ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152www.ijmece .com

Vol 5, Issue 2 April 2017

Cyber-Attacks and Mitigation in Blockchain Based Transactive Energy Systems

Asra Sultana, Syed Bader Anwar, N. Naresh Kumar

Abstract

Due to the quick uptake of erratic renewable energy sources and the expansion of energy storage technology, considerable adjustments are being made to power networks. These developments prompt smart-grid operators to think about a time when microgrids might be used for peer-to-peer energy trading, giving rise to Transactive Energy Systems. Due in large part to their high level of robustness, blockchains have attracted considerable interest from both academia and industry for its possible application in decentralised TES. The gateways that link market players to the system are the target of a novel class of attacks against blockchain-based TES that we introduce in this research. We present a broad model of TES built on blockchain technology and investigate various threat models and assault tactics. We also show how these attacks have an impact.

Index Terms

Transactive Energy System, Blockchain, Cybersecurity, Cyber-Physical System, Denial of Service, Microgrid

INTRODUCTION

Major adjustments are being made to power networks as a result of the quick adoption of erratic renewable resources (such wind and solar), together with energy storage technologies (e.g., residential batteries and electric vehicles). Additionally, Internet of Things (IoT) devices improve load and energy resource management. Due to their dual ability to create and consume energy, household users, also known as prosumers, have more capabilities thanks to these trends. In the future, prosumers will trade energy or services directly, increasing the effectiveness and dependability of power systems. Thus, future grids will use Transactive Energy Systems (TES) as a distributed management approach in which smart appliances or Internet of things (IoT) devices participate autonomously in electricity markets [1]. with a central entity, which collects bids and returns the energy price (and the transactions among participants). Centralized markets suffer from a single point of failure, because they rely on a single trusted entity to operate the market. Decentralized markets based on blockchains offer several desirable properties in energy applications. First, prosumers interact without intermediaries and conflicts are resolved through protocols. Second, transactions that have been recorded on the blockchain are immutable and publicly auditable by design. Third, the blockchain is fault tolerant, that is, it can operate even if some of the prosumers fail or act maliciously. These properties can ensure market transparency, as well as the availability of detailed information about the system. More recent blockchain implementations, such as Ethereum [2], also enable trustworthy computations through smart contracts [3]. Based on this functionality, these blockchains can implement various data verification and market clearing mechanisms for TES [4].

Asst. Professor[1,2,3]
Department of EEE

asrasultana205@gmail.com, baderanwarsyed@gmail.com, nnareshk@gmail.com

ISL Engineering College.

International Airport Road, Bandlaguda, Chandrayangutta Hyderabad - 500005 Telangana, India.

For example, smart contracts can enforce commitments as well as transfer of assets between peers. One benefit of blockchain based TES is resilience: to disrupt the integrity of the market (e.g., tamper with bids or with the clearing mechanism), an attacker needs to compromise a large number of blockchain nodes. A blockchain based system can also resist availability attacks, since the market remains operational even with many unavailable nodes [5]. However, some attacks may degrade the operation of the system. In practice, IoT devices lack resources required for participating in the computing-intensive consensus algorithms of many blockchains. Thus, prosumers have to connect to a blockchain-based system through gateway nodes; however, an adversary can attempt to "cut off" prosumers from the system by targeting these gateway nodes. For example, an adversary can launch a (distributed) denial of service (DDoS) attack against a gateway node to prevent a set of bids from arriving at the market, which change the market's equilibria. In this paper, we study blockchain based Transactive Energy Systems and introduce a novel class of attacks that target the gateways between prosumers and the system.

The following are our main contributions:

- We formulate a general model of blockchain based transactive energy systems, which includes both infrastructure and market mechanisms.

- We introduce a previously unconsidered class of attacks, which discard or delay trading bids. Our threat model includes three scenarios, which consider distinct capabilities and knowledge for the adversary.

- We study attack strategies for each scenario. We also discuss how to mitigate these attacks by taking advantage of the distributed nature of the system.

RELATED WORK

Recent cyber attacks against critical infrastructure, such as the attacks on the Ukrainian power grid in 2015 and 2016 [8], have motivated multiple research efforts to protect critical infrastructures, in particular, the power grid [9]. Prior works have shown how false data injection (FDI) attacks can modify sensor measurements to induce errors in a power system's operation [10], [11]. With a careful design, these attacks can damage the system or change the electricity prices. An adversary can also affect forecast systems, which are used to plan the power-system operation, by exploiting vulnerabilities of artificial intelligence models [12], [13]. In most cases, FDI attacks need information about the state of the system or the models used for making decisions (e.g., the system's state, its topology, or prediction models). However, some attacks leverage the market's infrastructure to bypass these restrictions. For example, an adversary that compromises bids can induce changes in the market's equilibria without knowing details of the system [14], [15]. DDoS attacks represent a significant threat for distributed electricity markets, because an adversary needs minimal knowledge (and resources) to mount attacks. Furthermore, with these attacks, it is extremely difficult to determine the identity of the adversary. For example, [16] reported that a company specializing in protection against DDoS attacks coauthored the Mirai malware to attack some of its customers. New technologies, such as Internet of Things (IoT) devices, introduce vulnerabilities for the power grid [17], [18]. As a result, adversaries can target customer-side components, such as smart meters, appliances, end-user generation systems (e.g., solar panels), and electric vehicles, to affect the power system's operation [19]. For example, adversaries can compromise IoT devices to change their bids [15].

SYSTEM MODEL

In this section, we present our system model for a decentralized TES. We make some assumptions based on the inspection of various industrial implementations of decentralized TES, such as LO3 [20] and Power Ledger [21], and scientific articles, such as Laszka et al. [22], [23] and Worner ¨ et al. [24]. A. Infrastructure Fig. 1 shows the overall architecture of the decentralized TES. Below we describe each component.

Prosumers:

Agents that can both produce and consume energy, e.g., residential users with solar panels or electric vehicles. Prosumers have both unresponsive and responsive loads. Responsive loads, such as heating, ventilation, and air conditioning (HVAC) systems can adjust their load to reduce costs (e.g., store energy in thermal form anticipating high energy prices). On the contrary, unresponsive loads do not change their consumption regardless of the prices (the flexibility of loads can change throughout the day). Prosumers express their intention (and conditions) to trade energy through bids. We represent a bid as the following tuple:

$$\langle \tau, \sigma, \pi \rangle,$$

where τ specifies the time interval in which energy exchange can occur; σ indicates the maximum amount of energy available to trade; and π denotes the reservation price (minimum or maximum price accepted by sellers or buyers, respectively). We assume that prosumers cannot change their bills by tampering the meters that measure their physical energy flow

Blockchain based Electricity Market:

A blockchain is a distributed ledger, this means that multiple nodes have a copy of the transactions. Special nodes (called miners) decide the state of the distributed ledger (e.g., the transactions) through a consensus protocol, which induces a high cost to modify the ledger e.g., Proof of Work (PoW) [7], [25] and Proof of Stake (PoS) [26]. The blockchain creates a chainlike data structure in which each block has a reference to previous blocks; in this way, the transactions recorded become practically immutable. Thus, blockchains provide trustworthy data storage and computation (in the form of smart contracts) without requiring a trusted entity.

Gateways:

Prosumers may not participate directly in the blockchain network, because consensus protocols typically have high computational and storage requirements, which IoT based energy trading devices cannot satisfy. Hence, prosumers may access the distributed energy market through gateway nodes. A gateway either forwards messages between the prosumers and the distributed energy market or acts as miner, whuch execute the blockchain consensus protocol. To protect the prosumers' privacy, the communication between prosumers and gateways may be encrypted and anonymized, as described in [27]. Gateways can be operated by the company that implements the TES or by a third party.

Distribution System Operator (DSO):

Besides the information infrastructure, the system needs a continuous management of the physical infrastructure. In this case, we assume that a DSO supervises the system and is responsible for managing the distribution grid, billing, installing smart meters, satisfying the net demand, and maintaining stability [28]. Although we refer to the DSO as the system's manager, other entities, such as electric utilities, can be in a better possition to provide these services.

THREAT MODEL

In this section we describe the adversary's capabilities, its goal, and attack strategies. A. Adversary's Capabilities We assume that the adversary cannot tamper with or remove bids accepted by the market, and it cannot tamper with or disrupt the market clearing mechanism (the blockchain guarantees that this requires a large amount of resources). However, the adversary— who may be one of the prosumers— can read past bids and clearing prices from the blockchain. Blockchains can suffer from several vulnerabilities, some of which lead to thefts of cryptocurrencies or public keys [34]. An adversary may leverage these vulnerabilities to tamper with the prosumers' bids. For example, an adversary may steal the public keys of prosumers to forge bids or compromise smart appliances or transactive controllers to modify their bidding strategies. However, it may be much easier to compromise a single node that is acting as a gateway for a group of prosumers, than attacking multiple prosumers individually. For example, the adversary can exploit bugs in the Ethereum software to either bypass authentications or to disable miners [35]. We consider three attack scenarios against miners that differ in the adversary's knowledge and capabilities of (see Table I for a summary). 1) Gateway Confidentiality and Integrity Attack: The adversary compromises a gateway and obtains sufficient access to delay or discard particular bids (i.e., prevent them from being recorded on the market). In this scenario, the adversary is also capable of reading all bids before deciding which bids to discard (e.g., by reading the bids submitted to the compromised gateway as well as the ones recorded on the blockchain by other gateways). 2) Gateway Integrity Attack: The adversary can discard or delay selected bids; however, the adversary must decide which bids to discard without complete information, relying only on historical data about the prosumers' past bids. 3) Gateway Availability Attack: The adversary cannot delay particular bids, but it has sufficient resources to launch a DDoS attack against one of the gateways. This attack prevents the processing of some bids in the market, but the adversary cannot read bids either.

Adversary's Goal

We consider a rational, profit-oriented adversary, who is interested in maximizing its own profit. The adversary's goal and strategy depend on its role (e.g., generator or consumer). We focus our attention on adverse generators, who discard(or delay) the bids of prosumers. Concretely, we assume that adverse generators pursue a market equilibria (q a , pa) that increases the generator's profit by λ%. We express this condition as

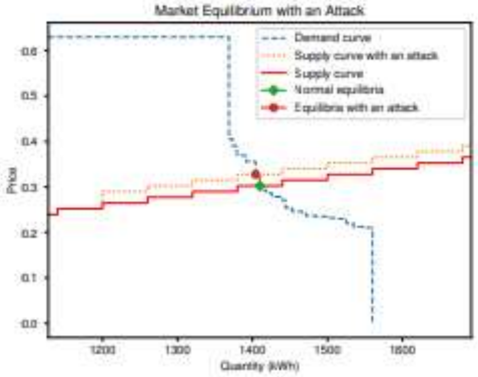
$$\sum_{j\in\mathcal{G}} u_j(q_j^a, p^a) = \sum_{j\in\mathcal{G}} (1+\lambda) u_j(q_j^*, p^*).$$

ANALYSIS

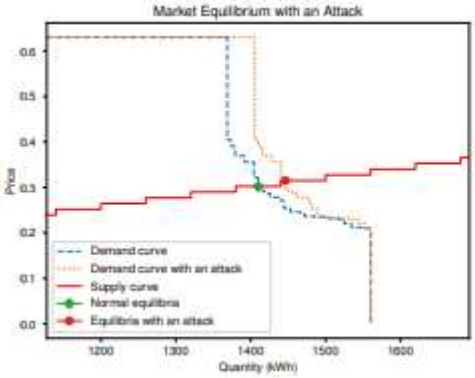
In this section, we discuss strategies that an adversary may use to increase its profit, given the capabilities that we assumed in Section IV-A. Then, we discuss strategies for mitigating such attacks.

Attack Strategy

An adverse generator benefits from delaying the bids of prosumers if the resulting market equilibrium increases its profit. Fig. 3 shows how a delay attack on either buying or selling bids changes the equilibrium. In a double auction, the offer and demand curves capture the trades (price and quantity) that buyers and sellers would accept. Their intersection corresponds to the market equilibrium, a condition in which no prosumer would change its trades. Delays in bids of competing generators (who offer lower prices) forces the market to procure energy from more expensive generators, which raises the prices (Fig. 1a illustrates this). We leave the analysis of such attacks to future work. The demand curve is constructed with bids ordered by descending price. In our case, the DSO constructs bids for the estimated unresponsive loads, which accept the maximum price allowed in the market. The demand curves in Fig. 1 have flat regions corresponding to bids of unresponsive loads. The decreasing regions correspond to the bids of responsive loads. Delays in buyers' bids can also benefit the adversary, because missing bids may lead to overestimation of the unresponsive loads. In other words, the DSO may assume that the appliances that do not submit bids will accept any price. In such cases, the demand curve changes reflecting a higher willingness to pay for energy, which raises the prices (see Fig. 1b). Next, we analyze this attack in the three scenarios that we introduced in Section IV-A.



Market equilibria when delaying the bids of generators.



Market equilibria when delaying the bids of consumers.

Fig. 1: An adverse generator can increase the market's equilibria price delaying bids of both buyers and seller

Confidentiality and Integrity Attack:

In this scenario, the adversary can collect all the bids submitted to the compromised gateway, and read the bids submitted to the other gateways. Hence, it can compute the market's clearing price p ∗ and the total energy traded Q∗ . The adversary uses thesevalues to calculate the desired deviation in the trades ΔQa (see Eq. (5)). Then, it selects a subset of bids V such that.

$$\sum\nolimits_{v\in\mathcal{V}} q_v^* \approx \Delta Q^a .$$

In practice the impact of the attack will be lower than ΔQa , because some appliances may reduce their load as a response to higher prices. This is an ideal scenario for the adversary, since it is able to discard bids possessing complete information about the market. Further, this scenario allows the adversary to determine which gateway is the optimal target for the attack

EXPERIMENTAL EVALUATION

Testbed Implementation

For experimental evaluation, we deployed GridLAB-D [39] and a private Ethereum blockchain network [2]. GridLAB-D simulates the smart grid, including prosumer logic for creating bids. GridLAB-D models retail markets through double auctions [31] that run every five minutes. Our power system has 58 residential commercial houses, which in turn incorporate appliances such as heating, ventilation, and air conditioning (HVAC) systems. GridLAB-D models the response of the loads to weather and market's prices, giving realism to the simulations. In this case, transactive controllers manage HVAC systems and make bids in the market. The blockchain stores bids, market clearing prices, and calculates the market equilibria with a smart contract. We built our testbed on the open-source TRANSAX framework [22], which provides the prosumer interfaces and a smart contract. Each prosumer is assigned to one of three Ethereum clients, which act as gateways to the private Ethereum network. Based on the prosumers' allocation, the attacker chooses one of the Ethereum clients to attack, and delays a subset of the bids sent to that client. Since each bid is valid for a single interval, this in effect discards the bids.

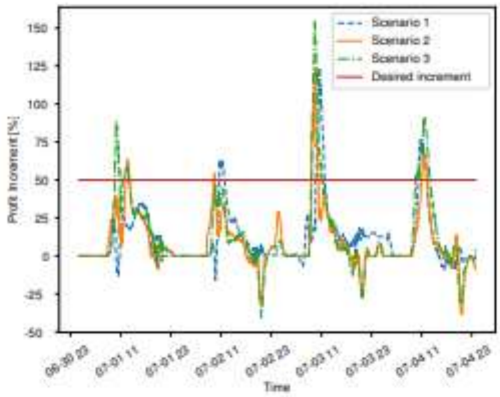


Fig. 2: Impact of attacks (snapshot of five days, from July 1 at 00:00 to July 5 at 00:00).

CONCLUSION

In this study, we looked at blockchain-based TES, which have recently drawn a lot of interest because of their special ability to provide integrity and resilience in decentralised systems. We developed a brand-new category of cyberattacks that target the interface between prosumers and the system rather than the trading system directly. We discovered that even more straightforward assaults, such (D)DoS, can successfully tamper with a market's clearing price based on blockchain technology. We have nevertheless shown that the threat can be reduced through detection and gateway switching. We assessed the impact of these attacks experimentally using a testbed based on GridLAB-D and a private Ethereum network. In the future, we will extend our analysis to consider proactive defenses (e.g., through random selection of gateways), more sophisticated attack detection, and cyber-attacks on individual prosumers (i.e., compromising their IoT devices)

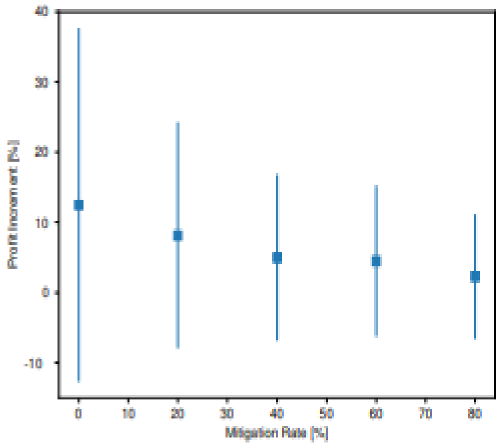


Fig. 3: Gateway Availability Attack: Attacker chooses a gateway and executes a (D)DoS attack, resulting in some random subset of bids being discarded.

REFERENCES

[1] K. Kok and S. Widergren, "A society of devices: Integrating intelligent distributed resources with transactive energy," IEEE Power and Energy Magazine, vol. 14, no. 3, pp. 34–45, 2016.

[2] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project – Yellow Paper, Tech. Rep. EIP-150, April 2014.

[3] A. Mavridou, A. Laszka, E. Stachtiari, and A. Dubey, "VeriSolid: Correct-by-design smart contracts for Ethereum," in 23rd International Conference on Financial Cryptography and Data Security (FC), February 2019, pp. 446–465.

[4] N. Wang, X. Zhou, X. Lu, Z. Guan, L. Wu, X. Du, and M. Guizani, "When energy trading meets blockchain in electrical power system: The state of the art," Applied Sciences, vol. 9, no. 8, p. 1561, 2019.

[5] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in 2017 Resilience Week (RWS). IEEE, 2017, pp. 18–23.

[6] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, "GridLAB-D: An open-source power systems modeling and simulation environment," in 2008 IEEE/PES Transmission and Distribution Conference and Exposition. IEEE, 2008, pp. 1–5.

[7] V. Buterin et al., "Ethereum white paper," 2013.

[8] K. Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," WIRED Magazine, March 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunningunprecedented-hack-ukraines-power-grid/

[9] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 13–27, 2016.

[10] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2011, pp. 5952–5955.

[11] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 659– 666, 2011.

[12] Y. Chen, Y. Tan, and B. Zhang, "Exploiting vulnerabilities of load forecasting through adversarial attacks," in 10th ACM International Conference on Future Energy Systems (e-Energy), 2019, pp. 1–11. [13] C. Barreto and X. Koutsoukos, "Design of load forecast systems resilient against cyber-attacks," in 10th Conference on Decision and Game Theory for Security (GameSec), 2019, pp. 1–20.

[14] C. Barreto and A. Cardenas, "Impact of the market infrastructure on the security of smart grids," IEEE Transactions on Industrial Informatics, pp. 1–1, 2018.

[15] C. Barreto and X. Koutsoukos, "Attacks on electricity markets," in 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton). IEEE, 2019.

[16] B. Krebs, "Who is Anna-Senpai, the Mirai Worm Author?" Krebs on Security, 2017, accessed: October 23rd, 2019. [Online]. Available: https://krebsonsecurity.com/2017/01/who-is-anna-senpai-themirai-worm-author/

[17] 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 Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3453–3495, 2018.

[18] W. Chin, W. Li, and H. Chen, "Energy big data security threats in iotbased smart grid communications," IEEE Communications Magazine, vol. 55, no. 10, pp. 70–75, Oct 2017. [19] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in 27th USENIX Security Symposium. Baltimore, MD: USENIX Association, 2018, pp. 15–32.

[20] L. Energy, "Exergy-building a robust value mechanism to facilitate transactive energy," LO3. Retrieved March, vol. 29, p. 2019, 2017.