energies

MDPI

Article

Cyber Attacks in Transactive Energy Market-Based Microgrid Systems

Rumpa Dasgupta *, Amin Sakzad and Carsten Rudolph

Faculty of Information Technology, Monash University, Clayton, VIC 3800, Australia; amin.sakzad@monash.edu (A.S.); carsten.rudolph@monash.edu (C.R.)
* Correspondence: rumpa.dasgupta@monash.edu

Abstract: Due to the increasing integration of distributed energy generation in the electric grid, transactive energy markets (TEMs) have recently emerged to balance the demand and supply dynamically across the grid. TEM enables peer to peer (P2P) energy trading and brings flexibility by reducing users' demand in the grid. It also enhances the system's efficiency and reduces the pressure on electricity networks. However, it is vulnerable to major cyber attacks as users equipped with smart devices are participating autonomously in the energy market, and an extensive amount of information is exchanged through the communication channel. The potential attacks and impacts of those attacks need to be investigated to develop an attack resilient TEM-based power system. Hence, in this paper, our goal is to systematically identify possible cyber attacks associated with a TEM-based power system. In order to achieve this goal, we classify the attacks during the P2P and flexibility schemes of TEM into three main categories. Then, we explore the attacks under each category in detail. We further distinguish the adversary roles of each particular attack and see what benefits will be received by an adversary through each specific attack. Finally, we present the impact of the attacks on the market operation, consumers, and prosumers of the TEM in this paper.

Keywords: microgrid system; transactive energy market; peer to peer energy trading; flexibility scheme; cyber attacks; impact analysis

Citation: Dasgupta, R.; Sakzad, A.; Rudolph, C. Cyber Attacks in Transactive Energy Market-Based Microgrid Systems. *Energies* **2021**, *14*, 1137. https://doi.org/10.3390/en14041137

Academic Editor: Edmund Widl

Received: 13 January 2021
Accepted: 17 February 2021
Published: 21 February 2021

1. Introduction

The introduction of distributed energy resources (DERs) in traditional electricity systems as a means of energy production brings a number of advantages, such as reducing environmental pollution, lowering the electricity cost of DER owners, minimizing system cost, and so on [1]. Moreover, DER owners can convert from consumers to prosumers by selling their surplus energy generation to other consumers and the grid [2]. For efficient energy management and incentivizing the DER owners properly, a new market framework called the transactive energy market (TEM) has emerged [3]. TEM encourages small-scale generators and consumers to join in conventional electricity markets to produce, sell and buy energy.

The conventional grid, where electricity is generated mostly in large central generators, brought to the distribution centers, and then distributed to the end-users, is upgrading to a smart grid through merging Information and Communication Technology (ICT) across the grid [4]. TEM enables Peer to Peer (P2P) energy trading in the grid [5], which makes a connection between consumers and prosumers for trading energy with each other. In the P2P energy trading, energy from small-scale DERs in dwellings, offices, factories, etc. is traded among neighboring prosumers and consumers. The benefits of P2P energy trading are bifold as the prosumers get financial advantages by selling their excess renewable generation, and consumers buy electricity at a cheaper rate from their peers instead of the grid. Moreover, implementing TEM in the smart grid enables flexibility schemes where prosumers/consumers can modify generation or consumption patterns of DERs based on

the request of different entities such as retailers and network service providers during the emergency period [6]. TEM also helps grid operators tackle the grid's growing complexity and coordinate energy consumption and production based on energy price signals.

However, TEM implementation in electric grids poses several challenges due to the intermittent energy generation of DERs as current electricity markets cannot react in real-time to the random generation from DERs [7]. Furthermore, energy prices in the market are often determined on a national level, which does not consider local energy shortage or surplus of supply. Hence, as a decentralized business model and a smaller version of the electric grid, microgrid [8] is used for implementing TEM in several practical projects. TEM maintains a dynamic supply-demand balance in the microgrid and maximizes the profit of energy producers and lessens the pressure on electricity networks during the peak demand period to sell renewable energy in the wholesale market.

Nonetheless, TEM creates opportunities for adversaries to conduct several cyber attacks as users equipped with Internet of Things (IoT) integrated DERs and smart appliances participate independently in the energy market. For example, an attacker may launch a False Data Injection Attack (FDIA) [9], a Denial-of-Service (DoS) attack [10,11], a replay attack [12], an eavesdropping attack [13], or an energy theft [14] attack to manipulate or reveal original data of the TEM users. All of these attacks and the impact of attacks are crucial and need to be analyzed in detail to develop a secure TEM-based power system.

In recent years, few researchers have studied and outlined several cyber security threats in TEM based power systems. For instance, Jhala et al. [15] discussed the impact of the FDIA on electricity price, demand, and distribution system voltage of TEM based power distribution system. Zhang et al. [16] developed different cyber attack models in the transactive energy system (in some literature, authors referred to the TEM as a transactive energy system. However, the functionalities of TEM and transactive energy system are similar) and studied their impact using data analytics and machine learning. In [17], Transactive Energy Security Simulation Testbed (TESST) is developed to simulate several transactive energy systems' cyber attacks. Carlo and Xenofon [18] considered a scenario where an adverse user manipulated the bids of other customers without damaging the power system. To mitigate the impact of the considered attack, they also proposed a defense scheme in [18]. A possible cyber risk through insecure IoT devices in the transactive energy system is investigated in [19].

Nevertheless, most of the works focused on the attacks through a communication channel to change bid-offer or electricity prices in the TEM. They overlooked some critical attacks such as manipulating forecasting data to change the energy demand, targeting specific users to minimize their benefits, intentionally unmet commitments by adverse users in real-time, and so forth. Moreover, none of them classify and analyze the impact of possible cyber attacks of the TEM-based microgrid system that involve the energy service and flexibility service during the P2P and flexibility market, respectively. As TEM is getting popular in microgrid systems while novel types of attacks are also emerging, various potential attacks through different means need to be identified to develop an attack resilient TEM based microgrid system.

Hence, in this work, we aim to systematically point out probable cyber vulnerabilities associated with the P2P and flexibility market of TEM based microgrid systems and to analyze the impact of these attacks in general. To identify the possible cyber threats, we have considered the Monash Microgrid as the system model in this study, as TEM is introduced in Monash Microgrid for energy management. In this work, first, we discuss the P2P energy trading process and flexibility scheme enabled by the TEM of Monash Microgrid. Then, we identify probable cyber attacks, specifically, FDIAs and classify the attacks during the P2P and flexibility market of Monash Microgrid in detail. Finally, we analyze the impact of these attacks on the TEM users and the market operation of the Monash Microgrid. It should be noted that, though we study the attacks and impact of attacks for Monash Microgrid in this paper, all these identified attacks, and their impacts,

are valid for any TEM-based microgrid system. In particular, we have made the following contributions through this paper:

- Classification of Attacks: We investigate and categorize potential attacks on the TEM-based microgrid system considering the Monash Microgrid as a system model into three broad categories. (i) attack through the communication channel; (ii) attack through devices; (iii) attack through adverse users.
- Impact Analysis of Attacks: We analyze and present the impact of these attacks on the TEM users and the market operation of Monash Microgrid based on the economic advantage of the attacker, inconvenience/decrease of welfare to the affected users, disturbance of regular market operation, a chance to occur any catastrophic event such as load shedding, power outage and risks for burglary due to the attack. Table 1 summarizes the impact of attacks for each category and we discuss the impacts thoroughly in Section 4.

Table 1. Impact of Attacks in the transactive energy market (TEM)-based microgrid system.

Attack Type	Economic Advantage of the Attacker	Decrease of Welfare to the Affected Users	Disturbance of Market Operation	Bring Catastrophic Events
Attack through communication channel	✓	✓	✓	✓
Attack through devices	✓	✓	✓	✓
Attack through adverse users	✓	✓	✓	✓

The remainder of the paper is organized in the following manner—Section 2 introduces TEM and presents our system model, Monash Microgrid, in detail. In Section 3, we investigate probable cyber attacks of the TEM. Section 4 analyzes the impact of the described attacks. The concluding remarks and future plans are presented in Section 5.

2. Transactive Energy Market (TEM)

Traditional power systems generate electric energy by using coal, diesel and natural gas-based generation units [20]. These conventional generation sources are responsible for greenhouse gas emissions, which cause global warming around the world. Therefore, conventional energy sources need to be replaced with renewable energy sources to produce energy and meet high global energy demand. Generally, small scale renewable sources are locally being installed in distributed systems and they are also known as DERs [1].

DERs produce renewable energy which can be consumed by the DER owner, and they can share or sell excessive energy with other consumers in a community and the grid [2]. This energy sharing or trading procedure converts a consumer into prosumer because they sell their excess energy to other consumers and the grid. For facilitating the integration of small-scale prosumers into the conventional electricity market, a novel framework is essential for energy trading. Transactive Energy (TE) is such a new framework that allows all sizes of consumers to join in different markets for generating, selling, and buying electricity [21]. The Gridwise Architecture Council (GWAC) [22] defined a transactive energy as an economic and control mechanism that considers value as a pivotal operational parameter to achieve a strong balance between the supply and demand of the whole power system. TE uses market-based solution for energy trading and sharing among prosumers. Also, energy is becoming a product for DER owners in the TE as they can sell their surplus energy to other DER or non-DER owners. Hence, a new market framework is needed for TE management to entitle and motivate DER owners to participate in different markets. The transactive energy market (TEM) [3] is a novel framework that instigates various advantages in integrating DERs into existing power systems. TEM envisages that mid

to small-sized energy generators and consumers can exchange energy and other services with each other in a distribution network following market rules. When both users and energy providers agree on the value of service at a particular point in time and place, then the consumer and prosumer can take the individual decision on whether they want to go ahead with this transaction at that specified price. Figure 1 illustrates the energy transaction process in TEM, where prosumers sell their excess energy directly to consumers through TEM. Also, prosumers can sell their surplus energy to the wholesale market or grid, and consumers can buy their deficit energy from the wholesale market at a higher price.

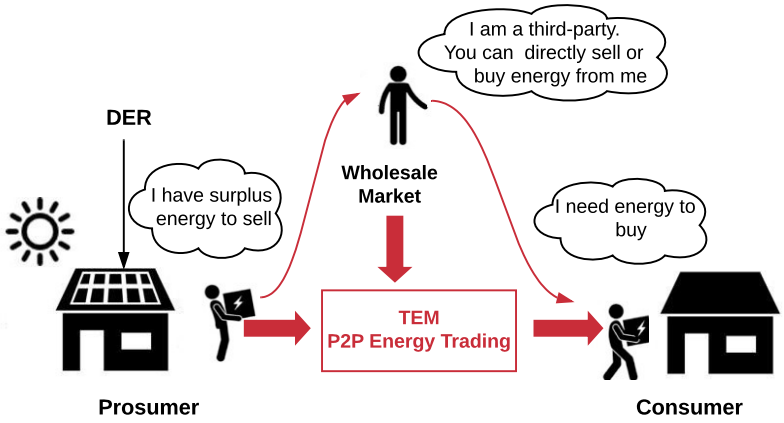

Figure 1. Energy trading process in a TEM.

TEM can provide various types of services through interactive internal and external markets such as energy service and flexibility service [23]. Energy service is a process to trade energy in distinct markets to decrease energy costs, while flexibility service means modifying DERs production or consumption pattern based on the request of retailers and network service providers. All DERs are transactive agents in a TEM. They show the fundamental behaviors of market participation and energy management where the market participation behavior allows the DER to compete as a discrete entity, and the energy management behavior contains the functionality to control, schedule, and manages the DER's available flexibility in the TEM framework.

The existing centralized power grid system is now changing towards a smart power grid paradigm to enhance different critical features of the traditional power system, such as efficiency, flexibility, sustainability and so forth, by making the grid automated and fully integrated. Smart grids provide a basis for TEM implementation because TEM brings flexibility to the grid by offering incentives to the consumers in exchange for modifying their consumption patterns and also gives solutions to manage the generation rate in both grid and demand sides [6]. For implementing TEM in the smart grid, several requirements are vital such as merge of ICT across the electricity grid, two-way communication flow, intelligent and remote supervision, advanced meter infrastructure and smart meters [24]. TEM expands the present concepts of wholesale power systems into retail markets by equipping end-users with intelligent energy management systems to encourage small-scale electricity customers for active participation in the electricity markets [25]. TEM also enables P2P energy trading [5] in smart grids where prosumers or DER-owners can trade the generation surpluses to other prosumers who deficit in energy and get financial benefits. On the other hand, deficit users can buy energy at a cheaper rate from neighbors or peers than purchasing energy from the grid.

TEM opens new opportunities in power grids relating to energy efficiency, the stability of the grid and the optimization of power flows. Simultaneously, DERs used for TEM bring new challenges for the grid due to its intermittent nature of energy generation and non-uniform deployment. Therefore, to tackle the challenges, TEM is implemented in decentralized energy systems such as microgrid nowadays [26,27]. A microgrid is a small version of a typical power grid, and the operations of the grid and microgrid are similar.

It consists of energy generators and consumers on a small scale. A microgrid converts to a smart microgrid by adding ICT and active energy management layer [28]. The smart microgrid is based on smart grid technologies where ICT-enabled energy generators and consumers can manage themselves. A smart microgrid can operate in both grid-connected or island mode. In the grid-connected mode, the microgrid shares its surplus energy or consumes the required energy from the grid based on the generation and load demand. During an emergency or power outage, the microgrid is disconnected from the grid and shifts to the island mode of operation. As part of a decentralized business model, both connected and disconnected smart microgrid can implement TEM to provide value streams by increasing economic advantages and DER integration. TEM brings opportunities for smart microgrids to obtain their financial benefits and aiding the reliability of the whole distribution system.

TEMs are pragmatically implemented and tested in a few smart microgrid projects, such as the Monash Microgrid [29], Brooklyn Microgrid [30], Allgau Microgrid [31], and the South Australian residential MG [32]. As a real-world implementation of TEM, this work has considered Monash Microgrid as the system model because it gives a realistic platform for research into business, technological and customer behavioral attributes of the deployment of DERs and their collaboration along with microgrid operations. Detail about Monash Microgrid is discussed in the following section.

2.1. Monash Microgrid

2.1.1. Project Overview

Monash Microgrid [29] is located at the Clayton campus, 20 km southeast of Melbourne's central business district, with a range of customers and DER assets. The microgrid is composed of 3.5 MW total controllable loads, 1 MW of Photovoltaic (PV) or solar power system, two 22 kW Electric Vehicle (EV) chargers, and 1 MWh of battery storage. The energy management of the microgrid and these DERs will be achieved by deploying a smart microgrid platform. The microgrid's 3.5 MW controllable loads are the mixture of the 20 multi-tenanted and mixed-use buildings. The microgrid's EV chargers also act as controllable loads. In the microgrid, eight different PV systems are installed on the rooftops of the buildings for 1 MW of solar generation. As PV systems are physically integrated with separate buildings, they can be considered individual DERs, not as a generator of the building when being managed. Along with PV systems, 1 MWh of battery storage system has been installed and integrated with one of the buildings and operated as an independent DER.

2.1.2. Smart Microgrid Platform

Efficient energy management is achieved in the microgrid by using a smart energy framework that introduces the compatibility with transactive energy governance.There are three layers in this framework, DER Integration layer, Active Grid Management layer, and Smart Energy Management layer. These layers provide the technical and functional abstractions that require to develop basic transactive microgrid behaviors.

- The DER Integration layer requires integrating an IoT device with each DER and developing a secure IoT network through networking of all IoT devices. In the Monash Microgrid, IoT devices are already integrated into DERs through connections to metering and control systems to deploy a smart microgrid platform.
- DERs are extended with grid management capabilities in the Active Grid Management layer for monitoring data and control capabilities of the microgrid's DERs. Applications are installed to IoT integrated DER devices to access DER energy data and control capabilities as IoT functions. Flexibility and forecasting capability of IoT integrated DER devices are needed for the participation of DERs in a distributed smart energy management system. Note that DER flexibility means the ability for a DER to change its supply and demand while guaranteeing that DER is operated safely, securely, and reliably. On the other hand, the DER forecasting capability allows the

prediction of the expected demand and supply of energy as well as the predicted level of available flexibility.

- The Smart Energy Management layer utilizes the aggregation and orchestration of forecasting and flexibility capabilities of DER to perform different energy management strategies such as transactive energy markets and optimizing DERs.

2.1.3. Market Scenario

Power systems typically use two types of markets; one is the day-ahead market, and the other is the real-time or intraday market [19]. In the day-ahead market, the market operator accepts bids of demand and supply for the next hours or day and finalizes commitments that prosumers and consumers must fulfill. It helps the system to reduce future uncertainties. Contrarily, the users participate in the real-time market to fulfill unmet commitments during the actual operation. In the Monash microgrid, a transactive energy market operator (TO) also runs both day-ahead and intraday market. In the day-ahead market, the whole day or 24 h period is divided into the thirty-minute time slots, while in the intraday market, the day is divided into the five-minute time slots. DER joins as a transactive energy market agent (TA) in both day-ahead and intraday markets. TAs have forecasting capability, and they forecast DER energy demand or scheduled energy and flexibility for different time slots. Afterwards, they participate in the market to trade energy with other TAs or the grid. On the other hand, TO maintains interaction with TAs and the grid operator and is responsible for clearing the market at the beginning of each time slot for the next time interval. TO also runs the flexibility market based on the requests from both internal and external market requesters. TO coordinates TAs during local trading and providing flexibility and pays agents based on their commitment. In the Monash microgrid, the intraday market is considered a balancing market where TA checks whether there is any change in the power or flexibility forecasting due to change in load, error in the forecast, and so forth. If there is any change, TA joins in the intraday market for trading energy to fulfill the unmet commitments. A brief comparison of the day-ahead and intraday markets is provided in Table 2.

Table 2. Comparison of the Day-ahead and Intraday Market.

Aspect	Day-Ahead Market	Intraday Market
Time Slot	30 min	5 min
TA's Role	Forecasts energy demand/supply and available flexibility	Checks change in the regular forecasting due to error or change in the load
	Participates to trade energy with other TAs or grid	Participates to trade energy to fulfill unmet commitments due to change in forecasting
TO's Role	Triggers flexibility market based on flexibility request	Runs flexibility market if receives flexibility request
	Coordinates and Pays TAs	Coordinates and Pays TAs

2.1.4. Market Settlement Approaches

In the Monash Microgrid, TO runs either a flexibility market or a joint flexibility and P2P market for flexibility and energy trading in each time slot based on the requests from internal or external market requesters. To settle the market or fix the market price, Monash Microgrid uses two types of pricing mechanisms. One is auction-based pricing, and another is a distributed optimization pricing. In the auction-based method, all agents submit their offers and its corresponding price to the market operator. After receiving all offers, the market operator determines the winners of the auction and the market clearing price. On the contrary, in the distributed optimization approach, all agents participate in the market

as price takers and receive a price from the market operator. Then agents respond to the market operator by declaring their demand/supply or offered flexibility. In this paper, we discuss an auction-based approach for the flexibility market and a distributed approach for joint flexibility and the P2P market of the Monash Microgrid.

2.1.5. Flexibility Market

This section presents the flexibility market operation, and Figure 2 illustrates the communication flow of the flexibility market in the Monash Microgrid. As discussed in Section 2, TEM can provide flexibility service in response to an external or internal request. During a hot day or peak demand period, the microgrid receives an external request from the retailer to minimize the energy demand in order to avoid high energy prices in the wholesale market or receives an internal signal from the microgrid monitoring function to reduce the demand because the possibility of exceeding peak demand level has been forecasted. By providing flexibility, the microgrid receives a payment from the requester. In the Monash Microgrid, when TO receives a flexibility request signal in the form of (F, λ_F), where F is the amount of requested flexibility, and λ_F is the monetary reward per unit of energy, it triggers the flexibility market by sending a bid request to all agents to provide the flexibility. To provide the requested flexibility, all the 20 buildings in the Monash Microgrid join as TAs in the flexibility market. After receiving a bid request from TO, each TA requests its corresponding forecasting manager to estimate the flexibility it can offer. The offered quantity with the price denoted by (f_i,λ_i) is sent back to the TO, where f_i and λ_i are energy quantity and per unit price of f_i offered by TA_i, respectively, for $i \in \{1, 2, 3, \ldots, N\}$ and N = total number of TAs. When TO receives offers from N TAs, it generates the aggregated flexibility curve [29]. The intersection point of the requested flexibility line and aggregated flexibility curve is considered the market-clearing point, and all TAs who offer prices lower than the price at the intersection win the auction. However, if the total flexibility is less than the requested flexibility, all TAs who offer a price lower than λ_F will consider as the winner. Then, TO informs the auction result to all TAs and sends a flexibility commitment message to the requester to inform how much flexibility the microgrid can provide in the response of their request.

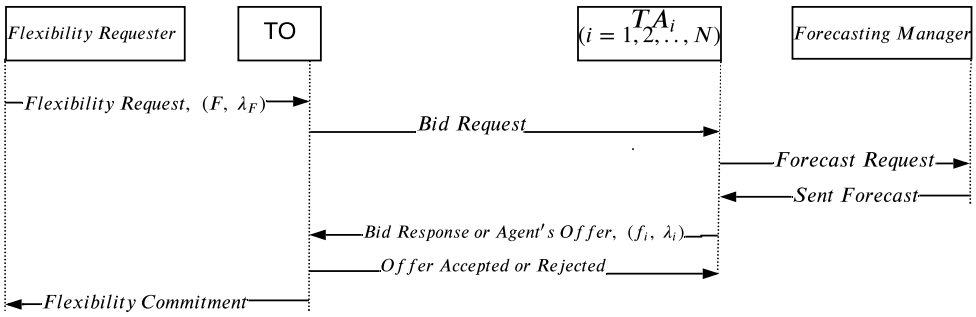

Figure 2. Sequence of communication flow of the flexibility market in the Monash Microgrid.

2.1.6. Peer-to-Peer and Flexibility Markets

This section presents joint flexibility and the P2P market for flexibility and energy trading in each time slot, and the communication flow during trading is depicted in Figure 3. As mentioned earlier, TA can forecast scheduled energy and provided flexibility of DER; hence, each TA participates in the market after forecasting either as a seller or a buyer for trading excess or deficit energy with other TAs or the grid. The objective of the TAs in the day-ahead trading is to buy (sell) their demand (generation) in such a way that their costs are minimized, and TO's objective is to minimize the total cost of TAs. TAs always trade energy with the grid with fixed prices, and it cannot be negotiated. In contrast, TAs can negotiate for the price in the P2P market to maximize their profit. Therefore, each TA aims to trade the maximal energy in the P2P market by considering traded energy with the grid is zero, and it is assumed that there is no flexibility request at this stage. More

specifically, TAs first settle their commitments to trade energy in the P2P market and then remaining available energy trade with the grid considering there is no flexibility request. After that, TO checks whether it receives any flexibility request from requesters or not. If it gets a request, then TO triggers the flexibility market by sending a flexibility request to the TAs. At this stage, TAs could not change their commitments with the P2P market. As a result, TAs offer flexibility during the flexibility market by altering their commitments with the grid. If we denote $P_{i,P}$, $P_{i,G}$, P_i, and ΔP_i as traded energy with the P2P market of TA_i, traded energy with the grid of TA_i, scheduled energy of TA_i, and provided flexibility by TA_i, respectively, then $P_{i,P} + P_{i,G} = P_i$, and $\Delta P_i = 0$, for $i \in \{1, 2, 3, \ldots, N\}$ and N being the total number of TAs.

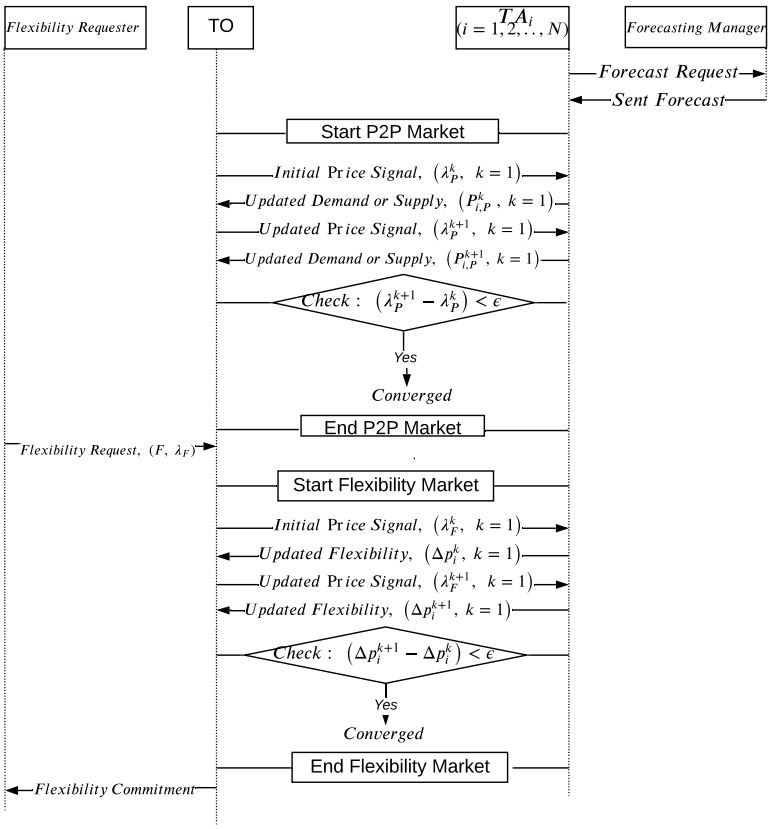

Figure 3. Sequence of communication flow of the Peer-toPeer (P2P) and flexibility market in the Monash Microgrid.

Initially, TO starts the P2P market by sending a price signal λ_P^k to all TAs. Here, k is the iteration number, and k = 1, 2, ... Each TA updates $P_{i,P}^k$ using λ_P^k and the updated $P_{i,P}^k$ is sent to TO. Then, TO updates its price signal based on aggregated demand from all TAs and sent the new price signal λ_P^{k+1} to all TAs. This process is iterative and stops when the convergence criterion $\lambda_P^{k+1} - \lambda_P^k < \epsilon$ is met, where ϵ is a small positive number to indicate the algorithm termination. The price at the convergence represents the P2P market price or clearing price for all agents. After that, each TA calculates their traded energy with the grid by using $P_{i,G} = P_i - P_{i,P}$. If there is a flexibility request from internal or external parties, TO initiates the flexibility market at this stage by sending a price signal λ_F^k to all TAs. TAs cannot alter their commitments in the P2P market. Hence, they provide flexibility by changing their traded power with the grid. In the flexibility market, all TAs are the flexibility sellers, while TO is the only buyer. Each TA calculates provided flexibility ΔP_i^k by using λ_F^k and broadcast it to TO. After receiving provided flexibility from all TAs, TO updates its price signal and sent a new price signal λ_F^{k+1} to all TAs. Like P2P market, this negotiation process in the flexibility market is iterative and repeats till the convergence criteria is met (i.e., $\lambda_F^{k+1} - \lambda_F^k < \epsilon$, where ϵ = small positive number for process termination).

Afterward, TO sends a flexibility commitment message based on the aggregated flexibility of all agents to the requester to inform how much flexibility agents can provide in response to flexibility request.

3. Cyber Attacks in the Transactive Energy Market

Though TEM brings a set of advantages to the modern power system by integrating DERs into the traditional electricity market, it also creates opportunities for several cyber attacks and security threats that never existed with the conventional grid, like FDIA [9], DoS attack [10,11], replay attack [12], eavesdropping attack [13] and energy theft [14]. In this section, we identify and discuss several potential FDIAs during P2P energy trading and flexibility schemes of the day-ahead and intraday market in the Monash Microgrid as TEM implemented for energy management in the microgrid, and we have considered the Monash Microgrid our system model. Note that we leave investigation and analysis of all other attack impacts for our future work.

3.1. False Data Injection Attacks (FDIAs)

Generally, FDIA can be defined as the procedure of injecting false data as an input or manipulating the existing data in the system. Attackers execute FDIA on the power system to acquire benefits for themselves, which cannot be obtained in a regular market scenario or to cause harm to users or to a utility provider with vicious intent. Figure 4. depicts FDIAs through Figure 4a a communication channel and Figure 4b an adverse prosumer. In Figure 4a, an adversary or third-party attacker executes FDIAs to manipulate bid-offer or price signal which is exchanged among prosumers, consumers, and market operators to bring financial loss for all market participants or create a disturbance of the regular market operation. On the other hand, in Figure 4b, an adverse or malicious prosumer acts as an attacker who provides false data to the market operator or peers to increase his own financial benefits. FDIA is also known as a data integrity attack as it strikes the integrity of a system and is considered as one of the vital cyber attacks for the modern power system due to its devastating impacts. After first investigating the impact of FDIA on state estimation of power grids by Liu et al. [33], researchers have carried out a number of studies in recent years to detect, prevent or mitigate the impacts of FDIA on the power grids [34–37].

In the TEM, a considerable amount of information is exchanged among several market components like IoT integrated DERs, different forecasters, market operators, prosumers, consumers, and so forth. This information is transferred between components through communication channels. FDIAs can take place during information transfer through communication channels as well as against most of the TEM's components. Nowadays, attackers target a large number of IoT devices that belong to consumers or prosumers in the TEM for FDIA. Due to the robust power system, these compromised IoT devices individually can not hamper the regular activity of the system, but their coordinated actions can generate major inconvenience [38,39]. Another threat may come from the user/consumer/prosumer of the TEM who seeks personal benefit instead of damage to the system. Adversaries can directly inject false data into the system without manipulating communication links or hacking TEM's components, and they can change bids from smart appliances or IoT devices to gain personal profit [19]. Besides gaining personal profit, FDIA causes a number of consequences in the TEM because the effectiveness of energy trading in the market critically depends on the availability of energy production and consumption information, along with the reliability of energy trading signals [40]. Due to FDIA, the market operator makes faulty decisions, which do not match with the actual market scenario. This attack also instigates excessive or insufficient production of power, economic losses and inconvenience for the users in the market.

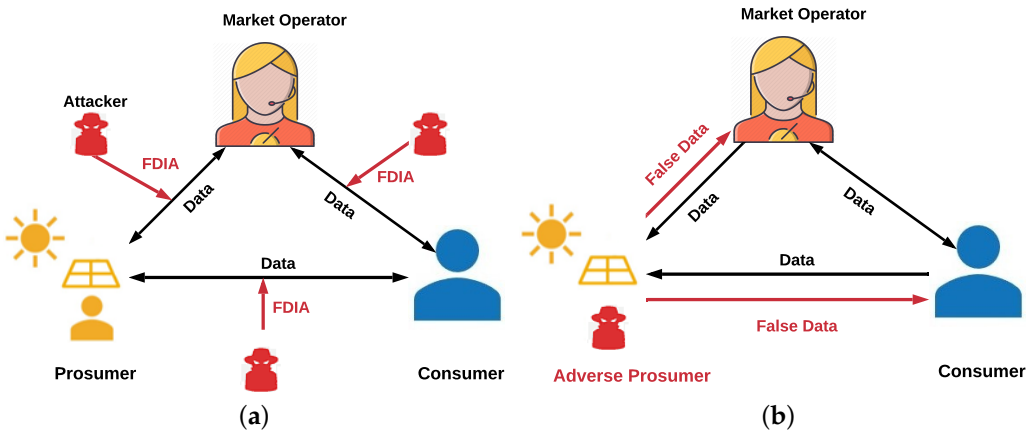

Figure 4. False Data Injection Attacks (FDIAs) through (**a**). Communication channels (**b**). An adverse prosumer

3.2. Attacks

In this subsection, we first investigate who acts as attackers during P2P energy trading and the flexibility scheme of the TEM. Adversaries and malicious users can act as attackers during energy trading and the provision of flexibility in the TEM-based microgrid system. Adversaries or third-party attackers are those who do not have direct access to the microgrid system but have access to the system interface. They do not directly participate in both the P2P market and the flexibility market to sell or buy energy or provide flexibility like prosumers and consumers. However, they aim to acquire, disrupt, or modify information illegitimately during market operation to bring economic disadvantages for all market participants or to disturb the regular market operation. On the other hand, malicious or adverse users (prosumers/consumers) have system access and participate in the P2P market and the flexibility market for trading (selling/buying) energy or providing flexibility. They provide false data to the market operator or manipulate other users' data like bid, price signal, demand/supply to enhance their personal benefits.

As described in Section 2, TEM involves various components such as smart devices, communication channels, users (prosumers, consumers), market operators, and so on. Among all of the market components, communication channels, smart devices and adverse users can act as prime media to perform different cyber attacks due to the fragile security mechanism and direct accessibility to the system. Hence, in this study, we classify the attacks into three main categories based on these attack-prone market components of TEM: (1) Attack through the communication channel; (2) Attack through devices; and (3) Attack through adverse users. It is worth noting that both adversaries and malicious users can plan for different attacks through the communication channel and devices, while only malicious users (consumers or prosumers) act as attackers in the third category. A detailed description of three different types of attacks is described in the following subsections.

3.2.1. Attack through the Communication Channel

In the TEM, an extensive amount of information is transferred from one market component to another via a communication channel during energy trading or providing flexibility. In the P2P and the flexibility market, all TAs send their energy demand and supply, as well as provided flexibility information, to the market operator through the communication link. The market operator sends price signals and TAs place their bid via the communication channel. Moreover, the market operator receives flexibility requests from external or internal requesters through communication links during the flexibility market. An attacker can plan FDIAs through communication links to modify the requested flexibility value, the monetary reward value of proving flexibility, price signals, and bid-offer of any particular user or other users. Moreover, an attacker may attempt to eavesdrop on important messages sent to the market operator using a communication channel. From

these critical messages, the attacker could reveal the private information of users, such as users' identities, meter readings, bid-offer, and information on energy supply/demand.

As discussed in Sections 2.1.5 and 2.1.6, TO runs a flexibility market or a joint flexibility and P2P market in each time slot of day-ahead and intraday market in the Monash Microgrid. During market operations, an adversary or a malicious user can launch FDIAs through communication channels to alter important information. To describe the attacks clearly, we consider the following attack scenario.

Example 1. *We assume that an external requester sends a signal to the TO for F = 1000 kW demand reduction of the microgrid in a specific time slot, and the monetary reward for the demand reduction is λ_F = 4 \$/kWh, which TAs will receive from network providers based on the amount of demand reduction in the real-time. Suppose an adversary changes the signal from (1000 kW, 4 \$/kWh) to (100 kW, 1 \$/kWh) and then sends the modified signal to the TO. After receiving flexibility request, TO triggers the flexibility market by sending bid requests for 100 kW flexibility instead of 1000 kW to TAs. In response, TAs send bid offers to the TO to provide available flexibility. An adversary attack in the communication link between the flexibility requester and TO and no verification process exists between them, TO could not identify the attack. Figure 5 depicts the scenario (highlighted by red color).*

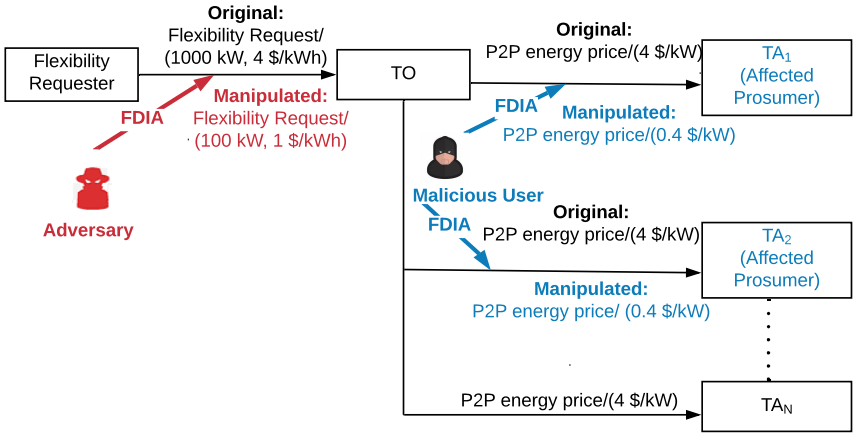

Figure 5. FDIAs through communication channel by an adversary and a malicious user highlighted by red and blue color, respectively.

Now consider the attack scenario for the operation of the P2P energy trading market. Suppose, TO sends initial price signal λ_P^k = 4 \$/kW to TAs. TAs determine traded energy in the P2P market $P_{i,P}^k$ based on λ_P^k. A malicious prosumer can conduct an FDIA and alters 4 \$/kW into 0.4 \$/kW and sent the manipulated λ_P^k to other TAs. In Figure 5, we illustrate the scenario highlighted by blue color. Also, a malicious consumer can act as an attacker in the above-described scenario and changes 4 \$/kW into 14 \$/kW before sending the signal to other TAs. The affected prosumer or consumer TAs cannot identify the attack due to the lack of verification process between TO and TAs.

3.2.2. Attack through Devices

TAs in the TEM are general users who pose fragile security mechanisms. Attackers exploit this vulnerability and design different cyberattacks by targeting less secure elements in the system, such as smart meters, smart home appliances, smart heating, ventilating and air conditioning (HVAC) systems and IoT-integrated DERs. As discussed in Section 2, TEM implementation requires an advanced meter infrastructure (AMI) in the grid systems where a smart meter is installed at each TA end to real-time measure energy usage. As all smart meters are connected in a smart community with a wired or wireless network, a malicious user can attack the smart meter of one particular or several TAs to manipulate the energy consumption report. This type of attack is known as an energy theft attack [14] where an

adversary could tamper his own meter to reduce the energy consumption measured by his smart meter and increase the measurement of the victim TAs' energy usage.

In the TEM, IoT integrated DERs introduce several potential vulnerabilities to a number of cyberattacks, as DER's forecasting data plays a vital role in power system planning. Generally, before starting a market in the Monash Microgrid, DER forecasting capability provides information about a user's demand or supply of energy for the next hours or days in advance, considering weather, load and energy generation. Then, TAs send information of surplus or deficit energy to TO for different time slots based on DER's forecasting. Suppose an adversary organizes FDIAs in numerous DERs to change their respective forecast data. In that case, the TEM operation may be impacted in various ways as robustness against forecast errors and attacks have not yet been addressed in the Monash Microgrid. To properly explain the attack through devices, an example is given below.

Example 2. *A malicious prosumer TA_i plans an FDIA through DERs. The attacker aims to increase the energy demand of TA_1 and TA_2 for time slot 1 p.m. to 3 p.m. to create manipulated energy demand in the market. To achieve the goal, TA_i hacks and takes control of IoT integrated DERs of TA_1 and TA_1 and increases the temperature data significantly for the specific period. Due to the rise in temperature data, the energy demand of respective users ($P_{1,P}$, $P_{2,P}$) grows too. Assume that the energy demand of TA_1 and TA_2 increases from 50 kW to 150 kW and 80 kW to 180 kW, respectively. Hence, TA_1 and TA_2 will join in the P2P market to buy manipulated deficit energy from other users. Figure 6 illustrates the described scenario, where the forecasting manager is a part of DER, which is responsible for providing an energy or flexibility forecast. Instead of rising energy demand, the attacker can reduce the energy demand of targeted users below the actual value by reducing the temperature data of the respective DERs.*

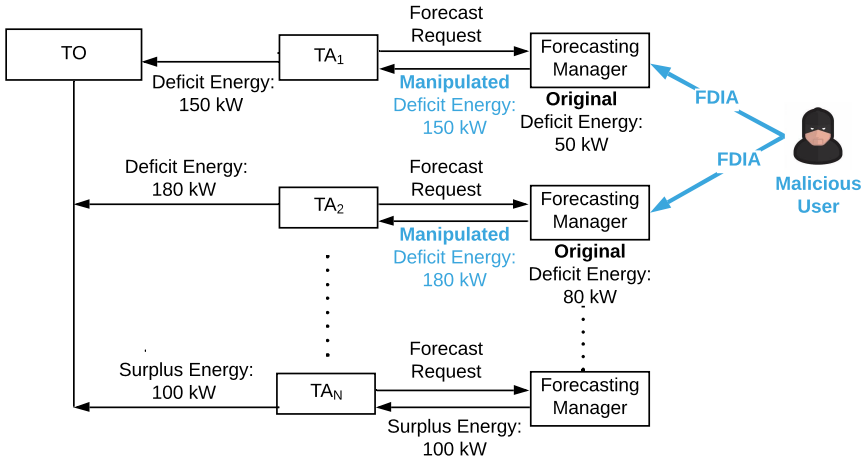

Figure 6. FDIAs through the distributed energy resources (DERs) of TEM by a malicious user.

An adversary can target DERs to manipulate the flexibility amount as TAs decide how much flexibility it can provide in a specified time slot during the flexibility market based on expected energy demand and supply. Suppose an adversary minimizes the energy demand of TA_i by lessening the temperature data of TA_i's DER from 12 p.m. to 1 p.m. When TA_i receives a bid request from TO to provide flexibility in this period, TA_i participates in the auction and provides an offer based on manipulated predicted data. However, during real operation, TA_i may not be able to provide the committed flexibility, ΔP_i, as its actual energy demand is more than the predicted value.

3.2.3. Attack through Adverse Users

TEM encourages small-scale producers and consumers to participate in different markets, such as the P2P market, flexibility market, local market, to trade energy with each other. It brings several benefits for both users and utility companies. Users (prosumers and consumers) receive economic benefits by selling or buying energy from their peers, while utility companies can reduce peak demand, operating costs and increase the overall

efficiency of the power system [41]. However, some users act as attackers in the TEM to escalate personal benefits or create disturbance in the regular operation of the market. In the previous two attack categories, we already discussed a number of attacks that can be done by adverse users through communication channels and devices. Note that, under this section, we will discuss some attack scenarios that adverse users could create intentionally and, due to these attacks, some severe consequences may arise in the power system such as power outage.

As mentioned in Section 2.1.3, TO runs the day-ahead market in the Monash Microgrid to finalize commitment for the next hours or day. Contrarily, the users participate in the intraday market to fulfill unmet commitments during the actual operation. Now, consider the following scenario.

Example 3. *An internal requester sent a message to TO to reduce F = 500 kW demand from 12 p.m. to 1.00 p.m. as a possibility of exceeding a peak demand level has been predicted. Then, TO triggers the flexibility market by sending bid-request to all TAs. Now, TA_i participates in the auction and submits an offer (f_i,λ_i) where f_i = 200 kW and λ_i = 2 \$/kWh. Assume that TA_i wins the auction and settles the commitment with TO to reduce 200 kW demand in the mentioned period with other users in advance. Anyhow, TA_i could not minimize his consumption from 12 p.m. to 1.00 p.m. and does not inform TO about the inability to provide flexibility beforehand deliberately. Due to the lack of proper information from TA_i, TO could not trigger the flexibility market for requesting 200 kW demand reduction from other TAs. Such adverse behavior of TA_i will bring serious problems to the microgrid system.*

Like the flexibility market, seller TAs settle their commitment in advance with buyer TAs regarding the energy supply of the particular time slots during the P2P market operation (settlement procedure described in Section 2.1.6). Assume that a seller TA, TA_i, joins in the P2P market and informs TO to sell $P_{i,P}$ = 100 kW surplus generation. Then, TA_i settles his commitment with TO to provide 100 kW energy. If TA_i could not generate the committed energy during actual operation and does not notify the condition to TO earlier, the market operation will be hampered differently.

4. Impact Analysis

Due to the attacks described in the above section, the TEM users and market operations in the Monash Microgrid can be severely impacted in many ways. Attackers execute these attacks to acquire benefits for themselves, harm a set of agents or users economically, hamper the market's activities, increase the operation cost of systems, create catastrophic events and so on. This section describes a set of impacts on the different attacks on the TEM.

4.1. Impact Analysis of Attacks through the Communication Channel

When attackers launch attacks over the communication channel during the flexibility market and P2P energy trading market, as described in Section 3.2.1, in the microgrid system, TEM operations will be affected in different ways. To describe the attack impact clearly, we refer to Example 1 of Section 3.2.1 here. In Example 1, the attacker manipulates the requested flexibility amount and monetary reward in return to provide flexibility through FDIA in the flexibility market. Due to the change of flexibility request value F from 1000 kW to 100 kW, users or TAs cannot provide sufficient flexibility to the requesters though some TAs have adequate energy generation during this particular period. As a result, many TAs who may have enough energy generation do not get a chance to provide flexibility and gain financial benefits during the mentioned time. Moreover, the attacker alters the monetary reward value λ_F to 1 \$/kWh from 4 \$/kWh. Therefore, only a few TAs who offer equal or less than 1 \$/kWh to provide flexibility win the auction (the auction mechanism is described in Section 2.1.5). However, in the attack-free scenario, many of them can win the auction and receive economic advantages as the original monetary reward is 4 \$/kWh.

In addition, due to the attack through communication channels in the P2P energy trading market, the adverse TA achieves financial gain, whereas victim TAs are affected

economically. In Example 1, the adverse prosumer launches FDIA over the price signal λ_P^k which TO sent to TAs during the P2P market and changes into a small value. TAs determine traded energy in the P2P market $P_{i,P}^k$ based on the λ_P^k and sent $P_{i,P}^k$ to TO to inform how much energy they want to sell or buy from the P2P market. Due to low energy price, victim prosumers may offer a limited amount of energy to sell in the market while the adverse prosumer sells their whole surplus energy. On the contrary, if a malicious consumer acts as an attacker and changes original λ_P^k to a high value, other consumers buy little or no energy from the market while the malicious consumer buys his necessary energy with lower prices.

Besides FDIAs, malicious users can increase their profits by eavesdropping on the bid/offer of other TAs through the communication channel. For instance, a misbehaving user can offer lower selling prices than other users in order to win the auction, which brings economic disadvantages for legitimate TAs as they repeatedly lose the auction for higher bids. It also disrupts the regular market operation. Moreover, an external attacker can reveal the private information of TAs by eavesdropping messages sent to the TO and leads to privacy threats of TAs. Attackers can identify one designated user's energy consumption pattern by monitoring how much energy the user is selling/buying in different time slots, especially in day-time or weekends. This pattern helps the attackers to reveal when the user is out of home and plan for burglary or robbery accordingly.

4.2. Impact Analysis of Attacks through Devices

In the TEM, attack through a number of smart devices could impact not only targeted users but also TEM's activities. A malicious user can perform an energy theft attack by tampering his and a certain user's smart meter to manipulate their respective energy usage reports. The adverse user decreases his meter measurement while enlarging the target users' energy usage. Thus, victim users receive raised bills and the bill for the adverse users is reduced.

In the TEM, forecasting data from DER plays a crucial role in users' energy and flexibility estimation as it directly affects the energy cost and system operation. To illustrate the impact properly, we refer to Example 2 here, where adverse prosumer TA_i increase the energy demand of TA_1, and TA_2 from 1 pm to 3 pm by FDIAs through their respective DERs. Due to the rise in energy demand, TA_1 and TA_2 join in the P2P market to buy their deficit energy $P_{1,P}$, and $P_{2,P}$, respectively. As energy demand escalates in the market, adverse prosumers dramatically raise the energy prices λ_P^k in the market. Consequently, victim users have to buy higher energy than the actual demand from peers at overpriced. Furthermore, if prosumers cannot supply enough energy in the P2P market, affected consumers need to purchase energy $P_{i,G}$ from the grid at an excessive rate as the grid's energy price is fixed and higher than the P2P market. Nevertheless, the attackers can decrease the temperature data or demand, which leads to load shedding as users do not arrange or schedule extra energy or generators for the remaining loads.

Moreover, FDIAs through devices during the flexibility market of the Monash Microgrid will also bring a number of consequences. In Example 2, TA_i settled his commitment with TO in advance to provide flexibility from 12 p.m. to 1 p.m. based on the false predicted forecast due to the attack. But actual energy demand is higher than the expected value. Hence, TA_i may not fulfill the commitment in real-time, which affects the system's reliability as TO made a commitment with requesters considering TA_i's flexibility. Also, it may create load shedding or a power outage in the system during this period if energy consumption of all users exceeded the peak demand level of the system.

4.3. Impact Analysis of Attacks through Adverse Users

In this subsection, we analyze potential damages for TEM introduced by adverse users of the system. In the flexibility scheme and P2P energy trading of the Monash Microgrid, some adverse users finalize their commitment during the day-ahead market but intentionally do not deliver the committed energy/flexibility in real-time. This article

considers such type of user's behavior as attacks because it can bring significant damages to the system. To depict the attack's impact, Example 3 is referred to here. In Example 3, TA_i settled commitment with TO about 200 kW demand reduction during the day-ahead market. If TA_i does not minimize his consumption in real-time, it would potentially cause load shedding from 12 p.m. to 1.00 p.m. as a possibility of surpassing a peak demand level has been forecasted by the microgrid monitoring function.

Furthermore, the malicious behavior of TA_i during P2P energy trading will impact on the operation cost of the systems. TA_i settle his commitment with TO to sell 100 kW energy. If TA_i could not generate the committed energy during actual operation, the buyer TAs who finalized their commitment beforehand needs to buy deficit energy from the grid or other sources during real-time at a higher rate, which leads to economic loss for the buyer TAs. Moreover, if seller TAs repeatedly made wrong commitments and fail to fulfill the commitment in the delivery time, this type of adversarial behavior also impacts the reliability of the TEM's operation along with the regular market operation.

Table 3 summarizes the probable impacts of three types of attacks in the Monash Microgrid system. Note that, though this paper investigates the attacks and analyzes the attack impacts based on the Monash Microgrid, attackers can execute the above-described attacks in any TEM-based microgrid system, which may bring the listed impacts on the TEM users and market operation of those microgrid systems as well.

Table 3. Impact of Attacks in the Monash Microgrid system.

Attack Type	Impact
• Attack through communication channel	• Financial losses of affected users • Economic benefits of malicious users • Privacy Threats • Risks for burglary or robbery • Disturbance of market operation
• Attack through devices	• Increase energy prices • Load shedding • Maximize personal gains of malicious users • Economic disadvantages of affected users • Disturbance of regular market operation
• Attack through adverse users	• Load shedding • Disturbance of regular market operation • Reduce system reliability • Financial losses of affected users

5. Conclusions and Future Work

In this paper, we have studied the potential cyber vulnerabilities generally existing in the TEM. Nowadays, TEM is getting popular and brings a number of advantages to the modern power system. It also opens the door for internal or external adversaries to launch different cyber attacks in order to maximize their personal gains, reduce the profits of other users, or interrupt the system's operation. Hence, we have identified and categorized the possible attacks on TEM during trading energy with peers or providing flexibility in response to external or internal requesters. Then, we have analyzed the impacts of these attacks in general.

For future work, we plan to execute, evaluate and analyze several FDIAs by changing the requested flexibility value, monetary reward value for providing flexibility, forecasting data from different forecasters such as weather forecaster, demand, or load forecasters against P2P energy trading and flexibility schemes of day-ahead and intraday market in the Monash Microgrid to evaluate the impact of attacks. Then, the impact of FDIAs on

microgrid users will be compared to the attack-free scenarios. We plan to investigate and analyze the impact of some other attacks such as DOS attacks and replay attacks during the P2P and flexibility market of the microgrid system. We also intend to propose attack detection schemes and deploy them in the Monash Microgrid in the future.

Author Contributions: Conceptualization, R.D.; investigation, R.D., A.S., C.R.; analysis, R.D., A.S., C.R.; writing—original draft preparation, R.D.; writing—review and editing, R.D., A.S., C.R.; supervision, A.S., C.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DER	Distributed Energy Resource
TE	Transactive Energy
TEM	Transactive Energy Market
ICT	Information and Communication Technology
P2P	Peer to Peer
IoT	Internet of Things
FDIA	False Data Injection Attack
DOS	Denial-of-Service
GWAC	Gridwise Architecture Council
PV	Photovoltaic
EV	Electric Vehicle
TO	Transactive Energy Market Operator
TA	Transactive Energy Market Agent
HVAC	Heating, Ventilating, and Air Conditioning

References

1. Martini, P.; Chandy, K.M.; Fromer, N.A. *Grid 2020: Towards a Policy of Renewable and Distributed Energy Resources*; California Institute of Technology: Pasadena, CA, USA, 2012.
2. Goncalves Da Silva, P.; Ilić, D.; Karnouskos, S. The Impact of Smart Grid Prosumer Grouping on Forecasting Accuracy and Its Benefits for Local Electricity Market Trading. *IEEE Trans. Smart Grid* **2014**, *5*, 402–410. [CrossRef]
3. Lezama, F.; Soares, J.; Hernandez-Leal, P.; Kaisers, M.; Pinto, T.; Vale, Z. Local Energy Markets: Paving the Path Toward Fully Transactive Energy Systems. *IEEE Trans. Power Syst.* **2019**, *34*, 4081–4088. [CrossRef]
4. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart Grid—The New and Improved Power Grid: A Survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980. [CrossRef]
5. Zhang, C.; Wu, J.; Zhou, Y.; Cheng, C.L. Peer-to-Peer energy trading in a Microgrid. *Appl. Energy* **2018**, *220*, 1–12. [CrossRef]
6. Ipakchi, A. Demand side and distributed resource management—A transactive solution. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–8. [CrossRef]
7. Monacchi, A.; Elmenreich, W. Assisted energy management in smart microgrids. *J. Ambient. Intell. Hum. Comput.* **2016**, *7*, 901–913. [CrossRef]
8. Hirsch, A.; Parag, Y.; Guerrero, J. Microgrids: A review of technologies, key drivers, and outstanding issues. *Elsevier* **2018**, *90*, 402–411. [CrossRef]
9. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1630–1638. [CrossRef]
10. Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Li, J. A denial of service attack in advanced metering infrastructure network. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June 2014; pp. 1029–1034. [CrossRef]
11. Wang, Q.; Tai, W.; Tang, Y.; Zhu, H.; Zhang, M.; Zhou, D. Coordinated Defense of Distributed Denial of Service Attacks against the Multi-Area Load Frequency Control Services. *Energies* **2019**, *12*, 2493. [CrossRef]
12. Hosseinzadeh, M.; Sinopoli, B.; Garone, E. Feasibility and Detection of Replay Attack in Networked Constrained Cyber-Physical Systems. In Proceedings of the 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 24–27 September 2019; pp. 712–717. [CrossRef]
13. Cleveland, F.M. Cyber security issues for Advanced Metering Infrasttructure (AMI). In Proceedings of the 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–5. [CrossRef]

14. Liu, Y.; Hu, S. Cyberthreat Analysis and Detection for Energy Theft in Social Networking of Smart Homes. *IEEE Trans. Comput. Soc. Syst.* **2015**, *2*, 148–158. [CrossRef]
15. Jhala, K.; Natarajan, B.; Pahwa, A.; Wu, H. Stability of Transactive Energy Market-Based Power Distribution System Under Data Integrity Attack. *IEEE Trans. Ind. Inform.* **2019**, *15*, 5541–5550. [CrossRef]
16. Zhang, Y.; Krishnan, V.V.G.; Pi, J.; Kaur, K.; Srivastava, A.; Hahn, A.; Suresh, S. Cyber Physical Security Analytics for Transactive Energy Systems. *IEEE Trans. Smart Grid* **2020**, *11*, 931–941. [CrossRef]
17. Zhang, Y.; Eisele, S.; Abhishek Dubey, A.L.; Srivastava, A.K. Cyber-Physical Simulation Platform for Security Assessment of Transactive Energy Systems. In Proceedings of the 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Montreal, QC, Canada, 15 April 2019.
18. Barreto, C.; Koutsoukos, X. Attacks on Electricity Markets. In Proceedings of the 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 24–27 September 2019; pp. 705–711. [CrossRef]
19. Barreto, C.; Neema, H.; Koutsoukos, X. Attacking Electricity Markets Through IoT Devices. *Computer* **2020**, *53*, 55–62. [CrossRef]
20. Boroojeni, K.G.; Amini, M.H.; Nejadpak, A.; Iyengar, S.S.; Hoseinzadeh, B.; Bak, C.L. A theoretical bilevel control scheme for power networks with large-scale penetration of distributed renewable resources. In Proceedings of the 2016 IEEE International Conference on Electro Information Technology (EIT), Grand Forks, ND, USA, 19–21 May 2016; pp. 0510–0515. [CrossRef]
21. Forfia, D.; Knight, M.; Melton, R. The View from the Top of the Mountain: Building a Community of Practice with the GridWise Transactive Energy Framework. *IEEE Power Energy Mag.* **2016**, *14*, 25–33. [CrossRef]
22. Melton, R.B. *GridWise Transactive Energy Framework*; Pacific Northwest National Lab. (PNNL): Richland, WA, USA, 2013.
23. Holmberg, D.G.; Hardin, D.; Melton, R.; Widergren, R.C.S. Transactive Energy Application Landscape Scenarios. 2016. Available online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=921591 (accessed on 19 October 2020)
24. Camarinha-Matos, L.M. Collaborative smart grids—A survey on trends. *Renew. Sustain. Energy Rev.* **2016**, *65*, 283–294. [CrossRef]
25. Rahimi, F.; Albuyeh, F. Applying lessons learned from transmission open access to distribution and grid-edge Transactive Energy systems. In Proceedings of the 2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), Minneapolis, MN, USA, 6–9 September 2016; pp. 1–5. [CrossRef]
26. Sanseverino, E.R.; Di Silvestre, M.L.; Gallo, P.; Zizzo, G.; Ippolito, M. The Blockchain in Microgrids for Transacting Energy and Attributing Losses. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 925–930. [CrossRef]
27. Akter, M.N.; Mahmud, M.A.; Oo, A.M.T. A hierarchical transactive energy management system for microgrids. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5. [CrossRef]
28. Sobe, A.; Elmenreich, W. Smart Microgrids: Overview and Outlook. *arXiv* **2013**, arXiv:1304.3944.
29. Khorasany, M.; Azuatalam, D.; Glasgow, R.; Liebman, A.; Razzaghi, R. Transactive Energy Market for Energy Management in Microgrids: The Monash Microgrid Case Study. *Energies* **2020**, *13*, 2010, [CrossRef]
30. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
31. Allgau Microgrid. Available online: https://lo3energy.com/innovations/ (accessed on 19 October 2020).
32. Residential Microgrid in South Australia. Available online: https://lo3energy.com/innovations/ (accessed on 19 October 2020).
33. Deng, R.; Zhuang, P.; Liang, H. False Data Injection Attacks Against State Estimation in Power Distribution Systems. *IEEE Trans. Smart Grid* **2019**, *10*, 2871–2881. [CrossRef]
34. Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Trans. Smart Grid* **2018**, *9*, 2862–2872. [CrossRef]
35. Kim, J.; Tong, L.; Thomas, R.J. Dynamic attacks on power systems economic dispatch. In Proceedings of the 2014 48th Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, USA, 2–5 November 2014; pp. 345–349. [CrossRef]
36. Giraldo, J.; Cárdenas, A.; Quijano, N. Integrity Attacks on Real-Time Pricing in Smart Grids: Impact and Countermeasures. *IEEE Trans. Smart Grid* **2017**, *8*, 2249–2257. [CrossRef]
37. Zhang, X.; Yang, X.; Lin, J.; Xu, G.; Yu, W. On Data Integrity Attacks Against Real-Time Pricing in Energy-Based Cyber-Physical Systems. *IEEE Trans. Parallel Distrib. Syst.* **2017**, *28*, 170–187. [CrossRef]
38. Soltan, S.; Mittal, P.; Poor, H.V. BlackIoT: IoT Botnet of high wattage devices can disrupt the power grid. In Proceedings of the SEC'18: Proceedings of the 27th USENIX Conference on Security Symposium, Baltimore, MD, USA, 14 August 2018; pp. 15–32. [CrossRef]
39. Huang, B.; Cardenas, A.A.; Baldick, R. Not everything is dark and gloomy: Power grid protections against IoT demand attacks. In Proceedings of the SEC'19 28th USENIX Conference on Security Symposium, Santa Clara, CA, USA, 14–16 August 2019; pp. 1115–1132. [CrossRef]
40. Majumder, R.; Bag, G.; Kim, K. Power sharing and control in distributed generation with wireless sensor networks. In Proceedings of the 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012; p. 1. [CrossRef]
41. Bayram, I.S.; Shakir, M.Z.; Abdallah, M.; Qaraqe, K. A survey on energy trading in smart grid. In Proceedings of the 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Atlanta, GA, USA, 3–5 December 2014; pp. 258–262. [CrossRef]