2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)
Virtual, October 26-28, 2020

Effects of false data injection attacks on a local P2P energy trading market with prosumers

Sara Mohammadi
Department of Informatics
University of Oslo(UiO)
Oslo, Norway
saramoha@ifi.uio.no

Frank Eliassen
Department of Informatics
University of Oslo(UiO)
Oslo, Norway
frank@ifi.uio.no

Yan Zhang
Department of Informatics
University of Oslo(UiO)
Oslo, Norway
yanzhang@ieee.org

Abstract— **In the energy sector, peer-to-peer (P2P) energy trading is a promising method for the future smart grid. Despite all the benefits, this method is vulnerable to some malicious attacks, e.g., false data injection attacks (FDIAs). This paper explores the vulnerability of local P2P energy trading to FDIAs. Previous works on FDIAs in energy neighborhoods consider consumers only, or do not consider the effect of including prosumers. We consider the situation where an attacker tries to modify the participants' demands to gain some benefits. Through simulations using real datasets, we demonstrate possible effects of FDIAs on both selling and buying energy prices in P2P energy trading involving both prosumers and local energy suppliers. From the simulations, we learn that the best chance for an attacker to remain undetected is to target a high number of prosumers and only modify their demand with a small fraction. Moreover, by comparing the results from the attack scenario with the normal situation, we observe that an attack generally leads to less favorable energy prices and thus reduced incentives to become or even remain an energy-selling prosumer.**

Keywords—false data injection, local P2P energy trading, prosumers, smart grid.

I. INTRODUCTION

Electricity markets are being enabled by new regulations to build the future grid. Unlike centralized markets, new market models are based on decentralization of energy resources. Local energy communities can trade energy in two ways: by an intermediate of a global market operator, or in a peer to peer (P2P) setting. In P2P energy trading, local prosumers have more flexibility in trading energy by exchanging surplus energy from multiple distributed energy resources (DERs) between themselves. This flexibility could increase the prosumers' financial welfare and result in significant cost savings for them. When prosumers generate their consumption energy locally, power flow over long distances can be reduced, and transformers can be replaced with smaller and cheaper equipment. Thus, local energy generation can result in major cost savings for the system [1].

Besides the benefits of local P2P energy trading as outlined above, a key challenge is ensuring the security of the market. This should be addressed as a part of the original design. If no security measures are taken, it can facilitate the way for insider and outsider attackers to penetrate the market, or cause faulty energy trading behaviours.

One of the most popular approaches to attack cyber physical systems is false data injection (FDI). The concept of FDI attacks (FDIAs) mainly refers to the deception attacks, which means that the attack aims to take down the consistency of power grid or to gain more benefits by tampering output data of power equipment [2]. There are several works which studied FDIA scenarios in P2P energy trading, as well as possible defense methods [3-6]. However, those works considered consumers only in energy neighbourhoods. To the best of our knowledge, there are no works analysing threat scenarios in P2P energy trading with both prosumers and consumers. When there are prosumers, the higher benefits that they gain from trading between themselves rather than with the grid, encourages consumers to become prosumers [8]. Therefore, this is a challenge for the suppliers. In this case, a malicious supplier may want to discourage consumers to become prosumers.

We choose an exploratory approach to quantify threats. In particular, we investigate a game theoretic approach to P2P trading. Game theory in P2P energy trading can simulate participants´ behaviour and their interactive trading with each other, and easily incorporate motivation (incentives) and pricing plan as a part of the game framework development. It can also create trust between participants within the network, and motivate them to cooperate in a game situation. Moreover, its potential to merge with some promising signal processing techniques like machine learning and fuzzy logic makes it useful [7]. In our investigation, the behaviour of all trading participants, including their individual preferences is modelled.

In this paper, a threat scenario, in which FDIAs are executed, in a P2P energy trading market including prosumers is proposed, and the resulting benefits for the attacker is investigated. We analyse the effects of FDIAs, when there are different number of attacked prosumers, on price and revenue of prosumers and attacker in different time slots, and compare them with the normal situation (without attack). We use a real dataset from Austin, Texas for doing the experiments. The experiments show that all prices and the average utility of prosumers increase and decrease respectively, by increasing the amount of attacked prosumers' demands. This leads to reducing the motivation of becoming or even remaining an energy-selling prosumer. The contributions of this paper are as follows:

- We analyse a threat scenario based on False Data Injection Attacks in a P2P energy trading model including prosumers.
- The consequences of false data injection attacks in a game-theoretic approach to P2P energy trading are analysed and experimentally explored.

The rest of the paper is organized as follows. Section 2 describes the system model. Section 3 details the threat scenario. Section 4 demonstrates the numerical simulation results followed by the conclusion in Section 5.

II. SYSTEM MODEL

The trading model that we explore in our work is adapted from [8]. In this model, a community-based P2P market is

978-1-7281-7100-5/20/$31.00 ©2020 IEEE

designed that includes different market participants such as pure consumers, prosumers (with solar generation), local suppliers (with their own energy generation from solar farms, wind parks, or conventional power plants), and one community coordinator. The behaviour of the participants is modelled as two non-cooperative games.

The market is modeled as a multi-agent system that consists of three types of agents; prosumer agent (both consumers and prosumers are considered as prosumers), supplier agent, and coordinator agent. In the game, both suppliers and prosumers try to maximize their own profit. The coordinator's job is to set up two pricing models that include an external pricing model for importing energy from suppliers to the local community, and an internal pricing model for the internal trading between local prosumers. In the following, the different players in the game are briefly described.

Suppliers compete with each other based on supply function equilibrium as in [9]. Let $N = \{1, \dots, N\}$ define a set of suppliers. Here, it is assumed that supplier $j \in N$ submits a parameter $w_j \geq 0$ to the coordinator. This parameter indicates that at an external price $p^{ext} > 0$, supplier j is willing to supply $S\ (p^{ext}, w_j)$ units of power (which is known as the supplier's bid) given by:

$$S\left(p^{ext}, w_j\right) = D - \left(\frac{w_j}{p^{ext}}\right) \tag{1}$$

$$p^{ext} = \frac{\sum_{j \in M} S_{j,t}}{\sum_{j \in M} D_{j,t}} \tag{2}$$

The parameter w_j may be understood as the revenue that supplier j is willing to forgo, because when the price is p^{ext}, $p^{ext}D$ is the total revenue, and $p^{ext}S(p^{ext}, w_j) = p^{ext}D - w_j$ is the revenue of supplier j when the price is p^{ext}. The external price for supplier j at time slot t is given by the equation (2).

In the prosumer side game, there are pure consumers (without generation) and prosumers (with generation). When the difference between generation and consumption is greater than zero, then prosumer acts as a seller. Otherwise, the prosumer act as a buyer. The prosumers try to adjust their energy consumption based on the internal prices (buying and selling prices) which are calculated by the coordinator to clear the market. As proposed in [8] the utility of the prosumer i at time slot t $(Utility_{i,t}(.))$ is expressed as follows:

$$Utility_{i,t}(x_{i,t}) = \begin{cases} k_{i,t} \ln(1, x_{i,t}) + p_t^s\left(E_{i,t}^g - x_{i,t}\right), E_{i,t}^g - x_{i,t} > 0 \\ k_{i,t} \ln(1, x_{i,t}) + p_t^b\left(E_{i,t}^g - x_{i,t}\right), E_{i,t}^g - x_{i,t} \leq 0 \end{cases} \tag{3}$$

$$p_t^s = \mu_t \frac{E_t^d - E_t^s}{\sum_{j \in M} D_{j,t}}, \qquad p_t^b = \lambda_t \frac{E_t^d - E_t^s}{\sum_{j \in M} D_{j,t}} \tag{4}$$

where $k_{i,t} \ln(1, x_{i,t})$ is the utility that the prosumer i gets by consuming $x_{i,t}$ amount of energy at time slot t. $k_{i,t}$ is the reference parameter of prosumer i; a prosumer with high $k_{i,t}$ is more interested to consume more of its energy to gain maximum utility. $E_{i,t}^g$ is the amount of energy that prosumer i is able to generate at time slot t. p_t^s and p_t^b are internal selling and buying prices at time slot t, and μ_t and λ_t are predefined parameters. $p_t^s\left(E_{i,t}^g - x_{i,t}\right)$ and $p_t^b\left(E_{i,t}^g - x_{i,t}\right)$ are the revenue that prosumer i gains by selling excess energy and the price of buying energy at time slot t, respectively. E_t^d and E_t^s are total energy supply and demand at time slot t, respectively. Prosumers update their energy buying/selling request $E_{i,t}^g - x_{i,t}$ only by updating $x_{i,t}$ [8].

The coordinator gathers all the bids from the suppliers, and the requests for selling and buying energy from the prosumers. Subsequently, it calculates both internal and external prices based on the model of internal and external pricing respectively. Details of these pricing models can be found in [8].

In the game, first, the prosumers send their energy buying/selling requests to the coordinator. Second, the coordinator will calculate the net load, which is equal to the difference between the sum of energy generation and consumption from the prosumer-side, and send it to the suppliers. Then, the suppliers send their bids to the coordinator, and the coordinator calculates both external and internal prices, and send them to both suppliers and prosumers. Finally, the suppliers and prosumers update their bids based on those prices, and the algorithm will continue until the results from all participants converge; i.e., when the difference between the new external price and the previous one is sufficiently small [8].

III. THREAT ANALYSIS

Although a local P2P electricity market based on game theory could provide financial benefits to users and general environmental benefits, it may also bring an opportunity for FDIAs by insiders or outsiders to reduce their cost or maximize their benefits. In this section, we design a threat scenario that is based on false demands.

A. Threat scenario

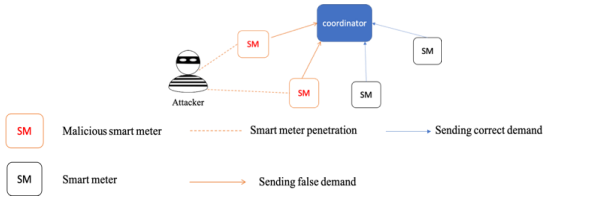
In this threat scenario, attacks can be orchestrated by a malicious supplier who engages an attacker acting as a prosumer, to gain more utility. The attacker aims to find the best way of modifying the prosumers'/ consumers' demand requests to minimize the chance of being detected.

a) Possible ways to attack

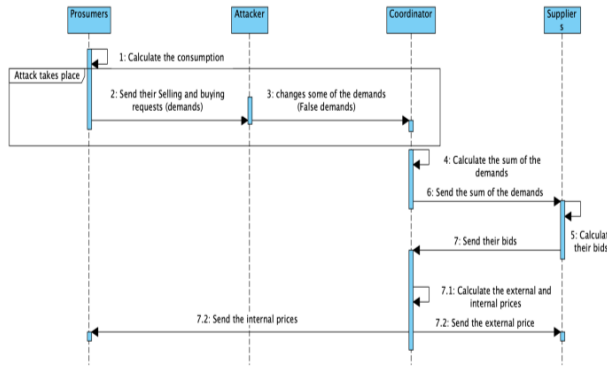
As it can be seen from Fig. 1, we consider two ways of attack. First, before the game starts (before the calculation of the prosumers' bids by their smart meters), and second, at the beginning of the game (after the calculation of the prosumers' bids by their smart meters). In the first method (Fig. 1 (a)), the attacker tries to intercept or modify the hardware/firmware code of the other prosumers' smart meters to make a disturbance in the process of calculating consumptions (to modify the demands). There are different ways to attack a smart meter; as explained in the following;

b) Possible threats for a smart meter

A smart meter has five main components which are control unit, smart meter collector, metrology system, home area network (HAN), and the optical interface [10]. Each of these components has various targeting attacks; e.g., the vulnerability of the control unit and metrology system are hardware and firmware reverse engineering. The smart meter collector is a radio system that communicates among the data collector in the AMI and the smart meter. Here, the dedicated design of the data and the data itself could be a target for a



(a)



(b)

Fig. 1. (a): attacking to some of the prosumers' smart meters before the game starts, (b): attacking in the beginning of the game by modifying some of the prosumers' demands

possible attack that may lead to an outage of the power grid, electricity theft and denial of power. The responsibility of HAN is to transfer real-time consumption readings from the smart meter to other devices in the user's premises. Data theft and denial of data are the main attack types in this context. Finally, the optical interface is applied for configuring and installing the smart meter. A severe denial of power and grid disruption could happen by interception or firmware attack.

In the second way of attack (Fig. 1 (b)), the attacker tries to connect to the communication network in the first round of the game to disrupt the legitimate communication between a victim prosumer and the coordinator. Here, the attacker controls the flow of the bids information in communication links to falsify some of the bids' by modifying their demands, which are sent by the prosumers' smart meters. One other possibility is that the attacker also modifies the bids during the game. There is, however, a risk that this would cause the game not to converge and thus cause disruption of the trading. Although this could be a possible approach of an attacker, we do not consider this case in the scenario, but leave it as future work.

After the attack happened, the coordinator receives false demands from some of the attacked prosumers, and the sum of the bids will be calculated by the coordinator based on the wrong amounts. As a consequence, all the processes of the game will be done based on the false initial demands. After finishing the game during a time slot, the final internal and external prices and amount of energy to sell or to buy will be sent by the coordinator to all participants.

IV. NUMERICAL RESULTS

In the simulations, a real dataset from Austin, Texas [11] is used. The use case focuses on the 1st day of August 2018, with efficient solar generation. The dataset has five main features; user (prosumer/consumer) ID, generation, sum of the loads, shiftable_load, base_load. We apply the attack data by modifying the shiftable and/or base loads, and by updating the sum of the loads based on the modified shiftable/ base loads.

The P2P system model contains 50 households; 20 of them are prosumers who are equipped with rooftop PV panels, while the remaining 30 are consumers with zero energy generation, and one attacker that intercepts prosumer/coordinator communication at the network level. Three companies act as suppliers in this P2P market. A buying prosumer has larger consumption than generation, while the opposite is the case for a selling prosumer.

We perform the simulations at a specific time slot of the dataset with different attack configurations to learn about the effects on energy trading with our threat scenario. We vary the attack configuration by increasing or decreasing the demand of both prosumers and consumers by different amounts, at the same time or separately, as well as the number of attacked prosumers/consumers. Furthermore, for prosumers, we assume the demand should not be modified in a way that causes its role towards the coordinator to be changed from seller to buyer or vice versa; this would make the attack easier to detect. We did some initial experiments to figure out how much an attacker had to change the demand to have a significant effect on trading in terms of prices and external supply. The range of both shiftable and base loads in the dataset is $(0kw, 6kw]$. When increasing the shiftable and/or base loads by less than $2kw$ on different percent of prosumers, we could not see any significant effects on the trading results. After initial experiments we increase shiftable and/or base loads of buyers in the experiments as described in the following. We distinguish between true demands in the range $[3kw, 6kw]$ and $[1kw, 3kw)$. These we refer to as R_1 and R_2 respectively. Let d and d' denote the true and false demands respectively. A *small increase* we define as up to three times of a true demand in R_1 ($d' = 3d$), and up to five times of a true demand in R_2 ($d' = 5d$). On the other hand, a *large increase* we define as up to 30 times a true demand ($d' = 30d$) in R_1 and up to 10 times a true demand ($d' = 10d$) in R_2. Increase by less than twofold are usually used for increasing the sellers' demands because of keeping their roles.

Besides keeping the buyers' role, on the other hand, the attacker should not reduce the loads to the extent that the total load turns from positive to negative. Therefore, we decrease shiftable and/or base loads of sellers and consumers as follows; at least $\frac{1}{3}$ times of a true demand ($d' = \frac{d}{3}$) in R_1 and $\frac{1}{5}$ times of a true demand ($d' = \frac{d}{5}$) in R_2 we refer to as a *small decrease*, while *a large decrease* we define as setting the false demand to at least 10% and 1% of the true demand ($d' = \frac{d}{10}$ and $d' = \frac{d}{100}$) in R_1 and R_2 respectively. Tuning the false demands to more than 50% of the true ones are usually used for decreasing the buyers' demands to keep their roles. Table I summarizes the effects of attacks with different configurations at time slot 10, and Table II shows the result of the experiments in the normal situation (without attacks) in the same time slot. We can see from Table I that the consumption data (shiftable/ base loads) are modified based on the ways we explained and the ranges of modified data are determined. In the different experiments, the percentage of attacked consumers and prosumers separately and together are 20%, 50% and 70%, respectively. The following observations can

TABLE I. AVERAGE UTILITIES OF PROSUMERS (A.U.P), CONSUMERS (A.U.C) AND SUPPLIERS (A.U.S), AND THE AMOUNT OF SUPPLY (SUP) UNDER FDIAS ON DIFFERENT NUMBER OF PROSUMERS (PR.) AND CONSUMERS (CON.) AT TIME SLOT 10.

Number of attacked participants (%)		Increasing demand (small increase)				Increasing demand (large increase)				Decreasing demand (small decrease)				Decreasing demand (large decrease)			
		A.U.P	***A.U.C***	***A.U.S***	***Sup***	***A.U.P***	***A.U.C***	***A.U.S***	***Sup***	***A.U.P***	***A.U.C***	***A.U.S***	***Sup***	***A.U.P***	***A.U.C***	***A.U.S***	***Sup***
Pr.	20%	0.13	0.23	4.21	110.4	-16.2	-0.4	43.6	409	0.54	0.24	2.76	104.9	0.49	0.31	2.42	102
	50%	-1.2	0.12	7.22	169.9	-169.7	-1.9	399	1225	0.52	0.22	2.70	103.8	0.52	0.32	2.35	96
	70%	**-2.7**	**0.04**	**10.6**	**204.4**	-239.8	-2.3	558	1447	0.7	0.37	1.69	88.5	0.6	0.37	1.88	87.2
Con.	20%	0.53	0.28	2.33	98.2	0.55	0.32	2.39	102.3	0.55	0.35	1.85	91.15	0.51	0.24	2.84	110
	50%	0.54	0.29	2.48	101.6	0.53	0.25	2.75	108.5	0.54	0.24	2.67	105.3	0.50	0.34	2.03	90.1
	70%	0.56	0.31	2.61	106.6	0.50	0.09	3.65	120.3	49.8	0.25	2.68	106.9	0.55	0.34	2.02	91.7
Pr.& Con.	20%	0.49	0.17	3.15	112.1	0.52	0.26	2.52	104.3	0.51	0.28	2.50	103.5	0.52	0.25	2.71	108
	50%	0.49	0.16	3.18	117.6	0.54	0.25	2.77	108.8	0.54	0.30	2.24	99.40	0.52	0.27	2.60	106
	70%	0.53	0.26	2.53	105	0.50	0.29	2.28	100.9	0.53	0.26	2.69	107.8	0.53	0.28	2.48	104

TABLE II. AVERAGE UTILITIES OF PROSUMERS (A.U.P), CONSUMERS (A.U.C) AND SUPPLIERS (A.U.S), AND THE AMOUNT OF SUPPLY (SUP) UNDER NORMAL SITUATION AT TIME SLOT 10.

A.U.P	A.U.C	A.U.S	Sup (KW)
0.5019	0.3460	1.9816	94.8453

be made by comparing Table I and Table II:

1) The attacker should increase the demands: compared with the normal situation, the utility of the malicious supplier is higher when the attacker increases the consumptions by both low and high amounts. The reason is that the sellers will sell less energy and buyers will buy more when their consumptions increase; based on the conditions in the right part of the equation (3), and then the suppliers have to supply more energy (equation (1)) which leads to the higher utility.

2) The attacker should attack just prosumers: when the attacker attacks consumers (increases their demands), the average utility of the consumers and prosumers decrease and increase respectively in comparison with the normal situation. This is because sellers will sell more energy; based on equation (3), and thus gain more utility. In contrast, the buyers will buy more, which results in lower utility. This situation encourages consumers to become prosumers which is contrary to the malicious supplier's goal. So, by attacking just to the prosumers, the average utility of the prosumers gets lower than the consumer's average utility which again may discourage consumers to become prosumers. This will be economically beneficial for the malicious supplier.

3) The attacker should increase the demands of a high number of prosumers with a low amount for each prosumer: Increasing the consumption by a high amount could be suspicious and noticed by the coordinator by checking the prosumer's history. For this reason, the attacker should increase the demands by a low amount i.e., with a low difference between the false demand and the real one. The attacker in our threat scenario wants to reduce the chance of being detected. Therefore, for being undetectable, the attacker should aim to attack a high number of prosumers by increasing their demands by a low amount instead of attacking a small number of prosumers and increase each of their demands by a high amount.

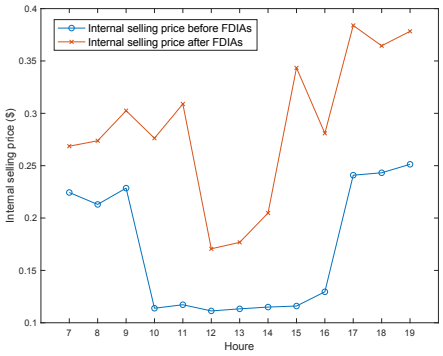
We apply the attack on the different percentage of prosumers in all time slots during the day to see the effects on both prices and utilities. Table III shows the percentage of attacked prosumers for which the most benefits are achieved for the attacker at each time slots (from 7:00 A.M to 19:00 P.M). Both internal and external prices under normal and attacked situations at similar time slots with Table III are investigated in the Fig. 2. As can be seen from Fig. 2, all prices increase after the attack; this is due to the increase in the demands.

Fig. 3, illustrates the profits of prosumers and consumers before and after the FDIAs, showing the decrease in profits. We can see that prosumers with solar generation get much more profits than consumers when there is no FDIAs. This may motivates consumers to become prosumers. While those motivations will be lost by decreasing the profits of prosumers and becoming lower than consumers' profits after the FDIAs; this has a high benefit for the malicious supplier.

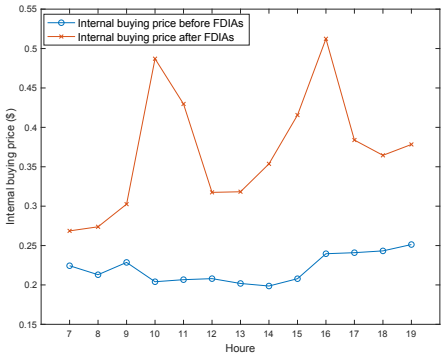
One lesson that we learnt from the experiments is that the game theoretic approach by itself can contribute to security. One effect of the approach is that an attacker cannot gain free energy by changing the demand at the beginning of the game. When the attacker increases the demands at the start of the game, the participants will in subsequent iterations update their demands based on the new price as normal, and finally, the game will converge with supply/demand balance and there will be no extra energy for the attacker. Alternatively, the attacker could manipulate the demands in each iteration of the game. From the experiments we observe that the game sometimes does not converge and thus cause disruption of trading. The way the demands are modified, must therefore be carefully considered by the attacker.

TABLE III. NUMBER OF ATTACKED PROSUMERS AT DIFFERENT TIME SLOTS

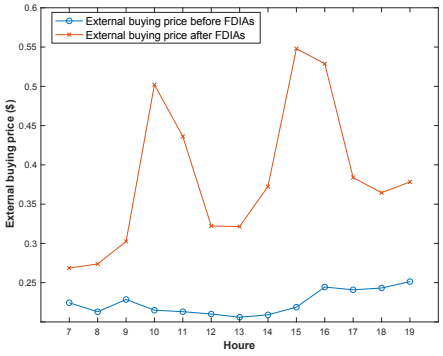
Time slots	Percent of prosumers (%)
7:00	40%
8:00	50%
9:00	60%
10:00	70%
11:00	80%
12:00	90%
13:00	95%
14:00	85%
15:00	65%
16:00	80%
17:00	75%
18:00	70%
19:00	55%



(a)



(b)



(c)

Fig. 2. (a): internal selling prices before and after FDIAs, (b): internal buying prices before and after FDIAs, and (c): external buying prices before and after FDIAs at different time slots.

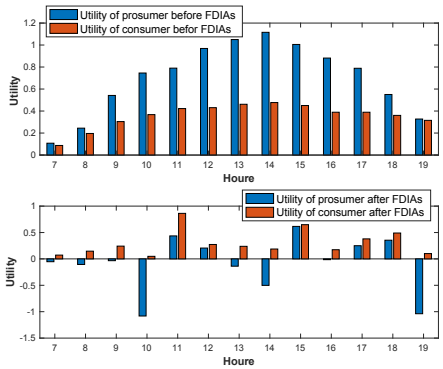


Fig. 3. profits of prosumers and consumers before and after FDIAs at different time slots.

V. Conclusion

In this paper we analyzed threat scenarios and experimentally explored the effects of false data injection attacks in a P2P energy trading model including their consequences on prosumers during trading. The effects were explored by comparing the trading outcome in a normal situation with the outcome of trading when under attack. The experimental results indicate that if the attacker modify the demands of prosumers by increasing their consumption demand, it will increase the profit of external energy suppliers and reduce the profit of prosumers. This reduction in profit may reduce the incentives to become or even remain an energy-selling prosumer. While, without FDIAs, the P2P trading model acts as an efficient incentive for pure energy consumers to become prosumers, due to the low internal prices and high utilities that it promotes. As future work, we will propose a novel mitigation technique to detect such false data injection attacks in local P2P energy trading.

Refrences

[1] H. Le Cadre, P. Jacquot, C. Wan, and C. Alasseur, "Peer-to-peer electricity market analysis: From variational to generalized nash equilibrium", *European Journal of Operational Research*, vol. 282, no. 2, pp. 753-771, 2020.

[2] M. Zhang, C. Shen, N. He, S. Han, Q. Li, Q. Wang, and X. Guan, *"False data injection attacks against smart gird state estimation: Construction, detection and defense", Science China Technological Sciences*, pp. 1-11, 2019.

[3] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation", *In 2010 44th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1-6, 2010.

[4] L. Liu, M. Esmalifalak, Q. Ding, V.A. Emesih, Z. Han, "Detecting false data injection attacks on power grid by sparse optimization", *IEEE Trans. Smart Grid*, vol. 5, pp. 612–62, 2014.

[5] S. N. Islam, M. A. Mahmud, and A. M. T. Oo, "Impact of optimal false data injection attacks on local energy trading in a residential microgrid", *Ict Express*, vol. 4, no. 1, pp. 30-34, 2018.

[6] G. Chaojun, P. Jirutitijaroen, M. Motani, "Detecting false data injection attacks in ac state estimation", *IEEE Trans. Smart Grid*, vol. 6, pp. 2476–2483, 2015.

[7] W. Tushar, C. Yuen, H. Mohsenian-Rad, T. Saha, H. V. Poor, and K. L. Wood, "Transforming energy networks via peer-to-peer energy trading: The potential of game theoretic approaches", *IEEE Signal Processing Magazine*, vol. 35, no. 4, pp. 90-111, 2018.

[8] M. Zhang, , F. Eliassen, A. Taherkordi, H. A. Jacobsen, H. M. Chung, and Y. Zhang, "Energy Trading with Demand Response in a Community-based P2P Energy Market", *In 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pp. 1-6, 2019

[9] R. Johari, J. Tsitsiklis, "Parameterized supply function bidding: Equilibirium and welfare", *Mathematics of Operations Research*, vol. 59, no. 5, pp. 1079-1089, 2011.

[10] A. M. Khattak, S. I. Khanji, and W. A. Khan, "Smart meter security: Vulnerabilities, threat impacts, and countermeasures" In *International Conference on Ubiquitous Information Management and Communication,* pp. 554-562, 2019.

[11] Dataport, 2019, [online] Available: https://www.pecanstreet.org