Cyber-Physical Simulation Platform for Security Assessment of Transactive Energy Systems

Yue Zhang*, Scott Eisele†, Abhishek Dubey†, Aron Laszka‡, Anurag K. Srivastava*
*Washington State University
†Vanderbilt University
‡University of Houston

Published in the proceedings of the 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES 2019).

***Abstract*—Transactive energy systems (TES) are emerging as a transformative solution for the problems that distribution system operators face due to an increase in the use of distributed energy resources and rapid growth in scalability of managing active distribution system (ADS). On the one hand, these changes pose a decentralized power system control problem, requiring strategic control to maintain reliability and resiliency for the community and for the utility. On the other hand, they require robust financial markets while allowing participation from diverse prosumers. To support the computing and flexibility requirements of TES while preserving privacy and security, distributed software platforms are required. In this paper, we enable the study and analysis of security concerns by developing Transactive Energy Security Simulation Testbed (TESST), a TES testbed for simulating various cyber attacks. In this work, the testbed is used for TES simulation with centralized clearing market, highlighting weaknesses in a centralized system. Additionally, we present a blockchain enabled decentralized market solution supported by distributed computing for TES, which on one hand can alleviate some of the problems that we identify, but on the other hand, may introduce newer issues. Future study of these differing paradigms is necessary and will continue as we develop our security simulation testbed.**

***Index Terms*—Cyber-attacks, Transactive Energy Systems, Cyber-Physical Security, Simulation Platform, Testbed.**

I. Introduction

Transactive energy systems (TES) have emerged as an anticipated outcome of the shift in the electricity industry, moving from centralized, monolithic business models characterized by bulk generation and one-way delivery, toward a decentralized hierarchical model in which end-users can play a more active role in both energy production and consumption [1], [2]. In the U.S., 36% of electricity demand is from single-family houses, which can contribute an even larger share during summer peak due to the usage of air-conditioning [3]. The development of smart home devices enables the deployment of TES to provide a more efficient and secure solution. There are a number of well-documented factors contributing to this shift, including the increasing penetration of distributed energy resources, growing number of control variables in the active distribution system, increasing deterioration and fragility of the existing grid, the regulatory and public mandate for environmental awareness, and general social trends toward the democratization of services as exemplified by the "sharing economy" [4].

TES involving responsive load and distributed generators have received significant attention in the literature. In [3], a transactive control approach is proposed to coordinate heating, ventilation, and air-conditioning systems to reduce load consumption. A distribution locational marginal pricing (DLMP) algorithm is developed to provide a price signal to relax congestion issues in systems with electric vehicles that can act as prosumers in [5]. A coordination method that can manage energy imbalance problems considering thermostatically controllable load is presented in [6]. An automated decentralized control scheme is introduced to provide ancillary and demand response services in [7]. A TES that could maximize resource utilization and balance demand and supply is proposed in [8], [9]. A TES that allows direct control of unit consumption through an aggregator is introduced in [10]. A double-auction market scheme that utilizes transactive controllers to operate the distribution system is designed in [11].

The transactive market can be implemented with multiple possible architectures. Most of the architecture will be hierarchical and can have alternate architecture at a different voltage level. Prosumers can coordinate with aggregators or campus grid, and aggregators/campus grid can coordinate with distribution system operators. DSO can coordinate with transmission system operators to optimize resources in the best possible way. We consider two different architectures: 1) hierarchical with centralized market clearing and 2) hierarchical with a mix of centralized and distributed market clearing enabled by enhanced communication. First architecture is well explored in literature but not much for security analysis. Information exchange between prosumers and a system operator or aggregators happens through a large number of distributed edge-computing and Internet of Things (IoT) devices. TES communication is conducted with digital infrastructure and requires interfacing with edge-devices, which have possible vulnerabilities and attacks especially with financial interest motives. The main actors are the consumers, which comprise primarily residential loads and prosumers who also have distributed energy resources (DERs), such as rooftop solar batteries or flexible loads capable of demand/response. Additionally, a distribution system operator (DSO) manages the network with possible additional interface with microgrid operator or campus grid operators and with prosumers directly

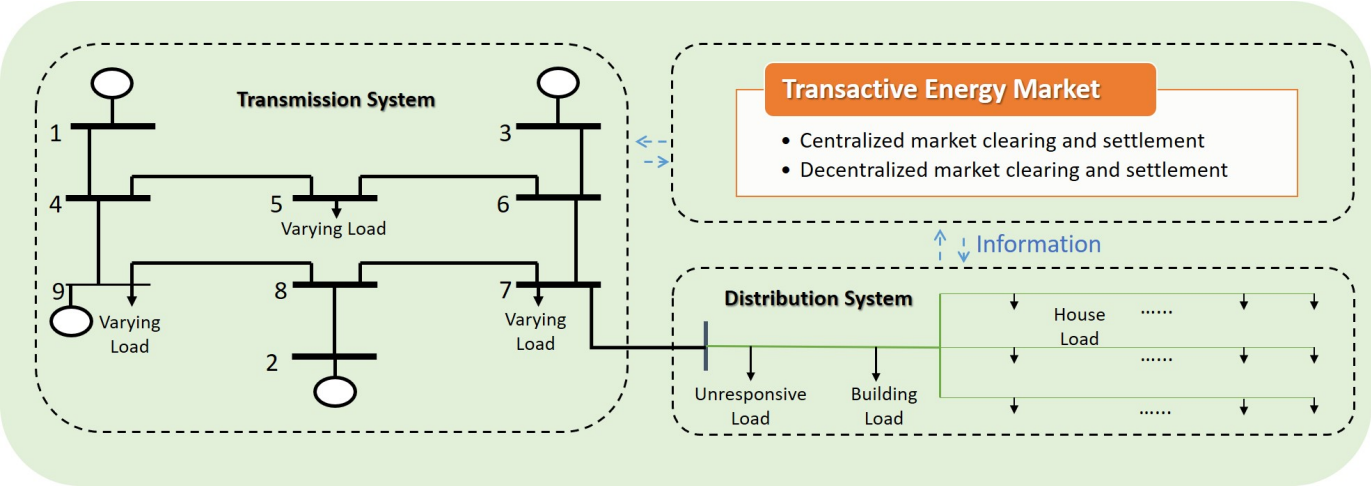

Fig. 1. Architecture of TESST.

or through aggregators.

For second architecture, such installations are equipped with an advanced metering infrastructure consisting of TE-enabled smart meters. In addition to the standard functionalities of smart meters (i.e., the ability to measure line voltages, power consumption and net metering, and to communicate these to the distribution system operator), TE-enabled smart meters are capable of communicating with other smart meters, have substantial onboard computational resources, and are able to access the Internet and cloud computing services as needed. Examples of such installations include the well-known Brooklyn Microgrid Project, [12] and the Sterling Ranch learning community (currently under development) [13].

The research community is increasingly advocating the use of distributed ledgers in TES, including our earlier work [14]. Blockchain technology enables the digital representation of energy and financial assets and their secure transfer from one set of parties to another. By design, the security of this value transfer is guaranteed by the interaction protocol itself and obviates the need for trusted transaction intermediaries. The execution of smart contracts (i.e., code that captures the market logic and participants' roles) is automated and guaranteed [15], [16]. Additionally, the blockchain constitutes an immutable, complete, and fully auditable record of all transactions that have occurred within the system. These properties ensure market transparency, as well as the availability of a detailed market load profile and grid utilization data.

Problem: In this paper, we specifically consider the problem of security in a transactive energy system. Unlike traditional power grid operation, the participation of the prosumers at the edge raises several concerns. The first concern is privacy: if private data is stored in a way that is easily accessible to unauthorized entities, it can leak private information. Consider that the transaction level data can provide much greater insights into a prosumers behavior compared to smart meter data [17]. Similarly, the market is an integral part of a TES. Hence, it is important that the market remains fair and cannot be manipulated. Consider the problem of a set of prosumers promising to supply energy at a lower bid and then choosing not to supply the power at the scheduled time.

Contributions: To systematically study these adverse scenarios, we must have access not only to a power system simulator but also to a system that can simulate market mechanisms, including distributed ledgers if they are integrated. In this paper, we build on the transactive energy simulation platform (TESP) developed by the Pacific Northwest National Lab (PNNL). We extended the TESP platform to study security scenarios by incorporating different attacks. We call this testbed the *Transactive Energy Security Simulation Testbed* (TESST). We highlight weaknesses in TES with a hierarchical and centralized market clearing system. Then, we discuss how some of these problems can be alleviated by the use of a decentralized market solution based on our earlier work [14]. Future work includes detailed security analysis for the ledger enabled TESP and integrating a suite of attack scenarios that can be used by the research community.

II. TESST: TES Testbed for Cyber Attack Simulation

Transactive Energy Security Simulation Testbed (TESST) is built upon the Transactive Energy Simulation Platform (TESP) by PNNL and TRANSAX designed by Vanderbilt University [14], [17]. The TESP platform is interfaced with Network Simulator 3 (NS3) to simulate cyber attacks on the TES [18], [19] (please see Figure 1).

A. Physical System

The physical system includes a modified IEEE 9 bus system and a distribution feeder connected at bus 7. The transmission system is modeled in PyPower and includes four fossil based generating units. The cost of the unit connected at bus 9 is higher than the other units. There are also three varying loads connected at buses 5, 7 and 9. The distribution system is modeled with Gridlab-D and EnergyPlus. In this distribution

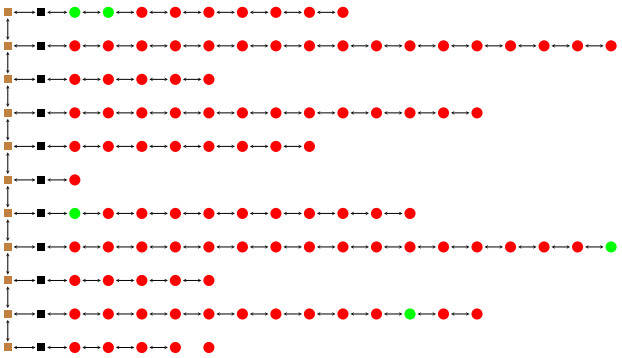

Fig. 2. Feeder diagram. Brown nodes are feeder junctions, numbered 1 to 11 from top to bottom. Black nodes are the overcurrent relays, which ensure that the total power flowing in and out of the feeder is below 20 kW. The green nodes are the junction points for the producers (5), and the red nodes are junction points for the consumers (97). There are 102 prosumers in total.

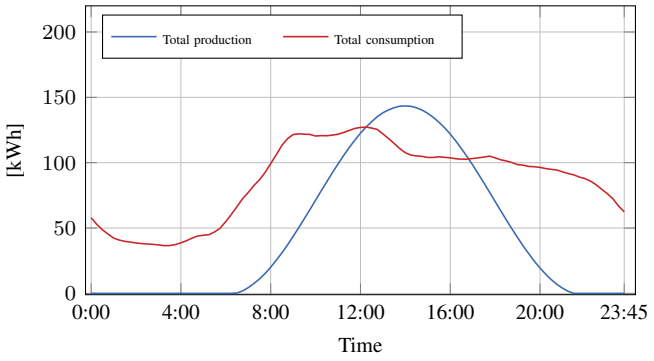

Fig. 3. Load profile (i.e., total consumption) and generation profile (i.e., total production) in kWh per 15 minute interval aggregated across the microgrid.

feeder, the 1.3MW unresponsive load is connected at 12.47KV voltage level. The building load is also connected to that voltage level through a 12.47kV/480V transformer. There are also 30 houses that are equipped with PV panels and Heating, Ventilation, and Air Conditioning (HVAC) systems, which are connected to the feeder through a 7200V/120V transformer. Moreover, a microgrid that containing 102 homes across 11 feeders (5 producers and 97 consumers) is also built. The feeder structure and its safety limits are plotted in Fig. 2.

B. Transactive Energy Market

Two trading options are designed for the TESST. The transactive energy market has one option with a centralized market clearing and settlement and the second has decentralized market clearing and settlements.

1) Centralized Market Option: The centralized option utilizes a double-auction market mechanism and aims to provide a trading platform for prosumers in both transmission and distribution systems. Both suppliers and consumers submit their bids to the TES management platform, and the market uses the auction to determine the clearing price which is published through the network to all participants.

The consumer bids are from smart HVAC controllers, which will adjust bid price and quantity based on the most recent

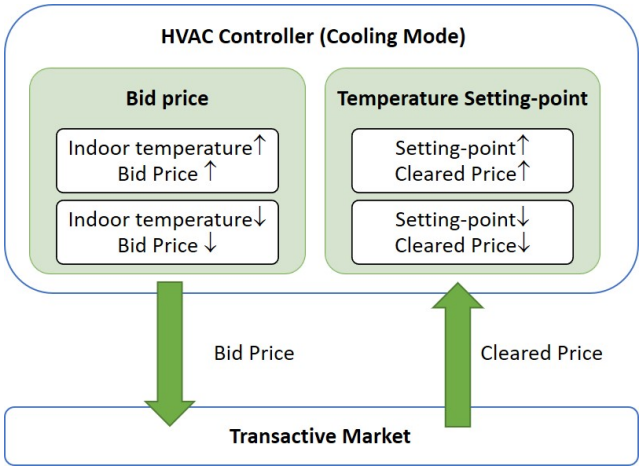

Fig. 4. Smart HVAC controller mechanism in cooling mode.

cleared price and the average and standard deviation of the cleared price over the preceding 24 hours. They can also adjust the temperature settings to earn more savings. For example, the adjustment process under cooling mode is described in Figure 4. The smart HVAC controller will adjust bid based on current temperature and adjust temperature setting based on current cleared price using the following two equations:

$$T_{\text{Set}} = T_{\text{Target}} + \frac{(P_{\text{Clear}} - P_{\text{Mean}}) \cdot |T_{max/min}|}{\sigma_T \cdot \sigma_P} \quad (1)$$

$$P_{\text{Bid}} = P_{\text{Mean}} + \frac{(T_{\text{Current}} - T_{\text{Target}}) \cdot \sigma_T \cdot \sigma_P}{|T_{max/min}|} \quad (2)$$

where T_{Set} is the new adjusted temperature setpoint; T_{Target} is the target temperature setpoint; P_{Clear} is the received cleared price; P_{Mean} is the average price over the last 24 hours; T_{max} and T_{min} are the maximum and minimum acceptable temperature; σ_T and σ_P are the standard deviation of temperature and price, respectively; P_{Bid} is the bid price from HVAC controller; T_{Current} is the current air temperature.

If the received cleared price is higher than the threshold, the temperature setpoint is moved to a higher value to decrease electricity consumption. Otherwise, the setpoint is moved to a lower value to gain a higher comfort level. The bid price is determined by the current air temperature. For example, on a hot day, if the temperature is very high, the HVAC controller will select a high bid price to increase the chance of acceptance for its bid. The smart HVAC controllers also utilize the average price information to adjust consumption patterns more efficiently to avoid frequently changing the setting for short-term variation.

2) Decentralized Market Option: The decentralized option utilizes a decentralized middleware called Resilient Information Architecture Platform for Smart Grid (RIAPS) [20] to create a framework for decentralized energy trading.

The actors and high-level data-flow of this platform can be seen in Figure 5. The typical workflow begins with producers and consumers of power (1) posting offers to the distributed ledger, offering to sell or buy energy for a time interval in

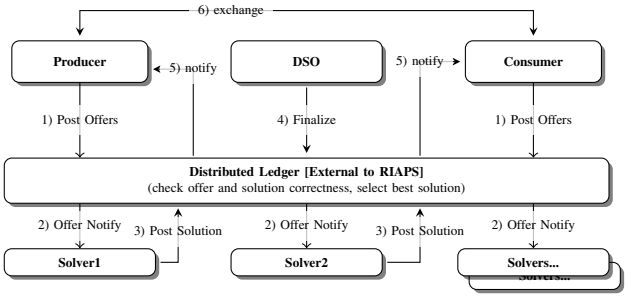

Fig. 5. Data flow between actors of in Transactive Energy application.

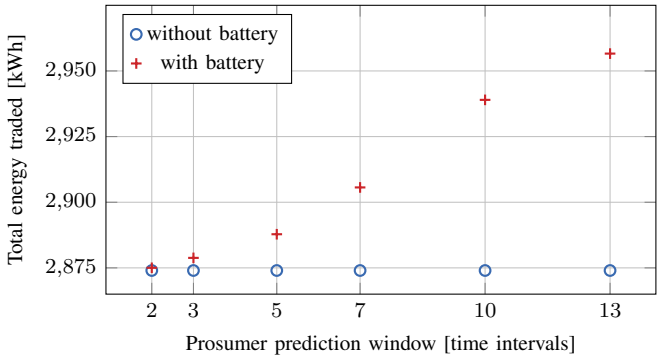

Fig. 6. Total amount of energy traded in the entire microgrid with and without batteries, for various prediction window lengths.

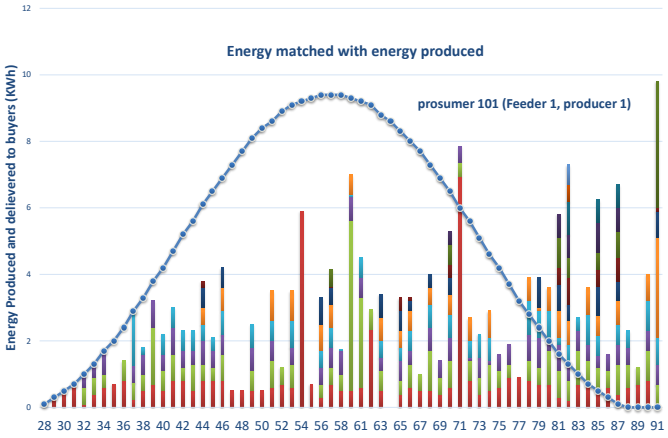

Fig. 7. Energy generated in each interval (blue line) and energy traded to a set of consumers in each interval (vertical bars) for the first prosumer of the first feeder. The stacked colors show the different consumers that were matched with the prosumer in each interval (note that the same color across multiple intervals does not necessarily mean the same consumer). When the energy traded exceeds the generation, the excess is drawn from the battery.

the future. In [14], we used Ethereum as the ledger. Solvers monitor the ledger, and when offers are posted, they (2) use an algorithm to match buyers to sellers. This match is (3) posted to the ledger. The solution for an interval may be updated until it is (4) finalized by the DSO. At this point, producers and consumers are notified and will (6) exchange the amount of power for which they were matched. RIAPS was used to provide inter-actor communication, management services, and time-synchronization for the actors to begin the transfer of power at the right time.

The trading scenarios that we consider involve consumers and prosumers that participate in a local P2P energy trading market by posting offers to sell produced energy or to buy and consume energy in a future time interval. An offer consists of the quantity of energy being bought or sold, the time interval in which the trade is to be delivered, and possibly a reservation price, i.e., the maximum (or respectively, minimum) price at which the buyer (or respectively, seller) is willing to trade.

We assume that each participant predicts their future power production and consumption (e.g., based on historical data) and does so prior to trading on the market. Moreover, each participant is represented by an automated trading agent that strategically posts offers to the TES management platform (TMP) based on these predictions and the participant's personal trading goals.

In the simplest trading scenario, the DSO sets the price p per kWh for the local market; p is the price paid by any buyer and received by any seller, including the DSO. The DSO can then dynamically adjust the price p to affect the market efficiency, which is evaluated as the number of local transactions vs. energy demand met from a bulk supplier. Another scenario includes a fully dynamic market where all sellers, including the DSO, post offers that include a reservation price. Each consumer then picks a selling offer on a first-come, first served basis. An extension of this scenario involves double auctions where both selling and buying offers are posted to the TMP, which executes an automated, regulator-approved market clearing algorithm as an immutable smart contract on the TMP's blockchain system. This algorithm selects the clearing price of p within each time interval.

One of the innovative capabilities of the decentralized trading platform is the ability to specify multiple time intervals in selling offers, enabling the integration of battery systems for delaying the sale or purchase of energy. Figure 6 shows the total energy traded for different tests. We varied the prediction window for the participants from 2 to 13. That is, in each interval, the participants submitted offers starting from the next 1 to 12 intervals (the current interval is always counted in the prediction window). The experiment simulated the whole day from the first interval starting at 0:00 (12:00 AM) to the 95^{th} interval ending at 23:59 (11:59 PM). As expected, increasing the prediction window with batteries improves performance, and without batteries has no effect on the total amount of energy traded. This is because any production must be dispatched within one-time interval, so the solver cannot optimize energy usage across multiple intervals even if future offers are available.

An example execution run of the system is shown in Figure 7. This figure shows the energy matched per interval for the first prosumer of the first feeder (Figure 2).

C. Network Simulator

The network simulator, as shown in Figure 8, creates communication channels among the prosumers and enables

the simulation of cyber attacks. The network simulator is built using the tap-bridge module of NS3; here, every container has a bridge and is linked to a tap device in NS3. All tap devices communicate through a virtual wireless network. Besides, random network traffic has been added to the simulation to mimic the real world network situation. The purpose of this random noise is to test if the data analytics implemented in this paper can detect the attacks in the most randomized dataset since the real datasets would also contain such random noise. The randomness in the dataset is equivalent to that of a workstation in a smart grid testbed, and it consists of web traffic and system updates. As the simulation begins, the communication between various components is collected using a packet sniffer tool. The collected information includes IP addresses, port numbers, length of packets, protocol, and number of bytes sent every five minutes.

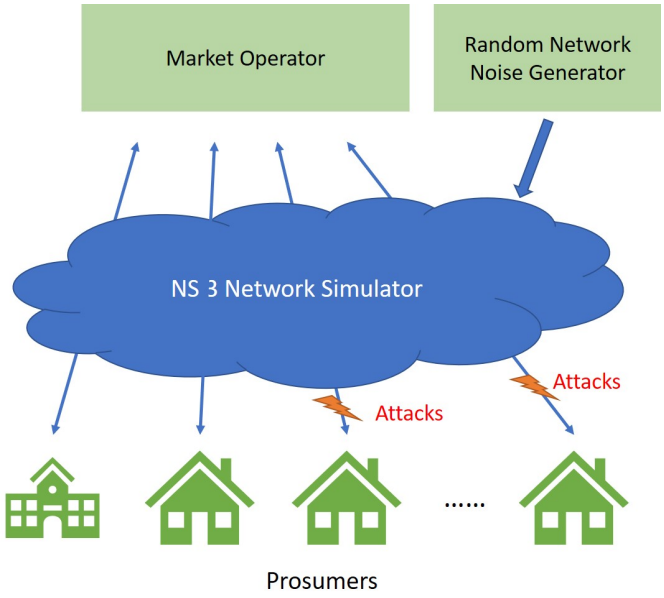

Fig. 8. Network simulator for TESST

III. Cyber Threat and Security Analysis

A centralized trading platform may be exposed to a variety of cyber-threats and privacy issues. Some attackers seek financial gain through network-based attacks, and they will manipulate the controllers to profit. Some attackers aim to disturb the operation of the TES. Similar to the notable cyber-attack against Ukrainian power systems in December 2015 [21], [22], attackers can inject malware into the market operation system and manipulate settings, such as DLMP limits or clearing time interval. An attacker could use a malicious channel to eavesdrop on the power system and can also steal critical information. Through stealing critical information from both the market operator and prosumers, attackers could devise a sophisticated targeted attack. They can also conduct Denial-of-Service (DOS) attacks that aim to cause a lack of availability of information, updates, prices, and resources. In contrast to the market operation system, individual smart HVAC controllers do not necessarily employ strong security mechanisms. Therefore, compromise a large number of smart HVAC controllers either for financial gain or to damage the system by sending massively manipulated bids to the market operator.

During the simulation of TESST, the prosumers will submit bids to buy or sell electricity and the market operator will collect those bids and produce a clearing price. This information is crucial for the operation of a TES. If this information is compromised, the operation of the transactive system may be impacted at multiple levels.

Here we explore two possible attacks that assume an attacker is able to manipulate the bid price and quantity. In the first scenario, the attacker seeks personal benefit by reducing the bid price and quantity by 50%. If only a limited number of prosumers launch such an attack, it will be difficult to detect because the impact on the total demand curves is small as seen if Figure 9.

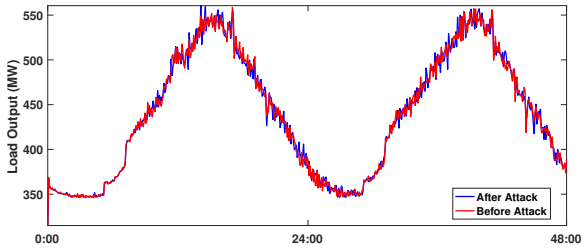

Fig. 9. Demand curve changes due to attacks aim for profits

In the second scenario, the attacker aims to disturb the operation of the transactive market, which can be done by changing the prosumers' bids to arbitrarily high or low values. Such drastic modifications will lead to significant changes in clearing price, the operation of smart HVAC controllers, and the overall demand as shown in Figure 10. This unexpected oscillation is likely larger than the system can sustain, and lead to a serious operational issue.

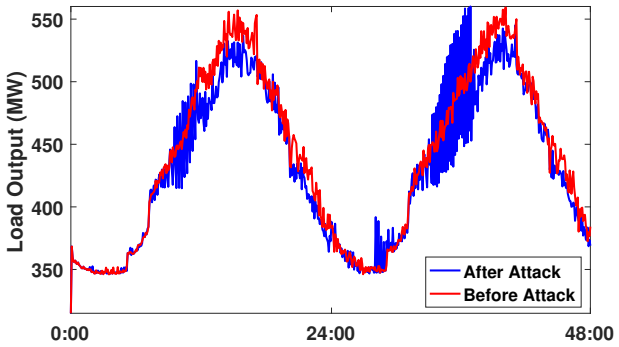

Fig. 10. Demand curve changes due to attacks aim for disturbing system operation

In the scenarios described above, we assume that attackers are able to manipulate the average bid price and quantity. Maintaining this assumption, these threats can be mitigated through the use of multiple solvers and a distributed consensus algorithm. If we use multiple solvers, an attacker will need to modify the bids received by all solvers. The decentralized market option presented previously in Section II-B2 provides this feature, and as shown in our prior work [23], it is resistant to solver failure. Transitioning to a decentralized market helps us to mitigate the threats presented here, but it also introduces additional challenges. TRANSAX addresses problems associated with faults in the system; however, its resistance to security threats needs further analysis. Regarding the issue of bid manipulation, a potential solution is assigning reputation values to actors, which enables removing misbehaving actors from the system. An alternative solution is imposing enforceable fines (e.g., by requiring security deposits) to disincentivize malicious or dishonest behavior. These questions can be addressed in detail as part of future work.

IV. Conclusions

In this paper, we have introduced a TES testbed, called TESST, which can simulate the operation of both centralized and decentralized TES platform. The centralized trading platform can establish all prosumers within the physical system, but it is less resilient to cyber attack. The decentralized trading platform is designed using blockchain, and it addresses security issues inherent in centralized systems. The operation and cyber-vulnerability of the centralized trading platform is analyzed in the simulation. Through simulation results, we demonstrated that it is relatively easy to manipulate a traditional centralized trading system and to cause financial and possible operational issues. The decentralized trading platform can effectively clear the market, and provide improvements to a centralized solution, but still need to be investigated using TESST in the future. This allows for the development of a secure and resilient decentralized trading platform, which is critical for the operation of TES.

V. Acknowledgement

Work reported in this paper is partially supported by the ARPA-E RIAPS, Siemens CT, National Science Foundation Activity-aware Cyber-Physical Systems and the Department of Energy under Award Number DE-IA0000025 for UI-ASSIST Project. We also acknowledge help from Dr. A. Hahn, K. Kaur and the Pacific Northwest National Lab in supporting this work.

References

[1] E. Cazalet, P. D. Marini, J. Price, E. Woychik, and J. Caldwell, "Transactive energy models," National Institute of Standards Technology, Tech. Rep., 2016.

[2] R. B. Melton, "Gridwise transactive energy framework," Pacific Northwest National Laboratory, Tech. Rep., 2013.

[3] A. Pratt, D. Krishnamurthy, M. Ruth, H. Wu, M. Lunacek, and P. Vaynshenk, "Transactive home energy management systems: The impact of their proliferation on the electric grid," *IEEE Electrification Magazine*, vol. 4, no. 4, pp. 8–14, Dec 2016.

[4] G. Bakke, *The Grid: The Fraying Wires Between Americans and Our Energy Future*. Bloomsbury USA, 2016. [Online]. Available: https://books.google.com/books?id=q8cfrgEACAAJ

[5] R. Li, Q. Wu, and S. S. Oren, "Distribution locational marginal pricing for optimal electric vehicle charging management," *IEEE Transactions on Power Systems*, vol. 29, no. 1, pp. 203–211, Jan 2014.

[6] J. L. Mathieu, S. Koch, and D. S. Callaway, "State estimation and control of electric loads to manage real-time energy imbalance," *IEEE Transactions on Power Systems*, vol. 28, no. 1, pp. 430–440, Feb 2013.

[7] S. P. Meyn, P. Barooah, A. Bui, Y. Chen, and J. Ehren, "Ancillary service to the grid using intelligent deferrable loads," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2847–2862, Nov 2015.

[8] L. Chen, N. Li, S. H. Low, and J. C. Doyle, "Two market models for demand response in power networks," in *2010 First IEEE International Conference on Smart Grid Communications*, Oct 2010, pp. 397–402.

[9] N. Li, L. Chen, and S. H. Low, "Optimal demand response based on utility maximization in power networks," in *IEEE Power and Energy Society General Meeting*, July 2011, pp. 1–8.

[10] H. Hao, B. M. Sanandaji, K. Poolla, and T. L. Vincent, "Aggregate flexibility of thermostatically controlled loads," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 189–198, Jan 2015.

[11] J. C. Fuller, K. P. Schneider, and D. Chassin, "Analysis of residential demand response and double-auction markets," in *2011 IEEE Power and Energy Society General Meeting*, July 2011, pp. 1–7.

[12] (2017) Brooklyn microgrid. [Online]. Available: http://brooklynmicrogrid.com/

[13] S. R. D. Company. (2017) The nature of sterling ranch. [Online]. Available: http://sterlingranchcolorado.com/about/

[14] A. Laszka, S. Eisele, A. Dubey, G. Karsai, and K. Kvaternik, "TRANSAX: A blockchain-based decentralized forward-trading energy exchange for transactive microgrids," in *Proceedings of the 24th IEEE International Conference on Parallel and Distributed Systems (ICPADS)(December 2018)*, 2018.

[15] S. Underwood, "Blockchain beyond Bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[16] A. Mavridou, A. Laszka, E. Stachtiari, and A. Dubey, "VeriSolid: Correct-by-design smart contracts for Ethereum," in *Proceedings of the 23rd International Conference on Financial Cryptography and Data Security (FC)*, February 2019.

[17] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers," in *Proceedings of the 7th International Conference on the Internet of Things (IoT)*, October 2017, pp. 13:1–13:8. [Online]. Available: http://doi.acm.org/10.1145/3131542.3131562

[18] V. V. G. Krishnan, Y. Zhang, K. Kaur, A. Hahn, A. Srivastava, and S. Sindhu, "Cyber-security analysis of transactive energy systems," in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T D)*, April 2018, pp. 1–9.

[19] A. Arman, V. V. G. Krishnan, A. Srivastava, Y. Wu, and S. Sindhu, "Cyber physical security analytics for transactive energy systems using ensemble machine learning," in *2018 North American Power Symposium (NAPS)*, Sep. 2018, pp. 1–6.

[20] S. Eisele, I. Mardari, A. Dubey, and G. Karsai, "Riaps: Resilient information architecture platform for decentralized smart systems," in *2017 IEEE 20th International Symposium on Real-Time Distributed Computing (ISORC)*, May 2017, pp. 125–132.

[21] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid: Defense use case," Electricity Information Sharing and Analysis Center (E-ISAC), Tech. Rep., 2016.

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

[23] S. Eisele, A. Laszka, A. Mavridou, and A. Dubey, "SolidWorx: a resilient and trustworthy transactive platform for smart and connected communities," in *2018 IEEE International Conference on Blockchain (Blockchain 2018)*, Halifax, Canada, Jul. 2018.