FDIAs on Hybrid Trading Transactive Energy Markets: Attacks, Impacts, and Prevention

Rumpa Dasgupta, Amin Sakzad, Carsten Rudolph, Rafael Dowsley
Dept of Software Systems and Cybersecurity, Monash University, Melbourne, Australia
rumpa.dasgupta@monash.edu, amin.sakzad@monash.edu, carsten.rudolph@monash.edu, rafael.dowsley@monash.edu

***Abstract*—Transactive Energy Market (TEM) operates a day-ahead market for efficient energy management and determines the energy prices in advance for the future period. This predetermined rate is used during real-time energy trading. Hence, it is crucial to provide the correct energy forecast to estimate fair energy prices for all users. However, this market poses a potential opportunity for attackers to manipulate energy prices through False Data Injection Attacks (FDIAs). Moreover, sharing energy forecasts with market operators (MO) or participants violates users' privacy. To address these issues, this paper first presents two FDIAs to a day-ahead TEM and then numerically evaluates their effects. Then, we design a novel framework to address the trade-off between sharing forecasts and user privacy. We show how users can share the energy forecast with MO and other participants securely while preserving privacy using the developed framework. Finally, we show how our proposed framework detects malicious activities of users (e.g., deviation of actual energy supply/demand from forecast beyond a threshold) and prevent FDIAs effectively.**

***Index Terms*—Transactive energy market, false data injection attacks, impact analysis, attack detection, user's privacy**

I. Introduction

The transactive energy market (TEM) is a new market framework for energy management in smart grids that enables the exchange of energy and services between different participants in the grid [1]. It allows for a more decentralized approach where individual users can generate energy from the distributed energy resources (DERs) instead of relying solely on centralized power generation and distribution [2]. Moreover, users have the ability to actively negotiate the sale of their extra energy to other users directly or via intermediaries [3]. This approach enables a more flexible, resilient and efficient energy system, while also empowering users to take greater control over their energy consumption and costs.

TEM can be categorized into three types, full peer-to-peer (P2P), community-based, and hybrid scheme [4]. In the full P2P case, users trade energy with each other without any mediator. On the other hand, a market operator (MO) runs trading activities in community-based and hybrid trading schemes. Among the three structures, hybrid schemes are more scalable than others as total market participants can be divided into smaller communities with fewer members which decreases the computational and communication overhead and enhances scalability [5]. TEM runs the day-ahead market a day or an hour prior to the actual energy generation [6]. Users join the market and commit with their peers or market authorities to provide/consume a certain amount of energy based on energy generation and load forecast, which must be met during real operation/time. This market plays a pivotal role in energy management as it helps to reduce future uncertainties and prepare the generators for their forthcoming operation. It determines energy prices using the auction-based or distributed method for a period/day in advance based on the total demand and supply forecast of energy [7]. Hence, it is crucial to provide correct energy data and maintain data integrity in TEM to estimate a fair energy price that benefits all users involved.

TEM comprises several market components such as IoT-integrated DERs, smart appliances, home energy management systems (HEMS), and communication channels which make it highly susceptible to false data injection attacks (FDIAs) through those components [8]. Moreover, an individual or group of participants may intentionally misbehave and provide false data regarding their energy consumption or production forecast to market authorities. Attackers are motivated to carry out FDIAs in order to obtain financial benefits or disrupt the market operation [9]. These FDIAs greatly manipulate energy prices in the market and move the system away from its optimal solution [10]. Therefore, an effective approach is necessary to ensure data security and prevent FDIAs.

Additionally, energy forecast data is sensitive for market participants as participants' privacy is related to it. Energy data can reveal a user's everyday activities to an unauthorised person which violates an individual's privacy [11]. Moreover, if market authorities have access to individual users' forecasts, they can use them for targeted marketing and pricing strategies for those customers. This approach may lead to unequal treatment of participants and could potentially compromise their privacy. Hence, it is necessary to design a market framework that will safeguard the privacy of users when sharing energy demand/supply predictions with others.

Considering the above-discussed issues, this work focuses on conducting a series of investigations. First, the study aims to explore the impact of FDIAs on the hybrid energy trading schemes of TEM. Then, we propose a new framework to provide security of energy forecast data and prevent FDIAs during trading energy. Our main contributions are to:

- present two FDIAs performed by malicious users on the hybrid energy trading scheme of TEM and analyze their impact. The results show that malicious users gain financial benefits from the market by injecting a small false prediction through other users' devices.

979-8-3503-9678-2/23/$31.00 ©2023 IEEE

- develop a novel framework using two advanced yet simple and efficient cryptographic primitives for FDIAs prevention and detection. We also analyze the security and privacy guarantees of the proposed framework for sharing energy data in tradings.

In contrast to [12], this study employs a hybrid TEM as a system model and introduces two FDIAs under the attack model. We implement both FDIAs and investigate their impact on market participants and operations through simulation. We have security assessments to prevent FDIAs and identify attackers or affected devices using the proposed framework. None of them are present in [12].

II. Related Work

In the existing literature, several research studies have focused on examining cybersecurity threats, vulnerabilities, attack detection, and mitigation strategies within TEM-based power systems [6], [13]–[15]. However, they have often overlooked a critical aspect: the potential for market participants and external attackers to launch various attacks, such as FDIAs, with the aim of manipulating original forecast data. These attacks may target various system components or involve injecting false forecasts directly using their controlled devices, all without significant security breaches. Moreover, they have not explored the detection and prevention of such FDIAs. Additionally, only a limited number of studies [16]–[19] have considered participants' privacy during energy trading in TEM. The current cryptographic-based solutions [18], [19] to preserve user privacy during energy trading in TEM are unsuitable for real-time market operations due to the high computational cost. Hence, a suitable solution is required to address all of the above discussed issues. In this work, we develop a novel framework for energy trading in hybrid TEM based on two well-known cryptographic primitives: additive secret sharing and Pedersen commitment, which are highly renowned for their computational efficiency and suitability for real-world applications. Moreover, their potential in addressing data security and user privacy issues within the TEM context has not been explored before.

III. System Model

In this work, we considered a hybrid market structure for energy trading as shown in Fig.1. Here, the total number of market participants/transactive agents (TAs) is N. N TAs can be divided into several communities. For the sake of simplicity, we divided N TAs into 2 communities in Fig.1. A market operator (MO) leads the trading activities of each community. In the community, each TA comprises a set of smart appliances, a set of DERs (solar panels, photovoltaic batteries), a HEMS, and a tamper-proofed smart meter. The HEMS is connected with all appliances and DERs. HEMS determines the optimal starting time of each connected device based on the energy generation forecast of DERs and the preference of TAs. Using device schedules and DER forecasts, HEMS makes an estimation of the surplus or deficit of energy for a specific period. Depending on whether it is consuming or generating energy for a particular time slot, the TA acts as either a consumer/buyer or a prosumer/seller in the market. TAs have the ability to communicate and exchange information with each other. However, to trade energy with each other, they have to talk via their own MO. The activities of all communities are monitored by a Distribution System Operator (DSO) on behalf of the grid, and the MO communicates with the DSO while trading energy from the grid. In this system, we assume that communication among market different entities happens through the authenticated link.

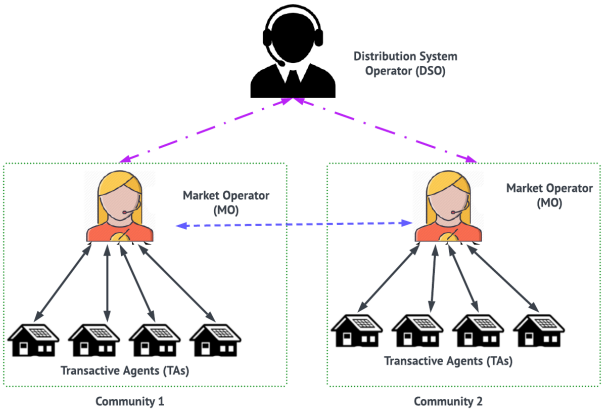

Fig. 1. System model overview.

This work divides the whole day or 24-hour period into equal time slots such as $t = 1, 2, \ldots, T$, where T is the total number of time slots. The whole market process is divided into two phases, the forecast phase, and the real-time/online phase. The forecast phase happens prior to the time referred to as t, while the online phase takes place after that time. To be more precise, if we split the entire day into 24 intervals of one hour each, the time frame between 12 AM to 1 AM is represented by $t = 1$. MO conducts the forecast phase before 12 AM. Based on HEMSs' forecasts, TAs participate in the market and agree with MO on the production or consumption of a certain amount of energy between 12 to 1 AM. After 1 AM, MO runs the real-time phase and verifies the real energy production or consumption by utilizing the energy information gathered from the smart meter of each TA.

To trade surplus/deficit energy, each TA has three options. 1) Intra-community, 2) Inter-community, and 3) Grid. In those cases, TA needs to communicate with other TAs, neighbouring MOs, or DSO via its own MO. TA can trade energy from its own or neighboring community members through active negotiation whereas TA receives fixed prices to sell or buy energy from the grid. In this study, we use the distributed market-clearing algorithm presented in [5] for trading energy in inter-community, intra-community, or grid. For details about the market-clearing/trading mechanisms, we refer interested readers to check [5].

IV. Attack Model

As TEM consists of smart appliances, IoT-integrated DERs, HEMS, communication channels, etc; attackers can use any one of them to conduct FDIAs. Moreover, some TAs (sellers/buyers) can act as attackers and deliver the wrong demand/supply forecast to the TEM through HEMSs or smart appliances. These devices can either belong to them and be under their direct control or they can be compromised devices located in a different household. Furthermore, a group of TAs can collaborate and inject false predictions collectively.

In TEM, the attackers have the ability to manipulate various types of data such as price signals, demand/supply, flexibility, etc. However, in this study, to analyze the impact of attacks through simulation, the focus is solely on FDIAs where a set of malicious TAs (sellers and buyers) introduce false demand information into the market. More specifically, we consider below two FDIA scenarios in this section.

FDIA 1: The first attack scenario considers a group of malicious seller TAs from different communities who intend to create a fraudulent increase in the overall energy demand of the market for some periods. To achieve this goal, malicious TAs target some TAs and hack their HEMS to gain illegal access. Then, they can escalate the temperature data for those particular periods or change some of the device schedules from other time slots to the specified time slots. As a result, the energy demand of the affected users rises significantly, leading to high energy demand in the market.

FDIA 2: In the FDIA 2, a set of malicious buyer TAs is involved in the attack. They can do the same activity as the first attack scenario. However, instead of escalating energy demand, this time the intention of attackers is to reduce energy demand in the market to get the illegitimate benefit. To do so, they can manipulate temperature forecasts to show lower temperatures or adjust device scheduling preferences to move the device start time from a high-demand period to a low-demand period. All of these activities result in a reduction of the user's energy demand forecast for specific time periods.

V. Impact Analysis

In this section, we examine the impact of the aforementioned attacks on the energy price, selling, and buying energy of the market using simulation results. The objective of this section is to investigate how (even small) false demand injection can significantly manipulate the market price and amount of traded energy in TEM. To simulate the energy trading process, we develop our source code in Python. We considered the hybrid TEM with 32 TAs, half of which act as sellers and the other half as buyers. These TAs are divided into four distinct areas/communities with a different number of sellers and buyers TAs in each area. Energy trading simulations are carried out for a single time interval, which is assumed to be one hour (1h). During the simulation, the projected energy supply and demand for each TA are randomly chosen within the range of 0 to 10 kW. We set the rest of the main parameters of each TA and MOs following [5].

To investigate the attack impact, first, we run the market without attacks and use the market-clearing algorithm described in [5] to determine energy prices of communities. We also estimate traded energy in each community. Then, we injected false demand through four random TAs, one from each community. More specifically, for FDIA 1, we raised the demand of consumers, while for FDIA 2, we decreased the consumer demand. To execute those attacks, we selected two different sets of consumer TAs and manipulated the energy demand in a random manner. The demand forecast of respective TAs before and after FDIAs are listed in Table I. Here, we define TA_i as i^{th} TA, where $i = 1, \ldots, N$.

TABLE I
Energy demand of TAs before and after FDIAs

TA	FDIA 1 Energy Demand (kW)		**TA**	FDIA 2 Energy Demand (kW)	
	Before Attack	After Attack		Before Attack	After Attack
TA_2	3.00	10.00	TA_3	6.23	1
TA_6	4.33	6.33	TA_5	6.47	1.47
TA_{21}	5.83	6.83	TA_{20}	5.35	2.35
TA_{30}	2.76	9.76	TA_{32}	9	2

The energy prices of four communities without and with FDIAs are illustrated in Fig. 2. The result shows that the energy price is not uniform across different communities. The reason is the demand and supply of TAs differ among the four communities and the number of TAs per community is also varied. Fig. 2 also shows that introducing a small amount of fake demand during the first FDIA causes a rise in energy prices in all communities. In contrast, if energy demand is reduced during the FDIA 2, it leads to a decrease in the market clearing price. From the simulation result, it is evident that the energy price is proportionally related to the energy demand of the market. In TEM, MO determines the energy price in advance for the future period and the predetermined rate is applicable to trade energy during the real-time market. Hence, malicious TAs can manipulate the price in both ways to escalate their own benefits. Seller TAs can inflate prices by injecting fake demand to obtain a higher selling price, while buyers TAs can decrease the overall demand to buy energy at a lower price.

Fig. 3 shows that both attacks have a significant impact on the traded energy of the market. As depicted in Fig. 3, the selling energy of each community rises up to 11 kW due to false demand injection. The reason is when an attacker introduces fake demand into the community, it will result in an escalation of the overall demand during that specific period. Hence, malicious seller TAs can sell more energy than in a normal period and increase their profit. In addition, the attack causes an increase in the total buying energy of each community, as misled buyer TAs join the market to buy the extra energy due to manipulated high demand, resulting in financial losses for them. On the other hand, the second FDIA could provide financial benefits for malicious buyer TAs. Since many TAs are not participating in energy trading due to low demand, malicious consumer TAs can take advantage of

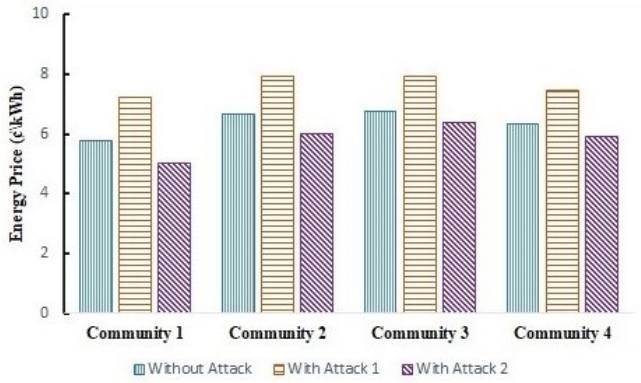

Fig. 2. Energy price of four communities without and with FDIAs.

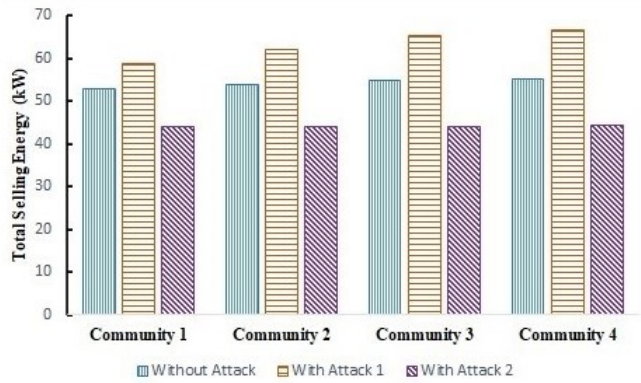

Fig. 3. Total selling energy of four communities without and with FDIAs.

this situation and purchase the energy they need from other community members at a lower price. However, the real-time scenario could be different and the actual demand can be much higher than the predicted demand in that specific period. In such scenarios, if the MO is unable to immediately manage and supply enough energy, the whole community can face severe consequences, such as a power outage. We have seen a similar pattern as Fig. 3 in the total buying energy of four communities without and with FDIAs.

VI. FDIAs detection and prevention

As demonstrated in Section V, inaccurate energy predictions can have significant consequences for TAs and market operations. Therefore, it is crucial to ensure that energy predictions are as accurate as possible to maintain a stable and reliable TEM. One possible approach to achieve this is by monitoring the energy predictions of each TA. However, a significant disadvantage of this approach is the compromise of TA's privacy, as MO must store the forecast data of each TA. If a TA's forecast data is accessed by others, it can expose sensitive information about the TA's home presence, patterns of appliance usage, and household members during specific periods in advance. This is a violation of the TA's privacy. Moreover, attackers can intercept the transmission link between TA and MO, or manipulate the MO's database to obtain forecast data. This information could be used to plan theft or burglary while the TA is away from home. Thus, in this paper, our focus is to design a novel energy trading framework for TEM called SePEnTra to detect TAs whose actual energy consumption/production deviates from their forecasted demand/supply beyond a threshold while preserving TAs' privacy. Detection of the TAs would facilitate the identification of the individuals or devices responsible for injecting false forecasts. Moreover, SePEnTra is designed to prevent the manipulation of energy prediction data by external attackers (who are not joining in TEM to trade energy), malicious TAs, and TA him/herself, as part of our efforts to prevent FDIAs. Here, it is important to mention that the energy forecast of individual TA may not perfectly align with the actual generation/consumption due to various unavoidable reasons, such as unpredictable weather changes, the intermittent nature of DERs, and unforeseen emergencies. However, it is vital to ensure that any deviations remain within acceptable limits to maintain a stable market operation and prevent any significant negative impacts.

A. SePEnTra: Secure & Privacy-Preserving Energy Trading

Fig.4 illustrates the five phases of SePEnTra, which are OneOffKeyGen, Negotiation, Commitment, CommitmentCheck, and Online. We refer readers to [12] for the sequential diagram of SePEnTra. The first four phases of SePEnTra are developed for the forecast phase of TEM while the fifth phase is designed for the real-time phase (see section III for the detail of the forecast and real-time phase). With the exception of OneOffKeyGen, the remaining phases are executed once per time slot. In contrast, OneOffKeyGen is performed once at the beginning, and the generated key is reused by the TAs in each subsequent period (unless it is compromised, in which case the procedure OneOffKeyGen is executed again to generate a new key). SePEnTra is developed using two advanced cryptographic primitives, namely Additive secret sharing [20] and Pedersen commitment [21]. Additive secret sharing is a method in secure multiparty computation (MPC) that partitions confidential information into multiple 'shares,' and when these shares are combined, they reconstruct the initial secret. In this process, each participant possesses one of these shares, and it is necessary to combine all of them to reconstruct the original secret. It is important to note that no subgroup of participants possesses sufficient information to unveil the secret. On the other hand, the Pedersen commitment scheme is an example of an additive homomorphic commitment scheme [22]. It enables a sender or committer to commit to a specific value, followed by the ability to later unveil the committed value. The recipient of this commitment can then verify whether the revealed value matches the one committed to initially. Additive secret sharing and the Pedersen commitment scheme are known for their computational efficiency and suitability for real-world applications. Given the extensive nature of TEM, which requires a careful balance of computational efficiency when deploying any mechanism, this study develops a TEM framework utilizing these two cryptographic primitives to ensure a low computational burden for practical implementation

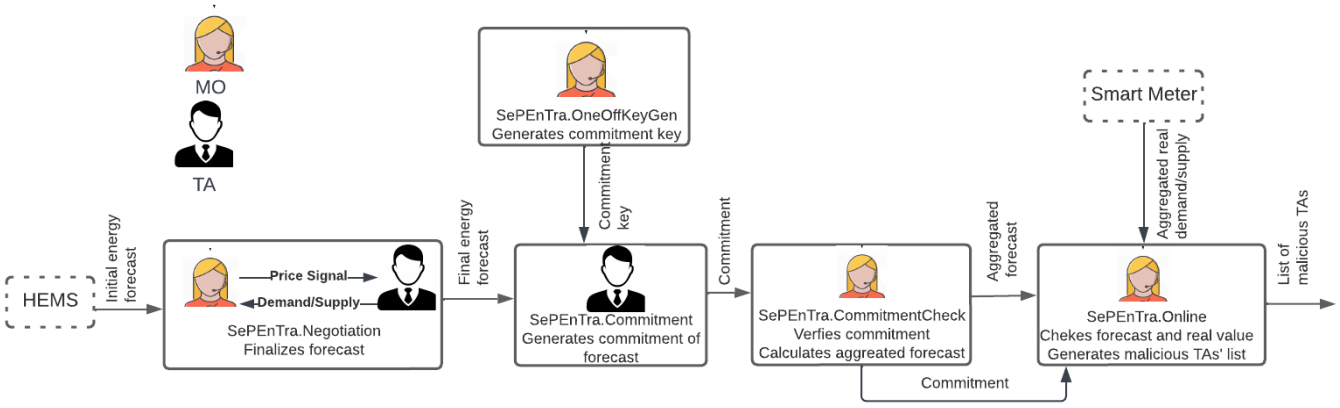

Fig. 4. Block diagram of our proposed secure and privacy-preserving energy trading mechanism.

while maintainng data security and user privacy. We describe five phases of our proposed model, SePEnTra, below:

SePEnTra.OneOffKeyGen: In our proposed framework, MO uses the Pedersen commitment scheme [21] to generate a commitment key ck, which is then distributed to all the TAs in the community. Each TA stores this key for future use.

SePEnTra.Negotiation: is responsible for finalizing the energy demand and supply forecast, denoted as E_i, for each period after a round of negotiation. In each round, TA_i updates the initial forecasts based on the price signal received from MO. On the other hand, MO requires the aggregated demand/supply information of the community to update the energy price in each round. Instead of sharing E_i^k (where k = round of negotiation), TA_i uses an additive secret sharing scheme to split E_i^k into N shares, with each share distributed to one TA. This process is applied to all TAs, resulting in each TA having N shares from N TAs. Then, TA_i sums up the N shares and sends the resulting value ($E_i^{k'}$) to MO. Finally, MO aggregates all the values received from the N TAs, which results in the aggregated energy demand/supply of the community and uses it to update the price signal in each round. Once the negotiation is stopped, TA_i stores its final energy demand/supply forecast E_i, which must be met during the actual operation or time.

SePEnTra.Commitment: Each TA generates the commitment of E_i using ck and Pedersen commitment [21]. Let C_{TA_i} denote the commitment of TA_i and determine it using (1)

$$C_{TA_i} = Commit_{ck}(E_i, r_i) = g^{E_i} h^{r_i} \mod q \qquad (1)$$

Here, r_i = randomness used for computing C_{TA_i}, q =prime number, and g, h = generators . Moreover, TA_i splits E_i and r_i into N shares using additive secret sharing and distributes one share to each of the N TAs. This process is repeated for all TAs, resulting in TA_i having N shares from each of the N TAs. TA_i then calculates the sum of the N shares of E_i to obtain $E_i{}'$, and the sum of the N shares of r_i to obtain $r_i{}'$. Finally, TA_i sends C_{TA_i}, $E_i{}'$, and $r_i{}'$ to MO.

SePEnTra.CommitmentCheck: MO verifies the commitment of each TA (C_{TA_i}) using the additive homomorphic property of Pedersen commitment [21] in this phase. MO estimates the commitment of the total energy forecast of N TAs and checks the value with the summation of individual TA's commitment. If TAs passed the verification, MO stores C_{TA_i}, total energy forecast (E), and sum of randomness to generate commitment (r) where $E = \sum_{i=1}^{N} E_i'$ and $r = \sum_{i=1}^{N} r_i'$. Otherwise, MO rejects TA's commitment and notifies TAs.

SePEnTra.Online: identifies the malicious TAs whose real energy usage deviates from their forecasted values beyond the threshold. Specifically, when one time slot is over, TA_i receives its actual energy generation or consumption (e_i) from the smart meter. Then e_i is a secret shared with the N TAs. Each TA calculates the sum of the N shares that they have received, resulting in the generation of e_i', which is then forwarded to MO. MO combines all the e_i' values to derive e, and compares it to the total forecast E to check whether the difference is within the acceptable range. If the discrepancy between the expected (E) and actual (e) energy usage is within the tolerable range, MO produces an empty list. Otherwise, MO instructs each TA to disclose their respective E_i, e_i, and r_i. Utilizing E_i and r_i, MO computes C'_{TA_i} and contrasts it with the earlier value of C_{TA_i}. If C'_{TA_i} matches C_{TA_i}, MO proceeds to verify whether e_i deviates beyond the prescribed threshold from E_i. In case the deviation surpasses the threshold, MO adds TA_i to the list of malicious TAs and outputs it.

VII. Security Assessment

SePEnTra ensures that TA_i's energy forecast (E_i) and real consumption (e_i) are hidden from other TAs as TA_i distributes a secret share to other TAs, which provides no useful information about E_i and e_i. Moreover, TA_i sends E_i' to MO at each iteration, but MO cannot derive E_i from E_i'. After convergence, TA_i transmits the commitment of the energy forecast (C_{TA_i}) to MO which hides the actual forecasting value from the MO. Hence, no other TAs and MO will know TA_i's energy forecast except TA_i, which preserves TA's

privacy during energy trading. Only TA_i reveals E_i and e_i to MO based on MO's request when the one-time slot is over. SePEnTra preserves TA's privacy against external attackers as well. Since the communications links are authenticated, an external attacker or malicious TAs cannot alter the energy forecast using FDIAs over the communication link.

Furthermore, SePEnTra verifies C_{TA_i} based on the commitment of the total demand/supply forecast. MO estimates the commitment of the total demand/supply forecast of N TAs and checks the value with the summation of individual TA's commitment. If the attacker manipulates C_{TA_i} or malicious TAs alter their forecast value E_i after the negotiation phase, this attack can be detected by MO. Hence, malicious TAs cannot intentionally inject excessive demand or supply during the forecast phase to manipulate energy prices. Even if malicious TAs or external attackers compromise other TAs' HEMS to inject false forecasts using those devices, MO can detect those TAs through the mismatch between forecast (E_i) and real value (e_i) in our proposed model. As SePEnTra effectively prevents all possible manipulation of E_i, the deviation of actual consumption from the forecast beyond a threshold indicates that either the TAs have provided inaccurate forecasts, or their devices are being subjected to an attack.

VIII. Conclusion

In this paper, we presented two FDIAs performed by malicious TAs on the hybrid TEM and analyzed the impact of attacks through simulation. The simulation result showed that attackers can gain significant financial benefits and create a disturbance in the regular market operation by injecting false demand forecasts. Thus, sharing accurate energy forecasts and keep tracking the energy forecast of each TA is crucial for efficient market operation. As it is directly related to user privacy, we proposed a novel framework, called SePEnTra for TEM. We discussed how SePEnTra enables market participants to share energy forecasts and actual energy data with all parties without compromising their privacy. Then we analyzed how the MO can utilize this information to generate accurate price signals and identify the TAs who have provided inaccurate forecasts, or whose devices are being subjected to an attack. Finally, we demonstrated how SePEnTra prevents FDIAs in several ways. In the future, our work can be extended by implementing SePEnTra in the full P2P TEM.

References

[1] D. Forfia, M. Knight, and R. Melton, "The view from the top of the mountain: Building a community of practice with the gridwise transactive energy framework," *IEEE Power and Energy Magazine*, vol. 14, pp. 25–33, 05 2016.

[2] O. Abrishambaf, F. Lezama, P. Faria, and Z. Vale, "Towards transactive energy systems: An analysis on current trends," *Energy Strategy Reviews*, vol. 26, p. 100418, 2019.

[3] F. Lezama, J. Soares, P. Hernandez-Leal, M. Kaisers, T. Pinto, and Z. Vale, "Local energy markets: Paving the path toward fully transactive energy systems," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 4081–4088, 2019.

[4] T. Sousa, T. Soares, P. Pinson, F. Moret, T. Baroche, and E. Sorin, "Peer-to-peer and community-based markets: A comprehensive review," *Renewable & Sustainable Energy Reviews*, vol. 104, pp. 367–378, 2019.

[5] M. Khorasany, Y. Mishra, and G. Ledwich, "Hybrid trading scheme for peer-to-peer energy trading in transactive energy markets," *IET Gen., Trans. and Distrib.*, vol. 14, no. 2, pp. 245–253, 2020.

[6] C. Barreto, H. Neema, and X. Koutsoukos, "Attacking electricity markets through iot devices," *Computer*, vol. 53, no. 5, pp. 55–62, 2020.

[7] R. Dasgupta, A. Sakzad, and C. Rudolph, "Cyber attacks in transactive energy market-based microgrid systems," *Energies*, vol. 14, no. 4, 2021.

[8] 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 Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[9] R. Dasgupta, A. Sakzad, and C. Rudolph, "Impact analysis of false data injection attacks in transactive energy market-based micro-grid systems," in *2021 IEEE PES ISGT Asia*, 2021, pp. 1–5.

[10] T. T. Dayaratne, F. T. Jaigirdar, R. Dasgupta, A. Sakzad, and C. Rudolph, *Improving Cybersecurity Situational Awareness in Smart Grid Environments*. Springer International Publishing, 2023, pp. 115–134.

[11] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1304–1313, 2016.

[12] R. Dasgupta, A. Sakzad, C. Rudolph, and R. Dowsley, "Sepentra: A secure and privacy-preserving energy trading mechanisms in transactive energy market," 2023. [Online]. Available: https://arxiv.org/abs/2304.06179

[13] K. Jhala, B. Natarajan, A. Pahwa, and H. Wu, "Stability of TEM-based power distribution system under data integrity attack," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 10, pp. 5541–5550, 2019.

[14] Y. Zhang, S. Eisele, A. Dubey, A. Laszka, and A. K. Srivastava, "Cyber-physical simulation platform for security assessment of transactive energy systems," in *2019 MSCPES Workshop*, 2019, pp. 1–6.

[15] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Trans. on Smart Grid*, vol. 11, no. 2, pp. 931–941, 2020.

[16] J. Abdella, Z. Tari, R. Mahmud, N. Sohrabi, A. Anwar, and A. Mahmood, "Hicoob: Hierarchical concurrent optimistic blockchain consensus protocol for peer-to-peer energy trading systems," *IEEE Transactions on Smart Grid*, pp. 1–1, 2022.

[17] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers," 10 2017.

[18] Y. Lu, J. Lian, and M. Zhu, "Privacy-preserving transactive energy system," in *2020 American Control Conference (ACC)*, 2020, pp. 3005–3010.

[19] Y. Lu, J. Lian, M. Zhu, and K. Ma, "Transactive energy system deployment over insecure communication links," 2020. [Online]. Available: https://arxiv.org/abs/2008.00152

[20] D. Escudero, "An introduction to secret-sharing-based secure multiparty computation," 2022. [Online]. Available: https://eprint.iacr.org/2022/062

[21] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *CRYPTO'91*, pp. 129–140.

[22] J. Groth and M. Kohlweiss, "One-out-of-many proofs: Or how to leak a secret and spend a coin," in *Advances in Cryptology - EUROCRYPT 2015*, E. Oswald and M. Fischlin, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 253–280.