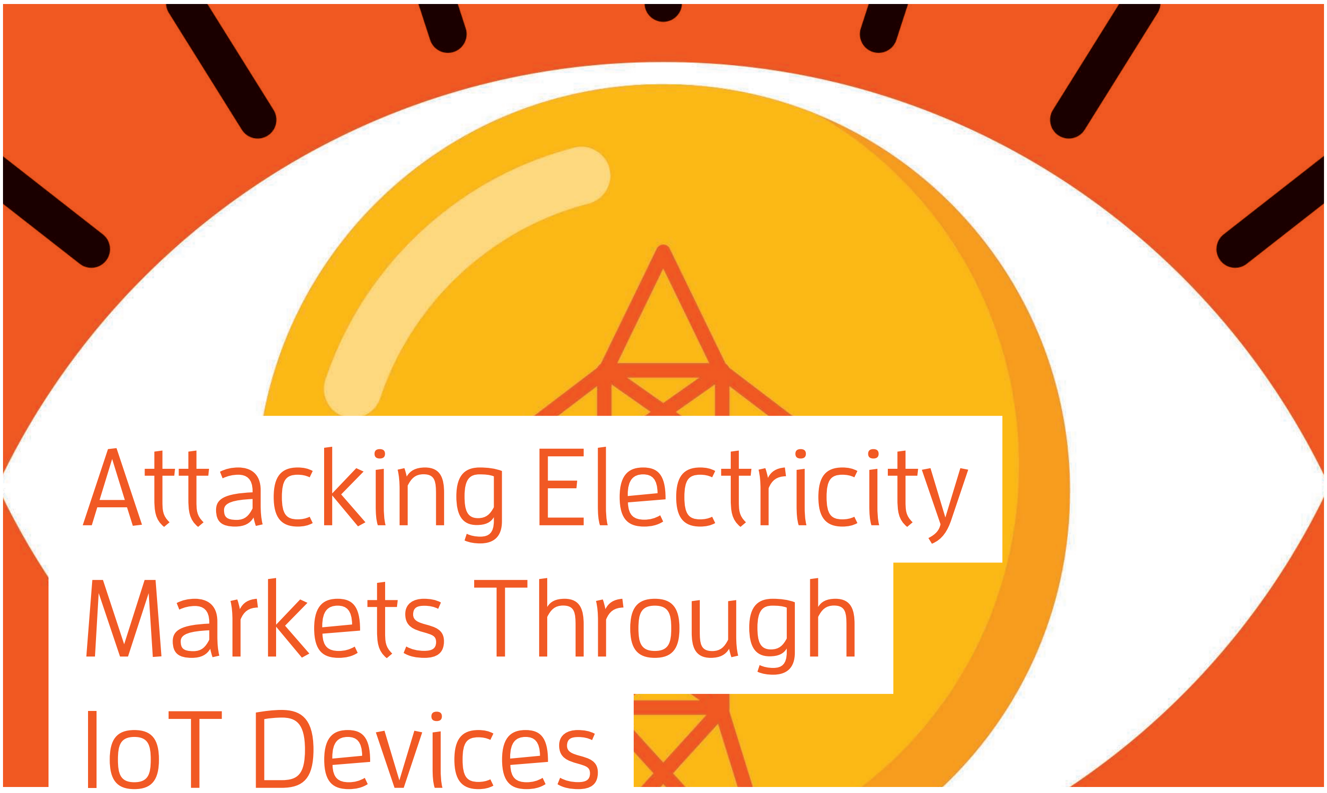

Attacking Electricity Markets Through IoT Devices

Carlos Barreto, Himanshu Neema, and Xenofon Koutsoukos, Vanderbilt University

Smart appliances, or Internet of Things devices, participate autonomously in electricity markets and improve grid efficiency, but their remote access and control capabilities also introduce vulnerabilities. We show how an adverse generator can manipulate market clearing prices and propose mitigation strategies to correct the impact.

The power grid is undergoing a modernization process to improve efficiency, resiliency, and reliability. Some innovations, such as transactive energy (TE), focus on improving the participation of users. TE is a distributed management approach in which smart appliances, or Internet of Things (IoT) devices, participate autonomously in electricity markets. Thus, appliances can adjust their demand to reduce system stress and support renewable resources integration. However, the introduction of IoT devices also brings new vulnerabilities to the power grid.

Research on power system security has focused mainly on the utilities' cyber risks, for instance, attacks that target critical elements such as generators and substations, among others.[1,2] Indeed, some hacker groups have targeted corporate networks to access critical equipment. For example, in 2015, Ukraine's utilities suffered a cyberattack that exposed their control networks and allowed external access to workstations that ran circuit breakers.[3]

The attacks experienced so far have had a relatively limited impact (for example, the attacks against Ukraine lasted 6 h and did not damage critical components), which suggests there are significant challenges to compromising control networks and causing long-term damage. For this

Digital Object Identifier 10.1109/MC.2020.2973951
Date of current version: 7 May 2020

reason, adversaries can design attacks to target less secure elements such as IoT devices.

Cyber risks from vulnerable customer-side devices differ in some aspects from utilities' cyber risks. First, adversaries can compromise a large number of IoT devices, rather than targeting critical components. Although these devices individually do not pose threats (the power system is robust and can withstand the failure of individual generators), their coordinated actions can create significant disturbances.[4,5] Second, utilities cannot address these vulnerabilities directly because the devices belong to third parties (customers).

ADVERSARIES CAN DESIGN ATTACKS TO TARGET LESS SECURE ELEMENTS SUCH AS IoT DEVICES.

Other risks come from adversaries that seek personal profit rather than harm to the system. Some works have shown that agents can profit from exploiting vulnerabilities in the market's infrastructure, for example, tampering with sensor measurements or price signals sent by the utilities.[6,7]

In this article, we analyze possible cyber risks for TE introduced by an insecure IoT. Specifically, we show how an adverse generator (or seller) profits by manipulating bids from smart appliances. We express the adversary's goal as a function of the bids originally submitted to the market. Thus, the adversary can achieve its ideal goal through what is known as a *false data injection* attack. We also propose a defense strategy that modifies some bids to mitigate the impact of the attack.[8] We validate the attack model and defense strategy on a realistic distribution system. For this purpose, we develop a design studio that extends GridLAB-D to evaluate the resiliency of power grids against cyber and physical attacks.[9]

ELECTRICITY SYSTEM

Power systems have three main subsystems: generation, transmission, and distribution. The generation subsystem includes sources of electricity, such as hydro or thermal generators, often scattered over large geographical areas. The transmission and distribution infrastructures connect generators with customers but differ in a few key aspects: the transmission system carries energy across large distances using high-voltage transmission lines, while the distribution system reduces the voltage and delivers energy directly to customers. In this article, we describe how power systems operate and highlight innovations that improve their efficiency and reliability.

Electricity markets

Power systems try to allocate resources (energy and capital) in an efficient way, that is, creating the highest social satisfaction. For this task, the power system uses market mechanisms such as auctions. An auction first collects bids, which specify the trades that agents would approve. Here, we consider auctions that request the marginal valuation and marginal cost functions of buyers and generators, respectively. Thus, each bid gives information about the benefit that each agent receives from a transaction. In a second stage, the auctioneer determines the market equilibria, that is, the transactions that maximize system efficiency. Many electricity markets trade energy using a single price, called the *market clearing price*, which balances demand and supply.

Power markets usually use what is termed *social welfare*, the aggregated benefit of all participants, as their efficiency metric. Some celebrated results from economics show that competitive markets incentivize efficient dispatch (an operation that maximizes social welfare) because generators must offer energy at prices close to their marginal costs. Therefore, the demand is served with the lowest cost. In our analysis, we consider an ideal market in which agents cannot get better profits modifying their own bids (in other words, exercising market power). However, we will show how an adverse generator can profit by modifying the bids of others.

Electricity systems often use two markets: the day ahead market (DAM) and the real-time market (RTM). The DAM plays a crucial role in planning future operation of the power system. In particular, the DAM accepts bids of supply or demand for a future period (such as the following day) and produces commitments that buyers and sellers must fulfill. In this way, generators can prepare in advance for their operation.

RTMs complement DAMs by correcting imbalances between demand and generation during the actual operation. For example, if a seller cannot provide the contracted energy, the system operator must purchase energy from other sellers that participate in the RTM. Likewise, if a buyer uses more (or less) energy, then the system operator buys (or sells) energy in the RTM. In general, the RTM accepts bids of supply or demand to correct deviations in DAM commitments during the next hour.

The operation of the power system has several constraints. For instance, the system's components can generate or carry a limited amount of power and operate at specific voltages and frequencies (e.g., 50 or 60 Hz). The power grid needs a balance between generation and demand to maintain frequency within acceptable levels. However, this is a nontrivial task because demand and generation change in response to external factors such as the weather or the system's faults. For these reasons, electricity markets need a central authority that monitors the system and enforces reliable allocations, in other words, allocations that comply with the physical constraints of the system.

In general, an independent system operator (ISO) manages both DAMs and RTMs and maintains short-term system reliability. The process of finding the most efficient operation, while avoiding violations of physical constraints, is called *economic dispatch*. The ISO monitors the grid's operation and executes control actions (such as adjusting the generator's production or connecting or disconnecting loads) through supervisory control and data acquisition (SCADA) systems.

TE

In general, customers do not participate (bid) directly in markets; instead, they purchase electricity from utilities at fixed prices. In this way, customers delegate to a third party a number of complex tasks, such as deciding bids, following the ISO's commands (for example, regulating consumption), and compensating generators. As a result, customers disengage from the market's activity, leading to inefficient operations. For instance, customers who ignore electricity prices miss opportunities to reduce costs by consuming less energy during periods with high prices.

The power grid is undergoing a modernization process that enhances the coordination of users to avoid inefficient outcomes and support the integration of renewable resources. In general, the mechanisms to coordinate users, also called *demand management systems*, use economic incentives to shape user demand. For example, direct load control programs compensate users who turn off their loads when the system is under stress. Other schemes, such as real-time pricing, time of use, and critical peak pricing, design prices to induce changes in consumption, such as reducing demand peaks.[10]

TE is a distributed management approach in which users participate in the market by trading energy and similar ancillary services.[11] Unlike other demand management systems, TE implements a two-way communication between suppliers and customers. This approach reduces load uncertainties loads because customers who participate in the market reveal information about their future consumption.

TE relies on transactive controllers, which bid in the market and regulate the demand of appliances based on market dynamics and owner preferences. For example, transactive controllers can prepare for periods with high demand (and high prices) by turning on the air conditioning systems when the prices are low (storing energy in thermal form). In this way, users can reduce costs at the expense of some degree of discomfort (some deviation from the desired temperature).

VULNERABILITIES OF THE POWER SYSTEM

In recent years, some sophisticated cyberattacks have exploited vulnerabilities in SCADA systems to degrade the operation of critical infrastructures. In 2015, Ukraine suffered the first confirmed cyberattack designed to cause power outages.[3] The adversaries first penetrated the corporate network of some power companies and then proceeded to steal credentials to access the companies' SCADA networks. The attackers then compromised operators' workstations, which allowed them to manually open circuit breakers. Ukraine suffered a second attack in 2016, but this time the attackers automated their actions using a malware called *Crash Override*. This malware automatically located control equipment and sent commands to switch the power flow on and off.

Experts believe that nation-states undertake most of the attacks against critical infrastructures. In particular, Thales and Verint[12] found 24 groups targeting the energy sector of 106 countries. However, despite the large number of skillful and motivated attackers, only two groups have created infrastructure failures: the Equation group, author of the Stuxnet malware, and the Sandworm team, responsible for the blackouts in Ukraine.[13]

The low number of successful attacks against power systems suggests significant challenges in compromising SCADA networks. Besides, power grids are resilient to failures.[5] For this reason, the attacks witnessed so far had a relatively limited impact (for example, the attacks against Ukraine, as noted previously, lasted 6 h and did not damage critical components). Nevertheless, adversaries can exploit other power system vulnerabilities.

The modernization of the market infrastructure and the introduction of IoT devices create new threats for the power grid (see Stellios et al.[14] for a survey on attacks enabled by the IoT). As

Soltan et al.[4] explain, adversaries can exploit vulnerabilities in the IoT to target customer side components, such as smart meters, appliances, end-user generation systems (solar panels), and electric vehicles.

Threats on customer-side devices differ in some ways from threats on SCADA systems. First, adversaries can compromise a huge number of IoT devices, exploiting their poor security practices, rather than target critical components, like the attacks against Ukraine. Although IoT devices individually do not pose threats (the power system is robust and can withstand the failure of individual generators), their coordinated actions can create significant disturbances, resembling the Mirai botnet, which used IoT devices to launch unprecedented distributed denial-of-service attacks.[15] Second, utilities cannot address these threats directly, such as by protecting the devices, because they belong to third parties (customers).

THE MODERNIZATION OF THE MARKET INFRASTRUCTURE AND THE INTRODUCTION OF IoT DEVICES CREATE NEW THREATS FOR THE POWER GRID.

ATTACK MODEL

We consider an adverse generator that exploits TE technology to change the market's equilibria and profit. In this case, the adversary has some restrictions. First, the attacker must prevent operation states that harm its own assets. Second, a successful attack must remain undetected long enough to generate profits, in other words, to guarantee that the benefits exceed the attack's costs. For simplicity, we assume that the adversary addresses these restrictions, regulating its attack to cause small deviations from the typical system operation.

We see the attack as a way to change the optimization problem solved in the economic dispatch. Specifically, the adversary designs its attack so that the economic dispatch maximizes what is called a *biased welfare* function. Unlike the social welfare function, which gives equal weight to all agents, the adversary's efficiency metric is biased toward itself. As a result, the economic dispatch would select equilibria that prioritize the adversary's benefit. In this case, the adversary can regulate the attack's impact by selecting the weights of the biased welfare function (see more details in Barreto and Koutsoukos.[8])

Recall that the optimal equilibria maximize the social welfare, which depends on the bids submitted by agents. This implies that an attack on the bids can change the market's equilibria. However, as discussed previously, the attacker can get no benefit changing only its own bids. For this reason, the adversary compromises smart appliances to change their bids in a way such that the economic dispatch maximizes the biased welfare function.

We leverage the market's equilibria conditions to find an optimal false data injection attack on the bids. In this case, the attack raises the price offered by buyers, signaling a higher willingness to pay for energy. Particularly, the optimal attack modifies the original bid, adding a term proportional to the market clearing price and the attack's impact (the additional weight for the attacker in the biased social welfare). Roughly speaking, the adversary needs the market clearing price to regulate the impact of the attack; however, such information is unknown at the moment of the attack. For this reason, we approximate the attack using the clearing price from the previous period (we assume that the price does not change significantly within consecutive time periods). In this way, the adversary adapts its attack dynamically to the system's state.[8]

Figure 1 illustrates the operation of the market with an attack. First, buyers and sellers submit their bids (that is, demand and offer curves) to the ISO; however, an adversary modifies at its convenience the bids of buyers. Then every few minutes, the ISO measures the system state (current load) and computes the market equilibria (the best allocation of resources and the price) based on the bids received. Once the one hour period finishes, the ISO calculates the payments (settlement) for each agent that participated in the market.

This attack strategy has several advantages. First, the adversary can deny responsibility for the attacks because it is difficult to attribute authorship to cyberattacks. Second, attacks with a small impact can avoid detection and also prevent system failures that might damage the adversary's assets. Third, unlike other attacks that target sensors,[7] our adversary does not need detailed information about the physical structure of the power system (for example, the grid's topology) because the economic dispatch has taken that information into account to find the optimal operation. Fourth, the adversary needs neither to access the corporate network nor to compromise well-secured critical elements.

MITIGATION

It is difficult to deal with false data injection attacks that target bids. Cybersecurity mechanisms may fail because IoT devices, which allow remote access and control, often have poor security practices. Thus, although secure communications (such as encryption) protect the integrity of messages (that is, the bids), the attacker can still compromise the transactive controllers that submit them. Moreover, it is difficult to assess the bids' legitimacy because they change dynamically as a response to external factors (like the temperature or the user's needs). Hence, the system operator may fail to identify anomalies.

Since cyberattacks cannot be prevented, we propose a strategy to mitigate their impact. Concretely, we remove some of the bids that offer the highest prices to signal a lower need for energy. Thus, the mitigation strategy reduces the market clearing price to compensate for the effect of compromised bids. The auctioneer needs some information about the attack to select the appropriate number of bids to drop. In other words, the ISO must estimate the impact of an attack to design the corrective actions.

We assume that the auctioneer cannot identify the bids compromised and ignores their original values. However, we assume that the ISO has historical data about the bids and that it can estimate the proportion of compromised devices (such as through audits). With such information, we can estimate the impact of an attack, that is, the expected increment in the equilibrium quantity (the total energy traded). In the estimation, we assume worst-case scenarios because we ignore the precise attack on each bid. The ISO then chooses the number of bids to drop to correct the attack's effect.

VALIDATING TE MODELS

Validations of TE models face several challenges due to the complexity of the power grid infrastructure and uncertain behavior of customers. Although the theory of electricity systems and markets has a strong theoretical background, it is difficult to assess the performance of

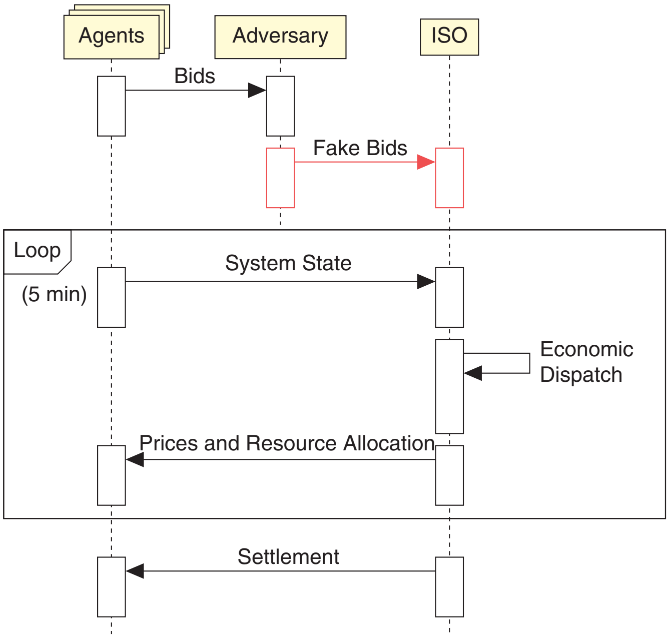

FIGURE 1. The operation of the RTM under attack.

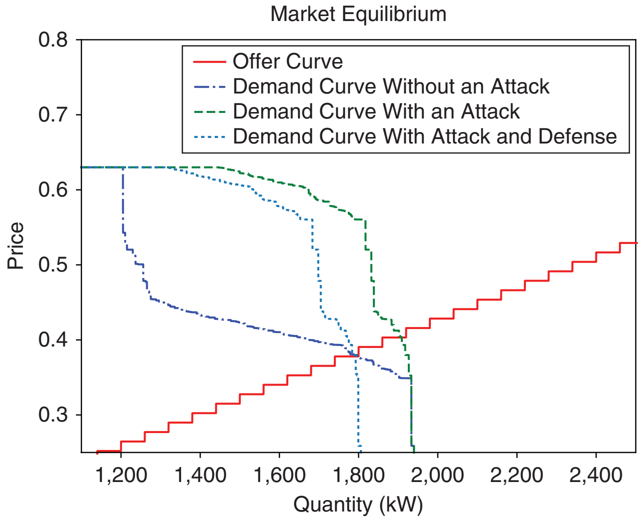

FIGURE 2. The attack increases both the price and production at the equilibrium (intersection of the offer and demand curves). The defense scheme moves the demand curve, compensating for the impact of the attack.

systems with many diverse components. For this reason, it is necessary to rely on detailed power systems simulators.

We use GridLAB-D[16] to simulate the operation of transactive controllers because it includes detailed models that take into account different factors, such as the energy price, weather, and customer's preferences. Moreover, GridLAB-D has been used to estimate the impact of pricing schemes and was also used to develop the transactive control system for the AEP Ohio gridSMART demonstration project.[17]

We developed a design studio that extends GridLAB-D to evaluate the resiliency of power grids against cyber and physical attacks.[9,18] The design studio provides a cloud-based graphical environment to edit and simulate power grid models. For each attack scenario, we schedule events that modify the attributes of objects according to the attack strategy. In our case, we create events that modify the bids of smart appliances. Since we define the attacks through the design studio, it is not necessary to modify or create modules within GridLAB-D.

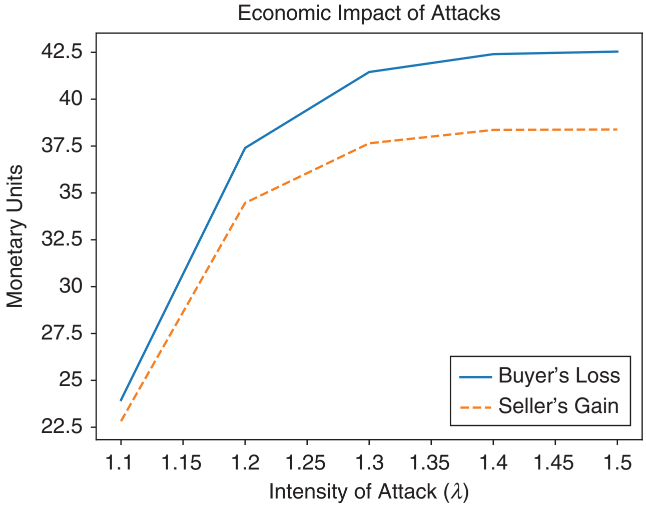

FIGURE 3. The economic impact of the attack for both customers and sellers as a function of the attack intensity λ. The customer's losses exceed the seller's benefit.

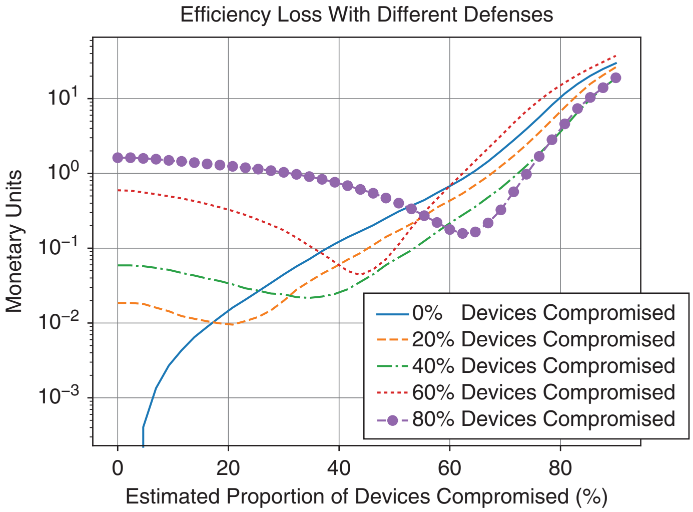

FIGURE 4. The efficacy of the defense scheme for different errors, estimating the proportion of devices compromised. The defense has the best performance with underestimations, but its efficacy decreases with the adversary's resources (number of devices compromised).

Market model

In an ideal market, the participants bid their supply or demand function; however, markets, in practice, restrict the form of the bids. For example, some markets assume that the cost functions are quadratic and allow bidders to choose some coefficients.[19] Likewise, GridLAB-D uses a simplified market model that accepts piecewise linear functions described with two quantities: the maximum capacity to either consume or produce energy and the unitary price accepted (or charged). The auction format restricts the adversary's strategies because it cannot send an arbitrary function. Nonetheless, the adversary still can implement a nearly optimal attack.

The transactive controllers report their current state in the bids. In particular, the controllers choose as the bid's quantity the current demand of their appliances, which approximates future demand. Furthermore, the bid's price is an estimation of the price necessary to maintain the current demand. Moreover, GridLAB-D assumes that the nonresponsive loads bid the maximum price allowed in the market.

EXPERIMENTAL RESULTS

We use the prototypical feeder R1-12.47-2 provided by the Pacific Northwest National Laboratory,[20] which represents a moderately populated area. Our distribution model has 570 commercial and residential loads that, in turn, incorporate appliances such as heating, ventilation, and air conditioning (HVAC) systems; water heaters; and pool pumps, among others. Moreover, we simulate weather from summertime in Nashville, Tennessee. The details of the market's structure are available in Neema et al.[9]

Impact of attacks

Figure 2 shows an example of the market's equilibria before and after an attack. The market equilibrium corresponds to the intersection between the demand and the offer curves, which guarantees that the total demand equals the total production. The offer curve corresponds to the marginal cost, while the demand curve corresponds to the marginal valuation. In this example, the adversary compromises 80% of HVAC systems and manages to raise prices and the total energy traded.

Figure 3 shows the economic impact of the attack as a function of the attack's intensity, that is, the weight used in the biased welfare function (denoted as λ). Observe that the adverse seller has positive gains, which increase with the attack's intensity; however, the damage to the customers exceeds the adversary's profit. As expected, the attack harms the social welfare because the adversary can benefit only by causing losses to other agents. Moreover, the adversary experiences diminishing marginal returns; that is, the attack's marginal benefit decreases as the intensity of the attack increases.

ABOUT THE AUTHORS

CARLOS BARRETO is a postdoctoral scholar at Vanderbilt University. His research interests include security and resiliency of cyberphysical systems, risk analysis, and game theoretic analysis of security problems. Barreto received a Ph.D. in computer science from the University of Texas at Dallas. He is Member of the IEEE. Contact him at carlos.a.barreto@vanderbilt.edu.

HIMANSHU NEEMA is a research assistant professor of computer science at Vanderbilt University. His research interests include heterogeneous simulation integration, modeling and simulation, cloud computing, model-integrated computing, design-space exploration, artificial intelligence, planning, and scheduling. Neema received a Ph.D. in computer science from Vanderbilt University. Contact him at himanshu.neema@vanderbilt.edu.

XENOFON KOUTSOUKOS is a professor with the Department of Electrical Engineering and Computer Science and a senior research scientist with the Institute for Software Integrated Systems, Vanderbilt University. His research is in the area of cyberphysical systems with an emphasis on security and resilience, control, diagnosis and fault tolerance, formal methods, and adaptive resource management. Koutsoukos received a Ph.D. degree in electrical engineering from the University of Notre Dame. He is a Fellow of the IEEE. Contact him at xenofon.koutsoukos@vanderbilt.edu.

Efficacy of the defense

Figure 2 shows an example of market equilibrium with the proposed defense scheme (we assume that the ISO knows the precise proportion of devices compromised). This example illustrates that our defense moves the demand curve to the left to compensate for the actions of the adversary. Now, let us evaluate the impact of estimation errors in the efficacy of the defense scheme. Figure 4 shows the social welfare loss when the mitigation strategy has errors in terms of estimating the number of devices compromised. We find that the defense cannot completely prevent the damage of the attack, and its efficacy decreases with the adversary's resources (number of devices compromised). The defense has the worst performance when the estimations exceed the real values because, in these cases, all bidders incur losses. Conversely, the best performance occurs with underestimations.

This work shows how an adverse generator can profit by compromising customer devices that participate in electricity markets (such as transactive controllers). Specifically, the adversary designs a false data injection attack on bids that changes the market's equilibria to its advantage. We propose a mitigation strategy that drops some of the bids to correct the impact of the attack. This strategy requires some information about the attack (such as number of devices compromised) to choose the appropriate number of bids to drop. In this article, we observe that the best performance occurs with underestimations. We validate our attack model and defense on a distribution system simulated in GridLAB-D. We designed some tools to extend GridLAB-D and facilitate resiliency analysis of power grids against attacks (both cyber and physical). C

REFERENCES

1. S. Hasan, A. Dubey, G. Karsai, and X. Koutsoukos, "A game-theoretic approach for power systems defense against dynamic cyber-attacks," *Int. J. Electr. Power Energ. Syst.*, vol. 115, p. 105432, 2020. doi: 10.1016/j.ijepes.2019.105432.
2. G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, July 2017. doi: 10.1109/TSG.2015.2495133.
3. K. Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," *WIRED Magazine*, Mar. 2016. [Online]. Available: http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
4. S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Security Symp. (USENIX Security 18)*, Baltimore, 2018, pp. 15–32.
5. B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks," in *Proc. 28th USENIX Security Symp. (USENIX Security 19)*, Santa Clara, CA, Aug. 2019, pp. 1115–1132.
6. C. Barreto and A. Cardenas, "Impact of the market infrastructure on the security of smart grids," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4342–4351, 2019. doi: 10.1109/TII.2018.2886292.
7. L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011. doi: 10.1109/TSG.2011.2161892.
8. C. Barreto and X. Koutsoukos, "Attacks on electricity markets," in *Proc. 57th Annu. Allerton Conf. Communication, Control, and Computing (Allerton)*, Sept. 2019, pp. 705–711. doi: 10.1109/ALLERTON.2019.8919711.
9. H. Neema, H. Vardhan, C. Barreto, and X. Koutsoukos, "Web-based platform for evaluation of resilient and transactive smart-grids," in *Proc. 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Apr. 2019, pp. 1–6. doi: 10.1109/MSCPES.2019.8738796.
10. P. Siano, "Demand response and smart grids: A survey," *Renew. Sustain. Energ. Rev.*, vol. 30, pp. 461–478, Feb. 2014. doi: 10.1016/j.rser.2013.10.022.
11. K. Kok and S. Widergren, "A society of devices: Integrating intelligent distributed resources with transactive energy," *IEEE Power Energy Mag.*, vol. 14, no. 3, pp. 34–45, May 2016. doi: 10.1109/MPE.2016.2524962.
12. "The cyberthreat handbook," Verint–Thales, Tech. Rep., 2019. [Online]. Available: https://www.thalesgroup.com/sites/default/files/database/document/2019-10/Press_kitEN_0.pdf
13. A. Greenberg, "How power grid hacks work, and when you should panic," *WIRED Magazine*, Oct. 13, 2017. [Online]. Available: https://www.wired.com/story/hacking-a-power-grid-in-three-not-so-easy-steps/
14. I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 2018. doi: 10.1109/COMST.2018.2855563.
15. B. Krebs, "Who is Anna-Senpai, the Mirai Worm author?" *Krebs on Security*, Jan .2017. [Online]. Available: https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
16. D. P. Chassin, K. Schneider, and Gerkensmeyer, "GridLAB-D: An open-source power systems modeling and simulation environment," in *Proc. IEEE/PES Transmission and Distribution Conference and Expo.*, 2008, pp. 1–5. doi: 10.1109/TDC.2008.4517260.
17. S. E. Widergren et al., "AEP Ohio gridSMART demonstration project real-time pricing demonstration analysis," Pacific Northwest National Lab. (PNNL), Richland, WA, Tech. Rep., 2014. [Online]. Available: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23192.pdf
18. "GridLAB-D design studio: In a nutshell," Cyber-Physical Systems Virtual Organization (CPS-VO), 2019 [Online]. Available: https://cps-vo.org/group/gridlabd
19. R. Baldick, "Electricity market equilibrium models: The effect of parametrization," *IEEE Trans. Power Syst.*, vol. 17, no. 4, pp. 1170–1176, 2002. doi: 10.1109/TPWRS.2002.804956.
20. K. P. Schneider, Y. Chen, D. P. Chassin, R. G. Pratt, D. W. Engel, and S. E. Thompson, "Modern grid initiative distribution taxonomy final report," Pacific Northwest National Lab., Richmond, WA, Tech. Rep., 2008. [Online]. Available: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-18035.pdf