit vulnerabilities in the system not known to the developers of the system [18], [19]. Accordingly, zero-day attacks can cause severe damages to the target system as they are not defended against. The zero-day attack introduced in this paper is based on a negative side effect of the demand response programs known as Cobweb effect. More precisely, the attack exploits the mutual dependency of the price of electricity and the power consumption of the flexible loads in the demand response framework. As a result, the attack amplifies the negative impact of the compromised

electric loads on the power distribution systems, making much more devastating impacts.

To demonstrate extreme danger of the zero-day attack, the shortcomings of the conventional attack prevention technique in forestalling the zero-day attack are discussed in the paper. One serious shortcoming is that, the conventional technique is based on similarity detection between real-time power consumption of the loads and their abnormal behaviors captured in simulated attack conditions [10], [11], [15]–[17]. Accordingly, the conventional attack prevention technique may fall short in forestalling the zero-day load altering attack for which the abnormal behaviors of the loads are not captured beforehand. Being backed by the above discussion, an urgent need is highlighted in the paper for a mechanism that can protect power distribution systems against zero-day load altering attacks. To this end, this paper takes the first steps to study promises of transactive energy in guarding against load altering attacks. The underlying motive behind such effort is the fact that, transactive energy is emerging to address shortcomings of demand response [20]. Through numerical simulations, it is shown that the transactive energy framework safeguards the power distribution system against the zero-day load attack introduced in this paper.

The rest of the paper is organized as follows: Section II discusses the three power balancing mechanisms in power grids and the load altering attacks against them. A zero-day load altering attack is introduced in Section III. Section IV studies the promises of the transactive energy framework in guarding against the zero-day load altering attack. Section V provides numerical studies on the impact of the zero-day attack on power distribution systems. Finally, the paper is concluded in Section VI.

II. POWER BALANCING IN POWER GRIDS

To ensure reliability of a power grid operation, a balance between power supply and power demand should be maintained at all time. Three mechanisms are incorporated in operation of power grids to maintain the required power balance, i.e., running wholesale electricity markets, employing Automatic Generation Control and deploying demand response. These three mechanisms are briefly discussed in this section.

A. Energy Trading in Wholesale Electricity Markets

In regions with deregulated electricity markets, a wholesale market runs every 5 minutes [21], [22] to enable energy trading between bulk power generators and energy utilities. In offering energy to the wholesale market, a bulk power generator submits a cost function to the market indicating the pay that must be paid to the generator as a function of the generator’s power generation. On the other hand, an energy utility submits to the market the amount of power that it needs to operate its power distribution system. The Independent System Operator of the power grid collects all the energy bids from the generators and energy utilities and clears the market by calculating the lowest-cost power dispatch in meeting energy demands of the energy utilities.

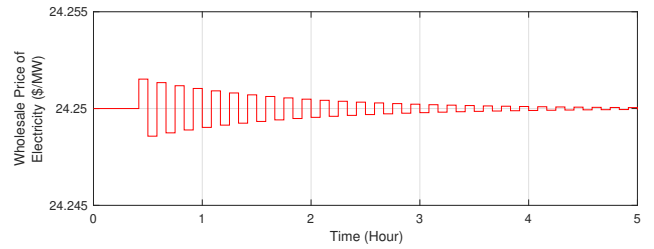


Fig. 1: In the demand response framework, the mutual dependency of the wholesale price of electricity and power consumption of the flexible loads produce volatility in the price of electricity; a behaviour known as Cobweb effect.

As a byproduct of the above market clearing process, the electricity is priced at all nodes of the power grid. The price of electricity ω set for an energy utility depends on the power consumption P of the utility:

$$\omega = \omega_0 + \lambda(P - P_0), \quad (1)$$

where the parameters ω_0 and P_0 are reference price of electricity and power consumption, respectively. For an energy utility, the parameters ω_0 , P_0 and λ can be derived from the historical data on power consumption of the utility and the price of electricity set for the utility.

B. Reserve Generation

In purchasing energy from wholesale market, an energy utility should forecast the power consumption of its power distribution system 5 minutes in advance of the operating time of the power grid. However, load forecasting methods [23] utilized by energy utilities are not perfect and come with limited accuracies. Accordingly, the real time power consumption of the distribution system may deviate from the power consumption scheduled in the wholesale market. The mismatch between scheduled and real time power consumption of the distribution system is compensated for by drawing additional power from reserve generators; a mechanism known as Automatic Generation Control. In fact, a mismatch between power generation and power consumption changes the frequency of the AC voltages throughout the power grid. The power generators offering reserve generation to the grid measure and react to the changes in voltage frequency. The responses of the reserve generators to the frequency changes are set up in a way that, the combined impact of all the responses counterbalances the mismatch between power generation and power consumption.

C. Demand Response

Demand response is another mechanism for keeping a balance between power generation and power consumption. In demand response, power consumers with flexible loads adjust their power consumption based on the price of electricity set for the distribution system. More precisely, when the price of electricity is high the flexible loads lower their power

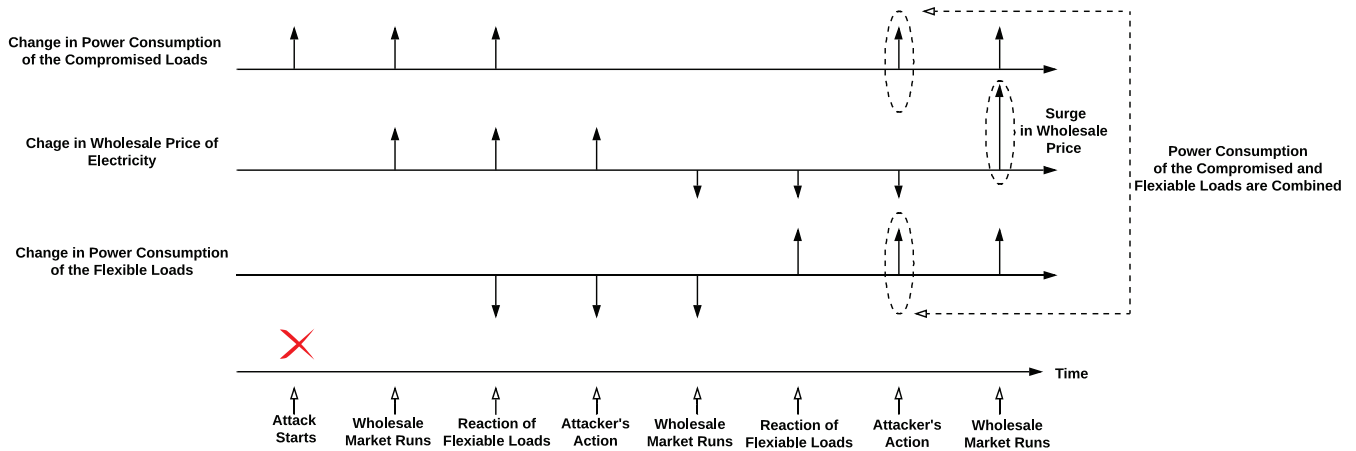


Fig. 2: The timeline of the zero-day load altering attack in Section III-C. By completing the steps shown in the timeline, the action of the attacker combines with reaction of the flexible loads, making a larger impact on the distribution system.

consumption and when the price of electricity is low the flexible loads increase their power consumption. In responding to the price of electricity, the flexible loads seek to maximize their utility functions. Accordingly, the response of a flexible load to the price of electricity can be modeled as following [24]:

$$\text{Power Consumption of the Flexible Loads} = F(\omega), \quad (2)$$

where $F(\cdot)$ gives the power consumption of the flexible load as a function of the price of electricity ω . We note that, controllable loads such as electric vehicles and data centers are among the flexible loads that can engage in demand response programs.

D. Load Altering Attacks

Load altering attacks against power grids aim to disturb the balance between power supply and power demand. In this section two different types of load altering attacks are discussed. In the first type of such attacks, the attacker gains control of several electric loads and maliciously alters the power consumption of the compromised loads so as to disturb the Automatic Generation Control mechanism discussed in Section II-B [10]–[14]. As a result of this type of attack, the stability of the power grid operation is disturbed and the possibility a blackout is strengthened. In the second type of load altering attacks, the attacker infiltrates into the advanced metering infrastructure and sends malicious fake prices of electricity to the smart meters. The fake prices of electricity are engineered in way that, power consumers experience a fake low-price hour and a fake peak-price hour, thereby shifting their power loads from the fake peak-hour price to the fake low-hour price [15]–[17]. As a result, the power consumption in the distribution system peaks substantially at the fake low-price, thereby increasing likelihood of a congestion in the distribution lines.

III. A ZERO-DAY LOAD ALTERING ATTACK

A zero-day cyber attack against a system is a novel attack that exploits a vulnerability in the system not known to the developers of the system [18], [19]. Accordingly, zero-day attacks can cause severe damages to the target system as they cannot be defended against. In this section, a zero-day load altering attack is introduced.

A. Infiltrating to Residential Networks

To carry out the zero-day load altering attack, the attacker needs to gain the remote control of few electric loads. The compromised loads should be controllable so that their power consumption can be changed remotely by the attacker. Electric vehicles [25], computer servers [7, page 27], [8] and energy storage units [26] are among the loads suitable for carrying out the zero-day attack in Section III-C. To gain control of these electric loads, the attacker can infiltrate to residential wifi networks through the Internet or other means, run network scanning software and find the electric loads that are controllable over the compromised network. The feasibility of such infiltration scenario is attested to by the proliferation of Internet-of-Things enabled electric loads with weak security architectures [27]. Nevertheless, in the rest of the discussion we assume that the cyber attacker can compromise few electric loads and can alter their power consumption all remotely.

B. Cobweb Effect in Power Grids

The zero-day attack is based on a negative side effect of the demand response framework known as Cobweb effect; see Fig. 1. The Cobweb effect is a consequence of the mutual dependency of the price of electricity and the power consumption of the flexible loads that operate in the demand response framework. As a result of the Cobweb effect, a set of successive intervals with over-supply and under-supply of energy are formed in the power grid [20], [28], [29]. More precisely, an under-supply of energy in the power grid results in a high price of electricity that enforces the flexible loads to

lower their power consumption. Once the flexible loads lower their power consumption, an over-supply of energy occurs in the power grid which decreases the price of electricity. The flexible loads react to the lowered price of electricity and increase their power consumption, thereby causing an under-supply of energy. Such back-and-forth between over-supply and under-supply conditions make the price of electricity to display a volatile behavior similar to a cobweb pattern.

Fig. 1 shows the Cobweb effect simulated on the IEEE 33-bus power distribution system using the pricing model in (1). In normal operation of the power grid, the price volatilities caused by the Cobweb effect fade over time, making the volatilities tolerable. However, the next section introduces a zero-day load altering attack that harms the stability of the power distribution system by exacerbating the price volatilities caused by the Cobweb effect.

C. The Zero-Day Attack Scenario

The zero-day attack scenario is schematically shown in Fig. 2. The attacker starts the attack by increasing the power consumption of the compromised loads. As a result, the power consumption of the distribution system increases leading to a rise in the price of electricity the next time that electricity market runs. The flexible loads in the distribution system respond to the increase in the price of electricity and lower their power consumption. In the meanwhile, the attacker lowers the power consumption of the compromised loads. As a result, the price of electricity drops to a level lower than the price of electricity before the start of the attack. The flexible loads respond to this low price of electricity by increasing their power consumption to a level higher than their power consumption before the start of the attack. In the meanwhile, the cyber attacker increases the power consumption of the compromised loads, which combines with the increase in the power consumption of the flexible loads to create a high unprecedented power consumption in the distribution system. As a result, the price of electricity in the next run of the wholesale market leaps to an unprecedented high level.

The attacker repeats the above steps over and over, exacerbating under-supply and over-supply conditions in the power distribution system. Upon completion of every full set of the above steps, the price of electricity leaps to a higher unprecedented level which have not been observed beforehand. Accordingly, as the attack scenario proceeds, the power consumption of the distribution system increases over and over resulting in congestion of the distribution lines and possibly a blackout in the distribution system. We note that, the increases in the wholesale price of electricity and power consumption of the distribution system continues until the flexibility of the flexible loads are fully exhausted. After that, the price of electricity and power consumption of the distribution system keep oscillating with dramatic fixed magnitudes. In Section V, through numerical simulations we will see that the magnitude of the oscillations in the power consumption of the distribution system is 86 times higher than the magnitude of the oscillations in the power consumption of the compromised

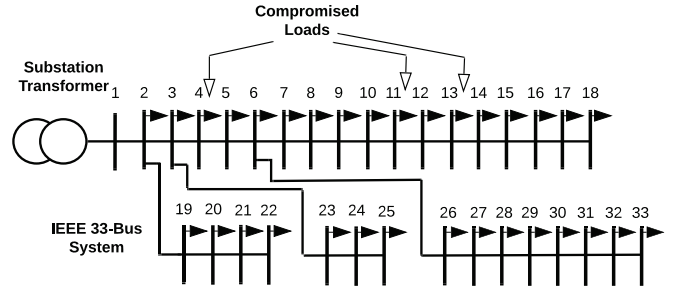


Fig. 3: The compromised electric loads are at buses 4, 11 and 13 of the IEEE standard 33-bus power distribution system.

loads. In other words, the zero-day cyber attack amplifies the negative impact of the compromised loads on the power distribution system by a factor of 86, causing a much more devastating harm to the operation of the distribution system.

IV. GUARDING AGAINST THE ZERO-DAY ATTACK

This section bolds the serious shortcomings of the conventional technique in preventing load altering attacks, thereby calling into question the effectiveness of this technique. Furthermore, the promises of the transactive energy in preventing these attacks are discussed.

A. The Conventional Attack Prevention Technique

The conventional technique in preventing load altering attacks is to look for similarity between the real time behavior of electric loads and the abnormal behaviors of the loads captured in simulated attack conditions. [10], [11], [15]–[17]. Once a similarity is found, the power distribution system operator is alarmed to take protective measures against the detected attack. This conventional technique suffers from at least two serious shortcomings. First, the conventional attack prevention technique is unable to detect load altering attacks that are deliberately obfuscated by the cyber attacker to become undetectable [14]. Second, the conventional technique falls short in detecting zero-day attacks for which no abnormal patterns of electric loads are captured beforehand. To avoid the above deficiencies of the conventional technique, a novel attack prevention mechanism is proposed in the following sections which can successfully guard against the zero-day load altering attack of Section III-C

B. Transactive Energy Framework

Transactive energy is an emerging paradigm to address shortcomings of demand response [20]. In contrast to the demand response framework where the flexible loads alleviate power imbalances by responding to the price of electricity, in the transactive energy framework flexible loads slash power imbalances by entering into peer-to-peer energy transactions with other power consumers. More precisely, in the transactive energy framework the flexible loads and other power consumers bid for energy in real time operation of the power grid.

The bids are collected by the distribution system operator and are translated into real time energy exchanges between power consumers [30].

Major benefits are attributed to the transactive energy framework including enhancement of distribution systems reliability, curtailment of power losses and reduction of electricity prices [30]–[34]. However, one key advantage pertaining to the topic of this paper is the absence of Cobweb effect in the transactive energy framework [20]. The absence of the Cobweb effect is due to the fact that, when a set of power consumers increase their power consumption in the transactive energy framework, another set of power consumers lower their power consumption simultaneously [33]. Accordingly, power consumers fulfill their energy demands without disturbing the power balance in the distribution system. By precluding Cobweb effect, the transactive energy framework shows great promise in guarding against zero-day attack scenario of Section III-C.

C. Transactive Energy to Guard against the Zero-Day Attack

In the attack scenario of Section III-C, the attacker exploits the mutual dependency of the price of electricity and the power consumption of the flexible loads to cause harm to the distribution system. Such an attack scenario is not workable when all the electric loads, including the compromised loads, are setup to procure their energy demands from real-time energy transactions. That is because, real time energy transactions enable power consumers to procure their energy demands without impacting neither the power consumption of the distribution system nor the price of electricity, see (1). As the price of electricity is not impacted by the energy transactions, the zero-day attack scenario is not functional in the transactive energy framework.

We note that, in the above discussion we have assumed that the real time energy transactions are carried out in a secure way and are not compromised by the attacker. For instance, the energy transactions can be performed by secure smart meters through a secure communication platform with proper authentication and encryption protocols. This is particularly a desirable approach, since the smart meters are usually maintained by energy utilities and can be setup to work securely. As a result, although the attacker may find a way to infiltrate to residential wifi networks and gain control of few electric loads, but cannot carry out the zero-day attack scenario of Section III-C.

V. NUMERICAL SIMULATIONS

Through numerical simulations, this section studies the impact of the zero-day load altering attack of Section III-C on power distribution systems.

A. Simulation Setup

The IEEE standard 33-bus system is selected as the power distribution system in the simulations. The load data for the IEEE 33-bus system are obtained from MATPOWER [35]. The attacker is assumed to have remote control over few electric loads at buses 4, 11 and 13 of the IEEE 33-bus system, see

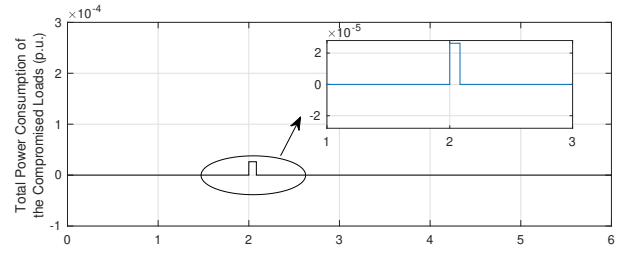


Fig. 4: Total power consumption of the compromised loads in their normal operation.

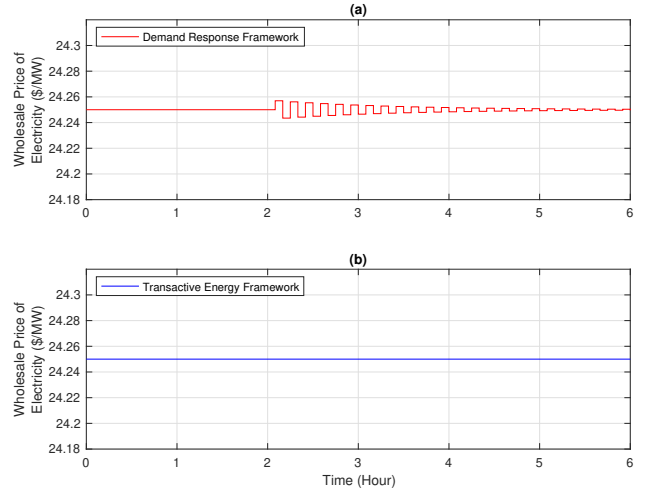


Fig. 5: The wholesale price of electricity, when the compromised loads operate normally.

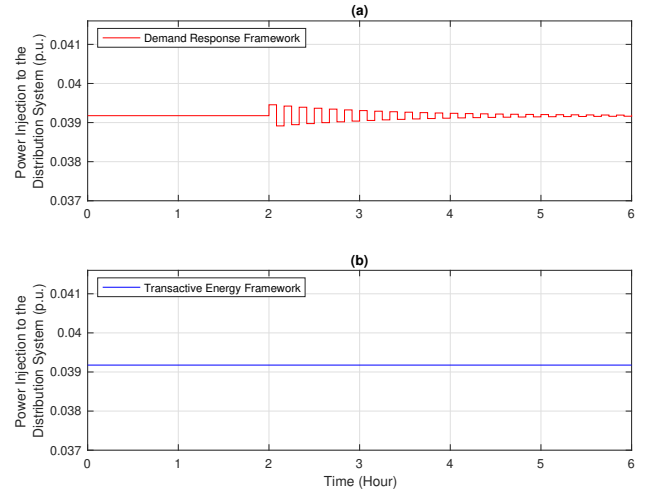


Fig. 6: The power consumption of the distribution system, when the compromised loads operate normally.

Fig. 3. The total power consumption of the compromised loads is 2.5 percent of the total loads at buses 4, 11 and 13. The compromised loads are remotely controllable. The attacker can send on/off control commands to the compromised loads, prompting these loads to operate in full-load or no-load conditions. The loads at buses 3, 5, 6, 7, 10, 15, 17, 19, 22, 23, 27, 28, 29, 30, 31 32 and 33 are flexible. The flexible loads

react to the wholesale price of electricity and lower or increase their power consumption up to 30 percent of their rated power consumption. Within this range, the power consumption of the flexible loads are set to change as a linear function of the price of electricity [24]. The parameters λ , ω_0 and P_0 in (1) are set to $\lambda = 25 \text{ \$/MW}^2$, $\omega_0 = 24.25 \text{ \$/MW}$ and $P_0 = 3.92 \text{ MW}$, respectively. The transactive energy framework used in the simulations is adopted from [30]. The simulations are performed on a computer with a CPU @2.60 GHz and 16 GB RAM.

B. The Normal Operation of the Power Distribution System

In this section, we consider a scenario where the compromised loads at buses 4, 11, and 13 of the distribution system are initially in no-load condition. The compromised loads then receive a control command prompting them to switch to full-load condition for a period of 5 minutes; see Fig. 4. The Fig. 5 and 6 show the impact of the control command on the wholesale price of electricity and the power consumption of the distribution system, for two different cases. In one case, the flexible loads respond to the price of electricity in a demand response framework. In the other case, the flexible loads enter into real time energy transactions with the compromised loads in a transactive energy framework. From Fig. 5(a) and 6(a), the control command to the compromised loads leads to the appearance of Cobweb effect when the flexible loads operate in the demand response framework. However, from Fig. 5(b) and 6(b) the control command doesn't impact the wholesale price nor the power consumption of the distribution system when the flexible loads operate in the transactive energy framework, see the discussion in Section IV-B. Consequently, the transactive energy framework beats the demand response framework by eliminating the Cobweb effect in power distribution systems.

C. The Abnormal Operation of the Power Distribution System

In this section, we consider a scenario where the compromised loads at buses 4, 11, and 13 of the distribution system operate maliciously. Following the attack scenario in Section III-C, the compromised loads are commanded by the cyber attacker to switch between no-load and full-load conditions every 5 minutes, see Fig. 7. The Fig. 8 and Fig. 9 show the wholesale price of electricity and the power consumption of the distribution system in the resulted abnormal operation of the distribution system. From Fig. 8 and Fig. 9, the fluctuations of the power consumption of the compromised loads produce wide fluctuations in the wholesale price of electricity and power consumption of the distribution system, when the flexible loads operate in a demand response framework. In contrast, the fluctuations in the power consumption of the compromised loads cannot impact the wholesale price of electricity or the power consumption of the distribution system, when the flexible loads operate in the transactive energy framework. Consequently, the transactive energy framework successfully guards against the zero-day load altering attack on the power distribution system.

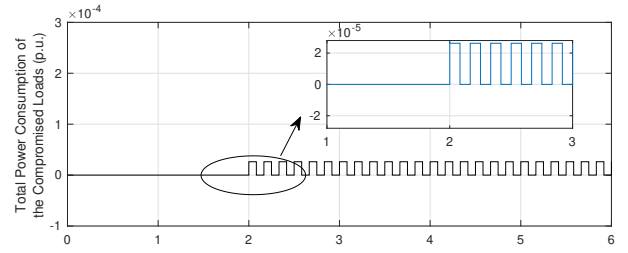


Fig. 7: Total power consumption of the compromised loads, when the compromised loads operate maliciously.

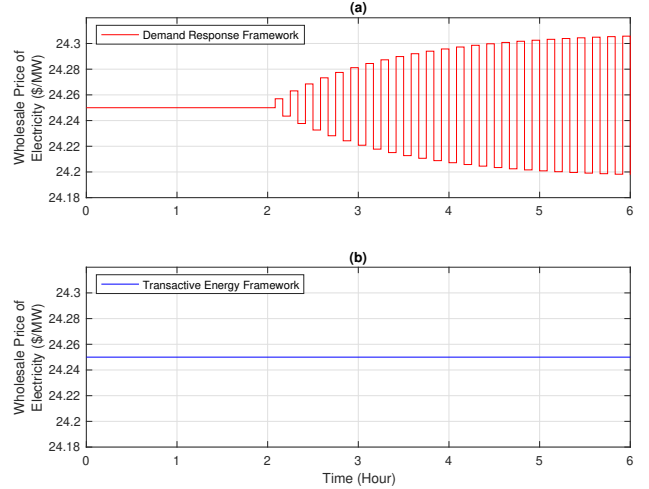


Fig. 8: The wholesale price of electricity, when the compromised loads operate maliciously.

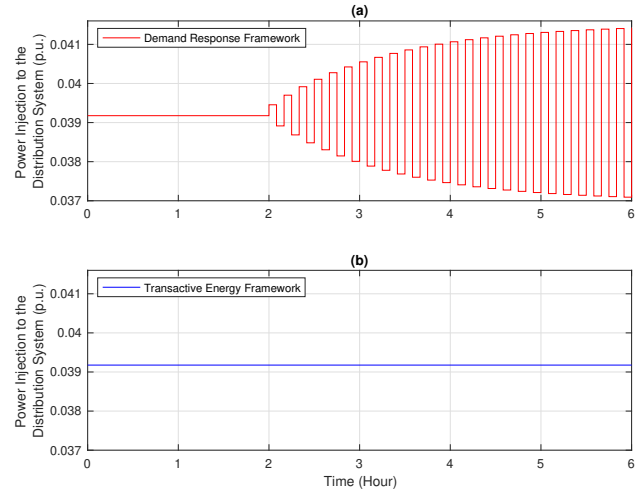


Fig. 9: The power consumption of the distribution system, when the compromised loads operate maliciously.

Also, as it can be seen from Fig. 7 the total power consumption of the compromised loads swing between 0 and $2.62 \times 10^{-5} \text{ p.u.}$ However, from Fig. 9 the power consumption of the distribution system swings between 0.0415 p.u. and 0.0370 p.u. in the demand response framework few hours after the start of the attack. Therefore, the zero-day attack scenario amplifies the negative impact of compromised loads

by a factor of $0.5 \times (0.0415 - 0.0370) \times (2.62 \times 10^{-5} - 0) \approx 86$ in the demand response framework, creating a much more devastating impact on the power distribution system. In contrast, the power distribution system is safeguarded against such devastating impacts when the flexible loads operate in the transactive energy framework.

VI. CONCLUSION

In this paper, a zero-day load altering attack against power distribution systems was introduced. The attack is based on a negative side effect of the demand response framework known as Cobweb effect. The attack exploits the mutual dependency of the price of electricity and the power consumption of the flexible loads in the demand response framework. Thereby, the attack amplifies the negative impact of the compromised electric loads on the power distribution system, making a much more devastating impact. Also, the serious shortcomings of the conventional attack prevention technique was bolded in the paper. Specially, it was highlighted that the conventional technique may fall short in detecting and preventing zero-day cyber attacks such as the one introduced in this paper. Through numerical simulations, it was shown that the transactive energy framework can safeguard the power distribution system against the introduced zero-day load altering attack.

REFERENCES

- [1] World Economic Forum, "The global risks report 2018," Geneva, Switzerland, 2018, 13th Edition. [Online]. Available: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf
- [2] Black Hat, "Portrait of an imminent cyberthreat," 2017. [Online]. Available: <https://www.blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf>
- [3] Mission Support Center, "Cyber threat and vulnerability analysis of the U.S. electric sector," Idaho National Laboratory, August 2016.
- [4] R. K. Knake, "A cyberattack on the U.S. power grid," *Contingency Planning Memorandum*, no. 31, 2017.
- [5] H. Thompson and S. Trilling, "Cyber security predictions: 2019 and beyond," November 2018. [Online]. Available: <https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond>
- [6] M. Asaad, F. Ahmad, M. S. Alam, and Y. Rafat, "IoT enabled monitoring of an optimized electric vehicle's battery system," *Mobile Networks and Applications*, vol. 23, no. 4, pp. 994–1005, 2018.
- [7] S. Goel, Y. Hong, V. Papakonstantinou, and D. Kloza, *Smart Grid Security*, London, U.K., April 2015.
- [8] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: coordinated load-changing attacks on power grids," in *proc. of Annual Computer Security Applications Conference*, Orlando, FL, December 2017.
- [9] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference mode," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018.
- [10] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, July 2018.
- [11] S. Amini, F. Pasqualetti, M. Abbaszadeh, and H. Mohsenian-Rad, "Hierarchical location identification of destabilizing faults and attacks in power systems: A frequency-domain approach," *Accepted for publication in IEEE Transactions on Smart Grid*, 2018.
- [12] M. Izbicki, S. Amini, C. R. Shelton, and H. Mohsenian-Rad, "Identification of destabilizing attacks in power systems," in *proc. of American Control Conference*, Seattle, WA, May 2017.
- [13] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Detecting dynamic load altering attacks: A data-driven time-frequency analysis," in *proc. of International Conference on Smart Grid Communications*, Miami, Florida, November 2015.
- [14] P. Xun, P. Zhu, S. Maharjan, and P. Cui, "Successive direct load altering attack in smart grid," *Computers and Security*, vol. 77, pp. 79–93, 2018.
- [15] J. Giraldo, A. Cárdenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: Impact and countermeasures," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249–2257, September 2017.
- [16] R. Tan, V. B. Krishna, D. K. Y. Yau, and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," in *proc. of the ACM SIGSAC Conference on Computer and Communications Security*, Berlin, Germany, November 2013.
- [17] Y. Liu, S. Hu, and T. Ho, "Leveraging strategic detection techniques for smart home pricing cyberattacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 220–235, March 2016.
- [18] S. Egelman, C. Herley, and P. C. V. Oorschot, "Markets for zero-day exploits: Ethics and implications," in *proc. of the New Security Paradigms Workshop*, Alberta, Canada, September 2013.
- [19] D. Palka and M. Zachara, "Learning web application firewall - benefits and caveats," in *Availability, Reliability and Security for Business, Enterprise and Health Information Systems*, A. M. Tjoa, G. Quirchmayr, I. You, and L. Xu, Eds., vol. 6908. Berlin, Heidelberg: Springer, 2011, pp. 295–308.
- [20] R. M. J. R. and Agüero, "Sharing the ride of power: Understanding transactive energy in the ecosystem of energy economics," *IEEE Power and Energy Magazine*, vol. 14, no. 2, pp. 70–78, 2016.
- [21] J. H. Yoon, R. Baldick, and A. Novoselac, "Dynamic demand response controller based on real-time retail price for residential buildings," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 121–129, 2014.
- [22] B. Kranz, R. Pike, and E. Hirst, "Integrated electricity markets in new york: Day-ahead and real-time markets for energy, ancillary services, and transmission," *NYISO*, November 2002.
- [23] T. Hong and S. Fan, "Probabilistic electric load forecasting: A tutorial review," *International Journal of Forecasting*, vol. 32, no. 3, pp. 914–938, 2016.
- [24] P. B. S. Kiran and N. M. Pindoriya, "Study of consumer benefit functions for demand response algorithm," in *proc. of National Power Systems Conference*, Bhubaneswar, India, December 2016.
- [25] M. Hashem Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, June 2017.
- [26] A. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, December 2011.
- [27] R. K. Pandey and M. Misra, "Cyber security threats — smart grid infrastructure," in *National Power Systems Conference*, Bhubaneswar, India, December 2016.
- [28] E. M. Larsen, P. Pinson, J. Wang, and Y. Ding, "The Cobweb effect in balancing markets with demand response," in *proc. of International Conference on the European Energy Market*, 2015.
- [29] H. T. Nguyen, S. Battula, R. R. Takkala, Z. Wang, and L. Tesfatsion, "Transactive energy design for integrated transmission and distribution systems," 2018.
- [30] M. Ghamkhari, "Transactive energy pricing in power distribution systems," in *proc. of IEEE Green Technologies Conference*, Lafayette, Louisiana, April 2019.
- [31] P. Siano and D. Sarno, "Assessing the benefits of residential demand response in a real time distribution energy market," *Applied Energy*, vol. 161, pp. 533–551, January 2016.
- [32] F. A. Rahimi and A. Ipakchi, "Transactive energy techniques: Closing the gap between wholesale and retail markets," *The Electricity Journal*, vol. 28, no. 8, pp. 29–35, October 2012.
- [33] M. Ghamkhari, "Transactive energy versus demand response in cutting wholesale electricity prices," in *proc. of IEEE international conference on smart grid and smart cities*, June 2019.
- [34] M. A. Rahaman and M. Ghamkhari, "Peer-to-peer and real-time energy exchanges with data centers in a transactive energy framework," in *proc. of IEEE international conference on Smart Grid Energy Engineering*, Oshawa, Canada, August 2019.
- [35] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MAT-POWER: Steady-state operations, planning and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.