UNIVERSITY
OF OSLO

Sara Mohammadi

# Local Energy Trading Markets with Prosumers Considering Fairness and Security

**Thesis submitted for the degree of Philosophiae Doctor**

**Department of Informatics**
**Faculty of Mathematics and Natural Sciences**


**2024**

*Series of dissertations submitted to the*
*Faculty of Mathematics and Natural Sciences, University of Oslo*
*No. 2721*

ISSN 1501-7710



Cover: UiO.
Print production: Graphic center, University of Oslo.

# Preface

This thesis is submitted in partial fulfillment of the requirements for the degree of *Philosophiae Doctor* at the University of Oslo. The research presented here was conducted at the Department of Informatics, UiO, under the supervision of professor Frank Eliassen, professor Yan Zhang, and professor Hans-Arno Jacobsen. This work was funded by the Norwegian Research Council under the SmartNEM project grant number 267967.

The thesis is a collection of three papers, presented in peer-reviewed scientific conference and journals in secure computing, machine learning, and energy. The papers are preceded by an introductory chapter that relates them to each other and provides background information and motivation for the work. I have been involved as a main contributor in each one of these papers, and they were written between 2019 and 2022 for the purpose of supporting the thesis.

## Acknowledgements

I would like to begin by expressing my sincere gratitude to the people that have played an invaluable role in the completion of my doctoral thesis. This journey has been long and challenging, and I could not have reached this milestone without the support, guidance, and encouragement of those around me.

First and foremost, I am deeply indebted to my main supervisor, Frank Eliassen, for his unwavering support, patience, and mentorship throughout this entire process. His commitment to academic excellence and his ability to inspire a passion for research in his students have been truly invaluable. I am deeply thankful for the hours he spent reviewing my work, providing constructive criticism, and fostering an environment of intellectual curiosity. Professor Eliassen's mentorship has not only enriched my academic experience but has also had a profound impact on my personal and professional growth.

I would also like to extend my sincere appreciation to my co-supervisors, Professor Yan Zhang and Professor Hans-Arno Jacobsen, for their invaluable contributions to my research. Their expertise in their respective fields added a multifaceted dimension to my work, and their support and guidance were instrumental in shaping the quality and depth of my thesis. I am grateful for the opportunities to collaborate with them and for their insightful feedback, which significantly improved the overall quality of my research.

I am also deeply appreciative of my manager at Volue, Gisle Tveit, for the exceptional support and understanding he has extended to me during the initial phase of my job. His willingness to grant me one month of dedicated time to work on my Ph.D. thesis has been instrumental in allowing me to strike a harmonious balance between my professional responsibilities and my academic pursuits.

I would like to express my heartfelt gratitude to my beloved parents. My mother, Esmat, and father, Ali Akbar, have been my steadfast pillars of support throughout my academic journey. Their boundless love, sacrifices, and encouragement have been the driving force behind my successes, including the completion of this Ph.D. thesis. Their belief in me, even during moments of doubt, has been an unshakeable source of strength. I am grateful to my sisters, Fatemeh and Najme, who, as my older siblings, have been a constant source of inspiration and encouragement. Their resilience and achievements have motivated me to strive for excellence in my academic pursuits. I also want to express my appreciation to my youngest sister, Shirin, whose presence in my life brings a special kind of joy and motivation. Her curiosity and enthusiasm nature have reminded me of the importance of curiosity and wonder in the pursuit of knowledge. I am grateful for their enduring love and the strength of our family bond, which has been a constant source of motivation and solace in the face of academic challenges.

Lastly, but not the least, I want to say a big thank you to my friends. I would like to especially thank Peyman for his invaluable support and the wealth of knowledge I gained from him in the field of Machine Learning. I also thank Elahe, Saba, Farzane, Sanaz, and Maryam who have always been there in both

good and tough times.

This thesis would not have been possible without the collective support and encouragement of all those mentioned above, and I am sincerely grateful to each and every one of you.

**Sara Mohammadi**
Oslo, February 2024

# Abstract

Renewable energy sources, such as solar and wind, play a vital role in combatting climate change and ensuring energy sustainability by reducing greenhouse gas emissions and air pollution. The advancements in renewable technologies have made them cost-effective and accessible, promoting a greener future. Integrating solar panels and other distributed renewable sources into homes and communities decentralizes and decarbonizes energy systems, while microgrids and peer-to-peer energy trading empower communities to optimize renewable resource utilization and engage in sustainable practices. However, there are challenges in apartment buildings regarding onsite renewable energy adoption due to limited rooftop space, complex ownership structures, and shared energy consumption patterns among multiple residents. The lack of specific regulations further complicates the situation, hindering apartment residents from accessing the benefits of locally generated clean energy. Therefore, tailored solutions need to be developed to overcome these barriers and ensure a more sustainable and equitable energy future for all residents.

In the rapidly evolving energy sector, peer-to-peer (P2P) energy trading has emerged as a promising and innovative approach for the future smart grid. P2P energy trading enables direct transactions between energy producers and consumers, fostering decentralized, efficient, and sustainable energy distribution. Despite the benefits, P2P energy trading faces challenges, particularly concerning security vulnerabilities. False data injection attacks pose a significant threat, allowing malicious actors to manipulate data within the trading system, disrupting its integrity and potentially causing unauthorized access or financial losses. Addressing these security concerns is crucial to maintain the reliable and secure operation of P2P energy trading and to ensure that this innovative approach contributes positively to the energy landscape.

This dissertation is dedicated to studying the above-mentioned challenges and contributes to two main categories. First, it focuses on securing energy trading markets in the smart grid. It analyzes some possible threats that can occur in a local peer-to-peer energy trading market and then explores the effects of the attacks. A proper defense is needed after finding possible ways to attack an energy trading market. Integrating detection methods into security strategies is vital to counter modern cyber threats like false data injection attacks (FDIAs). This thesis deploys machine learning-based techniques, which are now an effective solution for efficient cyber attack detection, to extract valuable insights from data to identify abnormal patterns. Second, it studies energy sharing in multi-unit buildings. It investigates the effects of shared distributed renewable energy sources, including PV panels and battery energy storage systems, in multi-unit buildings. In this regard, this thesis studies the main principles of energy justice

and analyses how these principles can be applied in energy trading and allocation processes to achieve fair energy sharing.

In the context of security issues in the P2P energy trading market, this thesis concludes that the ability to identify and detect potential threats, such as FDIAs, highlights the role of the P2P trading model as an effective motivator for traditional energy consumers to transition into prosumers. This shift is driven by the model's promotion of low internal prices and the provision of substantial utility benefits. Conversely, in the absence of robust security measures (i.e., machine learning-based attack detection models), prosumers may face significant economic losses due to these attacks. Consequently, this could diminish the incentive for participants to either continue as energy-producing prosumers or make the transition to becoming one.

In the setting of energy sharing in multi-unit buildings, this thesis demonstrates that developing distributed renewable energy sources in multi-unit buildings allows different groups of residents to gain financial benefit from the shared energy systems. Furthermore, this thesis suggests that applying the principles of energy justice to energy sharing models enables a fair and equitable energy-sharing system in the buildings, while also removing or reducing barriers to the active participation of end customers (consumers/prosumers) in the future smart and decentralized energy grid. In summary, this thesis concludes that justice principles must be incorporated into the design of energy-sharing models in the first step. These principles can be implemented in various ways, and their definition may vary depending on the context or situation. The application of energy justice principles in the proposed sharing models motivates residents to utilize the shared DRESs (Distributed Renewable Energy Sources) of their building, resulting in significant financial benefits for the building.

# List of Papers

## Paper I

Sara Mohammadi, Frank Eliassen, and Yan Zhang,"Effects of false data injection attacks on a local P2P energy trading market with prosumers", In: *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe) Conference*, October 26-28 2020, pp. 31–35. DOI: 10.1109/ISGT-Europe47291.2020.9248761.

## Paper II

Sara Mohammadi, Frank Eliassen, and Yan Zhang, and Hans-Arno Jacobsen,"Detecting false data injection attacks in peer to peer energy trading using machine learning", In: *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 3417-3431, 1 Sept.-Oct. 2022, DOI: 10.1109/TDSC.2021.3096213.

## Paper III

Sara Mohammadi, Frank Eliassen, and Hans-Arno Jacobsen,"Applying Energy Justice Principles to Renewable Energy Trading and Allocation in Multi-Unit Buildings", In: *Energies*, vol. 16, no. 3, pp. 1150, 2023, DOI: https://doi.org/10.3390/en16031150.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 Motivation

Conventional electricity supply systems are based on a centralized generating facility that supplies the transmission and distribution networks [1]. Such systems are generally costly, ineffective, and heavily reliant on fossil fuels, which are scarce and contribute substantially to pollution [2]. The idea of decentralizing the generation capacity of electricity supply systems has gained popularity in recent years [3-5]. Distributed generation systems, which primarily rely on renewable energy sources rather than fossil fuels, are more efficient. The emergence of renewable energy resources, smart homes, and smart grids presents an opportunity for individuals to generate energy to meet their own needs while selling surplus energy to their neighbors for their local needs [Las+17]. As a result, traditional consumers has become prosumers and peer-to-peer (P2P) energy trading has experienced significant growth in recent years [Par+21]. Studies have shown that renewable energy contributes to a country's economic progress [Dog+20]. A microgrid (MG) is a local energy grid with control capabilities that can operate in conjunction with the traditional power grid in connected or isolated modes. MG integrates distributed energy resources (DER) with storage devices and flexible loads to form low-voltage distribution systems that facilitate energy sharing [Ker+21]. With renewable energy resources distributed across MG, energy traders can engage in P2P energy transactions, allowing residents to generate, store, and trade energy in a local energy market without the need for a third party [Bul+18].

However, P2P energy trading requires bi-directional network communication, making the system vulnerable to various attacks that cause integrity loss. Therefore, energy trading raises security and privacy concerns for energy traders, including private data leakage, data breaches, distributed denial of service (DDoS), man-in-the-middle (MITM) attacks, and False data injection attacks (FDIAs). The impact of FDIA has been extensively studied for the past decade, but its impacts on P2P energy trading markets at a local level involving prosumers have not been well investigated. Examining this aspect is crucial as the presence of prosumers in a local energy market presents a challenge for energy sellers such as suppliers. Hence, we are motivated to investigate the possible ways of threats, such as FDIAs, in the local P2P energy trading markets and their impacts on the markets. Due to this multitude of threats, it is important to implement appropriate protection measures to secure energy trading processes in the smart grid. The security and performance of smart grid systems heavily depend on precise and dependable attack detection. Machine learning (ML) based attack detection techniques have the potential to identify and categorize cyber-attacks

accurately. They can detect unknown and known anomalies in the complex cyber-physical data flow in real-time. In this thesis, we use cutting-edge machine learning techniques as a defense strategy in P2P energy trading.

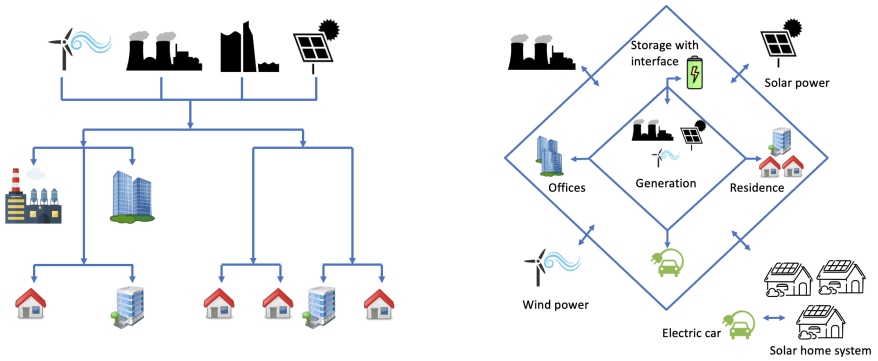
Although PV deployment in residential sector has mainly focused on detached houses in most areas, there is growing enthusiasm for maximizing solar self-consumption and self-sufficiency by installing PV panels on the roof of apartment buildings. Engaging all apartment residents as energy consumers and every apartment owner as an investor in PV infrastructure is crucial. However, this can be challenging. On the positive side, it presents an opportunity to establish new and innovative business associations among apartment owners and residents that allow for equitable distribution of the net advantages of rooftop PV production. Indeed, residents with different preferences and the diversity in load demands in apartment buildings can hamper the fair and equitable distribution of energy and benefits. Therefore, it is necessary to develop a framework to establish an equitable and fair energy-sharing system in multi-unit buildings that allows various groups of residents to reap the advantages of the shared DRESs within their building. According to these challenges, we are motivated to investigate energy sharing in multi-unit buildings and propose novel energy sharing models considering justice and fairness.

## 1.2 Background

### 1.2.1 Smart Grid Concepts

Today, the demand for reliable energy has increased due to the increasing global population, urbanization, and technological advancements. However, the conventional electric power infrastructure called 'the grid' faces challenges that hinder its reliability, scalability, and low-cost and effective operations. This has led to the development of an intelligent and modern grid known as the smart grid [Dil20]. Figure 1.1 shows the distinct differences between the infrastructure of the conventional power grid and the components of the smart grid. The conventional systems operate with a one-directional flow of energy, while smart energy systems allow for the flow of both energy and information in two directions between the generation and distribution sides. Unlike the rigid structure of conventional energy networks, the smart grid allows for electricity to be produced on the consumer side through renewable power sources such as solar and wind farms or distributed generation sources [Ghi+23].

This innovation has revolutionized the way we consume, generate, and manage energy. One of the significant outcomes of this evolution is residential smart metering, which transforms our houses into smart homes and allows residents to control and monitor their energy consumption effectively. Smart meters enable customers to monitor their energy usage patterns, identify energy-saving opportunities, and optimize their energy consumption to reduce energy bills. This has enabled households to make more informed decisions regarding their energy consumption, which results in significant savings. Additionally, smart meters transmit the energy consumption information of customers to energy industries,




(a) (b)

Figure 1.1: (a): conventional grid, (b): smart grid. Adapted from [Ghi+23]

enabling the industries to manage energy better. The data transmitted allows energy industries to forecast and predict energy demand, detect faults and outages, and improve their energy distribution systems' overall efficiency.

Environmental concerns and the efficient production and distribution of power have become important topics. Hence, the primary objective of the smart grid is to enhance the stability and efficiency of the grid while integrating renewable energy resources effectively. The smart grid has enabled the effective management of renewable energy sources, ensuring that energy generation meets the energy demand and reducing reliance on non-renewable sources such as fossil fuels. However, integrating digital processes and technologies into power systems to automate and make them intelligent has also made them vulnerable to cyber-physical attacks [Ghi+23].

### 1.2.2 Renewable Energy Resources

These days, the world is moving toward using renewable energy sources to supply parts of the global energy demands. The main types of renewable are wind, solar, biomass, geothermal, and hydro. Given that some of the renewables, such as biomass, geothermal, and hydro, have limited scalability, solar and wind energy are considered as important sources of renewable energy production [Esm+13].

Various factors are contributing to the growing demand for renewable energy sources. One of the primary reasons is the growing concern over climate change and the impact of greenhouse gas emissions on the environment. Using fossil fuels, such as oil and gas, significantly contributes to global warming, leading to rising temperatures, sea-level rise, and extreme weather conditions. Therefore, governments and institutions globally are committed to decreasing carbon emissions and promoting sustainable energy sources to mitigate the effects of climate change. Unlike conventional energy sources that require large centralized power plants, renewable energy systems can be deployed in smaller units, making

them ideal for remote and rural areas. Furthermore, renewable energy sources are generally more cost-effective in the long term as they do not require fuel costs and have lower maintenance costs compared to fossil fuels. With the continuous advancements in technology and the increasing demand for sustainable energy, the future of renewable energy looks promising, and solar and wind energy will continue to play a critical role in meeting the world's energy needs [Age22].

#### 1.2.2.1 Solar Photovoltaic (PV) Panels

Solar energy is a highly accessible renewable energy source that has become increasingly popular recently. The energy is generated through solar PV panels containing multiple solar cells that convert sunlight into direct current (DC) electricity. Once the DC electricity is generated, it needs to be converted into usable electricity that can power household appliances. This is done using an inverter, which converts the DC electricity into alternating current (AC) electricity that can be used throughout the home [Eneb]. The electricity generated by the PV panels can be used directly in the home to power appliances or stored in a battery for later use. In addition, excess electricity can be fed back into the main grid, allowing homeowners to earn credits on their energy bills. This can help reduce the overall electricity cost and make solar energy a more attractive option for homeowners. Overall, solar energy is a versatile and sustainable energy source that has the potential to meet a significant portion of our energy needs while also reducing our carbon footprint.

One of the main challenges with renewable energy is that it can be intermittent [INO20]. Solar energy sources depend on weather conditions and are not always available when energy demand is at its highest. This issue can lead to power outages and an unstable grid. Another significant challenge for renewable energy is storage. Given that energy production from renewable sources is not constant, it is crucial to establish a dependable and effective energy storage infrastructure to ensure energy supply during periods of low generation.

#### 1.2.2.2 Battery Energy Storage Systems

Battery energy storage systems (BESS) typically consist of one or more batteries, a power inverter, and a control system [Enea].The batteries used in BESS can vary depending on the application and requirements, with some of the most common types including lithium-ion, lead-acid, and flow batteries. Lithium-ion batteries are popular because of their ability to sustain long cycles of use, high energy density, and minimal maintenance requirements, while lead-acid batteries are more affordable and have a longer track record of use in energy storage systems. Flow batteries are another type commonly used in large-scale energy storage applications, as they can store large amounts of energy over long periods.

One of the primary benefits of BESS is that it can provide continuous power flow during power supply fluctuations due to weather or blackouts [Hid+17]. For example, if a home or business has a solar panel system installed, a BESS can store excess energy generated during the day and release it at night when energy

demand is high. Similarly, if there is a power outage or grid failure, a BESS can provide backup power to ensure the continuity of critical services. Further applications of BESSs are peak shaving and load shifting [Hid+17].

***Peak shaving*** is a technique to lower electricity demand during periods of high energy use, which can reduce energy costs for consumers and utilities. It involves using BESSs to store excess energy during low-demand periods and release it during high-demand periods. This helps commercial and industrial customers with high energy demands during specific times of the day.

***Load shifting*** is a technique that battery energy storage systems can facilitate to balance energy supply and demand, helping utilities maintain a stable energy supply. BESS can store excess energy during off-peak hours and release it during peak hours, reducing the need for utilities to rely on expensive and inefficient energy sources. This technique can improve the efficiency of the energy system, reduce energy costs, and contribute to a more sustainable and reliable energy future.

### 1.2.3 Cyber Threats in the Smart Grid

Smart grids are modern electricity distribution systems that incorporate advanced technologies, such as sensors, communication networks, and data analytics, to monitor and manage the flow of electricity. While these technologies have improved the efficiency and reliability of the grid, they have also increased the risk of cyber threats [El +18]. Cyber-security in smart grids is crucial because a successful cyber-attack can disrupt power supply, cause equipment damage, and compromise sensitive data. The National Institute of Standards and Technology (NIST) has determined several criteria, such as confidentiality, integrity, availability, and accountability, for providing security and protecting information in the smart grid. Each criterion is detailed below [El +18].

**Confidentiality:** In general, confidentiality protects information from unauthorized access. Confidentiality will be lost when an unauthorized disclosure of information happens. For example, in the smart grid, information such as smart metering data and billing information exchanged between customers and other stakeholders must be confidential and protected from the risk of manipulation. Some confidentiality threat examples are traffic analysis, eavesdropping, etc.

**Availability:** Availability in the smart grid ensures reliable access to information and data at any time. In the smart grid, for instance, loss of availability causes disruption in the process of controlling the system by stopping the flow of information through the network. Therefore, availability is considered as the most important security criterion in the smart grid. Some famous examples of availability threats are Denial of Service (DoS), trojan horse, and service spoofing.

**Integrity:** Integrity refers to protecting data against alteration or demolition by an unauthorized user. A lack of integrity can cause credential misuse, meaning unauthorized users are able to manipulate data for different purposes in an undetectable manner. Examples of integrity threats are false data injection attack, man-in-the-middle, electricity theft, and replay attack.

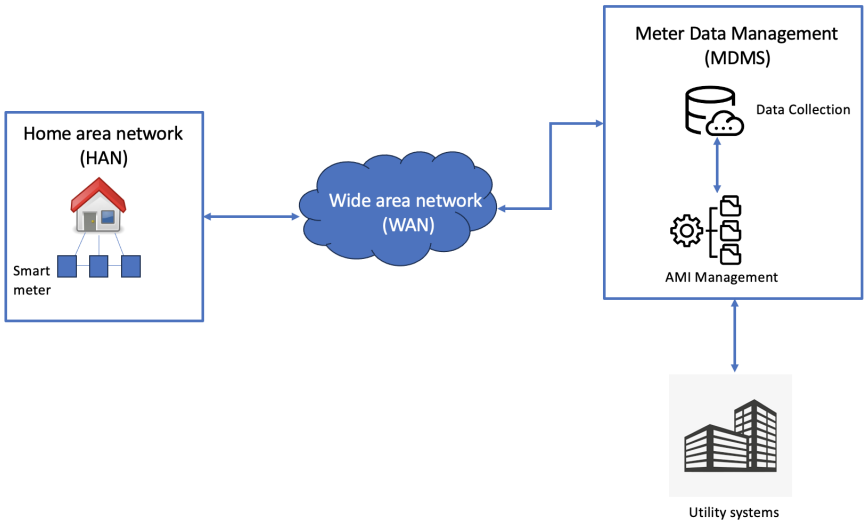



Figure 1.2: The AMI network model and its main components.

**Accountability:** Accountability means the system is traceable and every action is recordable, and hence helps to minimize or even prevent power theft. For example, a lack of accountability can affect the monthly electricity bills of users. An under attacked smart meter provides unreliable data regarding the cost of electricity. Hence, the customer will receive two different electricity bills, one from utility and the other one from the smart meter. Some instances of accountability threats are a physical intrusion, repudiation, etc.

The implementation of the smart grid involves several key components, with the Advanced Metering Infrastructure (AMI) being a crucial element that facilitates two-way communication between electric utility companies and their customers [AS15]. Figure 1.2 illustrates how the AMI integrates various components, such as the information/communication network, smart meters, and meter data management system (MDMS) [Wei+18]. The AMI's communication network comprises three critical areas: the home area network (HAN), the wide area network (WAN), and the utility system. Smart meters, the primary electronic devices installed on the customer side in the AMI, transmit the customers' electricity consumption data to the electric utility. The utility then uses this information to generate electricity bills, enable demand response, forecast user electricity consumption patterns, and update pricing in real-time.

#### 1.2.3.1 Cyber-Physical Threats in AMI

Ensuring the security of the AMI is a critical aspect of smart grid monitoring and operation, as well as protecting customer privacy. The AMI serves as a key point

of interaction between electric utilities and customers, and it is vulnerable to security breaches. For instance, a malicious attacker could manually manipulate smart meters and alter the meter readings, which would compromise the integrity of the reported data. In addition, integrating information and communication technologies (ICTs) with the AMI provides an opportunity for potential hackers to launch cyber attacks that could compromise electronic devices and inject malicious data into the communication network. The widespread deployment of AMI devices means that these cyber-physical attacks have the potential to not only disconnect electricity from end consumers but also cause cascading failures in other connected critical infrastructures, such as transportation and telecommunications. Therefore, securing the AMI against such threats is of utmost importance. Smart meters and communication networks are the primary attack surfaces in the AMI [Wei+18].

***Smart Meters*** Smart meters are electronic devices that track energy consumption and send the data back to the utility company at regular intervals. These meters enable dynamic electricity pricing, smart grid system monitoring, automated operation, and consumption-based customer services. While traditional meters were vulnerable to physical attacks due to their significance, smart meters provide cyber attackers with another potential point of access. Given a large number of deployed smart meters and limited defense resources, a number of theoretical and demonstrated attacks targeting these meters have been identified, such as denial of service (DoS) attacks, false data injection attacks (FDIAs), man-in-the-middle attacks, authentication attacks, etc. [JAL15], [BWS15], and [Jia+14].

***Communication Networks*** The AMI's communication network plays a vital role in connecting the devices through a wireless Frequency Hopping Spread Spectrum (FHSS) mesh or a similar cellular network. The network also establishes a link to the consumers' local HAN using WiFi, Zigbee, or Z-wave protocols. Then, the communication network connects to the utility's wide area network (WAN), typically an Ethernet infrastructure. In addition, the communication network is spread across an urban area alongside the smart grid, with the number of devices varying from a few hundred to thousands of smart meter data collectors. Each collector can serve thousands of smart meters, leading to thousands or even millions of devices. As a result, vulnerabilities in the AMI communication network could be exploited or disabled through attacks on the communication infrastructure, false user requests, unauthorized alteration of demand side schedules, and illegal market manipulation. Such attacks can disrupt system operations, causing power shortages, loss of trust, and negative economic impacts. The potential attacks targeting the communication network are distributed DoS (DDoS) attacks, FDIAs, data confidentiality attacks, and physical attacks [Cle08], [Esm+13].

Table 1.1provides an overview of the various cyber and physical attacks targeting the AMI systems, including the smart meter and the communication network.

Electricity theft is a significant security challenge for smart meters. This threat is primarily caused by meter manipulation and FDIA, enabling malicious attackers

Table 1.1: Cyber and physical attacks targeting the AMI

| | | Attack Target | |
|---|---|---|---|
| | | **Smart Meter** | **Communication Network** |
| **Physical Attacks** | | - Meter Manipulation<br>- Energy Fraud Attack | - Physical Attack |
| **Cyber Attacks** | **Availability** | - Denial of Service Attack (DoS) | - Distributed Denial of Service Attack |
| | **Integrity** | - False Data Injection Attack (FDIA) | - False Data Injection Attack (FDIA) |
| | **Confidentiality** | - Man-in-the-middle Attack<br>- Authentication Attack | - Wifi / Zigbee Attack<br>- Data Confidentiality Attack |

to modify consumption measurements obtained through smart meters. FDIAs can corrupt real-time data, including frequency, in any smart grid system. FDIAs, which involve injecting false signals, typically follow predefined attack patterns and are usually targeted at the metering system and control channels of smart grids.

### 1.2.4 Energy Markets

The electricity supply industry underwent restructuring to introduce market economy principles and promote social benefits through free competition. This change led to revised roles for electricity market participants. Deregulation processes in various countries involved separating electricity generation and retail from the natural monopoly of transmission and distribution and creating wholesale and retail electricity markets. Deregulation brought about a more efficient power market that facilitated power exchange between countries and increased supply security, while also ensuring reasonable electricity prices and optimal utilization of production resources and capacities. With the expansion of power transmission and generation capacity, cross-border power transmission has become more prevalent, resulting in a dynamic market where power can be more easily bought and sold across regions and countries [Sæt19].

Nord Pool is a collaborative electric power exchange market in the Nordic region, where electricity is purchased and sold at a price that reflects the balance of supply and demand, as is typical in other markets [NVE10]. The Nordic Power Market contains different price zones. The electricity prices in each area signal whether there is a surplus or shortage of electricity in the market, thereby providing correct price signals to producers and consumers. Consumers utilizing the power grid are charged for both the energy they receive and their use of the grid. The electricity bill usually includes two parts: the cost of the energy delivered and the grid rental fee. The cost of the energy delivered is calculated by multiplying the total amount of energy purchased from the supplier in the billing cycle by the market spot price. The local network company charges the grid rental fee, which covers all expenses associated with energy transfer and government taxes, and is determined by the utility tariff. In Norway, the typical electricity bill for residential buildings is approximately allocated as follows: 45% for energy usage and 55% for the grid rental fee [NVE10].

Nordpool operates day-ahead and intraday markets and manages the bidding process for these markets [Nora]. The primary platform for power trading is the

day-ahead market, where hourly spot prices are established at 12:00 CET for the following day after all buyers and sellers have submitted their bids to Nord Pool. These bids indicate the participants' hourly willingness to buy or sell a specific amount of power. The day-ahead spot prices are then determined at market equilibrium by the operator of the market, taking into account the availability of transmission capacity and the submitted bids [Nor13]. Additionally, the intraday market complements the day-ahead market and assists in maintaining the balance between supply and demand [Norb].

All consumers are responsible for paying a grid rent to the local utility company in addition to the cost of the energy they receive. The utility tariff, which contains the expenses associated with operating, maintaining, and developing the grid and government taxes, determines this fee. The amount a producer must pay to feed energy into the grid at a specific location is determined by the Feed-in Utility Tariff (FiUT). The FiUT's design varies based on the grid level to which the producer is connected. For example, the tariff structure differs between the distribution and regional power grid [Liu+17].

#### 1.2.4.1 Local Energy Market

In a conventional power grid, the electricity produced by generators in a centralized power generation system is transmitted to consumers through transmission and distribution systems. In the centralized system, power is produced by several bulk generating units and transmitted to households, and industrial and commercial consumers [Li+19]. As the level of distributed energy resources (DERs) integration on the consumer side increases, the centralized power generation system has been complemented by distributed power generation. In order to achieve a low-carbon energy transition, it is crucial to increase the production of renewable energy. This means it is necessary to find new methods of compensation for those who generate energy at home, called prosumers. This is particularly important given the growing number of distributed energy resources (DERs), which could have a significant impact on the energy market. To support the increase of renewable energy at the residential level, new market approaches are required to establish fair prices and decentralize and make the energy market and infrastructure more flexible. It is imperative to establish local energy markets where renewable energy can be traded directly between producers and consumers without intermediaries [Li+19].

The current power market restricts consumers from choosing their electricity supplier and limits prosumers from utilizing their DERs or feeding energy into the distribution grid. Consequently, prosumers generally strive for high levels of self-sufficiency and self-consumption within their households but may still need to procure from the wholesale market. Prosumers' involvement in the market creates the opportunity for a new community-based market to leverage the potential of prosumers and their installed DERs. Local energy communities can trade energy in two ways: by an intermediate of a global market operator, or in a full peer-to-peer (P2P) setting [Sot+21].

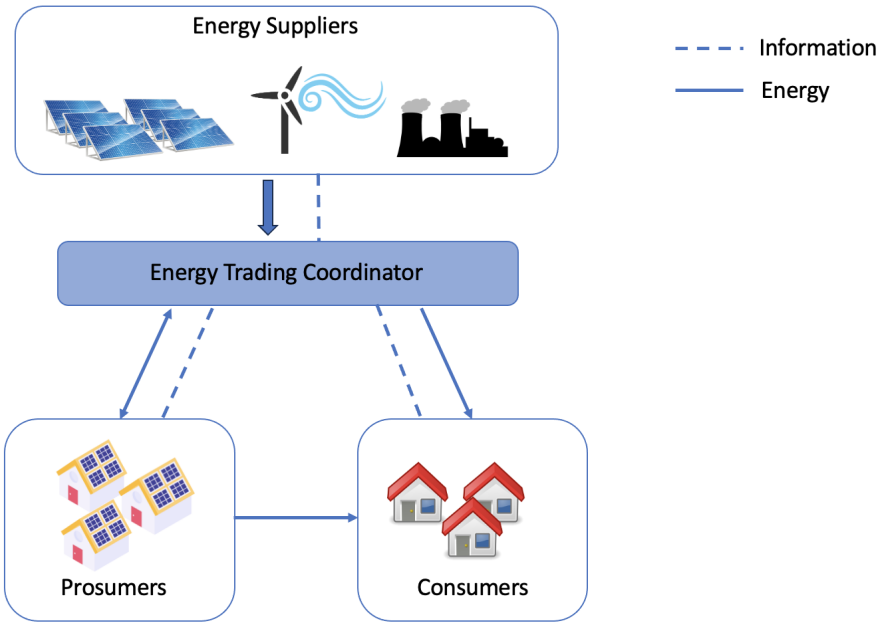



Figure 1.3: P2P energy trading model.

**Full P2P market:** Figure 1.3 shows a P2P energy trading model that encourages multi-directional trading within a local area. Through P2P collaboration within a local market, prosumers and consumers can share their generation and consumption at internal prices before trading with a retailer to balance any remaining electricity deficit or surplus. Typically, the local pricing scheme for P2P energy trading is established between the feed-in grid price and the price of grid electricity, providing benefits for all local participants. 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. 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.

**Community-based market**: In general, communities consist of members who share similar interests and objectives. Within a community-based P2P market, a community manager is responsible for coordinating the trading activities of community members. The market's design is founded on a distributed negotiation process between the community manager and members. The manager acts as a mediator between the community and the broader power system.

The literature contains a significant amount of research on the topic of energy trading between energy companies and prosumers. The energy market is undergoing significant changes due to the increasing number of DERs and energy prosumers. Sousa et al. [Sou+19] conducted a thorough assessment of P2P and community-based markets, analyzing the opportunities and challenges associated with these markets. Zhang et al. [Zha+18a] argue that P2P energy trading can improve the local balance between energy generation and consumption because of greater variety of energy generators. Furthermore, P2P energy trading supports the decentralization of the energy market [Men+18].

#### 1.2.4.2 Security of Local Energy Trading Markets

Besides the benefits of local P2P energy trading as outlined in the previous section, a key challenge is ensuring the security of the market. In order to ensure the security of local P2P energy trading, it is essential to address potential challenges and implement security measures from the outset. Without such measures, the market may become vulnerable to a range of insider and outsider attackers who could cause damage, disrupt trading, or manipulate the system for their benefit. It is, therefore, crucial to consider security as an integral part of the design process and to implement a range of measures that protect against threats and ensure the reliability and integrity of the market.

It is crucial to maintain the integrity of the data to ensure the security of an energy trading market [WL13]. False data injection (FDI) is a common technique used to compromise the integrity of energy markets. FDI attacks (FDIAs) typically involve deceptive actions that seek to disrupt the consistency of the power grid or manipulate output data from power equipment for personal gain. FDIAs can have a significant impact on the physical power system and its economic value. Such attacks can be targeted at the power distribution system in the smart grid, where the attacker seeks out optimal energy flow routes through nodes connected to energy production, distribution, or consumption. The distribution system employs several measurement tools, such as smart meters, smart relays, and voltage control regulators, to differentiate between nodes. These nodes communicate and share information to ensure proper system operation. The attacker uses energy-deception tactics on different nodes by injecting malicious energy information, response messages, or requests to manipulate the system. Such manipulation creates an imbalanced distributed power system based on false supply or demand, resulting in increased costs for distributed energy. The FDI attack also affects the energy market, with smart meters and AMI calculating energy settlement prices [Hab+23].

Extensive research is being focused on investigating the design and defence measures of FDIAs since Liu et al. suggested that attackers could utilize FDIAs against state estimation to avoid being detected by residual-based bad data detection methods [Liu+14]. Liang et al. [Lia+16] conducted a comprehensive review of construction techniques for FDIAs. Meanwhile, several approaches using statistical and probabilistic techniques have been proposed to defend against FDIAs, such as Kalman filter [Man+14] and sparse optimization [Liu+14].

However, these techniques rely on information on state of the system operation and distributions of measurement data, and the detection of FDIAs will become ineffective once those prerequisites change. Due to the rapid development of advanced metering infrastructure, which collects a large amount of data, machine learning and data-driven techniques are now widely used in power system operations. This is because they possess the capability to extract valuable information and can be easily extended to different applications [ZWC20].

Several machine learning techniques have been utilized to detect FDIAs in smart power grids. The most common approach involves using supervised learning classifiers to identify false data [YTH16], [Oza+15], [FS17], and [Gan+19]. These techniques leverage historical data to reflect the statistical characteristics of the power system and enable the training model to make better decisions if redundant power system measurements are available. Training data may include class labels for normal and tampered data, and the model uses this data to predict whether a new observation is false data or normal data. In the literature, supervised machine learning algorithms, such as support vector machine (SVM) [Oza+15] and [ZWX18], artificial neural network (ANN) [FS17], [**ref48**], and [XJL19], and k-nearest neighbor (KNN) [YTH16], have been utilized to detect FDIAs. Supervised learning techniques have a disadvantage in that they require a large amount of labeled data, which can be difficult to obtain. To address this issue, semi-supervised learning techniques have been developed, which make use of partially labeled samples. This approach aims to label unlabeled data points by leveraging information from a limited number of labeled data points. Semi-supervised algorithms have also been utilized in [Oza+15] and [FS17].

### 1.2.5 Renewable Energy Communities

As defined in the recast of the European Renewable Energy Directive (RED II) [Par+18], a renewable energy community (REC) is a legal association that generates, shares, and manages cost-effective renewable energy autonomously, decreasing carbon emissions. The members of a REC can be individuals, e.g., people who live in the same neighborhood or building, or any public or private entity that intends to build a REC. The establishment of more renewable energy communities can increase both the share of renewable energy and flexibility in electricity supply and electricity systems, respectively. According to the reviews of Lode et al. [Lod+22] and Bauwens et al. [Bau+22], the topic of REC has achieved great attention from REC developers and the research community. Although the RED II supports a framework to develop RECs, there are still challenges to an extensive uptake of RECs [Hoi+21]. Ines et al. [Inê+20] compared the local regulations of nine different European countries. They showed that the first challenge in developing RECs is to overcome the obstacles of local regulations for the purpose of benefiting the advantages provided by the legitimate framework at the EU level. In addition to the regulation issue, another challenge is understanding a citizen's incentive to participate in a REC.

Conradie et al. [Con+21] showed that some of the motivators could be financial benefits, connection with RESs, and environmental impact.

#### 1.2.5.1 Renewable Energy Sharing in Multi-Unit Buildings

The use of renewable energy sources has been considered as a practical way to supply some of the energy demand in buildings, particularly in urban areas, as they can provide flexibility in electricity systems and increase the share of renewable energy. While solar PV panels have become a popular solution for detached houses, their implementation in multi-unit buildings has been relatively limited [CBE17]. Despite the widespread adoption of distributed renewable energy sources (DRESs) in residential settings, the lack of a legal framework hinders the installation of PV panels and battery energy storage systems (BESSs) in buildings with several apartment units. The main reason for the low adoption of DRES sharing in multi-unit buildings is the absence of regulations that ensure proper taxation, grid rent, and settlement [Fin+18]. These challenges highlight the need for more regulatory support to enable the implementation of renewable energy solutions in buildings, especially in multi-unit dwellings. Furthermore, incompatible motivations between landlords, tenants, and owner-occupiers can prevent the deployment of PV panels in multi-unit buildings. According to [SMD20], barriers for multi-unit owners to not install PV panels are the challenge of coordination with other parties, the high installation cost, and the fear of renters of high management fees. Different energy sharing approaches that can be applied inside buildings have been discussed by the regulatory body, RME [**59**]. Equal sharing is one of the approaches studied in the RME proposal. In an equal sharing solution, all residents receive the same share of energy produced by shared PV panels in the buildings. The other solution is unequal sharing, in which residents receive different shares of energy according to, e.g., the size of the units, the cost that each resident invests in the shared PV panels, etc. Dynamic sharing is the third sharing solution in which residents receive energy based on their consumption at various time slots in a day. This sharing model attempts to maximize the utilization of the energy produced by PV panels in buildings.

Given that the units of multi-unit buildings are occupied by different groups of residents, e.g., tenants and unit owners with different preferences, the process of sharing energy from shared DRESs between these groups can be unjust and challenging. For instance, from the perspective of investing in shared DRESs, some residents could not afford the investment economically, or there might be a group of residents, such as tenants, who want to enjoy the benefits of shared DRESs for a short period because long-term investment is not affordable for them. In this regard, it is necessary to establish policy approaches to confirm efficient, fair, and equitable allocation and distribution of energy, costs, and benefits in multi-unit buildings, considering different groups of residents.

#### 1.2.5.2 Fairness in Renewable Energy Sharing

The current global conditions show an increase in inequality in different parts of society in terms of environment, economy, and society. A wide range of energy research is currently addressing renewables, technologies, distributed sources, and how to achieve economic benefits for different stakeholders. However, the "fairness" of those systems has received much less attention. Therefore, in the energy field, more attention is needed to design systems that are "fair" for different groups of stakeholders. The issue of fairness in energy systems has been interpreted from different perspectives, such as sharing of benefits, energy democracy, energy vulnerability, or public acceptance, in the literature.

Perlaviciute et al. [60] discussed that the various motives for social acceptance, of which fairness is one, should be considered when designing a project from scratch and during the implementation stage. One study [RSM22] shows that if energy is transparently and equitably shared in a sharing method, then the method is fair. Other studies present different interpretations [Per+21], [Jaf+20], and [Lov+20]. According to [Per+21], fairness is associated with the willingness-to-pay of a prosumer, equal satisfaction is another interpretation of fairness that is supported by Jafari et al. [Jaf+20], and Lovati et al. [Lov+20] proposed a peer-to-peer (P2P) energy trading model in which fairness has been achieved by transparency. Some works present different methods to assess fairness in the context of energy systems. For example, the standard deviation and variance are famous indices to quantify fairness [65]. Evelyn et al. proposed fairness ratios based on two factors of equality and equity to assess the fairness of the distribution of reliability between end-users in power systems. Long et al. [LZW19] proposed several indexes, including the equality index and participation willingness index, to evaluate their proposed P2P energy trading mechanism, while Chakraborty et al. [CBK20] used the Nash social welfare index for the same purpose. According to the literature, a common framework for evaluating fairness and justice in energy-sharing solutions is missing. Energy justice can be used as an evaluation framework to evaluate fairness in energy sharing models based on its three main principles that are studied in the following section.

#### 1.2.5.3 Energy Justice

Energy justice is crucial to our global efforts to address climate change and transition to sustainable energy systems. It is an essential concept that helps ensure that energy systems are equitable and just, providing access to affordable and reliable energy to all members of society while accounting for the environmental, economic, and social impacts of producing and using energy.

As a decision-making tool, energy justice empowers stakeholders such as consumers and producers to make informed choices grounded in fairness and equity considerations. By accounting for the distribution of costs and benefits associated with energy services, energy justice helps ensure that the burdens and benefits of energy production and consumption are equitably shared across society. This is particularly important as we transition to cleaner, more sustainable energy

systems, as it can help prevent the creation of new forms of energy injustice that disproportionately affect vulnerable and marginalized communities.

In recent years, scholars have worked to develop a shared understanding of energy justice that encompasses both the fair distribution of energy-related costs and benefits and equitable decision-making processes [SD15]. By doing so, they have sought to promote a more comprehensive understanding of the issues and challenges associated with energy justice and to provide a framework for addressing these challenges in a just and equitable manner. In general, energy justice represents a critical step towards creating a more sustainable, equitable, and just energy system that benefits all members of society. Energy justice integrates three distinct but interrelated principles: distributive justice, procedural justice, and recognition justice [McC+13]. Each principle addresses a unique aspect of justice that complements the others [McC+13].

**Recognition justice** ensures equal access to opportunities and resources in energy systems for all stakeholders, especially vulnerable groups. The unique needs and challenges of different stakeholder groups must be recognized and addressed to promote recognition justice in energy-sharing models. This may involve implementing targeted policies and programs to increase access to energy-efficient technologies for low-income households and ensure tenants have equal access to renewable energy technologies. Prioritizing recognition justice in designing and implementing energy-sharing models can lead to a more just and sustainable energy future for all.

**Distributive justice** focuses on ensuring a fair and balanced distribution of benefits and risks amongst stakeholders in energy systems. This means considering costs, profit, the deployment of DRESs, and the energy generated by shared Photovoltaic (PV) panels and assessing how these are distributed among all parties involved. This principle emphasizes the importance of fairness and equity in energy systems, and calls for a comprehensive analysis of the allocation of resources and benefits to ensure that everyone can reap the rewards of a sustainable energy future.

**Procedural justice** emphasizes the need for all stakeholders affected by energy systems to have equitable participation in decision-making. When designing energy-sharing models for multi-unit buildings, it is crucial to prioritize the involvement of residents using transparent procedures. By promoting transparency and involving all relevant parties in the decision-making process, we can create sustainable and fair energy systems that meet the needs of all involved.

## 1.3 Research Objectives

Generally, this thesis targets two main objectives. The first objective focuses on securing energy trading markets in the smart grid, while the second one mainly targets energy sharing in multi-unit buildings.

**Objective I.** *Securing energy trading markets in local area in the smart grids.* As stated before, a key challenge is ensuring the security of energy trading

markets that should be taken into consideration as a part of the original design. Cyber-security in energy trading markets is important because a successful attack can disrupt energy demand and supply, steal energy, and cause equipment, e.g., substation components, damage. We mentioned that data integrity preservation is crucial to guarantee the security of an energy trading market. There are different cyber and physical attacks targeting the integrity loss of energy trading markets of which FDIAs are the most common ones. Precisely, cyber attacks target digital systems and data, while physical attacks involve tangible harm to people or physical infrastructure. Various methods, such as physical protection and cyber-oriented approaches, have been used to mitigate such attacks. In this dissertation, we aim to, first, experimentally explore the possible ways of attacks and effects of FDIAs in local P2P energy trading markets, and then utilize data-driven ML methods, which are powerful tools in identifying potential threats, to detect the FDIAs.

**Objective II.** *Effective and fair renewable energy sharing in multi-unit buildings in the smart grids.* As previously discussed, DRESs solutions for multi-unit buildings have been relatively limited due to the absence of regulations that guarantee electricity tax, grid rent, and settlements are in line. In this dissertation, we aim to investigate the effects of shared DRESs, including PV panels and BESSs, in multi-unit buildings. There are several challenges with developing shared DRESs for multi-unit buildings. One of the main challenges is related to the different preferences of residents, which makes the process of energy sharing from shared DRESs unjust for some groups of residents. In this regard, the other goal of this thesis is to develop an energy-sharing model that enables the efficient and fair distribution of energy, costs, and benefits in multi-unit buildings considering different groups of residents.

## 1.4 Research Questions

To meet the research objectives of this dissertation, we aim to respond the following research questions:

**RQ1**: how to address the challenge of compromising the integrity of local energy trading markets in the smart grid caused by FDIAs?

This question is an attempt toward Objective I to ensure the security of energy trading markets, specifically local P2P energy trading markets. In this regard, an initial step is to find the possible ways to attack an energy trading market and then explore the effects of the attacks. To this end, we need to study the following sub-questions:

- what are the situations in which a P2P energy trading market can be attacked?
- what kind of new cyber-attacks in P2P energy trading markets can be imagined?

**RQ2**: how to defend against cyber-security threats in the smart grid?

This question complements RQ1 to achieve Objective I. After finding possible ways to attack an energy trading market, a proper defense is needed. There are various techniques for defense strategies against cyber-attacks, for example, FDIAs. The countermeasures of FDIAs can be classified into prevention-based and detection-based methods. Prevention-based methods can help to harden a system against attack; detection-based methods focus on detecting and remediating threats that have breached the system. However, prevention-based methods can manage a potential security breaches, it is not always effective. Integrating detection-based methods to security strategy is becoming crucial to protect against modern cyber-attacks, such as FDIAs. By detecting signs that shows that a breach has happened, a quick response and remediation step can take place to avoid the spread of both known and unknown attacks. Today, ML-based techniques are performed as a good solution for efficiently detecting cyber-attacks. ML-based methods are able to extract valuable information from data to detect abnormal patterns. To find a proper defence solution in an energy trading market we need to answer the following sub-questions:

- what kind of measures can be used to defend against the identified kinds of attacks in local P2P energy trading markets?
- how can machine learning be applied to defend against the attacker both considering existing approaches and identifying the need for new solution?

**RQ3**: how to address renewable energy sharing in buildings in the smart grid related to the effects of developing DRESs and sharing energy generated by DRESs in multi-unit buildings?

This question relates to Objective II to study renewable energy sharing in multi-unit buildings in the smart grid. As we mentioned before, PV panels are a settled and approved solution for detached houses, while PV solutions for multi-unit buildings have been relatively limited. In this thesis, we aim to show the benefits that residents of multi-unit buildings can achieve by using and sharing energy generated from shared DRESs, such as PV panels and BESSs, in the buildings. In this regard, we need to answer the following sub-questions:

**RQ4**: how to address fairness and justice in energy sharing in the smart grid?

Along with RQ3, answering RQ4 helps us to achieve Objective II. The main challenge in sharing DRESs in multi-unit buildings is related to fairness and justice. This means that energy from shared DRESs should be shared fairly among different groups of residents of the buildings. First, we need to know what fairness could be in this situation, and then how to achieve fairness in energy sharing in multi-unit buildings. We study the benefits of developing DRESs and fairly sharing the DRESs in multi-unit-buildings by considering how to define fairness in renewable energy sharing and how to apply justice to renewable energy sharing in multi-unit buildings to achieve fair energy sharing.

The research questions solved by each paper in this dissertation are summarized in Table 1.2.

Table 1.2: Research questions solved in this dissertation

| | |
|---|---|
| **Paper I** | RQ1 |
| **Paper II** | RQ1, RQ2 |
| **Paper III** | RQ3, RQ4 |

## 1.5 Solving Methodologies

### 1.5.1 Game Theory

Game theory has gained widespread recognition as a valuable tool in various fields, including the domain of smart grids. This section presents some key concepts associated with game theory, including the types and structure of games and the Nash equilibrium. Additionally, it covers different categories of games, such as non-cooperative and cooperative games. Game theory offers a framework to analyze and describe strategic situations by investigating the stakeholders' interactions and decisions.

Table 1.3: The payoffs of the prisoner's dilemma

| | Prisoner 1 confesses | Prisoner 1 remains silent |
|---|---|---|
| Prisoner 2 confesses | 5, 5 | 1, 9 |
| Prisoner 2 remains silent | 9, 1 | 2, 2 |

In game theory, a game is a situation where two or more individuals, known as players, have to make decisions that will affect the outcome of the game. Each player is provided with a range of potential actions or strategies that they can choose from, and the payoffs or outcomes associated with each possible combination of strategies determine the final outcome of the game. The payoffs represent the players' preferences or utility functions, which are mathematical representations of how much each player values the possible outcomes of the game. For example, in a simple two-player game, one player may prefer to win with a high score, while the other may prefer to win with a low score. These preferences are typically represented as numerical values, and the players aim to maximize their payoff by choosing the best possible strategy. Payoffs are essential in game theory, as they allow us to model and analyze the strategic interactions between players.

To better understanding the structure of games, we consider a simple example of the prisoner's dilemma, which is a classic game in game theory. In this game, two criminals (players) are arrested and interrogated separately. They are each given the opportunity to confess and betray the other criminal or remain silent (actions). If both remain silent, they will each receive a moderate sentence of two years in jail. If both confess, they will both receive a severe sentence of five years in jail. However, if one confesses and the other remains silent, the confessor will receive a sentence of one year in jail, while the one who remained silent will receive a severe sentence of nine years. The payoffs for each outcome

are the years of prison sentences that are represented in Table 1.3.

To define the best strategy for the players, we need to introduce Nash equilibrium. Nash equilibrium is a fundamental concept in the game theory that refers to a state in which no player can increase their payoff by unilaterally changing their strategy, given the strategies of the other players. In other words, it is a stable outcome of the game, where each player is making the best decision they can, given what the other players are doing. To find the Nash equilibrium in the prisoner's dilemma game, we need to look for a combination of strategies where neither player can improve their payoff by changing their strategy, given the other player's strategy. In this case, the Nash equilibrium is (confess, confess).

In game theory, games can be categorized into different types based on their characteristics and assumptions. Some of the most commonly studied game types are cooperative games, non-cooperative games, and Stackelberg games. A Non-cooperative game involves players making decisions independently without requiring formal agreement or coordination. The Prisoner's Dilemma is a famous example of a non-cooperative game where two individuals must choose between cooperating or defecting. A cooperative game involve players being able to coordinate their decisions and create binding agreements. The distinguishing feature of cooperative games is the formation of a coalition where players collaborate to achieve a shared goal. In a Stackelberg game, one player takes the lead and moves first, while the other follows and moves second. The leader has an advantage as they know the follower's strategy and can use this information to make their move. This type of game is often used to model situations where one player has more power or information than the other.

#### 1.5.1.1 Application of Game Theory in the Smart Grid

The smart grid involves various stakeholders, including consumers, prosumers, suppliers, and operators, whose interactions are crucial for maintaining the grid's stable operation. As a result, game theory has been utilized to examine the interactions between these entities. The use of Game Theory in energy trading has shown potential for designing pricing strategies, with both cooperative and non-cooperative game concepts being applicable from various perspectives. The cooperative game approach guarantees that each prosumer can earn some profit by participating in the game, rather than acting alone. A cooperative game solution is proposed in [MMM20] to distribute benefits fairly among community members. In a non-cooperative game, each prosumer aims to maximize their individual profit, and eventually, an equilibrium is reached among all prosumers. In [Cui+20]and [WH16], a non-cooperative game was employed to represent the interactions between buyers and sellers in an energy trading problem.

### 1.5.2 Optimization Theory

An optimization problem is a mathematical problem that involves finding the best solution from all possible solutions within a given set of constraints. The components of an optimization problem include:

1. Decision variables: the decision variables, which need to be determined before solving the optimization problem, are the variables that can be manipulated and adjusted to obtain the best possible solution.

2. Objective function: The objective function defines the quantity to be optimized. It can be a function of one or more variables, and the goal is to maximize or minimize this function.

3. Constraints: constraints are limitations or restrictions that must be satisfied for the solution to be considered feasible. They can be expressed as equations or inequalities, and they limit the possible values that the decision variables can take.

A typical optimization problem with three constraints can be expressed generally as follows:

$$\begin{aligned} \max_{x_1,\ldots,x_n} \quad & f(x) \\ \text{Subject to} \quad & g_1(x) \leq b_1 \\ & g_2(x) \geq b_2 \\ & h_1(x) = c_1 \end{aligned} \tag{1.1}$$

In (1.1), $x$ is the decision variable, $f$ is the objective function to be maximized, $g_1$ and $g_2$ are inequality constraints, $h_1$ is equality constraint, and $b_1$, $b_2$, and $c_1$ are constants. Suppose a variable $x^*$ satisfies the constraints of Problem (1.1) and has the highest objective value compared to all other choices. In that case, $x^*$ is considered optimal or a solution of Problem (1.1). This means that for all feasible solutions $x$ $f(x) \leq f(x^*)$.

Optimization theory seeks to develop mathematical models and algorithms to solve optimization problems, including linear and nonlinear programming, convex optimization, etc. In this context, we focus on discussing a group of optimization theories that are utilized for resolving convex optimization problems. These types of problems are considered more well-defined, and thus their solution methodology is relatively established. However, in cases where the optimization problem is non-convex, it may be necessary to utilize transformations or approximations to transform it into a convex optimization problem [BV04].

A convex optimization problem involves optimizing a convex objective function subject to constraints that are also convex functions. The convexity of the objective function depends on whether it is a minimization or maximization problem. For minimization problems, the objective function must be convex, while for maximization problems, it must be concave. Linear functions are a specific type of convex function, which means that linear programming problems are convex optimization problems. When both the objective function and the feasible region are convex, there exists only one optimal solution that is globally optimal. This means that any other solution that may exist will be suboptimal, which makes convex optimization problems more attractive than non-convex problems since it ensures that the obtained solution is the best possible one.

#### 1.5.2.1 Application of Optimization Theory in the Smart Grid

An optimization framework that enables the equitable allocation of DERs among multiple consumers was utilized in [Fle+18]. The proposed approach in [Fle+18] combines optimization and game theoretical models to achieve an optimal solution. An optimization model is proposed in [Jin+20] that assessed P2P multi-energy trading between residential and commercial prosumers while taking into account integrated demand-side management, including demand response and three types of storage. The optimization model aimed to find optimal trading prices for both electricity and heating through a Nash-type formulation that ensured fair benefit allocation between two prosumers.

### 1.5.3 Anomaly Detection

Anomaly detection, also known as outlier detection, involves detecting infrequent items, events, or observations that deviate significantly from the majority of the data, arousing suspicion [Flo18]. In general, anomalous data is often associated with some issue or uncommon occurrence. The energy trading process in a smart grid is vulnerable to a wide range of threats, making it crucial to prioritize its security. To this end, researchers have undertaken remarkable efforts to identify and mitigate attacks, such as false data injection attacks (FDIAs), in the electric power grid [CJM15], [BZ14], and [AMT15]. Various methods have been explored, including physical protection approaches and cyber-oriented approaches. Physical protection approaches pose challenges regarding the cost and feasibility of implementing protection schemes for measurement devices. The costs associated with implementing physical protection measures can be prohibitively high, and smaller power grids may not have the necessary resources or infrastructure to support such measures. Additionally, the feasibility of implementing such measures may be limited by the physical layout of the grid and environmental factors [Ahm+19].

In recent years, data-driven machine learning (ML) methods have been utilized for cyber-physical security analysis by predicting and identifying threats and anomalies in a system [Esm+14]. Since physical sensors like phasor measurement units can have flaws that result in bad or missing data, detecting and identifying anomalies in power grid data is essential for accurate performance analysis. By leveraging ML techniques, it is possible to improve the accuracy of performance analysis and mitigate the impact of physical sensor flaws on the analysis results. Effective security measures are critical for the reliable operation of smart grids, and using ML-based techniques can be a powerful tool in identifying and mitigating potential threats. In the following sections, we introduce the basics of machine learning, second we study machine leaning methods for attack detection. In the end, we study anomaly detection in the smart grid.

#### 1.5.3.1 Introduction on Machine Learning

Machine learning is a vast and multidisciplinary field that encompasses multiple areas of study, including computer science, probability and statistics, psychology, and brain science. The primary objective of machine learning is to imitate human learning activities using computers effectively. By doing so, machines can automatically discover and acquire knowledge. Machine learning approaches can be categorized into three primary groups based on the types of feedback they receive:

- Supervised learning: supervised learning involves feeding training samples with known category labels into classification or regression models during the training phase [IBM]. Some of the typical supervised learning techniques include support vector machine (SVM), decision tree (DT), artificial neural network (ANN), etc. One of the key advantages of supervised learning is that it can achieve high accuracy if the training data is representative and the model is appropriately designed and tuned. However, it requires labeled data, which can be time-consuming and expensive to obtain.
- Unsupervised learning: this technique involves inducing models using training samples that have no corresponding category labels [Mis17]. Examples of unsupervised learning techniques include clustering and auto-encoder. These techniques can be used to discover hidden patterns, structures, or relationships in data, which can help to gain insights and inform decision-making. However, evaluating the performance of unsupervised learning models can be challenging since there are no predefined labels to compare the results against.
- Reinforcement learning: reinforcement learning optimizes behavior strategies via trial and error [Bha18]. This learning type differs from the other two types of techniques mentioned above, as it does not rely on a pre-existing dataset with labeled examples. Instead, the algorithm learns through repeated interactions with the environment, receiving feedback in the form of rewards or penalties based on its actions.

#### 1.5.3.2 Anomaly Detection based on Machine Learning Methods

Figure 1.4 shows a general framework for anomaly detection utilizing machine learning [RAH18]. The first crucial step is data pre-processing, which encompasses filtering, data labeling, and feature selection. It is also critical to understand the data to make suitable design decisions. After selecting the features, training the model using prior knowledge of the system or data is necessary. This prior knowledge may take the form of defining a standard (normal) data profile to identify outliers as anomalies. After training the model, it can be employed to categorize new data to assess its effectiveness. It is crucial to incorporate data samples that represent the anomalous state during this step, regardless of whether they were utilized during the training phase. Choosing

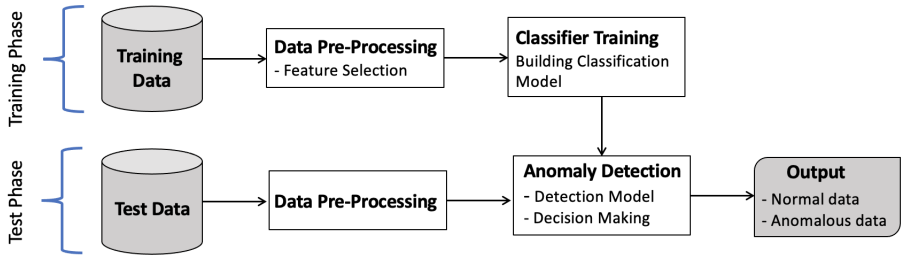



Figure 1.4: General Anomaly Detection Framework.

appropriate metrics for the application environment is a challenge during the evaluation phase of this algorithm, as this is necessary to analyze the outcomes thoroughly.

The performance of attack detection algorithms can be evaluated based on accuracy, detection (recall), precision, and false negative rates. The accuracy rate measures the percentage of correctly predicted test samples. Precision and recall measure the relevance of the output generated by attack detection algorithms. Precision is calculated as the ratio of correctly classified positive samples to all samples classified as positive. Recall is calculated as the ratio of correctly classified positive samples to all correctly classified samples. False negative rate is the probability that an actual attack will be missed by the test measures. The computation for accuracy, precision, recall, and false negative are as follows:

$$\begin{aligned} \text{Accuracy} &= \frac{TP + TN}{TP + TN + FP + FN} \\ \text{False negative rate} &= \frac{FN}{FN + TP} \\ \text{Precision} &= \frac{TP}{TP + FP} \\ \text{Recall} &= \frac{TP}{TP + FN} \end{aligned} \tag{1.2}$$

where true positive (TP) and true negative (TN) represent the number of correctly classified attack and normal data, respectively. On the other hand, false positive (FP) and false negative (FN) represent the number of normal data and attack data that are classified as attack and normal data, respectively.

Numerous techniques have been employed for detecting anomalies, but this thesis will concentrate on methods that leverage computational intelligence, particularly pattern recognition through machine learning. This approach involves utilizing a known dataset to establish the input/output relationship of the system, which can subsequently be used to classify an unknown dataset. In terms of interpretability, here we study several well-known interpretable (DT

and K-Means), semi-interpretable (SVM), and non-interpretable (Artificial NN) machine learning classifiers.

**DTs** are a widely used tool for classification and prediction, characterized by their structure consisting of nodes, arcs, and leaves. The feature attributes, which are most informative among the attributes not yet considered in the path from the root, are labeled on each node. The arcs out of a node are labeled with feature values for the node's feature, while each leaf is labeled with a category or class. A decision tree traverses from the tree's root to a leaf node to classify a data point. The leaf node provides the classification of the data points. Compared to other algorithms, DTs are highly interpretable and easy to understand, and they need less effort for data preparation in pre-processing. One limitation of Decision trees is that they are unstable. This means that small modifications in the data can lead to significant changes in the model's predictions. Hence, they may not be well-suited for handling dynamic data that undergoes changes over time [RAH18].

**K-means** algorithm is a conventional clustering approach that partitions data into k clusters, ensuring that data in the same cluster are similar while data in different clusters have low similarities. The K-means algorithm's sensitivity to outliers results in a superior detection performance. These algorithms possess low complexity and a high detection rate. Their drawback is the need to specify k, as well as their sensitivity to noise and outlier data points [RAH18].

**SVMs** are generally considered supervised learning classifiers that rely on labeled training data to map samples to one of two classes [44]. These SVM models are considered as binary or two-class linear models. Binary SVMs can handle nonlinear data by transforming them into a high-dimensional feature space utilizing the Kernel method. Unsupervised learning is frequently required in anomaly detection approaches because of the lack of training data. In such situations, one-class SVMs can be utilized, wherein the "normal" class is the only class, and anything that deviates from the norm is classified as an anomaly. The lack of training data is a significant disadvantage of binary SVMs, which is likewise applicable to multi-class SVMs since they are an extension of binary SVMs that enable categorizing samples into multiple classes [RAH18].

**ANNs** simulate the problem-solving capabilities of the biological brain to enable computational systems to learn in a similar way. Due to their ability to identify patterns in the input/output relationships of given datasets, neural networks are promising candidates for anomaly detection systems. Nevertheless, their inability to handle unseen data is a significant limitation in such applications, and thus ANNs are rarely utilized in isolation [RAH18].

Black-box anomaly detection models (e.g., ANNs and SVMs) can pose significant risks in critical applications. Since they do not provide reasons behind their predictions (i.e., explanations), it diminishes trust into their decision-making mechanism. Using explainable anomaly detection models that offer clear indications of why a particular data point is identified as an anomaly can be effective in increasing trust into the system and avoiding wrong decisions. In certain applications, providing such explanations can be equally vital as the detection accuracy. However, deriving explanations from black-box anomaly

detection models remains a challenging problem due to their complex structure. Therefore, developing inherently interpretable anomaly detection models is important. However, the primary challenge lies in achieving a well-balanced trade-off between the model interpretability and the predictive performance.

#### 1.5.3.3 Anomaly Detection in the Smart Grid

Several machine learning-based detection methods have been proposed in the literature to perform complicated tasks such as detecting FDIAs in the smart grid. The frequent use of SVM in detecting FDIAs is mainly related to its simplicity, as demonstrated in several studies [Esm+14], [Jin+16], and [Wan+19]. However, the selection of the kernel function and the high memory and CPU time requirements during training are the primary limitations of this algorithm. Studies such as [Wan+17], [KPJ18], and [El +17] have utilized Feedforward neural networks (FNNs) for FDIA detection, while Recurrent neural networks (RNN), which mimic the dynamical behavior of smart grids through internal memory and feedback loops, have been proposed in [AKE18] and [Aya+18]. A Deep neural network (DNN) has been employed in [VR17] to improve the precision of FDIA detection by incorporating more hidden layers. Additionally, Convolutional neural network (CNN), a special type of DNN that extracts different features in samples, has shown promising results in FDIA detection, as highlighted in [Wan+19]. Another algorithm used for FDIA detection is Autoencoder (AE), a deep neural network that compresses and expands measurement samples nonlinearly. The detection in AE is based on the error between the input and the decoded sample, and an alarm is raised when the error exceeds a certain level, as demonstrated in [Zha+18b]. However, a significant drawback of using the backpropagation method for training neural networks is the extensive amount of time required. Other supervised learning techniques used for detecting FDIA in smart grids are margin classifier (MC), a generalized form of SVM with more accurate performance, as shown in [Wan+17], and structure learning (SL) [SJ15], which is a prediction method based on the covariance of the samples' structure rather than their actual values. However, the main drawbacks of supervised learning approaches are the requirement for extensive learning and labeled data.

Studies such as [Zan+17] and [VV17] have applied K-means clustering in detecting FDIA. The main advantage of this method is its simplicity; however, it is highly sensitive to noise in the samples, which is a significant drawback. An extended version of K-means clustering is Fuzzy clustering (FC), or soft clustering, where a sample can belong to multiple clusters with varying degrees of membership. This results in a more detailed clustering process where clusters can overlap rather than having clearly defined boundaries. FDIA detection using FC was demonstrated in [Wan+19] and [VV17], where it yielded a slightly improved detection accuracy compared to the K-means clustering method.The above approaches generally suffer from a trade-off between transparency, speed, and accuracy, limiting their ability to achieve optimal results. For instance, some approaches that show high accuracy, such as DNNs and RNNs, suffer from low transparency owing to their inherent complexity. Conversely, transparent

methods such as DTs perform poorly in processing large datasets, resulting in slow speed.

## 1.6 Contributions of the Included Papers

This dissertation includes three papers (papers I-III) which are briefly presented in this section.

### 1.6.1 Paper I

S. Mohammadi, F. Eliassen, and Y. Zhang, "Effects of false data injection attacks on a local P2P energy trading market with prosumers," *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, The Hague, Netherlands, 2020, pp. 31-35.

In Section 1.5.2, we mentioned that a key challenge in local P2P energy trading is ensuring the security of the market. We also observed that FDIAs are one of the most popular approaches to attacking an energy trading market. There are some works that studied FDIA scenarios in P2P energy trading markets and possible defense methods [IMO18] and [Liu+14]. However, those works considered consumers only in energy neighbourhoods. When there are prosumers, the higher benefits that they gain from trading between themselves rather than with the grid, encourages consumers to become prosumers. Hence, it is a challenge for the suppliers. In this case, a malicious supplier may want to discourage consumers from becoming prosumers. In this regard, attacks can be orchestrated by a malicious supplier who engages an attacker acting as a prosumer, to gain more utility. The attacker tries to modify the demands of prosumers by increasing their energy consumption demand to increase the profit of the energy supplier and reduce the profit of prosumers. Therefore, it is of high interest to study the effects of FDIA on P2P energy trading where there are prosumers and consumers.

In paper I, we study the following research questions: "RQ1.1: what kind of measures can be used to defend against the identified kinds of attacks in local P2P energy trading markets?" and "RQ1.2: what kind of known cyber-attacks can be applied in P2P energy trading markets?". Therefore, in the paper, we explored the vulnerability of local P2P energy trading to FDIAs. 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 chose an exploratory approach to quantify threats. In particular, we investigated a game theoretic approach to P2P trading. We analyzed the effects of FDIAs, when there are different numbers of attacked prosumers, on the price and revenue of prosumers and the attacker in different time slots, and compared them with the normal situation (without attack).

### 1.6.2 Paper II

S. Mohammadi, F. Eliassen, Y. Zhang, and H. -A. Jacobsen, "Detecting False Data Injection Attacks in Peer to Peer Energy Trading Using Machine Learning," in *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 3417-3431, 1 Sept.-Oct. 2022.

In Paper I, we assumed the attack occurs before the game starts to reap benefits for the energy sellers (e.g., suppliers) by causing a reduction in incentives of becoming or remaining energy selling prosumers. We observed from the experiments that the profits of prosumers decreased after the FDIAs (when the prosumers' demand was increased by the attacker before the game started). This effect (reduction in prosumers' profits) could possibly reduce the consumers' motivation to become prosumers. We concluded that the attacker could not gain energy for free by only modifying the prosumers' demand at the beginning of the game or before the game started. This is due to the iterative nature of the game where prosumers will update their demands based on the new price in subsequent iterations. Subsequently, the game will converge with supply/demand balance and there will be no extra energy for the attacker.

Extending Paper I, in Paper II, we studied how energy could be gained for free through FDIA in local P2P energy trading scenarios. In this paper we studied RQ1.1 and RQ1.3 which are as follows: "RQ1.1: what kind of measures can be used to defend against the identified kinds of attacks in local P2P energy trading markets?" and "RQ1.3: what kind of new cyber-attacks in P2P energy trading markets can be imagined?". Accordingly, we developed a novel FDIA model based on two threat scenarios, in which the attacker tried to gain energy for free by intruding into the game realizing a P2P energy trading market. We assumed the FDIA is motivated by the desire to gain free energy and reap economic benefits for the attacker. Here, the attacker's goal to gain energy for free was realized by a novel way of manipulating the trading data with the effect that, in the end, the supply was greater than the "true" demand. In such a case, we assumed an attacker can use a "hidden" battery as a measure to prevent grid imbalance by consuming the resulting surplus energy. The opposite case is of no interest to the attacker as this would require the "hidden" battery to "supply" energy (discharge the battery) to prevent imbalance.

The trading game is iterative, and in order for the attacker to gain free energy, we found that the false data needs to be injected in all iterations. An essential issue, which was not studied in Paper I, is that the attack should not violate the convergence criteria of the game. Convergence happens in an iteration when no agent tries to modify its decision from the previous iteration. Violating the convergence condition disrupts trading. In Paper II, we referred to this problem as the convergence issue. We mathematically proved the convergence of the game given the injection method of the false data showing the effectiveness of our FDIA model. In this paper, we also studied the following research questions: "RQ2.1: what kind of measures can be used to defend against the identified kinds of attacks in local P2P energy trading markets?" and "RQ2.2: how can machine learning be applied to defend against the attacker both considering existing

approaches and identifying the need for new solution?". Hence, we introduced a highly accurate interpretable ML model together with a transparent decision-making process which rendered the model suitable for attack detection in P2P energy trading.

### 1.6.3 Paper III

S. Mohammadi, F. Eliassen, and H. -A. Jacobsen. "Applying Energy Justice Principles to Renewable Energy Trading and Allocation in Multi-Unit Buildings", *Energies 2023*, 16, 1150.

In Section 1.6.1, we mentioned that DRESs have been widely approved at the residential scale, especially in detached houses, but the lack of a legal framework prevents the installation of PV panels and BESSs in multi-unit buildings. Recent studies related to PV panel allocation in multi-unit buildings have focused more on evaluating the technical performance [GCG21] and analyzing the economic and technical feasibility of PV panels in microgrids [Qad22] and [WMC22]. However, shared DRESs, including PV panels and BESSs, in multi-unit buildings have not been investigated well.

The diversity of residents in multi-unit buildings, including tenants and unit owners, can make it challenging to share energy from shared DRESs. This process can be unfair for some residents, as some of them may not be able to afford the investment or may only want to enjoy the benefits for a short time. In this regard, in Paper III, we studied the following research questions: "RQ3.1: what are the effects of developing DRESs for multi-unit buildings" and "RQ3.2: how energy generated by DRESs can be shared in multi-unit buildings?". We proposed an energy-sharing model that enabled efficient, fair, and equitable allocation and distribution of energy, costs, and benefits in multi-unit buildings, considering different groups of residents.

In Section 1.6.3 we concluded that energy justice provides an effective decision-making tool that helps stakeholders, e.g., consumers and producers, to make more rational energy decisions. In general, energy justice addresses the equitable sharing of energy, costs, and benefits and identifies injustices within energy systems [SD15] and [Sar17]. The value of energy justice has not been studied within the concept of energy sharing in multi-unit buildings. Therefore, a set of steps has to be formulated to enable a fair and just energy-sharing system in multi-unit buildings where different groups of residents can participate and gain benefit from the shared DRESs in their building. Applying the principles of energy justice in energy sharing models removes or reduces barriers to the active participation of end customers (consumers/prosumers) in the future smart and decentralized energy grid. Therefore, it is of most interest to analyse how energy justice's principles can be applied in the energy trading and allocation processes to achieve fair energy sharing.

In Paper III, we proposed a new fair energy sharing model (FESM), which focused on energy allocation and trading inside different multi-unit buildings, considering energy justice principles. The basis for our definition of FESM was a network behind the meter in which the shared systems (PV panels and BESSs)

can be owned by the main owner of a multi-unit building or a group of residents living in the building. Although FESM and community-based microgrids have similarities in their configurations (e.g., both rely on centralized renewable sources), they have an important difference. In community microgrids, shared DRESs are located in front of the meter that are controlled by utility companies (i.e., they are controlled in an aggregate manner) that incur extra costs for the users who use the shared systems (e.g., there will be administrative costs). Since users of community DRESs do not own DRESs, they are deprived of having access to any of the tax credits and incentives of DRESs. However, in FESM, shared DRESs are installed behind the meter and are not controlled by utility companies; hence, additional costs are eliminated for users. Moreover, users in FESM can own a portion of DRESs and take advantage of the tax benefits.

After allocating shared DRESs and energy to the residents by the energy management operator (EMO) of the buildings, energy trading was enabled in FESM with expected prominent benefits such as cost-savings and carbon footprint reduction. The EMO of the buildings monitored and controled the trading stage and computed the trading price. During the energy trading process, the interests of sellers and buyers were protected, and they were given the opportunity to determine the amount of energy they want to sell and buy based on certain factors, such as priority factors, or after seeing the price. The priority factor was defined as one of the main elements of FESM to retain the fairness and interests of both buyers and sellers during energy trading. Moreover, in this paper, we studied research questions RQ4.1 and RQ4.2 as follows: "RQ4.1: how fairness can be defined in renewable energy sharing" and "RQ4.2: how can justice be applied to renewable energy sharing in multi- unit buildings to achieve fair energy sharing?". Hence, we analyzed justice and fairness in energy allocation and trading processes according to the main principles of energy justice. These analyzes helped to understand that justice can be defined differently for each building according to the building conditions (e.g., resident preferences, types of residents, etc.). Moreover, the revenue of the shared DRESs' users living in the multi-unit buildings were examined under different energy allocation processes. In addition to fairness and justice, the experimental results showed that our method increased the sellers' profit by 59.7–127% and decreased the buyers' cost by 8–21%, compared to the baseline methods. Moreover, applying the energy justice principles in the proposed sharing models could act as an efficient incentive for the residents of the multi-unit buildings to invest in the shared distributed renewable energy sources.

### 1.6.4 Main Contributions of the Dissertation

The main contributions of this dissertation can be summarized as follows:

- Studied the security issues in the smart grid focusing on AMI and its important components including smart meters and communication networks;

- Studied local energy trading markets in the smart grid and analysing its security issues focusing on FDIAs;
- Analysed and experimentally explored the consequences of FDIAs in a game-theoretic approach to P2P energy trading;
- Proposed two threat scenarios based on a novel false data injection attack model;
- Presented a solution for how the attacker may gain energy for free under the game-theoretic approach to P2P energy trading and prevent imbalance in demand-response caused by a FDIA;
- Proposed a reliable and transparent machine learning model for accurate and interpretable detection of FDIAs;
- Studied the challenges related to the establishment of renewable energy communities;
- Studied and explored the challenges of renewable energy sharing in multi-unit buildings focusing on fairness issues;
- Presented a novel fair energy sharing framework FESM plus two different applications of it;
- Studied energy justice and its main principles;
- Applied the main principles of energy justice in a systematic way in the design of energy allocation and trading processes to create justice and fairness.

## 1.7 Suggestions for Future Research

In this section, we discuss possible future directions to stimulate more studies into the extension or exploitation of the introduced methods in this dissertation. We categorized the ideas based on the researched topics below.

- **Privacy-Preserving in using shared DRESs:** In Paper III, a fair energy sharing model is proposed to enable using of shared DRESs in multi-unit buildings. However, we did not studied privacy issues related to residents who participate in energy sharing. Privacy concerns are dependent on the context in which they arise. Individuals have varying areas of concern, and some privacy issues may prevent data sharing more than other concerns. In literature, it has been found that the main privacy issue is that sharing the details of energy consumption data could expose home life information and intrude upon decision-making, autonomy, and control [**103**]. For future research, it is of interest to explore how to achieve trust among participants and how much information they should share during energy trading.

- **Energy justice as an interactive tool:** In Paper III, we have applied energy justice principles in the design of energy-sharing processes to make justice. As a future work, it might be interesting to develop the proposed framework into an interactive tool for exploring and comparing the effects of different approaches to energy justice. As an interactive tool, energy justice can be used to engage stakeholders in discussions and decision-making processes related to energy policies and projects. This tool identifies potential energy justice issues, such as the unequal distribution of energy benefits and burdens and the exclusion of specific communities from decision-making processes.

- **Uncertainty:** Another interesting topic that could be studied in the future is uncertainty. In this thesis, uncertainty can be explored in the context of cybersecurity issues in P2P energy trading markets, as well as within PV generation and consumption.

  In the context of local energy trading markets, cybersecurity is critical in ensuring the secure exchange of energy resources and data. Effective risk management within this context involves the identification, assessment, and mitigation of potential risks to protect the integrity of the energy trading ecosystem. A robust cybersecurity framework tailored to these markets can address uncertainty through various strategies, such as risk assessment, risk mitigation, incident response, and monitoring and adaptation. Addressing uncertainties in cybersecurity within local energy trading markets necessitates a comprehensive strategy that includes redundancy, resiliency, diversity, and the establishment of a robust risk management framework. These approaches are essential for local energy trading markets to effectively manage the constantly evolving and unpredictable nature of cyber threats. While it is not feasible to eliminate all uncertainties entirely, adopting a proactive and flexible approach can substantially enhance the posture and resilience of cybersecurity operating within these markets, helping them withstand and respond to the challenges faced by unknown cyber threats.

  There are multiple factors that affect solar PV generation, including weather conditions, location, and the efficiency of the solar panels. When it comes to weather conditions, events like cloud cover or storms can reduce the amount of sunlight that can reach the solar panels, which leads to lower energy production. Additionally, the efficiency of solar panels can fluctuate based on factors such as temperature and shading. The instability in solar energy production causes a challenge for grid operators, who must continually balance supply and demand in real-time. At times, surplus solar energy can be injected back into the grid, which may cause issues for grid stability, and necessitates the requirement of flexible backup power sources. On the consumption side, uncertainty in solar energy demand patterns can be impacted by several factors, including weather conditions, consumer behavior, and the availability of energy storage technologies. For

instance, changes in consumer behavior, such as increased use of energy-efficient appliances or changes in work-from-home policies, can change overall electricity demand and energy consumption times.

Uncertainties in solar PV generation and consumption can create challenges for the normal conduct of peer-to-peer (P2P) energy trading. One of the significant challenges is the difference between the actual demand and production and the predicted ones. This means that since the trading amounts of energy consumption and generation is based on predictions about the future, there will always be inaccuracies compared to the hour of actual consumption and generation. This problem usually creates some imbalance that needs to be compensated during the hour of actual consumption/generation to maintain grid balance.

Uncertainties can happen because of different factors such as weather conditions, deliberate changes in energy demand, or technical issues. For example, if a prosumer deliberately overestimates their solar energy production and sells more energy than they produce, it can create a shortage of energy for other consumers or the grid, leading to potential reliability issues. On the other hand, if a consumer deliberately underestimates their energy consumption and does not purchase enough energy from the grid or other prosumers, it can lead to potential energy shortages for themselves and the grid. One possible solution to address these intentional overestimations/underestimations, which can be categorized as FDIAs, could be to consider penalties to discourage them. For example, a penalty could be a higher energy price for the energy sold beyond the actual production or purchased beyond the actual consumption. However, these penalties could also affect the benefits of consumers/prosumers. For example, if a consumer overestimates their solar energy production and is penalized, it could affect their profits and savings from selling excess energy.

Therefore, similar to the wholesale market that maintain the grid balance using the balancing market, a solution for uncertainties in P2P energy trading markets may be needed to balance the market and for scalability reasons this may need to be handled locally (e.g., a role for the coordinator of the energy trading market).

## 1.8 Published Papers during Ph.D. Studies

During the Ph.D. studies, the author has contributed to the following conference and journal publications:

1. S. Mohammadi, F. Eliassen, and Y. Zhang, "Effects of false data injection attacks on a local P2P energy trading market with prosumers," *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, The Hague, Netherlands, 2020, pp. 31-35.

2. S. Mohammadi, F. Eliassen, Y. Zhang, and H. -A. Jacobsen, "Detecting False Data Injection Attacks in Peer to Peer Energy Trading Using Machine Learning," in *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 3417-3431, 1 Sept.-Oct. 2022.

3. S. Mohammadi, F. Eliassen, and H. -A. Jacobsen. "Applying Energy Justice Principles to Renewable Energy Trading and Allocation in Multi-Unit Buildings", *Energies 2023*, 16, 1150.

## References


[Age22] Agency, E. E. *A future based on renewable energy*. 2022. URL: https://www.eea.europa.eu/signals/signals-2022/articles/a-future-based-on-renewable-energy (visited on 05/18/2023).

[Ahm+19] Ahmed, A. et al. “Cyber physical security analytics for anomalies in transmission protection systems”. In: *IEEE Transactions on Industry Applications* vol. 55, no. 6 (2019), pp. 6313–6323.

[AKE18] Ayad, A., Khalaf, M., and El-Saadany, E. “Detection of false data injection attacks in automatic generation control systems considering system nonlinearities”. In: *2018 IEEE Electrical Power and Energy Conference (EPEC)*. IEEE. 2018, pp. 1–6.

[AMT15] Anwar, A., Mahmood, A. N., and Tari, Z. “Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid”. In: *Information Systems* vol. 53 (2015), pp. 201–212.

[AS15] Anzalchi, A. and Sarwat, A. “A survey on security assessment of metering infrastructure in smart grid systems”. In: *SoutheastCon 2015*. IEEE. 2015, pp. 1–4.

[Aya+18] Ayad, A. et al. “Detection of false data injection attacks in smart grids using recurrent neural networks”. In: *2018 IEEE power & energy society innovative smart grid technologies conference (ISGT)*. IEEE. 2018, pp. 1–5.

[Bau+22] Bauwens, T. et al. “Conceptualizing community in energy systems: A systematic review of 183 definitions”. In: *Renewable and Sustainable Energy Reviews* vol. 156 (2022), p. 111999.

[Bha18] Bhatt, S. *Reinforcement Learning 101*. 19.03.2018. URL: https://towardsdatascience.com/reinforcement-learning-101-e24b50e1d292 (visited on 05/29/2023).

[Bul+18] Bullich-Massague, E. et al. “Microgrid clustering architectures”. In: *Applied energy* vol. 212 (2018), pp. 340–361.

[BV04] Boyd, S. P. and Vandenberghe, L. *Convex optimization*. Cambridge university press, 2004.

[BWS15] Badrinath Krishna, V., Weaver, G. A., and Sanders, W. H. "PCA-based method for detecting integrity attacks on advanced metering infrastructure". In: *Quantitative Evaluation of Systems: 12th International Conference, QEST 2015, Madrid, Spain, September 1-3, 2015, Proceedings 12*. Springer. 2015, pp. 70–85.

[BZ14] Bi, S. and Zhang, Y. J. "Graphical methods for defense against false-data injection attacks on power system state estimation". In: *IEEE Transactions on Smart Grid* vol. 5, no. 3 (2014), pp. 1216–1227.

[CBE17] Castellazzi, L., Bertoldi, P., and Economidou, M. "Overcoming the split incentive barrier in the building sector". In: *Publications Office of the European Union, Luxembourg* (2017).

[CBK20] Chakraborty, S., Baarslag, T., and Kaisers, M. "Automated peer-to-peer negotiation for energy contract settlements in residential cooperatives". In: *Applied Energy* vol. 259 (2020), p. 114173.

[CJM15] Chaojun, G., Jirutitijaroen, P., and Motani, M. "Detecting false data injection attacks in AC state estimation". In: *IEEE Transactions on Smart Grid* vol. 6, no. 5 (2015), pp. 2476–2483.

[Cle08] Cleveland, F. M. "Cyber security issues for advanced metering infrasttructure (AMI)". In: *2008 IEEE power and energy society general meeting-conversion and delivery of electrical energy in the 21st century*. IEEE. 2008, pp. 1–5.

[Con+21] Conradie, P. D. et al. "Who wants to join a renewable energy community in Flanders? Applying an extended model of Theory of Planned Behaviour to understand intent to participate". In: *Energy Policy* vol. 151 (2021), p. 112121.

[Cui+20] Cui, S. et al. "A new and fair peer-to-peer energy sharing framework for energy buildings". In: *IEEE Transactions on Smart Grid* vol. 11, no. 5 (2020), pp. 3817–3826.

[Dil20] Dileep, G. "A survey on smart grid technologies and applications". In: *Renewable energy* vol. 146 (2020), pp. 2589–2625.

[Dog+20] Dogan, E. et al. "The impact of renewable energy consumption to economic growth: a replication and extension of". In: *Energy Economics* vol. 90 (2020), p. 104866.

[El +17] El Hariri, M. et al. "Online false data detection and lost packet forecasting system using time series neural networks for IEC 61850 sampled measured values". In: *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE. 2017, pp. 1–5.

[El +18] El Mrabet, Z. et al. "Cyber-security in smart grid: Survey and challenges". In: *Computers & Electrical Engineering* vol. 67 (2018), pp. 469–482.

[Enea] Energy, S. *Battery energy storage*. URL: https://www.siemens-energy.com/global/en/offerings/storage-solutions/battery-energy-storage.html (visited on 05/18/2023).

[Eneb] Energy, U. D. of. *Solar Photovoltaic Technology Basics*. URL: https://www.energy.gov/eere/solar/solar-photovoltaic-technology-basics (visited on 05/18/2023).

[Esm+13] Esmalifalak, M. et al. "Bad data injection attack and defense in electricity market using game theory study". In: *IEEE Transactions on Smart Grid* vol. 4, no. 1 (2013), pp. 160–169.

[Esm+14] Esmalifalak, M. et al. "Detecting stealthy false data injection using machine learning in smart grid". In: *IEEE Systems Journal* vol. 11, no. 3 (2014), pp. 1644–1652.

[Fin+18] Fina, B. et al. "Economic assessment and business models of rooftop photovoltaic systems in multiapartment buildings: case studies for Austria and Germany". In: *Journal of Renewable Energy* vol. 2018 (2018), pp. 1–16.

[Fle+18] Fleischhacker, A. et al. "Sharing solar PV and energy storage in apartment buildings: resource allocation and pricing". In: *IEEE Transactions on Smart Grid* vol. 10, no. 4 (2018), pp. 3963–3973.

[Flo18] Flovik, V. *How to use machine learning for anomaly detection and condition monitoring*. 31.12.2018. URL: https://towardsdatascience.com/how-to-use-machine-learning-for-anomaly-detection-and-condition-monitoring-6742f82900d7 (visited on 05/29/2023).

[FS17] Foroutan, S. A. and Salmasi, F. R. "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method". In: *IET Cyber-Physical Systems: Theory & Applications* vol. 2, no. 4 (2017), pp. 161–171.

[Gan+19] Ganjkhani, M. et al. "A novel detection algorithm to identify false data injection attacks on power system state estimation". In: *Energies* vol. 12, no. 11 (2019), p. 2209.

[GCG21] Gjorgievski, V. Z., Cundeva, S., and Georghiou, G. E. "Social arrangements, technical designs and impacts of energy communities: A review". In: *Renewable Energy* vol. 169 (2021), pp. 1138–1156.

[Ghi+23] Ghiasi, M. et al. "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future". In: *Electric Power Systems Research* vol. 215 (2023), p. 108975.

[Hab+23] Habib, A. A. et al. "False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction". In: *Computers and Electrical Engineering* vol. 107 (2023), p. 108638.

[Hid+17] Hidalgo-León, R. et al. "A survey of battery energy storage system (BESS), applications and environmental impacts in power systems". In: *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)*. 2017, pp. 1–6.

[Hoi+21] Hoicka, C. E. et al. "Implementing a just renewable energy transition: Policy advice for transposing the new European rules for renewable energy communities". In: *Energy Policy* vol. 156 (2021), p. 112435.

[IBM] IBM. *What is supervised learning?* URL: https://www.ibm.com/topics/supervised-learning (visited on 05/29/2023).

[IMO18] Islam, S. N., Mahmud, M. A., and Oo, A. M. T. "Impact of optimal false data injection attacks on local energy trading in a residential microgrid". In: *Ict Express* vol. 4, no. 1 (2018), pp. 30–34.

[Inê+20] Inês, C. et al. "Regulatory challenges and opportunities for collective renewable energy prosumers in the EU". In: *Energy Policy* vol. 138 (2020), p. 111212.

[INO20] Impram, S., Nese, S. V., and Oral, B. "Challenges of renewable energy penetration on power system flexibility: A survey". In: *Energy Strategy Reviews* vol. 31 (2020), p. 100539.

[Jaf+20] Jafari, A. et al. "A fair electricity market strategy for energy management and reliability enhancement of islanded multi-microgrids". In: *Applied Energy* vol. 270 (2020), p. 115170.

[JAL15] Jokar, P., Arianpoo, N., and Leung, V. C. "Electricity theft detection in AMI using customers' consumption patterns". In: *IEEE Transactions on Smart Grid* vol. 7, no. 1 (2015), pp. 216–226.

[Jia+14] Jiang, R. et al. "Energy-theft detection issues for advanced metering infrastructure in smart grid". In: *Tsinghua Science and Technology* vol. 19, no. 2 (2014), pp. 105–120.

[Jin+16] Jindal, A. et al. "Decision tree and SVM-based data analytics for theft detection in smart grid". In: *IEEE Transactions on Industrial Informatics* vol. 12, no. 3 (2016), pp. 1005–1016.

[Jin+20] Jing, R. et al. "Fair P2P energy trading between residential and commercial multi-energy systems enabling integrated demand-side management". In: *Applied Energy* vol. 262 (2020), p. 114551.

[Ker+21] Kermani, M. et al. "Intelligent energy management based on SCADA system in a real Microgrid for smart building applications". In: *Renewable Energy* vol. 171 (2021), pp. 1115–1127.

[KPJ18] Khanna, K., Panigrahi, B. K., and Joshi, A. "AI-based approach to identify compromised meters in data integrity attacks on smart grid". In: *IET Generation, Transmission & Distribution* vol. 12, no. 5 (2018), pp. 1052–1066.

[Las+17] Laszka, A. et al. “Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers”. In: *Proceedings of the Seventh International Conference on the Internet of Things*. 2017, pp. 1–8.

[Li+19] Li, Z. et al. “Blockchain for decentralized transactive energy management system in networked microgrids”. In: *The Electricity Journal* vol. 32, no. 4 (2019), pp. 58–72.

[Lia+16] Liang, G. et al. “A review of false data injection attacks against modern power systems”. In: *IEEE Transactions on Smart Grid* vol. 8, no. 4 (2016), pp. 1630–1638.

[Liu+14] Liu, L. et al. “Detecting false data injection attacks on power grid by sparse optimization”. In: *IEEE Transactions on Smart Grid* vol. 5, no. 2 (2014), pp. 612–621.

[Liu+17] Liu, N. et al. “Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers”. In: *IEEE Transactions on Power Systems* vol. 32, no. 5 (2017), pp. 3569–3583.

[Lod+22] Lode, M. et al. “A transition perspective on Energy Communities: A systematic literature review and research agenda”. In: *Renewable and Sustainable Energy Reviews* vol. 163 (2022), p. 112479.

[Lov+20] Lovati, M. et al. “Optimal simulation of three peer to peer (P2P) business models for individual PV prosumers in a local electricity market using agent-based modelling”. In: *Buildings* vol. 10, no. 8 (2020), p. 138.

[LZW19] Long, C., Zhou, Y., and Wu, J. “A game theoretic approach for peer to peer energy trading”. In: *Energy Procedia* vol. 159 (2019), pp. 454–459.

[Man+14] Manandhar, K. et al. “Detection of faults and attacks including false data injection attack in smart grid using Kalman filter”. In: *IEEE transactions on control of network systems* vol. 1, no. 4 (2014), pp. 370–379.

[McC+13] McCauley, D. A. et al. “Advancing energy justice: the triumvirate of tenets”. In: *International Energy Law Review* vol. 32, no. 3 (2013), pp. 107–110.

[Men+18] Mengelkamp, E. et al. “A blockchain-based smart grid: towards sustainable local energy markets”. In: *Computer Science-Research and Development* vol. 33 (2018), pp. 207–214.

[Mis17] Mishra, S. *Unsupervised Learning and Data Clustering*. 19.05.2017. URL: https://towardsdatascience.com/unsupervised-learning-and-data-clustering-eeecb78b422a (visited on 05/29/2023).

[MMM20] Moncecchi, M., Meneghello, S., and Merlo, M. “A game theoretic approach for energy sharing in the italian renewable energy communities”. In: *Applied Sciences* vol. 10, no. 22 (2020), p. 8166.

[Nora] NordPool. *About us*. URL: https://www.nordpoolgroup.com/en/About-us/ (visited on 05/21/2023).

[Norb] NordPool. *The Power Market*. URL: https://www.nordpoolgroup.com/en/the-power-market/ (visited on 05/21/2023).

[Nor13] Norway, E. F. *The Power Market*. 2022-05-13. URL: https://energifaktanorge.no/en/norsk-energiforsyning/kraftmarkedet/ (visited on 05/21/2023).

[NVE10] NVE$_R$*ME*. *Om kraftmarkedet og det norske kraftsystemet*. 2022-08-10. URL: https://www.nve.no/reguleringsmyndigheten/kunde/om-kraftmarkedet-og-det-norske-kraftsystemet/ (visited on 05/18/2023).

[Oza+15] Ozay, M. et al. "Machine learning methods for attack detection in the smart grid". In: *IEEE transactions on neural networks and learning systems* vol. 27, no. 8 (2015), pp. 1773–1786.

[Par+18] Parliament, E. et al. "Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources". In: *Off. J. Eur Union Belgium* vol. 20 (2018), p. 2.

[Par+21] Park, D.-H. et al. "A Hierarchical Peer-to-Peer Energy Transaction Model Considering Prosumer's Green Energy Preference". In: *International Journal of Control, Automation and Systems* vol. 19, no. 1 (2021), pp. 311–317.

[Per+21] Perger, T. et al. "PV sharing in local communities: Peer-to-peer trading under consideration of the prosumers' willingness-to-pay". In: *Sustainable Cities and Society* vol. 66 (2021), p. 102634.

[Qad22] Qadourah, J. A. "Energy and economic potential for photovoltaic systems installed on the rooftop of apartment buildings in Jordan". In: *Results in Engineering* vol. 16 (2022), p. 100642.

[RAH18] Ramotsoela, D., Abu-Mahfouz, A., and Hancke, G. "A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study". In: *Sensors* vol. 18, no. 8 (2018), p. 2491.

[RSM22] Roberts, M. B., Sharma, A., and MacGill, I. "Efficient, effective and fair allocation of costs and benefits in residential energy communities deploying shared photovoltaics". In: *Applied Energy* vol. 305 (2022), p. 117935.

[Sar17] Sarı, R. "Energy justice-a social sciences and humanities cross-cutting theme report". In: (2017).

[SD15] Sovacool, B. K. and Dworkin, M. H. "Energy justice: Conceptual insights and practical applications". In: *Applied Energy* vol. 142 (2015), pp. 435–444.

[SJ15] Sedghi, H. and Jonckheere, E. “Statistical structure learning to ensure data integrity in smart grid”. In: *IEEE Transactions on Smart Grid* vol. 6, no. 4 (2015), pp. 1924–1933.

[SMD20] Syed, M. M., Morrison, G. M., and Darbyshire, J. “Shared solar and battery storage configuration effectiveness for reducing the grid reliance of apartment complexes”. In: *Energies* vol. 13, no. 18 (2020), p. 4820.

[Sot+21] Soto, E. A. et al. “Peer-to-peer energy trading: A review of the literature”. In: *Applied Energy* vol. 283 (2021), p. 116268.

[Sou+19] Sousa, T. et al. “Peer-to-peer and community-based markets: A comprehensive review”. In: *Renewable and Sustainable Energy Reviews* vol. 104 (2019), pp. 367–378.

[Sæt19] Sæther, G. “Peer-to-Peer Energy Trading in Combination with Local Flexibility Resources in a Norwegian Industrial Site”. MA thesis. NTNU, 2019.

[VR17] Vimalkumar, K. and Radhika, N. “A big data framework for intrusion detection in smart grids using apache spark”. In: *2017 International conference on advances in computing, communications and informatics (ICACCI)*. IEEE. 2017, pp. 198–204.

[VV17] Viegas, J. L. and Vieira, S. M. “Clustering-based novelty detection to uncover electricity theft”. In: *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. IEEE. 2017, pp. 1–6.

[Wan+17] Wang, Y. et al. “A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids”. In: *IEEE Access* vol. 5 (2017), pp. 26022–26033.

[Wan+19] Wang, D. et al. “Detection of power grid disturbances and cyber-attacks based on machine learning”. In: *Journal of information security and applications* vol. 46 (2019), pp. 42–52.

[Wei+18] Wei, L. et al. “Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid”. In: *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*. IEEE. 2018, pp. 1–9.

[WH16] Wang, H. and Huang, J. “Cooperative planning of renewable generations for interconnected microgrids”. In: *IEEE Transactions on Smart Grid* vol. 7, no. 5 (2016), pp. 2486–2496.

[WL13] Wang, W. and Lu, Z. “Cyber security in the smart grid: Survey and challenges”. In: *Computer networks* vol. 57, no. 5 (2013), pp. 1344–1371.

[WMC22] Woo, J., Moon, S., and Choi, H. “Economic value and acceptability of advanced solar power systems for multi-unit residential buildings: The case of South Korea”. In: *Applied Energy* vol. 324 (2022), p. 119671.

[XJL19] Xue, D., Jing, X., and Liu, H. “Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework”. In: *IEEE Access* vol. 7 (2019), pp. 31762–31773.

[YTH16] Yan, J., Tang, B., and He, H. “Detection of false data attacks in smart grid with supervised learning”. In: *2016 International Joint Conference on Neural Networks (IJCNN)*. IEEE. 2016, pp. 1395–1402.

[Zan+17] Zanetti, M. et al. “A tunable fraud detection system for advanced metering infrastructure using short-lived patterns”. In: *IEEE Transactions on Smart grid* vol. 10, no. 1 (2017), pp. 830–840.

[Zha+18a] Zhang, C. et al. “Peer-to-Peer energy trading in a Microgrid”. In: *Applied Energy* vol. 220 (2018), pp. 1–12.

[Zha+18b] Zhao, H. et al. “Anomaly detection and fault analysis of wind turbine components based on deep learning network”. In: *Renewable energy* vol. 127 (2018), pp. 825–834.

[ZWC20] Zhang, Y., Wang, J., and Chen, B. “Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach”. In: *IEEE Transactions on Smart Grid* vol. 12, no. 1 (2020), pp. 623–634.

[ZWX18] Zhang, Z., Wang, Y., and Xie, L. “A novel data integrity attack detection algorithm based on improved grey relational analysis”. In: *IEEE Access* vol. 6 (2018), pp. 73423–73433.

# Papers

Paper I

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

I

**Sara Mohammadi, Frank Eliassen, and Yan Zhang**

Published in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe) Conference*, October 26-28 2020, pp. 31–35. DOI: 10.1109/ISGT-Europe47291.2020.9248761.

**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.

## Contents

## I.1 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 [Le +20].

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 [Zha+19a]. There are several works which studied FDIA scenarios in P2P energy trading, as well as possible defense methods [Kos+10], [Liu+14], [GCG21], and [BZ14]. 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 [Zha+19b]. 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 [Tus+18]. 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.

## I.2 System Model

The trading model that we explore in our work is adapted from [Zha+19b]. In this model, a community-based P2P market is 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 [JT06]. Let $N = 1, ..., N$ 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 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:

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

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

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 I.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 [Liu+14] the utility of the prosumer $i$ at time slot $t$ ($Utility_{i,t}(.)$) is expressed as follows:

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

$$p_t^s = \mu_t \frac{E_t^d - E_t^s}{\Sigma_{j \in M} D_{j,t}}, \quad p_t^b = \lambda_t \frac{E_t^d - E_t^b}{\Sigma_{j \in M} D_{j,t}} \tag{I.4}$$

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 $\mu_t$ and $\lambda_t$ are predefined parameters. $p_t^s(E_{i,t}^g - x_{i,t})$ and $p_t^b(E_{i,t}^g - x_{i,t})$ 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 $E_t^d$ 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 $x_{i,t}$ [Liu+14].

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 [Liu+14].

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 [Liu+14].

## I.3 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.

### I.3.1 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*

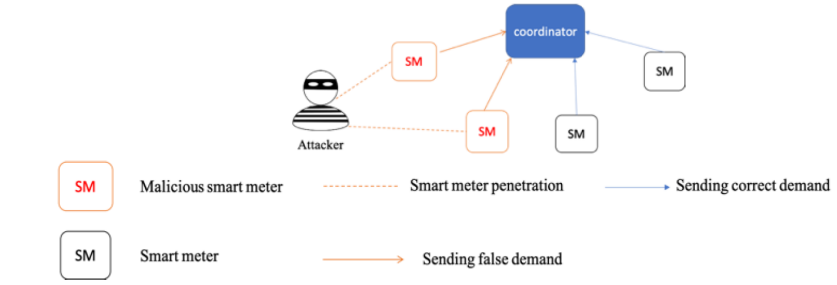
As it can be seen from Figure III.3, we consider two ways of attack. First, before the game starts (before the calculation of the prosumers' bids by their smart meters), and second, at the beginning of the game (after the calculation of the prosumers' bids by their smart meters). In the first method (Figure I.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*

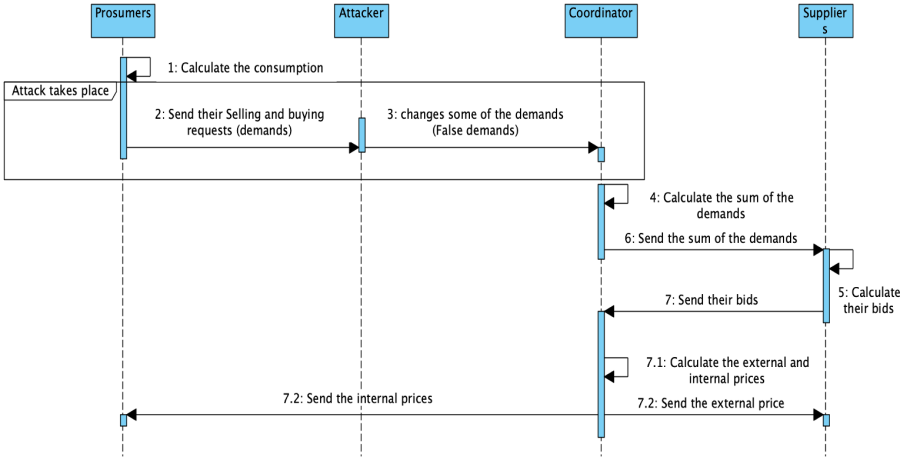
A smart meter has five main components which are control unit, smart meter collector, metrology system, home area network (HAN), and the optical interface [KKK19]. Each of these components has various targeting attacks; e.g., the vulnerability of the control unit and metrology system are hardware and 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 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 (Figure I.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




(a)




(b)

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

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.

## I.4 Nummerical Results

In the simulations, a real dataset from Austin, Texas [Dat19] 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 I.2 shows the result of the experiments in the normal situation (without attacks) in the same time slot. We can see from Table I.1 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

Table I.1: Average utilities of prosumers (A.U.P), consumers (A.U.C), and suppliers (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 I.2: Average utilities of prosumers (A.U.P), consumers (A.U.C), and suppliers (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 |

following observations can be made by comparing Table I.1 and Table I.2:

*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 I.3, and then the suppliers have to supply more energy (equation I.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 I.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

Table I.3: 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% |

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 I.3 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 I.3 are investigated in Figure I.2. As can be seen from Figure I.2, all prices increase after the attack; this is due to the increase in the demands. Figure I.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.

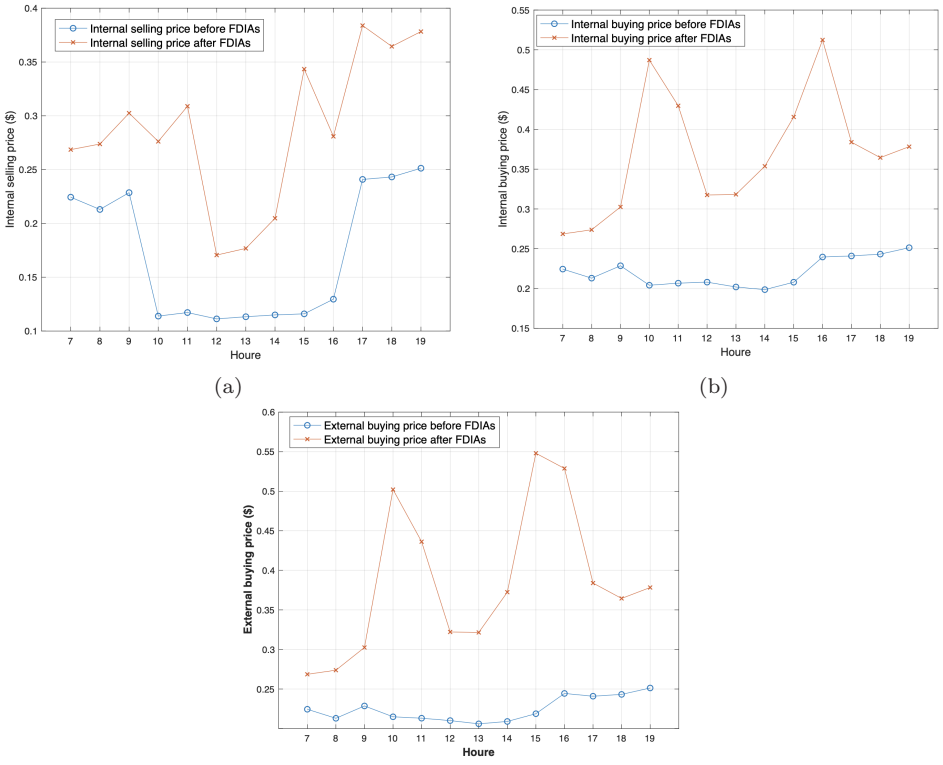



Figure I.2: (a): internal selling prices before and after FDIAs, (b): internal buying prices before and after FDIAs, and (c): external buying prices before and after FDIAs at different time slots.

## I.5 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.

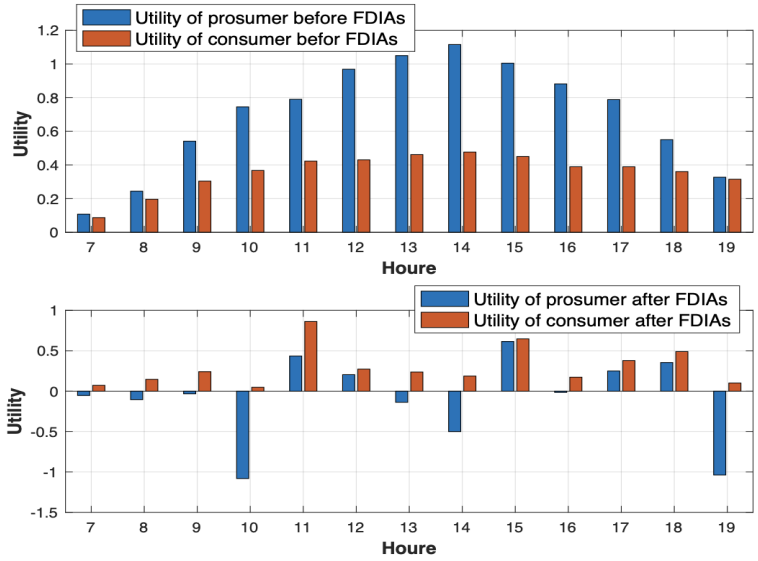



Figure I.3: profits of prosumers and consumers before and after FDIAs at different time slots.

**Acknowledgements.** The first author was partially supported by The Research Council of Norway.

## References

[BZ14] Bi, S. and Zhang, Y. J. "Graphical methods for defense against false-data injection attacks on power system state estimation". In: *IEEE Transactions on Smart Grid* vol. 5, no. 3 (2014), pp. 1216–1227.

[Dat19] Dataport. *Dataport*. 2019. URL: https://www.pecanstreet.org (visited on 04/09/2020).

[GCG21] Gjorgievski, V. Z., Cundeva, S., and Georghiou, G. E. "Social arrangements, technical designs and impacts of energy communities: A review". In: *Renewable Energy* vol. 169 (2021), pp. 1138–1156.

[JT06] Johari, R. and Tsitsiklis, J. N. "Parameterized supply function bidding: equilibrium and welfare". In: *Mathematics of Operations Research* (2006).

[KKK19] Khattak, A. M., Khanji, S. I., and Khan, W. A. "Smart meter security: Vulnerabilities, threat impacts, and countermeasures". In: *Proceedings of the 13th International Conference on Ubiquitous Information Management and Communication (IMCOM) 2019 13*. Springer. 2019, pp. 554–562.

[Kos+10] Kosut, O. et al. “Limiting false data attacks on power system state estimation”. In: *2010 44th Annual Conference on Information Sciences and Systems (CISS)*. IEEE. 2010, pp. 1–6.

[Le +20] Le Cadre, H. et al. “Peer-to-peer electricity market analysis: From variational to generalized Nash equilibrium”. In: *European Journal of Operational Research* vol. 282, no. 2 (2020), pp. 753–771.

[Liu+14] Liu, L. et al. “Detecting false data injection attacks on power grid by sparse optimization”. In: *IEEE Transactions on Smart Grid* vol. 5, no. 2 (2014), pp. 612–621.

[Tus+18] Tushar, W. et al. “Transforming energy networks via peer-to-peer energy trading: The potential of game-theoretic approaches”. In: *IEEE Signal Processing Magazine* vol. 35, no. 4 (2018), pp. 90–111.

[Zha+19a] Zhang, M. et al. “False data injection attacks against smart gird state estimation: Construction, detection and defense”. In: *Science China Technological Sciences* vol. 62, no. 12 (2019), pp. 2077–2087.

[Zha+19b] Zhang, M. et al. “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)*. IEEE. 2019, pp. 1–6.

### Authors’ addresses

**First Author** University of Oslo, Postboks 1337 Blindern, 0316 Oslo, Norway, fauthor@uio.no

**Second Author** Oxbridge University, 221B Baker Street, London NW1 6XE, United Kingdom, second.author@oxbridge.co.uk

Paper II

# Detecting false data injection attacks in peer to peer energy trading using machine learning

**Sara Mohammadi, Frank Eliassen, Yan Zhang, and Hans-Arno Jacobsen**

Published in *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 5, pp. 3417-3431, 1 Sept.-Oct. 2022, doi: 10.1109/TDSC.2021.3096213.

**Abstract**

In peer-to-peer (P2P) energy trading, the incorporation of distributed energy resources with unprotected data, originating from sources such as home energy management systems that are connected through the Internet, provokes vulnerabilities that can manifest security breaches. In this paper, two threat scenarios based on a novel false data injection attack (FDIA) model in a local P2P energy trading system are explored. In these scenarios, an attacker gains free energy by manipulating prosumers' consumption and demand. Precise and fast attack detection is needed to guarantee suitable countermeasures to prevent potential risks. We propose a novel instance-based machine learning (ML) classifier for detecting FDIAs. In contrast to black-box ML models, our algorithm provides a transparent decision-making procedure with significant predictive performance. We apply our detection model to a real-world dataset from Austin, Texas. Our experimental results show superior performance as compared to several popular interpretable and non-interpretable ML methods. On average, we achieve a 96.10% detection rate, a 96.18% accuracy rate, and a false negative rate of 1.97% with our approach.

II

## Contents

## II.1 Introduction

Peer-to-peer (P2P) energy trading [Zha+18] has emerged as a new energy management model in which the participants of the network, the prosumers, share a portion of their energy resources with one another without any direct action of a central controller. One of the benefits of a P2P trading platform is that a prosumer in need of energy can buy energy from other prosumers in the same network who have surplus energy to sell at a lower price as compared to the main grid selling price. Prosumers with excess energy, on the other hand, can reap more economic benefits by taking part in P2P energy trading in contrast to the feed-in tariff scheme [Tus+19].

Data integrity preservation is fundamental to certify the security of an energy trading market [WL13]. The integrity loss of an energy market is caused by corruption of data exchanges that result from attacks like False Data Injection Attacks (FDIAs), replay attacks, and man-in-the-middle attacks [El +19]. For the last decade, the impact of FDIA have been extensively studied. For example, Jiongcon et al. [Che+16] illustrate how FDIA can result in rescheduling of unessential generation and in load shedding by injecting false data, which causes unstable load conditions. Wu et al. [Wu+17] studied the effects of FDIA on frequency control of the smart grid and demonstrated how a simple FDIA could spread and lead to a blackout. The impact of FDIA on electricity markets are studied in [XMS10] and [Taj17]. Xie et al. [XMS10] present an FDIA against the state estimation with the knowledge of the system to cause financial misconduct, while Tajer et al. [Taj17] proposed a new FDIA on the locational marginal prices that can have a potential impact on the energy market without having full knowledge of the grid. However, none of the existing approaches investigate the impact of FDIA on a local P2P energy trading market with prosumers; this aspect is however important to study because the existence of prosumers in a local energy market constitutes a challenge for the energy sellers (e.g., suppliers).

Due to this multitude of threats, it is of utmost importance to secure the energy trading process in a smart grid. Researchers have made remarkable efforts on the identification and mitigation of FDIAs in the electric power grid [BZ14],[AMT15],[Ahm+19] . Some works are based on physical protection approaches while others are cyber-oriented approaches. From the physical security viewpoint, it poses challenges in cost and feasibility of implementing the physical protection scheme of measurement devices. For example, Chaojun et al. [BZ14] proposed a physical protection method by locking the basic measurement devices in boxes that are cost-intensive. On the other hand, Bi et al. [AMT15] proposed an optimal solution where they use a graphical method to protect the vulnerable components. To solve the problem of identifying those vulnerable components, Anwar et al. [Ahm+19] suggested an optimization-based hybrid cluster technique to order components in the grid based on their vulnerabilities to protect them. In recent years, data-driven machine learning (ML) methods have been used for cyber-physical security analysis by predicting and identifying threats and anomalies in a system [IBM]. Since physical sensors (e.g., phasor measurement units) often have flaws that causes

bad or missing data and can disrupt the analysis of true event data, detecting and identifying anomalies in power grid data is highly essential for accurate performance [Esm+14]. There are some anomaly detection methods that enhance the security of a power system. Such techniques are based on support vector machines (SVM) [FS17],[Hin+14a], naïve Bayes (NB) methods [PMA15], K-nearest neighbour (KNN) methods [FS17],[Hin+14b], artificial neural networks (ANN) [El +17], and recurrent neural networks (RNN) [FGL19] that have been applied on different attack scenarios such as cyber and physical layer attacks and power system disturbance attacks. However, we are not aware of any approach that applies ML algorithms as a defense strategy in P2P energy trading.

In this paper, we extend our own prior work [MEZ20] in which a game-theoretic approach to P2P energy trading was adopted to analyze FDIA. The vulnerability of local P2P energy trading, including both prosumers and consumers, to FDIAs was discussed as well. We also analyzed the effects of FDIAs on price and economic benefit and loss of both prosumers and attacker after applying the proposed attack model at different time slots over a day.

In our prior work, we assumed the attack occures before the game starts to reap benefits for the energy sellers (e.g., suppliers) by causing a reduction in incentives of becoming or remaining energy selling prosumers. We observed from the experiments that the profits of prosumers decreased after the FDIAs (when the prosumers' demand was increased by the attacker before the game started.) This effect (reduction in prosumers' profits) could possibly reduce the consumers' motivation to become prosumers. We concluded that the attacker could not gain energy for free by only modifying the prosumers' demand at the beginning of the game or before the game started. This is due to the iterative nature of the game where prosumers will update their demands based on the new price in subsequent iterations. Subsequently, the game will converge with supply/demand balance and there will be no extra energy for the attacker.

Extending our prior work, in this paper, we study how energy could be gained for free through FDIA in local P2P energy trading scenarios. We develop a novel FDIA model based on two threat scenarios, in which the attacker tries to gain energy for free by intruding into the game realizing a P2P energy trading market, and a novel ML model for detecting this kind of attacks. We assume the FDIA is motivated by the desire to gain free energy and reap economic benefits for the attacker. Here, the attacker's goal to gain energy for free is realized by a novel way of manipulating the trading data with the effect that, in the end, the supply is greater than the "true" demand. In such a case, we assume an attacker can use a "hidden" battery as a measure to prevent grid imbalance by consuming the resulting surplus energy. The opposite case is of no interest to the attacker as this would require the "hidden" battery to "supply" energy (discharge the battery) to prevent imbalance.

The trading game is iterative, and in order for the attacker to gain free energy, we find that the false data needs to be injected in all iterations. An essential issue, which is not studied in [MEZ20], is that the attack should not violate the convergence criteria of the game. Convergence happens in an iteration when no agent tries to modify its decision from the previous iteration. Violating the

convergence condition disrupts trading. Below, we refer to this problem as the convergence issue. We mathematically prove the convergence of the game given the injection method of the false data showing the effectiveness of our FDIA model. Most importantly, we introduce a highly accurate interpretable ML model together with a transparent decision-making process which renders the model suitable for attack detection in P2P energy trading.

We observe from our experiments that gaining free energy by the attacker causes an economic loss for prosumers, which means that the incentive of remaining or becoming energy selling prosumers is reduced. Consequently, this effect may be highly beneficial for energy sellers (e.g., suppliers). The efficiency of the proposed detection algorithm is evaluated using several case studies available in a real-world dataset from Austin, Texas [Tus+19], and it is compared with a number of popular interpretable (DT, KNN, NB), semi-interpretable (SVM), and non-interpretable (ensemble and deep neural network) machine learning classifiers. Our experiments demonstrate that under the attack, all prices increase and the average payoff (utility) of prosumers decreases. We also show how the attacker may gain economic benefits by acquiring free energy when it adversely increases the demand. Moreover, the experimental results illustrate that the proposed detection algorithm has higher accuracy and lower false negative rates as compared to the baseline ML algorithms.

The main contributions of this paper are as follows:

1. We propose two threat scenarios based on a novel false data injection attack model. The paper proposes an attack model that is able to manipulate the game by applying FDIAs and analyses its effects in a game-theoretic framework for a P2P energy trading market including prosumers.

2. We present a solution for how the attacker may gain energy for free under the game-theoretic approach to P2P energy trading and prevent imbalance in demand-response caused by a FDIA.

3. Most importantly, we propose a reliable and transparent machine learning model for accurate and interpretable detection of FDIAs.

The rest of this paper is organized as follows. Section 2 describes the P2P system model. Section 3 describes the false data injection attack model, which consists of two new threat scenarios; we then introduce our machine learning model for attack detection in Section 4. Section 5 presents experimental results followed by our conclusions in Section 6.

## II.2 P2P energy trading system model

A community-based P2P market is designed based on the model in [MEZ20]. The market is modeled as a multi-agent system that consists of four types of agents; $M$ prosumer agents modeling prosumers including pure consumers (without generation) and prosumers (with solar generation), $N$ supplier agents modeling suppliers (with their own energy generation from solar farms, wind parks,

or conventional power plants), one coordinator agent modeling a community coordinator, and one attacker agent who acts as an attacker during the game. In the game, both suppliers and prosumers try to maximize their own profit, and their behavior is modeled as a non-cooperative game. In the following, the process of trading in the game is briefly described.

The suppliers are equipped with their own energy production means. They want to sell the generated energy to the neighborhood prosumers, such as when the local solar generation from the prosumers cannot satisfy the demand. Prosumers decide how much energy they should buy or sell for each hour of the day according to their own solar power generation and load consumption. After that, they send their demand (buying/selling requests) to the coordinator. In the meantime, the attacker intercepts the communication to falsify the demand from the prosumers' side of the game.

After having received all demand requests from prosumers, including the falsified demands from the attacker, the coordinator calculates the net load, which is equal to the difference between the sum of energy generation and consumption from the prosumer-side and sends it to the suppliers. The suppliers then send their bids to the coordinator, and the coordinator calculates both external and internal prices, which are used for trading among local prosumers and with suppliers, respectively, and sends them to both suppliers and prosumers. Finally, the suppliers and prosumers update their bids and demands based on those prices. The attacker also falsifies the updated demands of the attacked prosumers and forwards the falsified demands to the coordinator. The process of modifying the demands by the attacker happens in each iteration of the game such that at the end of the game, more energy than the 'true' demand is supplied. This extra energy can be consumed by the attacker for free through suitable means such as a 'hidden battery.' The procedure above is repeated until convergence, i.e., when the difference between the last calculated external price and the one in the previous iteration is sufficiently small.

## II.3 False data injection attack models

In general, FDIA injects false data as an input or manipulates the existing data in the power system. FDIAs can happen through a communication channel by an adversary or a third-party attacker to manipulate information (bid or price offers) which are exchanged among market participants (e.g., prosumers, consumers, suppliers, etc.) to cause financial loss for them or create a disturbance in the market process [DSR21]. On the other hand, an adversary could be one of the market participants like a malicious prosumer who can directly inject false data into the market system or attack through devices (smart meter, HEM unit, etc.) to gain own financial benefits [DSR21],[BNK20],[LH15]. During FDIA, the market operator (the coordinator) makes decisions based on false information, which do not match with the true market scenario. In this section, we design two threat scenarios that are based on FDIA adversely changing demands.

### II.3.1 Threat scenario 1

**Attack motivations:** In this threat scenario, an attack can be undertaken by a malicious energy seller like a supplier who engages an attacker in a prosumer role. The other possible motivation can be to make a profit for the suppliers which could be achieved by decreasing the incentives to become an energy selling prosumer [MEZ20]. Here, the attacker attempts to find the best way of modifying the prosumers/consumers' demands to gain benefits or for the purpose of sabotage while minimizing the chance of being detected.

**Problem formulation:** In order to satisfy the objective of the attacker and at the same time to avoid injecting forged data randomly but rather follow a specific pattern of FDIA behaviour, we suggest the demand falsification follows a pattern given by II.1. Here, the falsified demand of prosumer $i$ can be expressed as a function of the prosumer's true demand, as follows:

$$d^{'}_{i,t} = d_{i,t}(1 + \beta \times f(d_{i,t})) \tag{II.1}$$

where $d^{'}_{i,t}$ is the falsified amount of energy, and $d_{i,t}$ is the demand declared by the prosumer $i$ in an iteration of the game at time slot $t$, $f(.)$ is a bounded, non-negative monotonically increasing function and $\beta$ is a scaling constant that can be negative or positive depending on the attacker's goal (increasing or decreasing the demands). We will show that for a suitable choice of function $f$ and $\beta$, the game can be proven to converge. Intuitively, to make the attacker hard to detect, the demands should only be modified by a small amount in proportion to the true demand. In this case, a sigmoid function can be useful to model the FDIAs' behavior. In addition to the fact that the sigmoid function has all the mentioned features of function $f$, another reason that makes it superior to similar functions (e.g., the trapezoidal or triangular functions) is that it does not require knowledge of historical data for its definition. We choose to use a common type of sigmoid function, the logistic function, which is defined as follows;

$$S(x) = \frac{1}{1 + e^{-x}} \tag{II.2}$$

It is easy to see that $S(.)$ has codomain $(0, 1)$. We substitute II.2 into II.1 for $f(.)$ and get

$$d^{'}_{i,t} = d_{i,t}(1 + \beta \times (\frac{1}{1 + e^{-d_{i,t}}})) \tag{II.3}$$

In order for II.3 to be applicable to any demand profile, the value of $\beta$ should be determined based on the magnitude of the true demand. According to our earlier experience [Pil+20], modifying the demand in an arbitrary way (i.e., selecting a random value for $\beta$) causes the demand modification method to work only on a specific group of household demands. Due to this, $\beta$ should be defined by some functional relationships with the true demand; $\beta = f(demand)$. Here, we choose $\beta = (\frac{demand}{c})$ for some variable $c$. Keeping the prosumers' role is an important factor that is achieved by considering a suitable dependency for $c$ with the demand. If we consider $c$ as a constant value then we need to have a

priori knowledge of the demand to select a proper $c$, and hence it does not work correctly for keeping the role of the prosumers. Overall, the attacker should learn the demand during the attack to find the right values for $\beta$ and $c$. In light of such considerations, II.3 should work well on any demand profile.

When the attacker modifies the demand during the game, the convergence issue can be asserted by proving the uniqueness of the prosumer-side game. Let $L = \{1, \ldots, l\}$ and $M = \{1, \ldots, m\}$ where $L$ is a subset of $M$ denoting the victim prosumers and all prosumers, respectively. Prosumer $i \in M$ is able to generate $E^g_{i,t}$ and consumes $x_{i,t}$ amounts of energy at time slot $t$. It should be noted that $E^g_{i,t} = 0$ for a pure consumer. Prosumers use internal selling price ($p^s_t$) and internal buying price ($p^b_t$) for trading with other prosumers. Internal prices are defined to be a function of the aggregated net load ($E^d_t$ - $E^s_t$) and bids from all prosumers and suppliers, respectively. In this model, the payoff of the prosumer $i$ at time slot $t$ ($Utility_{i,t}(.)$) and both selling and buying prices are expressed as follows [JT06]:

$$Utility_{i,t}(x_{i,t}) = \begin{cases} k_{i,t}\ln(1 + x_{i,t}) + p^s_t(E^g_{i,t} - x_{i,t}), & E^g_{i,t} - x_{i,t} > 0 \\ k_{i,t}\ln(1 + x_{i,t}) + p^b_t(E^g_{i,t} - x_{i,t}), & E^g_{i,t} - x_{i,t} \leq 0 \end{cases}, \tag{II.4}$$

$$p^b_t = \lambda_t\left(\frac{E^d_t - E^s_t}{\sum\limits_{j \in \boldsymbol{M}} \beta_{j,t}}\right), p^s_t = \mu_t\left(\frac{E^d_t - E^s_t}{\sum\limits_{j \in \boldsymbol{M}} \beta_{j,t}}\right) \tag{II.5}$$

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 $t$. The energy consumption $x_{i,t}$ is bounded by the minimum and maximum load consumptions which are denoted as $x^{min}_{i,t}$ and $x^{max}_{i,t}$ respectively. $x^{min}_{i,t}$ is the base load that should always be supplied, while the consumptions should not be more than $x^{max}_{i,t}$. $k_{i,t}$ is the reference parameter of prosumer $i$ at time slot $t$; a prosumer with high $k_{i,t}$ is more interested to consume more of its energy to gain maximum utility. $\mu_t$ and $\lambda_t$ are predefined parameters. $p^s_t(E^g_{i,t} - x_{i,t})$ and $p^b_t(E^g_{i,t} - x_{i,t})$ are the revenue that prosumer $i$ gains by selling excess energy and the price of buying energy at time slot $t$, respectively.

Second, the utility function in II.4 is changed by replacing the true demand ($E^g_{j,t} - x_{j,t}, j \in L$) with the falsified demand ($d^{'}_{j,t}, j \in L$) of $|L|$ prosumers. The modified utility function for $L$ prosumers is given by II.6.

$$Utility_{j,t}(d^{'}_{j,t}) = \begin{cases} k_{j,t}\ln(1 + (E^g_{j,t} - d^{'}_{j,t})) + p^s_t(d^{'}_{j,t}), & d^{'}_{j,t} > 0 \\ k_{j,t}\ln(1 + (E^g_{j,t} - d^{'}_{j,t})) + p^b_t(d^{'}_{j,t}), & d^{'}_{j,t} \leq 0 \end{cases}, \tag{II.6}$$

Now, we are going to prove the existence of the Nash equilibrium by showing the uniqueness of the prosumer-side game with the presence of the attacker;

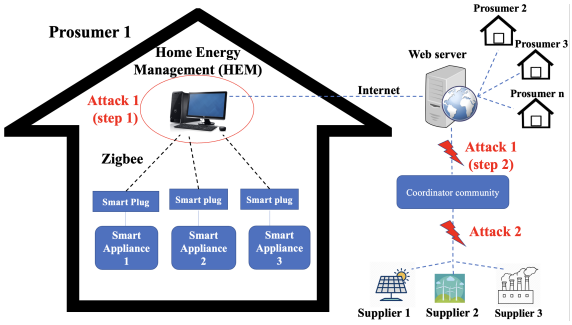



Figure II.1: HEM architecture with possible ways of attacks.

Let $\boldsymbol{d_t^*}$ denote the Nash equilibrium strategies of $|\boldsymbol{M}|$ prosumers at time slot $t$, and

$$Utility_{i,t}(\boldsymbol{d_t}^*) \geq (Utility_{i,t}(d_{i,t}, \boldsymbol{d_{-i,t}}^*)),\ \forall i \in \boldsymbol{M}. \tag{II.7}$$

where $\boldsymbol{d}^*_{-i,t}$ represents the set of demands (including both modified and non-modified demands) from all other $|\boldsymbol{M}|$ prosumers who use Nash equilibrium strategy, except prosumer $i$, and $\boldsymbol{d_t}^* = \{d^*_{i,t}\}$.

**Theorem II.3.1.** *The prosumer-side game, that is formulated with II.4 and II.6, is an $|M|$-person game, and has a unique pure strategy Nash equilibrium.*

*Proof.* There exists a unique strategy Nash equilibrium for this game if the following optimization problem, which is the combination of the utility functions II.4 and II.6, is strictly concave and has a unique solution [Ros65].

$$\begin{aligned} &\text{maximize} && Utility_{i,t}(d_{i,t}, d_{-i,t}) \\ &\text{subject to} && E^g_{i,t} - x^{max}_{i,t} \leq d_{i,t} \leq E^g_{i,t} - x^{min}_{i,t} \end{aligned} \tag{II.8}$$

II.8 applies to both sellers and buyers in the following way. The constraint in II.8 shows that the demand should not be less than the difference between the generation and the maximum load and should not be more than the difference between the generation and the base load for sellers ($E > 0$). The constraint also indicates that the demand should not be less than the negative maximum load and should not be more than the negative base load for consumers ($E = 0$). It can be seen that the utility (payoff) function in II.8 is strictly concave as its second order derivative is always negative. The choice of II.1 and the choice of $\beta$ and $f(.)$ ensure this result. So, there exists a unique solution for II.8, and the existence of the Nash equilibrium of this game is proven. ■

**Attack process:** The threat scenario takes place in two steps; first, the attacker intercepts or intrudes into a targeted home energy management (HEM) system in the first round of the game to make a disturbance in the process of calculating consumptions. Second, the attacker connects to the communication

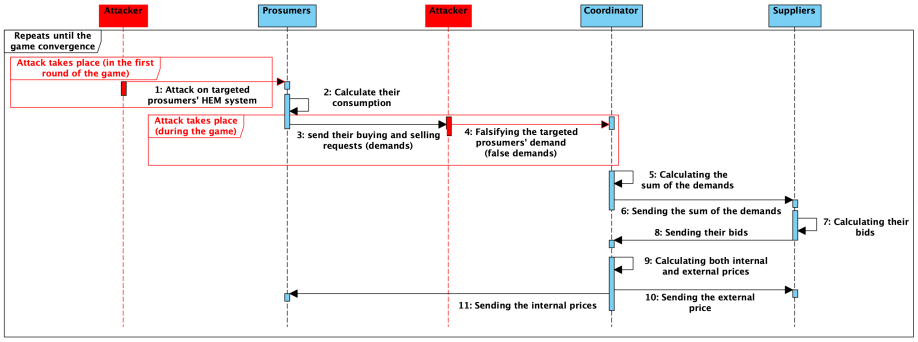



Figure II.2: Sequence diagram of the proposed threat scenario 1.

network during the game to intrude into the legitimate communication between the victim prosumer and the coordinator. The attacker intrudes into the targeted prosumers' HEM system as explained next.

Fig. II.1 illustrates components of the HEM system and possible ways of attacks. The HEM unit considers priority settings for appliances and controls the total consumption of the household. Smart plugs provide and transfer their data to the HEM unit through a Zigbee network. The household consumption data are provided by the HEM unit and could be shared with other households (prosumers) and the coordinator through web services. The physical HEM system could be threatened by an adversary to modify the household consumptions [Anu+18] that can happen in two ways [Sah+14]; an insider attack by attacking directly the physical HEM host, or an outsider attack (that we consider in our threat scenario) by attacking through the web network. The attacked HEM unit (attack 1) provides false consumption data to the web server and then to the coordinator that causes wrong demand within a neighborhood. After attacking the HEM system, the attacker controls the flow of the demand information in communication links between the web server and the coordinator to falsify some of the demand sent by the prosumers' HEM systems.

Fig. II.2 depicts the sequence diagram of threat scenario 1. As can be seen from the figure, the attacker acts at the beginning of the game by falsifying some of the initial consumptions (shiftable loads+base loads) of the prosumers, and during the game by modifying the updated victim prosumers' demands. In the first round of the game, the attacker modifies the shiftable and/or base loads of the targeted prosumers by attacking their HEM systems. In each game iteration, the coordinator calculates both internal and external prices based on the falsified demands, and prosumers update their demands based on the false prices. As explained above, the attacker's challenge is to modify the demand only in such a way that the game converges. In the converging iteration, the victim prosumers send their last updated demands to the coordinator, and the attacker changes the demands before the coordinator receives them. Finally, the

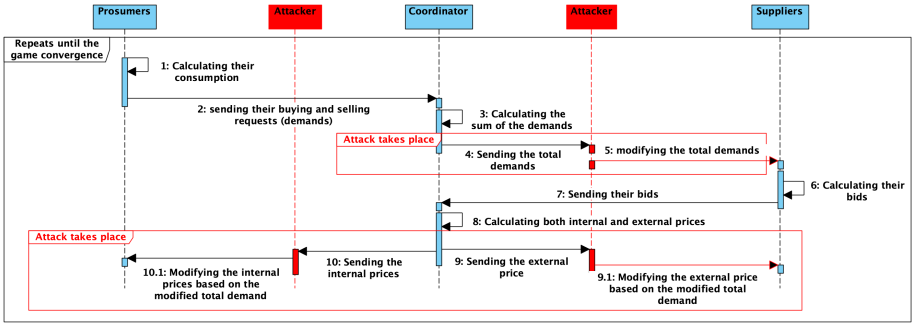



Figure II.3: Sequence diagram of the proposed threat scenario 2.

coordinator sends the final prices to both suppliers and prosumers, and suppliers supply energy based on the falsified demands.

**Attack effects:** At this point, the supplied amount of energy will differ from the total true demand of the prosumers. This will generally lead to grid imbalance. If the suppliers provide more energy than the true demand, the extra energy will not be consumed by the prosumers. This is because the attacked prosumers will not be aware that their last demand has been increased by the attacker. This creates an opportunity for the attacker to consume this extra energy for free, e.g., by installing a battery on the grid side of his house's smart meter. In this way, the smart meter cannot record the amount of energy consumed by the battery storage, which provides the energy free to the attacker.

### II.3.2 Threat scenario 2

**Attack motivation:** In this threat scenario the attack could be aimed at a sabotage or gaining free energy similar to threat scenario 1. Since attacking many of prosumers' HEM systems is challenging, we present an alternative attack scenario to gain energy for free by the attacker that does not involve attacking individual HEM systems. This attack scenario is illustrated in Fig. II.3.

**Problem formulation:** In this threat scenario, the attacker manipulates the total demand which is calculated by the coordinator. Afterward, all prices will be changed based on the modified total demand by the attacker. We follow the total demand falsification based on II.3. In this threat scenario, the attacker learns just the total demand of all prosumers during the attack and thus does not need to consider and be aware of the prosumer's role. For this reason, in this case, II.3 works for all demand profiles even without the variable $\beta$. So, for the above reasons, we set $\beta$ equal to 1. The falsified total demand $D_t^{'}$ of all prosumers is given by II.9.

$$D_t^{'} = D_t(1 + (\frac{1}{1 + e^{-D_t}})) \tag{II.9}$$

In this case, when the attacker manipulates the total demand during the game, convergence can be proven by affirming the uniqueness of the internal prices II.5 [JT06]. Let $D_t$=$E_t^d$-$E_t^s$ denotes the net loads of all prosumers. The internal prices in II.5 is changed by replacing the true total demand ($D_t$=$E_t^d$-$E_t^s$) with the falsified demand ($D_t^{'}$). The modified internal prices are as follow,

$$p_t^b = \lambda_t(\frac{D_t^{'}}{\sum_{j\in M}\beta_{j,t}}), p_t^s = \mu_t(\frac{D_t^{'}}{\sum_{j\in M}\beta_{j,t}}) \tag{II.10}$$

The uniqueness of the internal prices and hence the convergence can be proved in the following way.

**Theorem II.3.2.** *The coordinator-side game, that is formulated with II.10, is a one person game, and has a unique pair of internal prices.*

*Proof.* There exists a unique internal prices pair in this game if the following price functions have unique answers at each time.

$$\begin{aligned} p_t^b &= \lambda_t(\frac{D_t(1+(\frac{1}{1+e^{-D_t}}))}{\sum_{j\in M}\beta_{j,t}}), \\ p_t^s &= \mu_t(\frac{D_t(1+(\frac{1}{1+e^{-D_t}}))}{\sum_{j\in M}\beta_{j,t}}) \end{aligned} \tag{II.11}$$

Since the sigmoid function is a monotonically increasing function, here, it has a unique value for a certain amount of total demand. Therefore, considering $D_t$, and one of the pre-set coefficients ($\lambda_t$ or $\mu_t$), a unique pair of internal prices can be easily found. ■

**Attack process:** According to Fig. II.1, the attack (attack 2) takes place at the network level targeting the communication between the coordinator and the suppliers. As seen in Fig. II.3, the attacker alters the total demand calculated by the coordinator, then modifies both external and internal prices based on the new total demand. Those modifications are implemented in all iterations until the game converges.

**Attack effects:** At the end of the game, suppliers will provide more energy than the real demand, resulting in grid imbalance unless the attacker consumes the surplus energy by charging his hidden battery.

### II.3.3 Attack challenges and possible solutions

Generally, getting free energy poses some challenges for the attacker. One challenge concerns the hidden battery capability to consume all the extra supplied energy beyond the true demand, caused by the attack. Typical capacities of batteries that the attacker might use include EV batteries with capacity in the range of 10 kWh to 100 kWh [EV] [Wik], and home Battery Energy Storage

Systems (BESS) with capacity around 2-13.5 kWh [Sol20]. If the attacker wants to ensure that the extra energy does not cause imbalance, the trading game needs to be controlled in such a way that the extra energy does not exceed the battery capacity. One possible solution to this dilemma could be *fake convergence* which means that the attacker modifies the last external price to make it close enough to the previous one. To realize the fake convergence, first, the attacker should listen to the communication link between the suppliers, when they send their bids, and the coordinator all the time during the game. In that way, the attacker is able to be aware of when the surplus supplied energy is getting close to the battery's capacity and terminate the game at the point by modifying the last calculated external price to a value close enough to the previous one. In this case, the grid balance could be retained by controlling the value of surplus energy which is provided by the suppliers through the game. If the extra supplied energy goes beyond the battery's capacity, there will be an imbalance in the network. This may cause a blackout depending on the magnitude of the imbalance and the protection mechanisms in the distribution network.

## II.4 Machine learning model for attack detection

Detecting malicious activities within a P2P energy trading market is challenging due to the various groups of participants. These systems are vulnerable toward different attacks such as unauthorized device (e.g., HEM units, Smart Meters, etc.) access, software vulnerabilities, and malware. These attacks are able to spoof and interfere with transaction messages to falsify data like price, the value of energy buying or selling requests, etc. Several approaches have been suggested for the purpose of detecting attacks in the energy markets. Two main methods are model-based and data-driven detection algorithms. In contrast to the model-based algorithms, data-driven algorithms (e.g., ML algorithms) act independently of the system's parameters and models in the attack detection process, making them more efficient.

Detecting malicious activities can be considered as an ML classification problem where the duty of the ML model is to classify a new activity as either normal or attack. The majority of the state-of-the-art ML algorithms (e.g., deep neural networks and random forests) demonstrated a high accuracy rate while suffering from a non-interpretable, complex decision-making process that makes them appear as black-boxes. Recently, the accuracy and interpretability of ML models are becoming inseparable elements. It is obvious that every machine learning model has pitfalls when it comes to detecting new, unseen instances due to several reasons, for example, inadequate training data, lack of expressiveness of the model, the bias in the data, etc. Imagine a black-box model (say a deep neural network) is used for classifying activities in a P2P energy trading system. In this case, the model can only predict the label of the activity (normal or attack) without providing any explanation about the prediction. Here, we only have one choice which is to trust in the prediction which can be correct or incorrect. In contrast, consider a transparent, interpretable ML model that

outputs explanations along with the prediction of the new instance. In this case, the user can look into the explanations and decide about the correctness of the prediction. As we mentioned earlier, for many reasons, ML models may have bugs in some regions of the decision boundary, which can lead to misprediction. The provided explanations aids the expert on P2P energy trading whether to trust the generated prediction of the model or neglect it. Moreover, an interpretable model is considered as a knowledge extractor which reveals some hidden patterns in the data and enhances the knowledge of the domain expert about the system. Therefore, we are interested in a ML model that provides a high level of prediction accuracy with a transparent decision-making mechanism.

In this section, we propose a highly accurate interpretable machine learning classifier that benefits from a computationally-efficient training phase and straight-forward testing phase. The proposed method consists of three main steps including training phase, testing phase, and attack detection. The training and testing phases are described in Algorithm 1. The created model of our algorithm consists of clusters of ground-truth training data (e.g., Austin, Texas, July 2018 dataset) that act as prototypes for classifying new test data. Both training and testing are reliable and simple procedures with a negligible computational burden. The interpretability is provided in the sense that a single cluster and eventually a single member of the cluster is decisive about the label of a new input. Therefore, by visualizing the cluster that the new input belongs to and comparing the input with the instance of the cluster (decisive instance), the interpretability is provided. The main phases of the proposed algorithm are described below.

### II.4.1 Training phase

The output of this step is a model in the form of data clusters used to determine the label of new inputs in the test phase. The training phase in Algorithm 1 includes five main steps (step 1 to step 5). In this algorithm, the initialization is done as the first step. In step 2, the mutual information (MI) between each sample and all other data points is computed. The incentive of considering MI is its susceptibility to measure dependency between two random variables that lead to a non-negative value and its sensitivity to both linear and non-linear correlations [MDK18]. The mutual information between two discrete data point $d_1$ and $d_2$ can be described in the following way:

$$MI(d_1; d_2) = H(d_1) + H(d_2) - H(d_1; d_2) \tag{II.12}$$

where $H(d_1)$ and $H(d_2)$ are information entropies. Entropy is the degree of the uncertainty between two random variables $d_1$ and $d_2$. $H(d_1; d_2)$ is the joint entropy of $d_1$ and $d_2$. Hence, the entropy and the joint entropy of two variables can be described by the probability and joint probability of them, respectively. $H(d_1)$, $H(d_2)$ and $H(d_1; d_2)$ are defined as specified below:

$$H(d_1) = -p(d_1) \log p(d_1) \tag{II.13}$$

**Algorithm 1** Proposed interpretable ML classifier

*Input* : Training dataset $D = \{d_1, d_2, ..., d_n\}$, Test dataset $T = \{t_1, t_2, \ldots, t_m\}$.
*Output* : A predicted class ($Y$) for a test data $t_i \in T$.
[*Training phase*]
*Step*1. Initialization: Set $G$= number of main groups, $g$= number of subgroups, $Candidates = \varnothing$, and $D_{new} = \varnothing$.
*Step*2. Compute $MI(d_i; d_j)$, $d_i$ and $d_j \in D$, $i = 1, \ldots, n$ ,$j = 1, \ldots, n$. Insert the results in $Matrix_1$.
*Step*3. Create $G$ groups by applying $K$-means clustering on $Matrix_1$.
*Step*4. Do the following steps for each group in G:
    *Step*4.1. Compute $LCC(d_i; d_j)$,
    *Step*4.2. Create $g$ subgroups by applying K-means clustering on $Matrix_2$.
*Step*5. Do the following steps for each subgroup in $g$:
    *Step*5.1. Compute:
    $argmax_{d_i}(MLCC(d_i; d_{-i}))$,
    ($d_{-i}$: all set of data in a subgroup in $g$ except $d_i$.) Then, set:
    $Candidates = Candidates \cup d_i$,
    $D_{new} = Candidates$.
[*Testing phase*]
*Step*1. Compute:
    $argmax_{d_i}(LCC(t_i; d_i))$, $t_i \in T$, $d_i \in D_{new}$
*Step*2. Do the following step for each data $d_j$ in subgroup $g$ that $d_i \in g$ and $D_{new}$:
    *Step*2.1 Compute:
    $argmin_{d_j}(E = LCC(d_i; d_j) - LCC(t_i; d_j))$,
*Step*3. Set:
    $Y$= *class of* $d_j$

$$H(d_2) = -p(d_2) \log p(d_2) \tag{II.14}$$

$$H(d_1, d_2) = -p(d_1, d_2) \log p(d_1, d_2) \tag{II.15}$$

$p(d_1)$ and $p(d_2)$ are probability of $d_1$ and $d_2$, and $p(d_1, d_2)$ is the joint probability of them. The results of computing MI between every data point is collected in a matrix as follows:

$$Matrix_1 = \begin{bmatrix} r_{1,1} & \cdots & r_{1,j} \\ \vdots & \ddots & \vdots \\ r_{i,1} & \cdots & r_{i,j} \end{bmatrix} \tag{II.16}$$
$$r_{i,j} = MI(d_1; d_2), d \in D$$
$$i = 1, 2, ..., n, j = 1, 2, ..., n$$

where $n$ is equal to the number of samples in the dataset $D$.

In the next step, a K-means clustering algorithm is applied to each row of the $Matrix_1$ to generate $G$ groups. Then, steps 2 and 3 are repeated for data in each $G$ group to make $g$ subgroups (step 4). The difference between step 2 and step 4 is in the manner in which the dependency between each data point is determined by the Linear Correlation Coefficient (LCC) measure [Amb+16]. The simplicity and low computational cost of the LCC make it a popular method. The linear correlation coefficient of two variables $d_1$ and $d_2$ can be defined as follow:

$$LCC_{(d_1,d_2)} = \frac{Cov(d_1, d_2)}{\sigma_{d_1}\sigma_{d_2}} \tag{II.17}$$

where $Cov(d_1, d_2)$ is the covariance between $d_1$ and $d_2$; $\sigma_{d_1}$ and $\sigma_{d_2}$ are standard deviations of $d_1$ and $d_2$, respectively.

To discover the relation between more than two variables, all those variables should be considered at once to promote the accuracy. Thus, in such cases, the multivariate linear correlation coefficient (MLCC), which is able to determine the dependency of more than two variables at the same time, has better performance than the LCC [MMG17]. Here, the MLCC between each sample and remaining samples in each subgroup in $g$ is calculated to select a candidate data point that has the maximum MLCC (step 5). After selecting candidate data points, we include them in a new data ($D_{new}$). The selection of such candidate data through data clustering contributes to the interpretability of the testing phase. The square of the MLCC between independent variables $a_n$ and the dependent variable $b$ is obtained by II.18.

$$\begin{aligned} MLCC^2 &= corr^T R_{aa}^{-1} corr, \\ corr &= (r_{a_1,b}, r_{a_2,b}, ..., r_{a_n,b})^T, \\ R_{aa} &= \begin{bmatrix} r_{a_1,a_1} & \cdots & r_{a_1,a_n} \\ \vdots & \ddots & \vdots \\ r_{a_n,a_1} & \cdots & r_{a_n,a_n} \end{bmatrix} \end{aligned} \tag{II.18}$$

where $corr$ is the vector of correlations $r_{a_n,b}$ between the independent variables $a_n$ and the dependent variable $b$, and $corr^T$ is the transpose of $corr$. Matrix $R_{aa}$ shows the correlation between independent variables, and $R_{aa}^{-1}$ is the inverse of matrix $R_{aa}$.

### II.4.2 Testing phase

We determine the label of a new data point by measuring its similarity with the created clusters in the training phase through this step. Since the dimensions of the dataset are reduced by selecting some candidate data in the training phase, the testing phase's process speeds up. The testing phase has three main steps (step 1 to step 3). First, the LCC between the test data ($t_i$) and each candidate data ($d_i$) from $D_{new}$ is calculated. Then, the candidate data, which has the maximum dependency with the test data, is selected. Afterward, the evaluation

function $E$ for all members of subgroup g, where the selected candidate $d_i$ (in step 1 (test phase)) belongs, and the test data is computed (step 2). In other words, the data which has a maximum correlation with the test data $t_i$ and the candidate data $d_i$ is selected, and its class is considered as the class of the test data $t_i$ (step 3). The evaluation function $E$ increases the labeling accuracy by considering the relations of each selected subgroup's member with both test data and the subgroup's candidate rather than comparing the test data with only the chosen candidate data or the selected subgroup's members. The process of labeling explicitly states the reason for selecting the label, and it is easy to track which label belongs to which data in which subgroup; this makes the testing phase highly interpretable.

### II.4.3 Attack detection

In this work, we have two classes of events, namely attack (FDI) event and normal event, for decision making. After data pre-processing and applying FDI attack, the proposed classifier will be trained to differentiate attack events from normal ones. Specifically, it predicts the status of a new input (whether attack or normal event) in the testing phase by measuring the similarity between the input and a set of candidate data that is determined in the training phase of the model. Since the label of a new input is selected according to the label of some candidate ground-truth data, our attack detection model can be classified as a prototype-based interpretable model. Therefore, the behavior of the model is transparent as its decisions are made according to the similarity of the test data to some representative ground-truth data (determined in the training phase).

The proposed ML classifier for detecting false data injection attacks in the P2P energy trading system is described as follows. The first step is data pre-processing, in which the relevant features are selected and/or generated. In this work, we need six main features for each household, including the household's identification number (user ID), energy generation (KWh), shiftable loads, base loads, energy consumption (shiftable loads+base loads), and household's energy buying or selling request. After applying the FDIAs on the dataset and before feeding the data to the classifier, it is important to label the data. The original dataset has one class corresponding to the normal demands and consumptions (Normal event).

After applying FDIAs, the dataset will include an additional class corresponding to the falsified data (FDI event). Now, the data is ready for the next step, i.e., training the classifier. After the training phase, the test data is given to the classifier for making a decision. When the prediction is an FDI event, it means that the victim prosumer is detected. The classifier model is executed in the first round of the game before the attack takes place in threat scenario 1 (Fig. II.2), and during the game in threat scenario 2 (Fig. II.3).

Table II.1: Average utilities of the prosumers, consumers, and suppliers, and the supply and the true demands amounts under FDIAs at the threat scenario 1, and the economic benefits for the attacker by adjusting $\beta$ and $c$ at time slot 11.

| | **Increasing demands ($+\beta$ for buyers) Increasing demands ($+\beta$ for sellers)** $\beta_b$**= consumption / (c=average of the consumptions) (In the first round of the game)** $\beta_b$ **= demand / (c=average of the demands) (During the game)** | | | **Increasing demands ($+\beta$ for buyers) Decreasing demands ($-\beta$ for sellers)** $\beta_b$ **= consumption / (c=average of the consumptions) (In the first round of the game)** $\beta_b$ **= demand / (c=average of the demands) (During the game)** | | |
|---|---|---|---|---|---|---|
| | $\beta_s$ **= d/(c=0.5d)** | $\beta_s$ **= d/(c=d)** | $\beta_s$ **= d/(c=1.5d)** | $\beta_s$ **= -d/(c=d)** | $\beta_s$ **= -d/(c=1.5d)** | $\beta_s$ **= -d/(c=2d)** |
| Num. of attacked prosumers | 12 | 11 | 13 | 11 | 11 | 11 |
| Average utility of prosumers | -0.15 | -0.12 | -0.19 | -0.36 | -0.46 | -0.27 |
| Average utility of consumers | -0.09 | -0.10 | -0.09 | -0.22 | -0.40 | -0.13 |
| Average utility of suppliers | 16.41 | 16.49 | 16.64 | 22.26 | 20.92 | 16.77 |
| Internal buying price ($) | 0.72 | 0.65 | 0.65 | 0.70 | 0.64 | 0.64 |
| Internal selling price ($) | 0.41 | 0.37 | 0.37 | 0.40 | 0.36 | 0.36 |
| External buying price ($) | 0.74 | 0.67 | 0.67 | 0.72 | 0.66 | 0.66 |
| Final supply(kw) | 130.15 | 136.50 | 135.34 | 150.32 | 144.15 | 142.69 |
| True demands (kw) | 80.06 | 64.44 | 54.44 | 56.07 | 54.44 | 54.44 |
| Economic benefits ($) | 36.06 | 46.84 | 52.59 | 65.97 | 57.41 | 56.48 |

Table II.2: Average utilities of the prosumers, consumers, and suppliers, and the supply and the true demands amounts under normal situation and FDIAs at the threat scenario 2, and the economic benefits for the attacker at time slot 11.

| | **Threat scenario 2** | **Normal situation** |
|---|---|---|
| **Average utility of prosumers** | 0.33 | 0.82 |
| **Average utility of consumers** | 0.49 | -0.50 |
| **Average utility of suppliers** | 5.01 | 4.67 |
| **Internal buying price** | 0.38 | 0.35 |
| **Internal selling price** | 0.23 | 0.20 |
| **External price** | 0.40 | 0.36 |
| **Supply** | 170.94 | 160.47 |
| **True total demand** | 85.47 | - |
| **Economic benefit ($)** | 32.48 | - |

## II.5 Experimental Results

### II.5.1 Description of the dataset

We generated attack datasets [Moh+21]

[1] based on real data from Austin, Texas [Tus+19]. The use case focuses on the 1st day of August 2018, with efficient solar generation. A day is divided into T time slots, and the length of a time slot equals one hour. The evaluation of the model's performance is done from 7 to 19 because there is no solar generation during the evening. The dataset has six main features; user (prosumer/consumer) ID, energy generation, shiftable loads, base loads, energy consumption (shiftable loads+base loads), and household's demand (it is equal to the difference between the generation and the consumption). Attack data in the threat scenario 1 is generated by modifying at least once (e.g., in the first round of the game) the shiftable load and/or the base load of prosumers (who act as buyers), and by updating the sum of the consumptions based on the modified shiftable/base loads. The first day of August 2018 dataset is used for training our machine

[1] The attack datasets are available online at AttackDatasets-Austin-Texas-2018.

learning classifier, and the data from the month prior (the first day of July 2018) is chosen as testing data. Moreover, we assume that the attacker has an EV including a battery, which is used as the hidden battery, with 100 kWh capacity.

The P2P system model contains two groups of households; group 1 contains 50 households where 20 of them are prosumers who are equipped with rooftop PV panels that one of them is the attacker, while the remaining 30 are consumers with zero energy generation. Group 2 includes 23 households (13 prosumers and 10 consumers) and one attacker that intercepts prosumer/coordinator communication at the network level. Three companies act as suppliers in this P2P market. First, we perform the simulations at a specific time slot for the households in group 1 with different attack configurations to learn about the effects on energy trading with our threat scenario. Then, we apply the other group to see the validity of the final selected attack configurations on group 1.

We vary the attack configuration by adjusting the variable $c$ (in II.3) to different values and by setting the parameter $\beta$ (in II.3) to positive and negative to increase and decrease the demand of prosumers, respectively. Furthermore, we assume the demand should not be modified in a way that causes the role of a prosumer towards the coordinator to be changed from seller to buyer or vice versa; this would make the attack easier to detect. We apply II.3 on a number of prosumers' energy buying or selling requests (demands), which are calculated by subtracting a prosumer's generation from its consumptions (shiftable load+base load), at a specific time slot (11:00 A.M). We first do some initial experiments to learn how much an attacker has to change the demand of prosumers to have a significant effect on the trading result in terms of prices and external supply, by determining corresponding values for $c$ in the definition of $\beta$ (II.3). Due to the fact that the magnitude of the prosumers' demands is different at each time slot of the day, the number of prosumers that is attacked is different at each time. Therefore, the minimum number of prosumers that the attacker needs to attack to gain economic benefits will be determined after some initial experiments.

## II.5.2 Performance evaluation

### II.5.2.1 Attack analyses

Table II.1 and Table II.2 summarize the effects of the threat scenarios 1 and 2 respectively on group 1 households with different configurations of parameter $\beta$ (in threat scenario 1) at time slot 11, and the result of the experiments in the normal situation (without attacks) at the same time slot is presented in the Table II.2. As it can be seen from Table II.1, the parameter $\beta$ is different for sellers ($\beta_s$) and buyers ($\beta_b$). When $\beta$ in II.3 is positive, it means that the prosumer's demand/consumption increases, while the opposite happens when it is negative. When the attacker changes the demand during the game (Fig 2, step 3.1), it just affects the prices in II.5, and the victim prosumer is not aware of the modified demand and updates its demand based on its previous unchanged selling or buying request. For this reason, it is necessary to alter the target prosumer's consumption at least once in the first round of the game (Fig.

Table II.3: Number of attacked prosumers and economic benefits of the attacker for group 1 and group 2 households after applying threat scenarios 1 and 2 at different time slots.

| | **Threat scenario 1** | | | | **Threat scenario 2** | |
|---|---|---|---|---|---|---|
| **Time slots** | ***Num. of attacked prosumers (group 1)*** | ***Num. of attacked prosumers (group 2)*** | ***Economic benefits ($) (group1)*** | ***Economic benefits ($) (group 2)*** | ***Economic benefits ($) (group1)*** | ***Economic benefits ($) (group 2)*** |
| 7:00 | 5 | 7 | 27.16 | 11.33 | 16.15 | 8.12 |
| 8:00 | 5 | 4 | 18.05 | 10.78 | 13.30 | 7.57 |
| 9:00 | 14 | 5 | 45.30 | 17.39 | 19.46 | 30.56 |
| 10:00 | 13 | 8 | 54.48 | 21.86 | 12.37 | 9.62 |
| 11:00 | 11 | 10 | 65.97 | 55.15 | 28.29 | 24.34 |
| 12:00 | 9 | 7 | 51.78 | 46.03 | 15.91 | 13.54 |
| 13:00 | 14 | 5 | 46.76 | 33.99 | 16.58 | 18.65 |
| 14:00 | 13 | 6 | 45.02 | 43.39 | 31.05 | 13.35 |
| 15:00 | 14 | 7 | 37.50 | 40.47 | 17.52 | 14.44 |
| 16:00 | 12 | 8 | 33.95 | 35.16 | 16.89 | 12.68 |
| 17:00 | 12 | 9 | 48.77 | 24.10 | 9.01 | 6.44 |
| 18:00 | 10 | 4 | 52.92 | 15.34 | 15.65 | 10.93 |
| 19:00 | 8 | 5 | 58.42 | 23.03 | 28.60 | 11.89 |

II.3, step 1). Following that, $\beta_b$ depends on both consumptions and demands in the beginning and during the game, respectively. The constant $c$ in $\beta_b$ and $\beta_s$ should not be independent of the consumption or the demand values. After performing some initial experiments, we find that a suitable value for $c$ in the parameter $\beta_b$ can be the average of the attacked prosumers' consumptions and demands.

As can be seen from Table II.1, there are two main columns where the attacker increases the demands of both sellers and buyers (left side) and increases and decreases the demands of buyers and sellers respectively (right side). In the left side of the table, the positive signs for $\beta_b$ and $\beta_s$ display an increase in demands or consumptions (by considering $+\beta_b$ or $+\beta_s$ as $\beta$ in II.3. Three value ranges for the constant $c$ ($c > demand$, $c = demand$, and $c < demand$) are tested when both selling and buying requests are increased by the attacker. On the right side of the table, the positive sign for $\beta_b$ and negative sign for $\beta_s$ depict an increase in buyers' demands/consumptions and a decrease in sellers' demands. In this case, the attacker should consider positive values ($c \geq demand$) in $\beta_s$ when decreasing the selling requests to handle the challenge of keeping the role of the sellers, otherwise (if $c < demand$) the role of the seller will be changed to the buyer. In this table, some important factors affected by the attack (including the number of attacked prosumers, average utilities of the participants, internal and external prices, the final supply amount, true demand, and the economic benefits for the attacker) are investigated. Here, the number of attacked prosumers includes the minimum numbers that lead to the lower average utility of prosumers than consumers. The true demand in the table is the last adjusted true demand that the prosumers (coordinator) submit(s) in the last iteration of the game

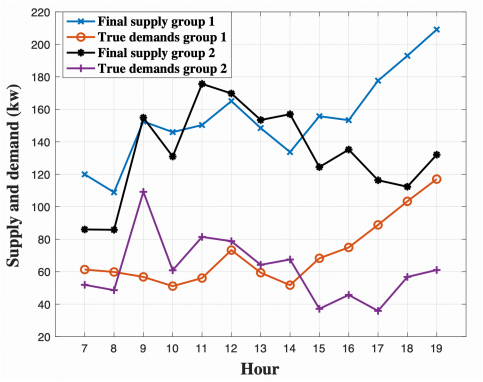



Figure II.4: Final supply amount and the true demand after applying the threat scenario 1 at the last iteration of the game at different time slots for groups 1 and 2 households.

before being changed by the attacker. The difference between the final amount of energy supply and the true demand corresponds to the amount of free energy that the attacker can acquire. The attacker's economic benefits are obtained by multiplying the internal buying price (at time slot 11) by the difference between the final total energy supply and the total true demand.

By comparing Table II.1 with the normal situation, the utility of the suppliers is increased, and the attacker gains economic benefits when increasing the demands (both selling and buying requests) or increasing and decreasing the buying and selling requests, respectively. Hence, the suppliers have to supply more energy corresponding to the falsified demands, which results in higher utility for the suppliers. According to Table II.1, the attacker gains more economic benefits when decreasing the selling request into the possible lowest amount (without changing the role) by adjusting the constant $c$ in II.3 for parameter $\beta_s$ to a value equal to the demand. As a result, selling less and buying more leads to more energy being supplied by the suppliers, which causes greater utility loss for the prosumers than the consumers (according to II.4). This situation may discourage consumers to become prosumers. This will be economically beneficial for the suppliers. Regarding to the Table II.2, the similar factors from the Table II.1 except the number of attacked prosumers are considered. This is because the attacker only attacks the total demand (Fig 3, step 5) in the threat scenario 2. By comparing the results under FDIAs with the normal situation in Table II.2, suppliers supply more energy, resulting in more utility for the suppliers and economic profits for the attacker.

We apply the FDIA to the prosumers at all time slots of the day for both group 1 and group 2 households to see the effects on all prices, economic benefits, demands, and supplies. The battery can not be used at all time slots, since it needs to be discharged or consumed to be able to be charged again in later time slots. Hence, the attacker can only attack at certain times of the day. Fig. II.4

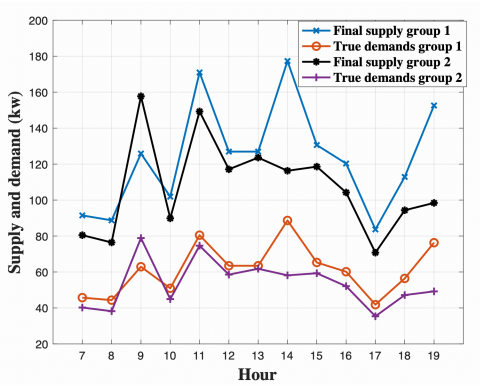



Figure II.5: Final supply amount and the true demand after applying the threat scenario 2 at the last iteration of the game at different time slots for groups 1 and 2 households.

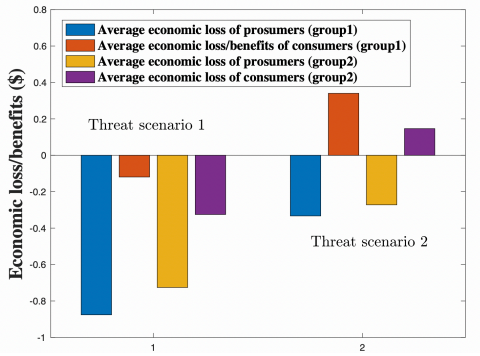



Figure II.6: average economic loss/ benefits of prosumers and consumers after applying threat scenarios 1 and 2, for both Group 1 and Group 2 households.

and Fig. II.5 illustrate the effects of the attack, including final supply amount and the true demand after applying threat scenarios 1 and 2 at all time slots of the day. In some cases, the attacker has to cause a fake convergence before the supply value rising higher than the battery capacity. Given this, the fake convergence happens at several hours of the day (9 to 19 and 11 to 16 for group 1 and group 2, respectively) in threat scenario 1 where the difference between the true demand and the final supply value is more than the battery capacity (100 KWh). The convergence always happens before the supplied energy gets higher than the battery capacity during the threat scenario 2.

The number of attacked prosumers and the economic benefits that the attacker gains through both threat scenarios at each time slot are listed in Table II.3. In this table, the economic benefits column shows the profits that the attacker can gain by attacking the minimum number of prosumers and the coordinator over

Table II.4: Optimal values of hyper-parameters for baseline ML models

| | Threat scenario 1 | | Threat scenario 2 | |
|---|---|---|---|---|
| **Methods** | **Dataset 1 (group 1)** | **Dataset 2 (group 2)** | **Dataset 1 (group 1)** | **Dataset 2 (group 2)** |
| **MLPNN** | hidden layer size:10<br>Neuron numbers:20 | hidden layer size:10<br>Neuron numbers:10 | hidden layer size:15<br>Neuron numbers:20 | hidden layer size:20<br>Neuron numbers:25 |
| **Ensemble** | Method: AdaBoostM1<br>Number of learning cycles: 300<br>Learners: tree | Method: AdaBoostM1<br>Number of learning cycles: 200<br>Learners: tree | Method: AdaBoostM1<br>Number of learning cycles: 200<br>Learners: tree | Method: AdaBoostM1<br>Number of learning cycles: 250<br>Learners: tree |
| **DT** | Maximum number of splits: 8<br>Minimum leaf size: 8<br>Minimum parent size: 10 | Maximum number of splits: 10<br>Minimum leaf size: 8<br>Minimum parent size: 15 | Maximum number of splits: 10<br>Minimum leaf size: 8<br>Minimum parent size: 12 | Maximum number of splits: 20<br>Minimum leaf size: 10<br>Minimum parent size: 25 |
| **KNN** | Distance metric: Euclidean<br>Number of neighbours: 3 | Distance metric: Correlation<br>Number of neighbours: 5 | Distance metric: Euclidean<br>Number of neighbours: 5 | Distance metric: Correlation<br>Number of neighbours: 4 |
| **NB** | Distribution names: Kernel<br>Kernel type: Gaussian | Distribution names: Kernel<br>Kernel type: Gaussian | Distribution names: Kernel<br>Kernel type: Gaussian | Distribution names: Kernel<br>Kernel type: Gaussian |
| **SVM** | Kernel function: Linear<br>Box constraint level: 200<br>Kernel scale: 20 | Kernel function: Linear<br>Box constraint level: 200<br>Kernel scale: 10 | Kernel function: Linear<br>Box constraint level: 100<br>Kernel scale: 10 | Kernel function: Linear<br>Box constraint level: 300<br>Kernel scale: 10 |

the threat scenarios 1 and 2, respectively, at each time slot of the day.

Fig. II.6 demonstrates the average economic loss (negative values) or economic benefits (positive values) of both prosumers and consumers generated after the FDIAs throughout the day. The figure shows that all of the prosumers make financial losses, while some of the consumers gain economic profits after the attack. We can see that prosumers with solar generation obtain much more economic benefits than consumers when there is no FDIAs (normal situation). This may motivate consumers to become prosumers, while this incentive could be lost by decreasing the financial benefits of prosumers after the FDIAs that cause a greater economic loss for prosumers relative to consumers.

### II.5.2.2 Classifier system evaluation

To evaluate the performance of our proposed classifier system, four performance metrics are applied. These metrics are defined as follows:

$$Detection\ rate\ (DR) = \frac{TP}{TP + FN} \tag{II.19}$$

$$Accuracy\ rate\ (AR) = \frac{TP + TN}{TP + TN + FN + FP} \tag{II.20}$$

$$Precision\ rate\ (PR) = \frac{TP}{TP + FP} \tag{II.21}$$

$$False\ negative\ rate\ (FNR) = \frac{FN}{FN + TP} \tag{II.22}$$

where true positive ($TP$) and true negative ($TN$) show the number of attack data and the number of normal data which are classified correctly, respectively. False positive ($FP$) and false negative ($FN$) show the number of normal data

and attack data, which are classified as attack and normal data, respectively. As a mitigation solution, we apply the machine learning detection model in the first round of the game to prevent entering the FDIAs in the game. To evaluate the efficiency of the proposed algorithm, we conduct a comparison between some popular interpretable machine learning algorithms (such as Naïve Bayes (NB), K-Nearest Neighbours (KNN), and decision tree (DT)), a semi-interpretable model (support vector machine (SVM)), and also robust none-interpretable classifiers (ensemble and multi-layer perceptron neural network (MLPNN) methods). The proposed model has been developed in MATLAB programming language. We used the Statistics and Machine learning Toolbox [Mat] for implementing the ML models with tuned hyper-parameters. We performed a random search method to find optimal values of hyper-parameters for each ML model. Table II.4 describes the optimal values of hyper-parameters on both datasets under threat scenarios 1 and 2. The average results of $DR$, $AR$, and $FNR$ of our method and the baseline algorithms on both household groups are summarized in Table II.5. The results indicate a better performance of our proposed algorithm. Overall, the introduced method has a remarkable increase in $DR$ and $AR$, and a decrease in $FNR$ in comparison with the baseline methods. Moreover, our model's processing time is compared with the ML models. The training and testing time on dataset 1 including threat scenario 1's attacks, that has more data than other attack datasets, are available in Table II.6. It can be observed that our model's testing time is lower than other baseline methods. The reason is new data should be tested with only one cluster of data selected in the training phase of our model that accelerates the process. Our model's training time is slightly slower than other ML models which is negligible considering our model's transparency and the improved performance. Here the purpose is to compromise between transparency, speed-up, and accuracy to get the best possible result.

#### II.5.2.3 Interpretability of the proposed classifier

Our proposed ML algorithm follows a transparent mechanism for making predictions. This allows us to understand the rationale behind its decision through various techniques, for example, visualizing the distribution of a cluster that a test sample is allocated to and extracting importance of features in each prediction. Since our model makes decisions based on clusters of ground-truth data, constructing a linear regression model on a cluster provides reliable and faithful explanations concerning the cluster and the test sample. Here, we demonstrate an example of the utility of such a model in increasing the understandability of the prediction which consequently enhances the expert's trust into the model. We have selected a normal and an attack instance from the threat scenario 1 (presented in Table II.7) that are correctly classified via our proposed detection model. For each sample, we retrieved the cluster that the sample was assigned to and created linear regression model using the cluster data and its ground-truth labels. Later, we extract the coefficient of each feature from the linear model. The intuition for applying this approach is explaining local neighborhoods of the dataset (created clusters in the training phase) for

Table II.5: Summary of classification performance comparison on two datasets

| | Threat scenario 1 | | | | | | | | Threat scenario 2 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Dataset 1 (group 1) | | | | Dataset 2 (group 2) | | | | Dataset 1 (group 1) | | | | Dataset 2 (group 2) | | | |
| **Methods** | ***DR%*** | ***AR%*** | ***PR%*** | ***FNR%*** | ***DR%*** | ***AR%*** | ***PR%*** | ***FNR%*** | ***DR%*** | ***AR%*** | ***PR%*** | ***FNR%*** | ***DR%*** | ***AR%*** | ***PR%*** | ***FNR%*** |
| **Our Method** | **96.41** | **91.22** | **93.36** | **2.01** | **98.12** | **90.97** | **94.63** | **1.88** | **94.02** | **93.92** | **93.91** | **2.13** | **98.18** | **98.43** | **96.15** | **1.81** |
| **MLPNN** | 92.19 | 90.34 | 88.12 | 7.06 | 93.14 | 88.79 | 92.36 | 7.85 | 90.19 | 93.57 | 91.87 | 9.02 | 95.42 | 96.28 | 95.91 | 4.64 |
| **Ensemble** | 91.06 | 90.43 | 85.18 | 10.93 | 78.13 | 83.39 | 71.90 | 21.86 | 88.91 | 84.42 | 83.23 | 16.43 | 93.21 | 91.45 | 94.30 | 6.83 |
| **DT** | 83.35 | 91.45 | 89.96 | 16.64 | 80.59 | 85.22 | 81.73 | 18.40 | 85.32 | 81.43 | 83.16 | 16.64 | 90.25 | 91.12 | 89.37 | 9.21 |
| **KNN** | 79.78 | 90.72 | 84.33 | 20.21 | 76.36 | 86.56 | 82.42 | 23.63 | 90.32 | 89.65 | 88.43 | 9.65 | 94.82 | 90.32 | 95.02 | 6.24 |
| **NB** | 54.30 | 85.84 | 79.14 | 45.61 | 19.52 | 71.56 | 59.70 | 80.47 | 36.71 | 69.30 | 61.33 | 63.28 | 75.28 | 80.95 | 73.77 | 24.71 |
| **SVM** | 57.52 | 88.00 | 87.99 | 42.47 | 77.03 | 87.09 | 81.76 | 24.96 | 83.24 | 90.23 | 90.45 | 16.85 | 79.20 | 81.62 | 78.71 | 18.40 |

Table II.6: Summary of processing time comparison on dataset 1

| Methods | Training time (s) | Test time (s) |
|---|---|---|
| **Our Method** | 3.465 | 0.043 |
| **MLPNN** | 2.783 | 1.642 |
| **Ensemble** | 2.267 | 1.231 |
| **DT** | 1.783 | 0.875 |
| **KNN** | 1.954 | 0.965 |
| **NB** | 1.451 | 0.721 |
| **SVM** | 1.398 | 0.652 |

Table II.7: Feature values of selected instances for explanation.

| | Values | |
|---|---|---|
| **Features** | **Normal sample** | **Attack sample** |
| **Generation** | 0.315 | 0.2274 |
| **Demand** | -0.1292 | -1.9802 |
| **Shiftable load** | 0.1225 | 0.7023 |
| **Base load** | 0.3218 | 09891 |
| **Consumption** | 04443 | 1.6915 |

understanding the local behavior of the original model. The extracted coefficients for features are listed in Table II.8. For each normal and attack sample, important features are sorted in a descending order. By observing the achieved results it can be clearly seen that two features "Consumption" and "Demand" in the attack instance have had the most influence in the prediction (1.744 and 1.550, respectively) which is the result of the attack strategy that specifically targets these two features. While for the normal sample, the top two important features are "Demand" and "Generation".

## II.6 Conclusion

In this paper, two attack scenarios are studied to model the false data injection attack using the sigmoid function in local P2P energy trading. We considered a game-theoretic approach to evaluate our attack scenario. In the first threat scenario, the attacker attempts to gain economic benefits through achieving free energy by increasing both prosumers' consumptions (in the first round of the game by attacking their HEM systems) and demands (during the game by attacking the network communication between the HEM system and the

Table II.8: Features importance in the prediction of the selected instances.

| **Features importance** | |
|---|---|
| **Attack sample** | **Normal sample** |
| Actual Label: 2 | Actual Label: 1 |
| Predicted Label: 2 | Predicted Label: 1 |
| **High importance** | |
| Consumption = 1.774 | Demand = 1.554 |
| Demand = 1.550 | Generation = 1.455 |
| Generation = 1.408 | Consumption = 1.273 |
| Shiftable load = 0.351 | Base load = 0.604 |
| Base load = 0 | Shiftable load = 0 |
| **Low importance** | |

coordinator) by intruding into the game. We proposed the second threat scenario that settled the challenge of attacking a number of prosumers' HEM systems by modifying the total demand, which is computed by the coordinator, before sending it to the suppliers. The attacker uses a hidden battery to save the surplus supplied energy, while the battery itself has some challenges like its capacity. Due to the battery challenge, we presented how the attacker could control the game not to cause more energy than the battery capacity. As a result of the proposed FDIAs scenarios, all prosumers experienced a remarkable economic loss compared with consumers, which led to a loss of incentive for participants to remain or become an energy selling prosumer. This has a high benefit for suppliers.

In view of the fact that stealing energy may happen in a P2P energy trading market, an early and accurate detection of such attacks is necessary. Hence, a reliable and interpretable classifier is proposed to increase detection and accuracy rates while decreasing the false negative rate. The efficiency of the proposed approach is verified in comparison to the three popular interpretable ML methods, such as decision tree, KNN, naive Bayes, a semi-interpretable like SVM, and two robust non-interpretable ML classifiers, such as ensemble and multi-layer perceptron neural network, on two different groups of households from Austin, Texas. The results illustrate higher detection rate (DR) and accuracy rate (AR) and lower false negative rate (FNR), and fast testing time compared to the other methods on both groups of households.

**Acknowledgements.** This work is supported by the Norwegian Research Council under the SmartNEM project (project number: 267967).

## References

[Ahm+19] Ahmed, A. et al. "Cyber physical security analytics for anomalies in transmission protection systems". In: *IEEE Transactions on Industry Applications* vol. 55, no. 6 (2019), pp. 6313–6323.

[Amb+16] Ambusaidi, M. A. et al. “Building an intrusion detection system using a filter-based feature selection algorithm”. In: *IEEE transactions on computers* vol. 65, no. 10 (2016), pp. 2986–2998.

[AMT15] Anwar, A., Mahmood, A. N., and Tari, Z. “Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid”. In: *Information Systems* vol. 53 (2015), pp. 201–212.

[Anu+18] Anuebunwa, U. R. et al. “Investigating the impacts of cyber-attacks on pricing data of home energy management systems in demand response programs”. In: *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE. 2018, pp. 1–5.

[BNK20] Barreto, C., Neema, H., and Koutsoukos, X. “Attacking electricity markets through iot devices”. In: *Computer* vol. 53, no. 5 (2020), pp. 55–62.

[BZ14] Bi, S. and Zhang, Y. J. “Graphical methods for defense against false-data injection attacks on power system state estimation”. In: *IEEE Transactions on Smart Grid* vol. 5, no. 3 (2014), pp. 1216–1227.

[Che+16] Chen, J. et al. “Impact analysis of false data injection attacks on power system static security assessment”. In: *Journal of Modern Power Systems and Clean Energy* vol. 4, no. 3 (2016), pp. 496–505.

[DSR21] Dasgupta, R., Sakzad, A., and Rudolph, C. “Cyber attacks in transactive energy market-based microgrid systems”. In: *Energies* vol. 14, no. 4 (2021), p. 1137.

[El +17] El Hariri, M. et al. “Online false data detection and lost packet forecasting system using time series neural networks for IEC 61850 sampled measured values”. In: *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE. 2017, pp. 1–5.

[El +19] El Mrabet, Z. et al. “Detection of the false data injection attack in home area networks using ANN”. In: *2019 IEEE International Conference on Electro Information Technology (EIT)*. IEEE. 2019, pp. 176–181.

[Esm+14] Esmalifalak, M. et al. “Detecting stealthy false data injection using machine learning in smart grid”. In: *IEEE Systems Journal* vol. 11, no. 3 (2014), pp. 1644–1652.

[EV] EV. *Electric vehicle (EV)*. URL: https://batteryuniversity.com/learn/article/electric_vehicle_ev (visited on 07/21/2020).

[FGL19] Fenza, G., Gallo, M., and Loia, V. “Drift-aware methodology for anomaly detection in smart grid”. In: *IEEE Access* vol. 7 (2019), pp. 9645–9657.

[FS17] Foroutan, S. A. and Salmasi, F. R. “Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method”. In: *IET Cyber-Physical Systems: Theory & Applications* vol. 2, no. 4 (2017), pp. 161–171.

[Hin+14a] Hink, R. C. B. et al. “Machine learning for power system disturbance and cyber-attack discrimination”. In: *2014 7th International symposium on resilient control systems (ISRCS)*. IEEE. 2014, pp. 1–8.

[Hin+14b] Hink, R. C. B. et al. “Machine learning for power system disturbance and cyber-attack discrimination”. In: *2014 7th International symposium on resilient control systems (ISRCS)*. IEEE. 2014, pp. 1–8.

[IBM] IBM. *What is supervised learning?* URL: https://www.ibm.com/topics/supervised-learning (visited on 05/29/2023).

[JT06] Johari, R. and Tsitsiklis, J. N. “Parameterized supply function bidding: equilibrium and welfare”. In: *Mathematics of Operations Research* (2006).

[LH15] Liu, Y. and Hu, S. “Cyberthreat analysis and detection for energy theft in social networking of smart homes”. In: *IEEE Transactions on Computational Social Systems* vol. 2, no. 4 (2015), pp. 148–158.

[Mat] Mathworks. *Statistics and Machine Learning Toolbox*.

[MDK18] Mohammadi, S., Desai, V., and Karimipour, H. “Multivariate mutual information-based feature selection for cyber intrusion detection”. In: *2018 IEEE electrical power and energy Conference (EPEC)*. IEEE. 2018, pp. 1–6.

[MEZ20] Mohammadi, S., Eliassen, F., and Zhang, Y. “Effects of false data injection attacks on a local P2P energy trading market with prosumers”. In: *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. IEEE. 2020, pp. 31–35.

[MMG17] Mohammadi, S., Mirvaziri, H., and Ghazizadeh-Ahsaee, M. “Multivariate correlation coefficient and mutual information-based feature selection in intrusion detection”. In: *Information Security Journal: A Global Perspective* vol. 26, no. 5 (2017), pp. 229–239.

[Moh+21] Mohammadi, S. et al. $AttackDataset_Austin_Texas2018$. 2021.

[Pil+20] Pilz, M. et al. “Security attacks on smart grid scheduling and their defences: a game-theoretic approach”. In: *International Journal of Information Security* vol. 19 (2020), pp. 427–443.

[PMA15] Pan, S., Morris, T. H., and Adhikari, U. “A Specification-based Intrusion Detection Framework for Cyber-physical Environment in Electric Power System.” In: *Int. J. Netw. Secur.* vol. 17, no. 2 (2015), pp. 174–188.

[Ros65] Rosen, J. B. "Existence and uniqueness of equilibrium points for concave n-person games". In: *Econometrica: Journal of the Econometric Society* (1965), pp. 520–534.

[Sah+14] Saha, A. et al. "On security of a home energy management system". In: *IEEE PES Innovative Smart Grid Technologies, Europe*. IEEE. 2014, pp. 1–5.

[Sol20] Solarguide. *Solar Battery Storage: The Best Solar Batteries*. 2020. URL: https://www.solarguide.co.uk/solar-batteries (visited on 06/15/2020).

[Taj17] Tajer, A. "False data injection attacks in electricity markets by limited adversaries: Stochastic robustness". In: *IEEE Transactions on Smart Grid* vol. 10, no. 1 (2017), pp. 128–138.

[Tus+19] Tushar, W. et al. "A motivational game-theoretic approach for peer-to-peer energy trading in the smart grid". In: *Applied energy* vol. 243 (2019), pp. 10–20.

[Wik] Wikipedia. *Electric vehicle battery*. URL: https://en.wikipedia.org/wiki/Electric_vehicle_battery (visited on 11/21/2020).

[WL13] Wang, W. and Lu, Z. "Cyber security in the smart grid: Survey and challenges". In: *Computer networks* vol. 57, no. 5 (2013), pp. 1344–1371.

[Wu+17] Wu, Y. et al. "Resonance attacks on load frequency control of smart grids". In: *IEEE Transactions on Smart Grid* vol. 9, no. 5 (2017), pp. 4490–4502.

[XMS10] Xie, L., Mo, Y., and Sinopoli, B. "False data injection attacks in electricity markets". In: *2010 First IEEE International Conference on Smart Grid Communications*. IEEE. 2010, pp. 226–231.

[Zha+18] Zhang, C. et al. "Peer-to-Peer energy trading in a Microgrid". In: *Applied Energy* vol. 220 (2018), pp. 1–12.

Paper III

# Applying Energy Justice Principles to Renewable Energy Trading and Allocation in Multi-Unit Buildings

**Sara Mohammadi, Frank Eliassen, and Hans-Arno Jacobsen**

Published in *Energies*, vol. 16, no. 3, pp. 1150, 2023, doi: https://doi.org/10.3390/en16031150.

**Abstract**

Although rooftop PV panels and battery energy storage systems have been well established for detached residential buildings, there is still a lack of access to the advantages of onsite renewable energy generation and consumption for residents of multi-unit buildings. To understand the effects of developing distributed renewable energy sources for multi-unit buildings, a new fair energy-sharing model in which different groups of residents can gain benefit from the shared energy systems is proposed. Despite the potential benefits of developing renewable technologies in multi-unit buildings, the energy trading and allocation processes in the buildings can be unfair for some groups of residents. Accordingly, this work studies the main principles of energy justice and analyses how these principles can be applied in the energy trading and allocation processes to achieve fair energy sharing. In addition to fairness and justice, the experimental results show that our method increases the sellers' profit by 59.7%–127% and decreases the buyers' cost by 8%–21%, compared to the baseline methods. Moreover, applying the energy justice principles in the proposed sharing models acts as an efficient incentive for the residents of the multi-unit buildings to invest in the shared distributed renewable energy sources.

## Contents

## III.1 Introduction

Solar photovoltaic (PV) generation is one of the main technologies for decentralizing and decarbonizing energy systems. To date, PV panels are a settled and approved solution for detached houses, while PV solutions for multi-unit buildings have been relatively limited. Recent studies focus mainly on PV usage in single residential buildings [Com+15] as well as commercial buildings [Liu+14], [Liu+17]. Although distributed renewable energy sources (DRESs) have been widely approved at the residential scale, especially in detached houses, the lack of a legal framework prevents the installation of PV panels and battery energy storage systems (BESSs) in buildings that are composed of several apartment units. The primary reason for the low uptake of sharing DRESs in multi-unit buildings is the lack of regulations to ensure that electricity tax, grid rent, and settlements are in line [CBE17]. Recent studies related to PV panel allocation in multi-unit buildings have focused more on evaluating the technical performance [GCG21] and analyzing the economic and technical feasibility of PV panels in microgrids [Qad22], [WMC22]. However, shared DRESs, including PV panels and BESSs, in multi-unit buildings have not been investigated well.

Given that the units of multi-unit buildings are occupied by different groups of residents, e.g., tenants and unit owners with different preferences, the process of sharing energy from shared DRESs between these groups can be unjust and challenging. For instance, from the perspective of investing in shared DRESs, some residents could not afford the investment economically, or there might be a group of residents, such as tenants, who want to enjoy the benefits of shared DRESs for a short period because long-term investment is not affordable for them. In this regard, this study proposes an energy-sharing model that enables efficient, fair, and equitable allocation and distribution of energy, costs, and benefits in multi-unit buildings, considering different groups of residents.

Energy justice provides an effective decision-making tool that helps stakeholders, e.g., consumers and producers, to make more rational energy decisions [Sar17]. In recent years, scholars have reached a joint definition of energy justice in which the costs and benefits of energy services are fairly distributed, and equitable energy decision-making is provided[SD15]. In general, energy justice addresses the equitable sharing of energy, costs, and benefits and identifies injustices within energy systems [Sar17], [SD15]. Energy justice integrates three different, but interconnected principles that include distributive justice, procedural justice, and recognition justice [McC+13]. Each principle relates to a particular aspect of justice that complements each other. Distributive justice refers to whether all groups share equally in specific services and goods. Procedural justice deals with the equitable participation of stakeholders in decision-making processes. Recognition of justice gives attention to the demands and rights of different

groups in society, especially underrepresented or vulnerable groups, to decrease social inequalities [McC+13]. The value of energy justice has not been studied within the concept of energy sharing in multi-unit buildings. Therefore, a set of steps has to be formulated to enable a fair and just energy-sharing system in multi-unit buildings where different groups of residents can participate and gain benefit from the shared DRESs in their building. Applying the principles of energy justice in energy-sharing models removes or reduces barriers to the active participation of end customers (consumers/prosumers) in the future smart and decentralized energy grid.

In this paper, a new fair energy sharing model (FESM) is proposed, which focuses on energy allocation and trading inside different multi-unit buildings, considering energy justice principles. The basis for our definition of FESM is a network behind the meter in which the shared systems (PV panels and BESSs) can be owned by the main owner of a multi-unit building or a group of residents living in the building. Although FESM and community-based microgrids have similarities in their configurations (e.g., both rely on centralized renewable sources), they have an important difference. In community microgrids, shared DRESs are located in front of the meter that are controlled by utility companies (i.e., they are controlled in an aggregate manner) that incur extra costs for the users who use the shared systems (e.g., there will be administrative costs) [WZ]. Since users of community DRESs do not own DRESs, they are deprived of having access to any of the tax credits and incentives of DRESs. However, in FESM, shared DRESs are installed behind the meter and are not controlled by utility companies; hence, additional costs are eliminated for users. Moreover, users in FESM can own a portion of DRESs and take advantage of the tax benefits.

After allocating shared DRESs and energy to the residents by the energy management operator (EMO) of the buildings, energy trading is enabled in FESM with expected prominent benefits such as cost-savings and carbon footprint reduction. The EMO of the buildings monitors and controls the trading stage and computes the trading price. During the energy trading process, the interests of sellers and buyers are protected, and they are given the opportunity to determine the amount of energy they want to sell and buy based on certain factors, such as priority factors, or after seeing the price. The priority factor is defined as one of the main elements of FESM to retain the fairness and interests of both buyers and sellers during energy trading. Justice and fairness are analyzed in energy allocation and trading processes according to the main principles of energy justice. These analyzes help to understand that justice can be defined differently for each building according to the building conditions (e.g., resident preferences, types of residents, etc.). Moreover, the revenue of the shared DRESs' users living in the multi-unit buildings are examined under different energy allocation processes. The experimental results show that our method is highly beneficial for all participants as their revenue increases dramatically compared to the baseline methods.

The main contributions of this work are as follows:

1. We present a novel fair energy sharing framework FESM plus two different

applications of it. In FESM energy demand of buildings is supplied by shared distributed renewable energy sources, including PV panels and battery energy storage systems. FESM is a behind-the-meter network that enables energy allocation and trading inside the buildings.

2. To the best of our knowledge, this work is the first to apply the main principles of energy justice, including procedural justice, recognition justice, and distributive justice, in a systematic way in the design of energy allocation and trading processes to create justice and fairness. Moreover, we propose a novel priority factor to prioritize users to secure fair sharing of energy generated by shared DRESs for residents.

3. A new and simple pricing mechanism is proposed that increases the profits for sellers and decreases the cost for buyers, and makes the overall operation of the system simple.

The rest of the paper is organized as follows. In the following section, first, we present a brief overview of the shared renewable energy system in multi-unit buildings by discussing the status quo of energy sharing in four countries, including Germany, Austria, France, and Norway. Then, fairness in energy sharing is reviewed, and we discuss how energy justice principles can be applied in an energy-sharing process. The details of the FESM network are presented in Section III.3; then, the strategies for energy trading for all participants, such as sellers, buyers, and energy management operators, are summarized in Section III.4. Section III.5 presents comprehensive experimental results, and the paper is concluded in Section III.6.

## III.2 Background

### III.2.1 Shared Renewable Energy Systems

Renewable energy sources have been potentially considered as a practical solution to supply parts of the load in buildings, especially in urban areas [PD20]. The establishment of more renewable energy communities can increase both the share of renewable energy and flexibility in electricity supply and electricity systems, respectively. Currently, many European countries have not fully considered the particulars of renewable energy communities in their energy support frameworks. However, Germany has the most experience with community energy [Inê+20]. In the following, we briefly review the current situation of energy sharing in multi-unit buildings in four countries.

*Germany and Austria:* In Germany and Austria, shared PV systems can be implemented legally in multi-unit buildings. Germany makes the hardest efforts to increase the uptake of shared PVs in buildings among European countries [PD20]. In [**59**], a techno-economic analysis of the self-consumption of rooftop solar panels for different types of buildings in Germany, including multi-unit buildings, is performed. In the course of different projects in Germany, it has been proven that energy generated from PV panels can be successfully shared

in buildings under a novel concept called the "Mieterstrommodel" [RSM22]. Under this scheme, landlords or owner communities known as 'legal suppliers' may generate energy from rooftop PV panels and sell it to their tenants [PC21]. Tenants receive the same feed-in tariff compensation for extra energy fed into the grid. However, they receive an extra 'tenant-electricity surcharge' for their self-consumed energy [PC21]. In July 2017, Austria also adopted relevant legislation to enable the uptake of shared PV panels in multi-unit buildings. In Austria, suppliers are also able to supply the energy demand of residents via energy produced by their buildings' PV panels [PD20].

*France:* On 8 November 2019, law no. 2019-1147 was approved in France. It regulates collective electricity self-consumption (In French: autoconsommation collective d'électricité) of energy and climate [Per+21]. In France, users willing to contribute to a collective self-consumption (CSC) operation can establish themselves as an Organizing Moral Person (OMP) responsible for sharing locally produced energy among users. Moreover, each user must be connected to the public distribution network via a meter. The OMP considers the energy sharing ratio equal to the ratio of the total consumption of one household to the consumption of all households. Other sharing ratios among users can be defined by the OMP, and communicated to the distributed system operator (DSO). , among users and sends it to the DSO. Each user's bill is calculated based on the consumption of the household minus the community generation assigned to the household by the supplier, which the user has chosen. CSC communities can be considered platforms for creating innovation in energy sharing. However, community-wide operating rules that adopt consumption practices for single houses, buildings, or neighborhoods are essential for any energy community [Per+21].

*Norway:* In Norway, customers in detached houses, with both consumption and production behind their connection point, can today utilize their own production without paying grid rent and other fees [Jaf+20]. However, customers in multi-unit buildings do not enjoy the same benefits. This means that, according to the current regulations, it is not possible for customers in multi-unit buildings who have several measuring points to use their own production without paying grid rent and fees [Jaf+20]. Recently, a new regulation was proposed by the regulating body, RME [Jaf+20], which, if approved, will change the rule of sharing energy in buildings. In the RME proposal, different sharing models that can be applied inside the buildings and how energy can be allocated to the residents who joined the sharing solution are discussed. Below, the proposed sharing solutions are reviewed.

1. Equal sharing: the simplest way is allocating the production of shared PV panels to residents equally. This means that all residents receive the same share. Although this sharing model is easily managed by network companies, it poses some weaknesses. This model is fair when all building units have the same area, but this is not fair for units with different areas. A larger unit requires more energy than a smaller one.

2. Unequal sharing: unequal sharing means that each resident receives

different shares of the energy generated by the shared PV panels in the building, e.g., based on the size of the units, the cost that each resident invests in the shared PV panels, etc. In FESM, we focus on the unequal sharing model as a guideline for specializations of the framework that we explore in this paper.

3. Dynamic sharing: in this model, residents receive energy based on their consumption at various time slots in a day. This sharing model attempts to maximize the utilization of the energy produced by PV panels in buildings. In this case, the energy is sent back to the grid only for hours, where the total generation exceeds the total consumption in the building. The dynamic share of a resident at a time slot is the ratio of the resident's consumption to the total consumption of the residents at that time slot.

Legalizing the shared use of PV panels in multi-unit buildings and giving the right to the residents to trade their shared energy with neighbors inside their building benefits the residents (e.g., financial benefits) and the environment (e.g., carbon reduction). To realize that, the above regulations need to be developed with the intention of legalizing energy trading inside multi-unit buildings.

### III.2.2 Fairness in Renewable Energy Sharing

Fairness in energy sharing has been interpreted in different ways in the literature. For example, one study [Lov+20] shows that if energy is transparently and equitably shared in a sharing method, then the method is fair. Other studies present different interpretations [Pau+18], [Wu+16], [Cui+20]. According to [Pau+18], fairness is associated with the willingness-to-pay of a prosumer, equal satisfaction is another interpretation of fairness that is supported by Jafari et al. [Wu+16], and Lovati et al. [Cui+20] proposed a peer-to-peer (P2P) energy trading model in which fairness has been achieved by transparency.

There are several works that use game theoretical approaches to conduct energy sharing in buildings [Fin+18], [Cic10]. For instance, Cui et al. [Par+16] proposed a non-cooperative game to manage the energy-sharing process, and they believe that energy sharing is fair when all participants gain benefits. A contribution-based and non-pricing energy trading mechanism between microgrids was proposed by Park et al. [LAG16], but they did not show how to calculate the contribution factor. Jadhav et al. [JPG18] extended the work in [LAG16] by proposing a priority factor for buyer microgrids according to their contributions and energy demand. However, prioritizing buyers based on their energy demand makes buyers with the highest demand receive more energy which can be unfair. The authors in [JPG18] also presented an energy trading mechanism based on Nash bargaining theory in which a trading price was computed based on minimizing the total cost of buyer microgrids. In [LAG16], [JPG18], only the interests of the buyer microgrids are considered, which makes the energy trading unfair to the seller's microgrids. In this work, the energy trading method used in [LAG16] is extended in such a way that the benefits of both buyers and sellers are supported in the calculation of the energy trading

price. In addition, the priority factor is modified and calculated for both sellers and buyers according to the trading situations.

Some works present different energy-sharing methods and compute a proper fairness index to evaluate the performance of their methods. For example, Long et al. [LZW19] proposed several indexes, including the equality index and participation willingness index, to evaluate their proposed P2P energy trading mechanism, while Chakraborty et al. [CBK20] used the Nash social welfare index for the same purpose. According to the literature, a common framework for evaluating fairness and justice in energy-sharing solutions is missing. Energy justice can be used as an evaluation framework to evaluate fairness in energy-sharing models based on its three main principles. In the following, we will study how justice and fairness can be achieved in energy-sharing systems through the main principles of energy justice.

Recognition justice: This principle of energy justice takes care of different groups of stakeholders, especially vulnerable groups, to have equal access to opportunities and resources in energy systems [SD15], [McC+13]. When recognition justice is considered in designing an energy-sharing model, we have to explore to what extent different groups (e.g., low and high-income groups, tenants, and unit owners) have access to technologies used in the model.

Distributive justice: This principle is about benefit and risk being equitably distributed among stakeholders in energy systems [SD15], [McC+13]. According to this principle, we have to evaluate how cost, profit, DRESs, and energy generated by shared PV panels are distributed among stakeholders (e.g., residents and owners of multi-unit buildings).

Procedural justice: This principle emphasizes that all stakeholders affected by the energy systems have to participate equitably in decision-making [SD15], [McC+13]. In designing an energy-sharing model for multi-unit buildings, we have to focus on how residents can significantly participate in decision-making with transparent procedures.

## III.3 Proposed FESM Framework

We assume a building that has an owner who can be a legal entity such as a person, a company, a municipality, or a cooperative, etc. The energy-sharing model is decided by the owner of the building. The energy-sharing model is the basis for energy allocation and trading. The energy allocation and trading processes in the building are handled by EMO, who could be the owner of the building, a third party, or consortium of residents, etc. The building is comprised of $N$ units denoted by the set $\mathcal{U} = \{1, 2, \ldots, N\}$. Each unit has an owner and can be occupied by the owner, called unit-owner, or a tenant. Let $|\mathcal{U}_O| = N_O$, where $\mathcal{U}_O \subseteq \mathcal{U}$ and $N_O < N$, and $|\mathcal{U}_T| = N_T$, where $\mathcal{U}_T \subseteq \mathcal{U} - \mathcal{U}_O$ and $N_T = N - N_O$, be the sets of unit-owners and tenants, respectively, who live in the building. Each unit is characterized by a set of parameters, such as the area of the unit and the number of members living in the unit, that can be input into the sharing model. The building can be equipped with a number of PV panels that belong

to the set $\mathcal{PV} = \{1, \ldots, P\}$. PV panels have an owner that can be the owner of the building, a third party, or a legal entity formed by residents who each own a share. Depending on the sharing model, the residents can lease a share of the PV panels from the owner. Since PV panels may produce more energy than residents need during some time slots in a day, a set of BESSs $\mathcal{B} = \{0, 1, \ldots, B\}$ are shared between residents of buildings. Similar to PV panels, each BESS has an owner that can be the owner of the building or a group of residents. Both unit owners and tenants can lease a share of BESSs. Residents can trade their excess energy generated by PV panels inside the building.

In FESM, the allocation process refers to the step where the EMO of the building allocates a fair share of energy generated from PV panels or the energy saved into the shared batteries to the residents of the building. The unequal sharing model proposed by the RME proposal [Jaf+20] (see Section III.2.1) is used for the allocation process in the building. Compared with other sharing models, the unequal sharing model allows the owner of the building to allocate a fair and different share of energy (i.e., $x\% \times Generation^{PV}$, where $Generation^{PV}$ is the total generation of PV panels) or capacity of BESSs (i.e., $x\% \times BESS^{capacity}$, where $BESS^{capacity}$ is the total capacity of BESS) to the residents. The allocated share ($x\%$) can vary between the residents participating in the sharing solution as long as $\sum x = 100$, and can be based on different factors, such as the resident's need or the amount the resident invests in DRESs, etc. In the allocation process, recognition justice will be achieved when all groups of residents, including tenants, unit owners, low-income families, etc., have the opportunity to exploit the building's DRESs. In the building, a fair share of energy can be allocated to each unit of the building based on factors such as the area of the unit, family members living in the unit, etc. Hence, in this case, distributive justice will be achieved by distributing energy generated by DRESs among the units based on unit characteristics. In other cases, residents can invest in DRESs based on their ability to pay. In this situation, distributive justice is realized by allocating energy to the residents in proportion to the cost that they have invested in DRESs. Moreover, in the energy allocation process, residents can participate in decision-making in which, for example, they can decide whether to invest in DRESs or pay only for their consumption. Therefore, procedural justice will also be fulfilled in the allocation process.

After the allocation step, energy trading takes place in one step, where local energy is traded between the residents of the building. During energy trading, justice is realized so that participants, including sellers, buyers, and the EMO of the building, can participate in decision-making processes (procedural justice), and all groups of residents have the opportunity to participate in energy trading (recognition justice) and gain financial benefit by selling or buying excess energy from DRESs (distributive justice). The following sections discuss the fair energy allocation and trading processes within the proposed framework for two different multi-unit buildings, i.e., Building A and B, illustrating two different approaches to applying the principles of energy justice. These two approaches will be experimentally compared with regard to distributive justice, recognition justice, and procedural justice.

### III.3.1 Building A

Building A has an owner who is a person. This building consistents of $N_A$ units identified by the set $\mathcal{U}_A$ such that $\mathcal{U}_A \subseteq \mathcal{U}, \mathcal{U}_A = N_A$, and $N_{O,A}$ and $N_{A,T}$ of the units, where $N_{A,O} < N_A$ and $N_{A,T} = N_A - N_{A,O}$, are occupied by unit-owners and tenants, respectively. Building A is equipped with $P$ rooftop PV panels and $B$ BESSs funded by the owner of the building. The EMO of Building A is the building owner who allocates a fair share of DRESs and energy generated by the PV panels to each unit of the building. After the allocation process, energy trading managed by the EMO of the building takes place in one step, where the local surplus energy is traded between the building occupants. The possible ways of allocating energy in Building A are discussed in the following.

Energy allocation: In building A, the EMO of the building allocates a certain share of PV panels and BESSs to each unit of the building, giving all residents the opportunity to enjoy the benefits of shared DRESs in their building. The allocation process in Building A is based on the unequal sharing model [Jaf+20]. In this regard, the EMO of the building allocates $x_i\%$ of PV panels (i.e., $x_i\% PV^{area,A}$) and BESSs (i.e., $x_i\% BESS^{capacity,A}$ ), where $x_i$ is based on the area of unit $i$ and the number of family members living in the unit. The PV panel share ($PV_i^{share,A}$) and BESS share ($BESS_i^{share,A}$) for the $i$th unit in Building A are computed as follows:

$$PV_i^{share,A} = (\alpha \frac{Unit_i^{area,A}}{Unit^{area,total,A}} + (1-\alpha)\frac{Members_i^A}{Members^{total,A}})PV^{area,A}, \quad \forall i \in \mathcal{U}_A \tag{III.1}$$

$$BESS_i^{share,A} = BESS^{capacity,A}(\alpha \frac{Unit_i^{area,A}}{Unit^{area,total,A}} + (1-\alpha)\frac{Members_i^A}{Members^{total,A}}), \forall i \in \mathcal{U}_A \tag{III.2}$$

where $PV^{area,A}$ and $Unit_i^{area,A}$ are the total area of the PV panels and the area of the $i$th unit in Building A, respectively. $Members_i^A$ and $Members_i^{total,A}$ are the number of members who live in unit $i$ and the total number of residents living in Building A, respectively. In the above equations, $\alpha$ is a weight factor that gives importance to the number of family members living in a unit and the area of the unit while allocating PV panels and BESSs. In this work, the value of $\alpha$ is set to 0.5 to give equal importance to both numbers of family members and the area of the unit. In Equation III.2, $BESS^{capacity,A}$ is the total capacity of the building's battery.

If the shared PV panels in building A generate $G_i^{PV,A}$ amount of energy at time slot $t$, unit $i$ will receive $E_i^{allocated,A}$ share of energy according to the following equation:

$$E_{i,t}^{allocated,A} = PV_i^{share,A} G_i^{PV,A}, \forall i \in \mathcal{U}_A \tag{III.3}$$

In Building A, residents can decide whether to lease their share or just pay for their consumption. The latter is most suitable for temporary residents, such as

tenants or residents who cannot afford the lease cost. leasing PV panels/BESSs allows residents to sell the remaining energy from their share; otherwise, the remaining energy belongs to the building owner. The lease cost for a resident who leases a share of a PV panel is computed as a certain percentage of the benefit that the resident gain by using the PV panel. The percentage value is defined by the building owner and should not be set too high to avoid loss of benefit. Hence, the value is set to 10%.

### III.3.2 Building B

Similar to Building A, Building B has an owner who is a person and acts as the EMO of the building. We assume that Building B does not possess PV panels and BESSs. Hence, a group of or all building residents decide to install PV panels on the roof of the building with the permission of the building owner. In this case, residents who cooperate to buy PV panels or BESSs are considered owners of PV panels or BESS, respectively. Building B has $N_B$ units; let $|\mathcal{U}_B| = N_B$, where $\mathcal{U}_B \subseteq \mathcal{U}$, be the set of the units. In the building, there are $N_{B,O}$ and $N_{B,T}$ units, where $N_{B,O} < N_B$ and $N_{B,T} = N_B - N_{B,O}$, that are occupied by unit-owners and tenants.

Energy allocation: In Building B, $n_{pv-o}$ of unit-owners buy PV panels for the building. Let $\mathcal{U}_{B,O}$ be the set of such unit-owners such that $|\mathcal{U}_{B,O}| = n_{pv-o}$, where $n_{pv-o} \leq N_{B,O}$. A number of those unit-owners (i.e., $m_{pv-o}$ of $n_{pv-o}$, where $m_{pv-o} \leq n_{pv-o}$) live in the building, and the rest (i.e., $n_{pv-o} - m_{pv-o} = N_{B,T}$) rent their units. In this building, the EMO of the building defines an ownership concept to distribute energy to unit-owner $i$, where $i \in \mathcal{U}_{B,O}$, based on the size of the unit owner's investment in PV panels. Given that the ownership factor varies for each unit-owner $i$, the EMO of the building follows the unequal sharing model [Jaf+20] for allocating the energy generation of the PV panels in the building. The ownership factor ($Ownership_i^{PV,B}$) for the $i$th unit-owner who owns a share of PV panels and lives in Building B, where $i \in \mathcal{U}_{B,O}$, is equal to the ratio of the cost ($Ct_i^{PV,B}$) that is invested by the unit-owner to the total cost ($Ct^{PV,total,B}$), and can be written as follows:

$$Ownership_i^{PV,B} = \frac{Ct_i^{PV,B}}{Ct^{PV,total,B}}, \forall i \in \mathcal{U}_{B,O}, \tag{III.4}$$

In addition, the amount of energy $E_i^{allocated,B}$ that the $i$th unit-owner in Building B will receive is computed as follows:

$$E_{i,t}^{allocated,B} = Ownership_i^B G_t^{PV,B}, \forall i \in \mathcal{U}_{B,O}, \tag{III.5}$$

where $G_t^{PV,B}$ is the amount of energy generated by the PV panels in Building B at time slot $t$.

The investment cost ($Cost_i^{investment,B}$) of unit-owner $i$ per day in Building B is given by the following Equation.

$$Cost_i^{investment,B} = \frac{Ct_i^{PV,B}}{Payback^B} \tag{III.6}$$

where $Payback^B$ is the period of time it will take the unit-owner $i$ to pay off the total cost of the PV panel share. Similar to Building A, the lease cost for the tenant who leases a share of PV panels from their unit owner is a certain percentage of the tenant's benefit and is set to 10%.

Residents of Building B can also contribute to buying BESSs for the building. Let us assume there are $n_{b-o}$ unit-owners who pay for a share of BESSs, and $|\mathcal{U}_{B,b-o}| = n_{b-o}$, where $n_{b-o} \leq N_{B,O}$, is the set of such unit-owners. The ownership factor $Ownership_j^{battery,B}$ for the $j$th unit-owner who owns a share of BESSs, where $j \in \mathcal{U}_{B,b-o}$, is computed as follows:

$$Ownership_j^{battery,B} = \frac{Ct_j^{battery,B}}{Ct^{battery,total,B}}, \forall j \in \mathcal{U}_{B,b-o}, \tag{III.7}$$

In addition, the share of BESS $BESS_j^{share,B}$ that is allocated to the $j$th unit-owner in Building B is:

$$BESS_j^{share,B} = Ownership_j^{battery,B} BESS^{capacity,B}, \forall j \in \mathcal{U}_{B,b-o}, \tag{III.8}$$

Generally speaking, residents can charge their share of the battery. If some residents have available capacity in the battery, they can allow other residents to use their capacity at a specific time slot in a day until an agreed-upon time.

Regarding investing in PV panels and BESSs, there are some situations that should be taken into consideration. In Building B, unit owners who do not live in the building and own a share of PV panels or BESSs can lease a part of their share to their tenant. In this case, tenants benefit from energy generated by PV panels by paying for their energy consumption or a fee in excess of their housing rent. In the latter case, tenants can sell the excess energy from their share of PV panels. There might be residents who do not have the opportunity to use PV panels/BESSs in the building. Examples can be tenants whose unit-owners do not invest in PV panels/BESSs, residents who cannot afford the investment cost, residents who just moved into the building and want to own a share of PV panels and there is no available space on the roof of the building for installing PV panels, etc. This issue of fairness is outside the scope of this paper.

### III.3.3 Overview of Fair Local Energy Trading in FESM

Regardless of the group of the building, the EMO of the building has the duty to fulfill the energy demand of all residents. The residents with extra and lack of energy are considered sellers and buyers, respectively. A non-cooperative game takes place between buyers and sellers separately to adjust their energy demand through the game. In contrast to cooperative energy trading games in which participants try to maximize social benefit

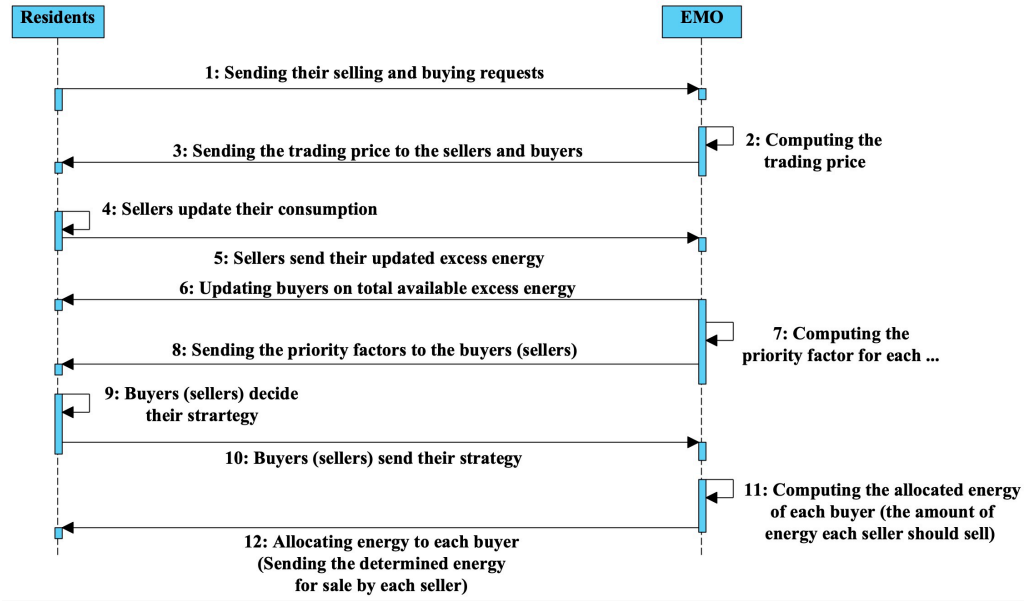



Figure III.1: Sequence diagram for the proposed fair local energy trading in FESM .

via cooperation based on a particular agreement, in non-cooperative games, participants compete to maximize their own financial benefits (i.e., sellers and buyers compete to maximize their benefits and minimize their costs, respectively) [HL22]. Hence, defining the energy trading price is important in effective energy trading and fair distribution of profit. In this paper, it is assumed energy trading takes place inside the building as depicted in Figure III.1.

As seen from Figure III.1, first, residents send their selling and buying requests to the EMO of the building. The EMO of the building then decides the trading price in a way that benefits sellers and buyers. The trading price should be bound by the grid buying and selling prices. By considering this, both sellers and buyers prefer to trade energy in the building rather than in the main grid. When seeing the trading price, each seller is allowed to decide its strategy by adjusting its consumption to maximize its own benefit. The sellers then update the EMO on their excess energy, and the buyers are notified by the EMO. In the next step, the EMO calculates the priority factor for each buyer or seller depending on the situation (i.e., buyers are prioritized when the total energy demand of buyers is higher than the total excess energy, and sellers are prioritized in the opposite situation). The EMO considers the priority factor for the purpose of obtaining a fair and stable energy trading system. The priority factor of a buyer/seller is calculated based on the number of times the buyer/seller contributed as seller and buyer in the previous energy trading steps until now, the ownership factor

of the buyer, the number of family members of the buyer, the area of the buyer's unit, and the amount of energy the seller want to sell. In this trading model, a participant with a higher priority factor can trade more energy than other participants. The priority factors are sent by the EMO to the corresponding buyers or sellers. Depending on the situation, the buyer (seller) decides on how much energy to buy (sell) to maximize its benefits based on the buyer's (seller's) priority factor and the updated total excess energy available in the building (the total energy demand of buyers). After receiving the strategies, the EMO allocates a specific amount of energy to each buyer (seller) based on the buyer's (seller's) strategy, the priority factor of the buyer (seller), and the total energy demand (excess energy). If, after the trading process, there is still excess energy in the building, the energy is fed into the main grid, typically based on a pre-set feed-in tariff, or if there is still unsatisfied demand, it is fulfilled by the main grid at market price.

### III.3.4 The Proposed Energy Trading Model

In this section, the proposed local energy trading inside the building is described in detail.

Let $C_{i,t}$ denote the energy demand of the $i$th resident at time slot $t$. Moreover, resident $i$ can have a share in BESSs and $E_{i,t}^{saved}$ of energy saved in the battery during a given time interval of the day. After allocating energy to all residents based on their share of PV panels or ownership factors, if $E_{i,t}^{allocated} + E_{i,t}^{saved} < C_{i,t}$, the resident $i$ needs to buy energy from sellers inside the building. Let $\mathcal{R}_t^b$ be the set of residents who act as buyers at time slot $t$. If $E_{i,t}^{allocated} + E_{i,t}^{saved} > C_{i,t}$ for some residents in the building, then these residents are considered sellers. Let $\mathcal{R}_t^s$ be the set of such sellers in the building at time slot $t$.

In the first stage, buyers send their buying demand to the EMO of the building. The energy demand of buyer $i \in \mathcal{R}_{b,t}$ is given by:

$$D_{i,t} = |(E_{i,t}^{allocated} + E_{i,t}^{saved}) - C_{i,t}|, \forall i \in \mathcal{R}_t^b. \tag{III.9}$$

and the total energy demand of all buyers in the building at time slot $t$ is

$$D_t^{total} = \sum_{i \in \mathcal{R}_t^b} D_{i,t} \tag{III.10}$$

The excess energy of the $i$th seller after fulfilling its essential needs is equal to its minimum consumption at time slot $t$, i.e., $C_{i,t} = {Cons_{i,t}}^{min}$, is

$$E_{i,t}^{excess} = (E_{i,t}^{allocated} + E_{i,t}^{saved}) - Cons_{i,t}^{min}, \forall i \in \mathcal{R}_t^s \tag{III.11}$$

and the total excess energy from solar panels at time slot $t$ is given by

$$E_t^{excess,total} = \sum_{i \in \mathcal{R}_t^s} E_{i,t}^{excess}. \tag{III.12}$$

According to Step 4 in Figure III.1, sellers have the opportunity to manage their energy consumption. This means that the seller $i \in \mathcal{R}_{s,t}$ intends to adjust its consumption $Cons_{i,t}$ s.t. $Cons_{i,t} \geq Cons_{i,t}^{min}$ and sells its surplus energy $((E_{i,t}^{allocated} + E_{i,t}^{saved}) - Cons_{i,t})$ to the neighboring buyers via the proposed energy trading model. In this regard, the updated excess energy of the $i$th seller after settling its energy consumption is as follows:

$$E_{i,t}^{excess^*} = (E_{i,t}^{allocated} + E_{i,t}^{saved}) - Cons_{i,t}, \forall i \in \mathcal{R}_t^s \tag{III.13}$$

and consequently, the total excess energy available in the building at time slot $t$ is updated as follows:

$$E_t^{excess^*,total} = \sum_{i \in \mathcal{R}_t^s} E_{i,t}^{excess^*}. \tag{III.14}$$

Following that, available energy in the building is traded between participants. Finally, after energy trading is completed, if there are still residents with unsatisfied demand, the energy demand is purchased from the main grid via the EMO of the building. In contrast, the EMO sells the extra energy to the main grid.

## III.4 Players Strategies in Energy Trading

In this section, the strategies of the participants, including the EMO of the building, buyers, and sellers, in the proposed fair energy trading model are discussed. In the model, the purpose of each seller is to maximize its utility by adjusting its consumption after knowing the trading price determined by the EMO of the building. Furthermore, each seller attempts to sell as much of its excess energy as possible when the total excess energy is more than the total energy demand in the building. Buyers' goal is to gain as much energy as possible by setting their strategy to meet their own energy demands. At the same time, the EMO of the building tries to maximize the welfare of the building.

### III.4.1 Buyers Strategies

Buyers intend to gain as much energy as possible from the local energy market via the EMO of the building, bounded by their energy demand. To this end, buyers participate in a non-cooperative game where they decide their strategy to request a certain amount of energy from the EMO. Thereafter, the EMO allocates energy to each buyer according to their strategy, priority, and the total amount of excess energy available in the building. To allocate energy fairly to each buyer, the priority factor is used to prioritize buyers. The priority factor is also used as an incentive factor to encourage local energy trading.

#### III.4.1.1 Priority Factor for Buyers

While determining the priority for a buyer in the energy trading step, three factors are considered:

1. Total previous contributions of the buyer as seller or buyer
2. Number of family members of the buyer
3. Area of the buyer's unit ($m^2$)

Thus, the priority factor $Pr^b_{i,t}$ of the $i$th buyer at time slot $t$ is calculated as follows:

$$Pr^b_{i,t} = \frac{(\beta C^s_{i,t}) + C^b_{i,t}}{C^{total}_t} + \frac{Unit^{area}_i}{Unit^{area,total}} + \frac{Members_i}{Members^{total}}, \forall i \in \mathcal{R}^b_t \qquad \text{(III.15)}$$

The first part of Equation III.15 refers to the contribution factor, Here, $C^s_{i,t}$ and $C^b_{i,t}$ are the number of times the buyer contributed as seller and buyer, respectively, until the present time slot $t$, and $C^{total}_t$ is the total contribution as seller and buyer by the buyers until the present time slot $t$. Here, $\beta$ is a scaling factor such that when $\beta > 1$, more importance is given to the past contributions made as sellers, which will encourage participants to consume less and save energy to act as sellers in the future. In general, the contribution factor motivates participants to trade among themselves instead of trading with the main grid. The second and third parts of the equation are the number of family members for a particular buyer $i$ and the area of the buyer's unit ($m^2$), respectively, which indicate that the priority factor should be a function of the number of family members and the area of the unit. $Members^{total}$ and $Unit^{area,total}$ are the total number of family members of all buyers and the total area of all buyer units who live in the building.

#### III.4.1.2 Utility of Buyers

In this section, the utility function of buyer $i$ $U^b_{i,t}$, living in the building at time slot $t$, which is always a non-negative function, is defined. The utility of buyer $i$ is computed based on the priority factor of the buyer and the ratio between the strategy of the buyer to the energy allocated by the EMO of the building (i.e., $\frac{AE^b_{i,t}}{S^b_{i,t}}$). There are some assumptions regarding the utility of the buyer that must be taken into consideration. The first assumption is that $U^b_{i,t}$ must be a strictly increasing function of $\frac{AE^b_{i,t}}{S^b_{i,t}}$, which means fulfillment increases by the ratio between the amount of energy that is allocated to the buyer and the required energy of the buyer as its strategy. Second, the utility function must be a concave function of $AE^b_{i,t}$, i.e., as the allocated energy increases, the increasing rate of satisfaction decreases. Since the EMO of the building allocates more energy to buyers who have high priority, the utility function must be proportional to the priority factor considering a weight ($\theta > 0$) factor for the priority. The

weight factor ($\theta$), which is a dynamic value selected by the EMO of the building, gives importance to the priority during energy trading. Therefore, the utility function of buyer $i$ ($U^b_{i,t}$) is computed using a modified version of the function given in [LAG16]:

$$U^b_{i,t} = (Pr^b_{i,t})^\theta \log(1 + \frac{AE^b_{i,t}}{S^b_{i,t}}), \forall i \in \mathcal{R}^b_t \tag{III.16}$$

where $Pr^b_{i,t}$ is the priority factor of the $i$th buyer at time slot $t$. $AE^b_{i,t}$ and $S^b_{i,t}$ are the energy allocated to buyer $i$ by the EMO of the building and the demand strategy of the $i$th buyer at time slot $t$, respectively.

Each buyer demands a different amount of energy; however, the buyer desires to obtain as much energy as possible, bounded by the initial demand of the buyer (e.g., the buyer $i$ should decide its strategy from $[0, D_{i,t}]$). Accordingly, buyers participate in a non-cooperative game using Algorithm 2 to ask for a certain portion of excess energy available from the EMO of the building. Algorithm 2 gives the optimal strategy ($S^b_{i,t}$) for each buyer $i$ participating in the game at time slot $t$. The existence and uniqueness of the Nash equilibrium solution of the game have been proven in [LAG16]. The utility function of all buyers $U(S^b)$ is defined as follows [JPG18]:

$$\begin{aligned} U(S^b) = \underset{AE^b}{\text{argmax}}[ & \sum_{i \in \mathcal{R}^b_t} (Pr^b_{i,t})^\beta \log(1 + \frac{AE^b_{i,t}}{S^b_{i,t}})] \\ s.t. \quad & 0 \leq AE^b_{i,t} \leq S^b_{i,t}, \forall i \in \mathcal{R}^b_t \\ & \sum_{i \in \mathcal{R}^b_t} AE^b_{i,t} \leq E^{excess^*}_{i,t}. \end{aligned} \tag{III.17}$$

where $S^b_{i,t}$ is the strategy of the $i$th buyer at time slot $t$. A non-cooperative game is used to formulate competition among buyers.

Algorithm 3 provides the optimal solution of the problem in Equation III.17, which is a revised version of the famous water-filling problem [Zha+19]. According to the water-filling problem [LAG16], there are $N$ tanks, and any two tanks are connected by a pipe. Let $M = \{1, 2, \ldots, N\}$ be the set of all the tanks, $\{(Pr^b_1)^\beta, (Pr^b_2)^\beta, \ldots, (Pr^b_N)^\beta\}$ be the set of tank widths, and $\{\frac{S^b_1}{(Pr^b_1)^\beta}, \frac{S^b_2}{(Pr^b_2)^\beta}, \ldots, \frac{S^b_N}{(Pr^b_N)^\beta}\}$ be the set of tank heights. It is assumed that tank $i$ has to be on the base of height $\frac{S^b_i}{(Pr^b_i)^\beta}$ for all $i \in M$. The total volume of the water that is used to fill the set of tanks is $E^{excess^*}_{i,t}$. Therefore, tank $i$ is filled by pouring $AE^b_{i,t}$ volume of water which is the optimal solution for tank $i$.

### III.4.2 Sellers Strategies

It is assumed that sellers are interested in selling their excess energy to buyers at an appropriate price rather than selling them to the main grid at a lower price. Each seller $i$ gains a payoff by trading its excess energy

$(((E_{i,t}^{allocated} + E_{i,t}^{saved}) - Cons_{i,t})$ with neighbouring buyers and also by managing its consumption $Cons_{i,t}$ subject to $Cons_{i,t} \geq Cons_{i,t}^{min}$ after seeing the trading price $P^{tr}$. The payoff of the $i$th seller $(U_{i,t}^{s})$ at time slot $t$ is defined as follows:

$$U_{i,t}^{s} = r_{i,t} \ln(1 + Cons_{i,t}) + P_t^{tr}((E_{i,t}^{allocated} + E_{i,t}^{saved}) - Cons_{i,t}), \\ (E_{i,t}^{allocated} + E_{i,t}^{saved}) - Cons_{i,t} > 0, \forall i \in \mathcal{R}_t^s \tag{III.18}$$

The above equation is inspired by the utility function in [PF05]. The first part of the equation expresses the utility that is achieved by seller $i$ through consuming $Cons_{i,t}$ amount of energy, where $r_{i,t} > 0$ is the preference parameter of the seller at time slot $t$. A seller with high $r_{i,t}$ is more interested in consuming more of its energy to maximize its utility. The second part of the equation represents the profit that the $i$th seller achieves by selling its excess energy to neighboring buyers at trading price $P_t^{tr}$, which is calculated by the EMO of the building. Each seller $i$ has the objective of maximizing its utility by adjusting its own energy consumption $Cons_{i,t}$. Therefore, the objective of the seller $i$ at time slot $t$ is as follows:

$$\max_{Cons_{i,t}} (U_{i,t}^{s}) \\ s.t.\ Cons_{i,t} \geq Cons_{i,t}^{min}, \forall i \in \mathcal{R}_t^s \tag{III.19}$$

The objective in Equation III.21 can be achieved by computing the first-order derivative of (15), which is:

$$\frac{r_{i,t}}{1 + Cons_{i,t}} - P_t^{tr} = 0 \tag{III.20}$$

and hence Equation (21) is achieved by further solving Equation (20):

$$Cons_{i,t} = \frac{r_{i,t}}{P_t^{tr}} - 1 \tag{III.21}$$

According to Equation III.21, each seller's decision on its energy consumption is affected by the trading price, which is set by the EMO of the building. It can also be observed that the seller's consumption and the trading price are inversely proportional to each other, which means that sellers are encouraged to reduce their energy consumption and sell more energy when the trading price is high and vice-versa. It is important to note that $r_{i,t}$ should be large enough in such a way that Equation III.21 is always positive for all $Cons_{i,t} \geq Cons_{i,t}^{min}$. Moreover, the lease cost or the investment cost of the seller is subtracted from the total utility of the seller at the end of the day.

We also study the situation where the total excess energy at each trading stage is more than the total energy demand. In this case, after the sellers adjust their consumption, they can also decide their strategy (i.e., demand for selling energy) by participating in a non-cooperative game to sell as much energy as possible to the local energy market, limited by their available excess energy. Similar to Algorithms 2 and 4 uses a non-cooperative game among sellers when

the total excess energy is more than the total demand of buyers. In Algorithm 4, each seller chooses its strategy based on some important factors, such as the seller's priority factor and its updated excess energy. The EMO of the building then uses Algorithm 5 to decide on how much energy each seller should sell based on the seller's priority factor, the amount of the seller's excess energy, and the total demand of buyers.

### Priority Factors for Sellers

For each seller $i$, the EMO of the building calculates the priority factor to prioritize sellers when there is more energy to sell compared to the total energy demand of the buyers. The priority factor of the $i$th seller relies on the ratio of the number of contributions the seller has made until the present time slot $t$ as a seller ($C^s_{i,t}$) to the total contributions of the sellers and the ratio of the excess energy that the seller intends to sell to the total excess energy in the building. Hence, the following equation is used to calculate the priority factor of the $i$th seller at time slot $t$ $Pr^s_{i,t}$:

$$Pr^s_{i,t} = \frac{C^s_{i,t}}{C^{total}_t} + \frac{E^{excess^*}_{i,t}}{E_t{}^{excess^*,total}}, \forall i \in \mathcal{R}^s_t \tag{III.22}$$

where $C^s_{i,t}$ and $C^{total}_t$ are the number of contributions the seller $i$ has made and the total contributions that have been made by sellers who live in the same building as the seller $i$. $E^{excess^*}_{i,t}$ and $E_t{}^{excess^*,total}$ are the excess energy that seller $i$ wants to sell energy at and the total excess energy available in the building. When the total excess energy is more than the total energy demand, the utility function of the $i$th seller is directly proportional to its priority factor and the ratio of the amount of energy decided by the EMO that the seller $i$ can sell and the seller's strategy. Thus, the utility function of the seller $i$ ($U^s_{i,t}$) at time slot $t$ is defined as follows:

$$U^s_{i,t} = (Pr^s_{i,t})^{\beta} \log(1 + \frac{AE^s_{i,t}}{S^s_{i,t}}), \forall i \in \mathcal{R}^s_t \tag{III.23}$$

where $Pr^s_{i,t}$ is the priority factor of seller $i$ at time slot $t$. $AE^s_{i,t}$ is the amount of energy to be sold by the seller $i$, and $S^s_{i,t}$ is the selling strategy of the seller $i$ at time slot $t$.

## III.4.3 Building's EMO Strategy

The EMO of the building has several roles to maximize the building's welfare, i.e., the sum of the fulfillment of all buyers and sellers in the building. In this regard, one of the main functions of the EMO is to determine the trading price, $P^{tr}$, for energy trading inside the building. The trading price should be bounded by the grid buying and selling prices, $G^{b,p}$ and $G^{s,p}$, respectively. The EMO should compute the trading price in a way that is at the fulfillment level of

buyers and sellers. Hence, the objective of the EMO is defined as follows:

$$\begin{aligned} &\max_{P_t^{tr}}[\frac{1}{Ct_t^b} + \sum_{i \in \mathcal{R}_m} U_{i,t}^s] \\ &s.t.\ G^{b,p} \leq P_t^{tr} \leq G^{s,p} \end{aligned} \tag{III.24}$$

The above equation expresses the aim to maximize the building's welfare. According to Equation III.24, the satisfaction of sellers and buyers is met by simultaneously maximizing the inverse ratio ($\frac{1}{Ct_t^b}$) of the total cost of buyers (i.e., minimizing the total cost of buyers) and the total utility of sellers at time slot $t$.

During energy trading, in addition to the cost of buying energy from neighboring sellers, the total cost of buyers ($Ct_t^b$) at time slot $t$ also relies on the cost of the remaining energy purchased from the main grid to keep the energy balance, and is calculated as follows:

$$Ct_t^b = \begin{cases} (E_t^{excess^*,total} P_t^{tr}) + (D_t^{total} - E_t^{excess^*,total}) G^{s,p}, & \text{if } D_t^{total} \geq E_t^{excess^*,total} \\ D_t^{total} P_t^{tr}, & \text{otherwise} \end{cases} \tag{III.25}$$

Now, we can use the first-order optimality condition of the EMO's objective function (i.e., Equation III.24) in the cost function (i.e., Equation III.25) and in the sellers' utility function to obtain the trading price in trading step. Hence, we have the following equation by using the first-order optimality of Equation III.24 in Equations III.25 and III.18:

$$\frac{\delta(\frac{1}{Ct_t^b})}{\delta P_t^{tr}} + \frac{\delta(\sum_{i \in \mathcal{R}_m} U_{i,t}^s)}{\delta P_t^{tr}} = 0 \tag{III.26}$$

After solving Equation III.26; we have

$$P^{tr} = \begin{cases} \frac{1-(D_t^{total} - E_t^{excess^*,total}) G^{s,p}}{E_t^{excess^*,total}}, & \text{if } D_t^{total} \geq E_t^{excess^*,total} \text{ and } P^{tr} > G^{b,p} \\ G^{b,p} + \varepsilon, & \text{if } P^{tr} < G^{b,p} \end{cases} \tag{III.27}$$

where $\varepsilon > 0$ is a very small value to keep the trading price $P_t^{tr}$ higher than the grid buying price $G^{b,p}$ at time slot $t$. The other main function of the EMO to maximize the building's welfare is to fairly distribute energy generated from the building's PV panels and energy stored in BESSs among residents. Moreover, the EMO attempts to fairly allocate energy to participants during energy trading to maximize the building's welfare. Let $U_{i,t}^b(AE_{i,t}^b)$ and $Utility_{j,t}^s(AE_{j,t}^s)$ be the fulfillment of buyer $i$ when the total demand exceeds the total excess energy and the satisfaction of seller $j$ when the total excess energy is higher than the total energy demand, respectively, from the perspective of the EMO of the building. $\sum_{i \in \mathcal{R}_t^b} AE_i^b$ and $\sum_{j \in \mathcal{R}_i^s}$ are the social welfare of the system during

energy trading. The optimization problem to determine the amount of energy that the seller $j$ should sell ($AE^s_{j,t}$ amount of energy) at time slot $t$ is given by

$$\begin{aligned} \max_{AE^s}[\sum_{j\in\mathcal{R}^s_t}(Pr^s_{j,t})^\beta \log(1+\frac{AE^s_{j,t}}{S^s_{j,t}})] \\ s.t. \quad 0 \le AE^s_{j,t} \le S^s_{j,t}, \forall j \in \mathcal{R}^s_t \\ \sum_{j\in\mathcal{R}^s_t} AE^s_{j,t} \le D^{total}_t \end{aligned} \tag{III.28}$$

According to Theorem 1 in [LAG16], the optimal amount of energy that should be sold by each seller at time slot $t$ ($AE^{*,s}_t = \{AE^{*,s}_{j,t} | j \in \mathcal{R}^s_t\}$), when the total excess energy exceeds the total energy demand is computed as follows:

$$AE^{*,s}_{j,t} = \begin{cases} (h(Pr^s_{j,t})^\beta - S^s_{j,t}), & \text{if } 0 < (h(Pr^s_{j,t})^\beta - S^s_{j,t}) < S^s_{j,t} \\ S^s_{j,t}, & \text{if } (h(Pr^s_{j,t})^\beta - S^s_{j,t}) \ge S^s_{j,t} \\ 0, & \text{otherwise} \end{cases} \tag{III.29}$$

where $h$ is a real number satisfying $\sum_{j\in\mathcal{R}^s_t} AE^s_{j,t} = D^{total}_t$.

Similarly, the optimization problem for allocating energy to buyer $i$ at time slot $t$ is as follows:

$$\begin{aligned} \max_{AE^b_t}[\sum_{i\in\mathcal{R}^b_t}(Pr^b_{i,t})^\beta \log(1+\frac{AE^b_{it}}{S^b_{i,t}})] \\ s.t. \quad 0 \le AE^b_{i,t} \le S^b_{i,t}, \forall i \in \mathcal{R}^b_t \\ \sum_{i\in\mathcal{R}^b_t} AE^b_{i,t} \le E^{excess^*,total}_t \end{aligned} \tag{III.30}$$

By using Theorem 1 in [LAG16], the optimally allocated energy $AE^{*,b} = \{AE^{*,b}_{i,t} | i \in \mathcal{R}^b_t\}$, when the total energy demand exceeds the total excess energy, is given as follows:

$$AE^{*,b}_{i,t} = \begin{cases} (hPr^b_{i,t}{}^\beta - S^b_{i,t}), & \text{if } 0 < (h(Pr^b_{i,t})^\beta - S^b_{i,t}) < S^b_{i,t} \\ S^b_{i,t}, & \text{if } (h(Pr^b_{i,t})^\beta - S^b_{i,t}) \ge S^b_{i,t} \\ 0, & \text{otherwise} \end{cases} \tag{III.31}$$

where $h$ is also a real number such that $\sum_{i\in\mathcal{R}^b_t} AE^b_{i,t} = E^{excess^*,total}_t$.

Problems (28) and (30) are different versions of the water-filling problem [Zha+19], and their optimal solutions are given by Algorithms 3 and 5 by performing a modified version of the water-filling algorithm given in [LAG16].

## III.5 Evaluation Results

### III.5.1 Description of the Dataset

Below, two multi-unit buildings with ten units in each building are assumed, which follow the sharing model Building A and Building B, respectively. All units are allocated real household load profiles. To illustrate the potential of the proposed fair energy allocation and trading, data from Austin, Texas [Dat19] is used. Building A is equipped with three PV panels and one BESS. Building B is equipped with two PV panels and one BESS. The capacity of each PV panel is 10 kW and costs about $20,000 [Sena]. Tesla Powerwall batteries with a usable energy capacity of 13.5 kWh are considered storage systems [TES]. The performance of the proposed energy trading model is evaluated from 9 to 19 o'clock each day because there is no solar generation during the early morning and the evening, and the length of the time slot is one hour. The grid selling and buying prices are set to 0.8 cents/kWh and 2.4 cents/kWh, respectively, and the values of $\beta$ and $\alpha$ are set to 1.5 and 0.5. The PV panels' payback period for Buildings A and B are assumed 12.5 and 10 years, respectively [Har+17]. The proposed model has been developed in the Python programming language. The Gurobi solver [Senb] is used to solve the involved optimization problems in Pyomo [Opt16].

### III.5.2 Performance Evaluation

#### III.5.2.1 Energy Trading Analyses

Data used for allocating energy generated by PV panels to residents at time slot 10 is given in Table III.1. The Type of Residents column in the table denotes whether a resident is a unit owner or a tenant. In Building A, Units 1–5 are occupied by the owner of units, and Units 6–10 are occupied by tenants. Units 1–4 and 6–8 of the building lease a share of PV panels and BESSs from the building owner, while Units 5, 9, and 10 pay for their energy consumption. In Building B, Units 1–3 and 6–8 are occupied by their owner, and the rest are occupied by tenants. In this building, the owners of Units 1–5 buy PV panels, separately, while the owners of Units 6–8 cooperate in buying PV panels. The owners of Units 9 and 10 in Building B do not contribute to buying PV panels. All the unit owners in Building B except Units 5, 9, and 10 contribute to paying for a share of the BESS's cost. The EMO of the building decides the amount of energy to be allocated to the residents of the building utilizing the resident's share of PV panels or the ownership factor and the total energy generated by the PV panels of the building. After allocating energy to the relevant residents, energy trading takes place. The overall process of our energy trading method during time slot 10 is depicted in Table III.2.

Table III.1: System data for allocating energy generated by PV panels to residents of Buildings A and B at time slot 10 (O: unit-owner, T: tenant).

| **Building** | **Type of Residents** | **PV Share ($m^2$) (Building A) Ownership Factor (Building B)** | **BESS Share** | **PV Generation (kWh)** |
|---|---|---|---|---|
| A | [O, O, O, O, O, T, T, T, T, T] | [18.27, 17.55 13.13, 21.98, 11.70, 16.84, 13.84, 7.28, 10.99, 12.42] | [1.71, 1.65, 1.23, 2.06, 1.10, 1.58, 1.30, 0.68, 1.03, 1.16] | 18.69 |
| B | [O, O, O, T, T, O, O, O, T, T] | [0.19, 0.18, 0.23, 0.18, 0.08, 0.05, 0.08, 0.03, -, -] | [1.93, 1.93, 1.93, 1.93, -, 1.93, 1.93, 1.93, - , - ] | 11.23 |

Table III.2: The energy trading step in Buildings A and B at time slot 10.

| **Time Slot (hour)** | 10 | |
|---|---|---|
| **Building** | A | B |
| $EA - Cons^{min}$ | [−2.34, +2.34, −0.64, +3.72, −0.02, +1.22, +0.08, +1.25, +0.32, +0.39] | [−2.18, +2.38, +1.77, +2.61, −0.70, −1.52, −0.22, −0.10, −1.11, −1.22] |
| **Updated excess energy ($E_i^{excess*}$)** | [-, 2.34, -, 2.72, -, 1.22, 0.08, 1.25, 0, 0] | [-, 2.38, 1.77, 2.61, -, -, -, -, -, -] |
| **Priority factor** | [-, 0.53, -, 0.58, -, 0.40, 0.22, 0.40, -, -, 0.34] | [0.54, -, -, -, 0.45, 0.37, 0.55, 0.28, 0.30, 0.35 |
| **Optimal strategy of buyer/seller** | [-, 0.74, 0, 0.84, -, 0.48, 0.08, 0.49, -, -, 0.37] | [2.18, -, -, -, 0.70, 1.34, 0.22, 0.10, 1.01, 1.22] |
| **EMO decision** | [-, 0.74, 0, 0.84, -, 0.48, 0.08, 0.49, -, -, 0.37] | [2.18, -, -, -, 0.70, 1.34, 0.22, 0.10, 1.01, 1.22] |
| **Final energy demand or excess energy at time slot 10** | [0, +1.60, 0, +2.88, 0, +0.74, 0, +0.76, 0, 0, +0.34] | [0, 0, 0, 0, 0, −0.19, 0, 0, −0.10, 0] |

As can be seen from Table III.2, units 1, 3, and 5 of Building A act as buyers because the energy allocated to the units is less than their minimum energy consumption at time slot 10. In contrast, units 2, 4, and 6–10 of the building act as sellers. The EMO of the building has information, such as energy consumption and the selling and buying energy demands of the residents, and preference parameters of the sellers in the building. According to this information, the EMO is able to calculate a trading price in the range [0.8, 2.4] using Equation III.27 for the building. Trading prices calculated by the EMO of Buildings A and B are 1.74 and 1.81 Cents/kWh, respectively. By seeing the trading price, several sellers modified their excess energy; for example, units 4, 9, and 10 of Building A decreased their excess energy from 3.72 kWh, 0.32 kWh, and 0.39 kWh to 2.72 kWh, 0 kWh, and 0 kWh, respectively. Therefore, the total excess energy available from residents as sellers in Building A decreases from 9.32 kWh to 7.61 kWh. Given that units 5, 9, and 10 in Building A and unit 5 in Building B pay only for their energy consumption, the rest of their excess energy belongs to the building owner and the unit owner, respectively. To this end, the total energy that goes back to the owner of Buildings A and unit 5 in Building B are 0.71 kWh and 0 kWh, respectively.

It can be observed from Table III.2 that the total excess energy available for sale in Building A is higher than the total buying energy demand, while the opposite is true for Building B. Accordingly, the EMO of Buildings A and B calculates a priority factor for each seller and each buyer of their building, respectively. Based on the priority factor, each seller/buyer decides its strategy. Then, the EMO of Building A decides how much energy each seller should sell, and the EMO of Building B allocates an optimal amount of energy to the buyers of the building. By observing the decision of the EMO, sellers and buyers with higher priority sell and buy more energy, respectively. After fulfilling the local demands by the EMO at time slot 10, the total energy required for Building B is 0.29 kWh, and the total excess energy available from Building A is 6.32 kWh.

To emphasize the advantages of our method, we compared our results with the method in [JPG18], called Method 1, and the situation where energy can only be fed into the main grid for a fixed tariff, called Method 2. All three methods follow the energy allocation process performed in each building, while the energy trading process is different in each method. The average utility of sellers after subtracting the lease cost and the investment cost of sellers from their utility throughout the day are illustrated in Figures III.2(a) III.2(c). The average cost of buyers after adding the lease cost and investment cost of buyers to their cost throughout the day is shown in Figures III.2(b) III.2(d). In general, the figure shows that the average revenue of sellers and the average cost of buyers increases and decrease, respectively, when using our method. In comparison with our method, Method 1 only minimizes the total cost of buyers in calculating an energy trading price. Accordingly, the energy trading prices computed in Method 1 (see Figure III.3) are mostly close to the grid buying price, which makes sellers prefer consuming the whole or a part of their excess energy rather than selling them at a low price. For this reason, compared to our method, buyers have to buy most of their energy demand from the main grid at a high price, which

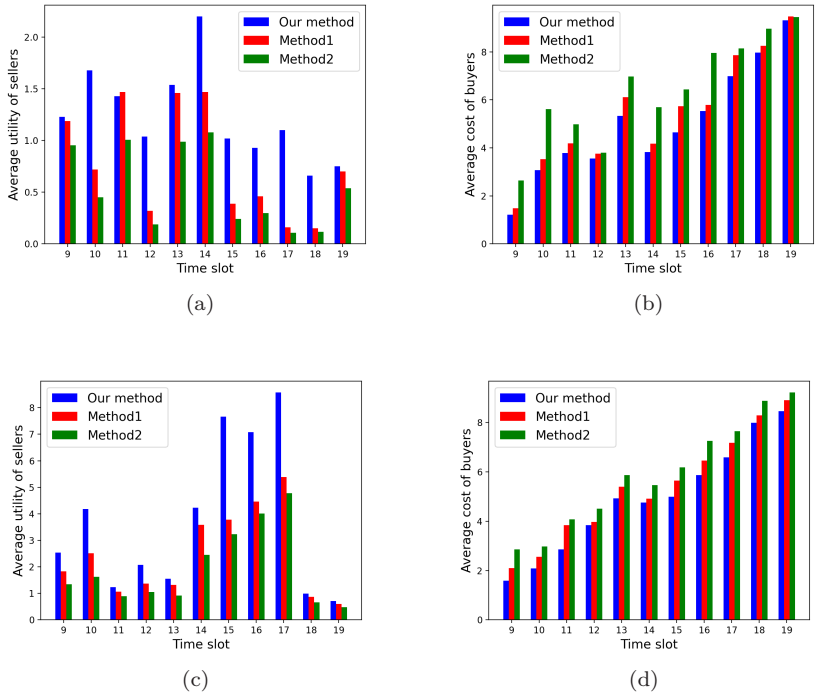



Figure III.2: (a): Average utility of sellers, (b): Average cost of buyers, of Building A, (c): Average utility of sellers, (d): Average cost of buyers, of Building B using Methods 1 and 2, and our method throughout the day.

increases the total cost of buyers in Method 1 (see Figure **??**b,d). As can be observed from Figure III.3, the trading prices calculated by our method are close to the average feed-in tariff prices. This is due to considering the financial benefits of sellers and buyers in calculating the energy trading price, which encourages sellers to sell their excess energy to their neighbors and supports buyers to buy energy at a lower price than the grid tariff price. Therefore, all sellers and buyers make significant financial benefits when utilizing our method.

### III.5.2.2 Energy Justice Analyses

The proposed framework is specialized into two cases with the aim of analyzing what is fair for each building. This means that fairness in energy sharing can vary from building to building. Analyzing all three principles of energy justice in the design of energy-sharing models in Building A and B helps to understand how design choices can lead to justice. In the following, the energy allocation and trading processes in the buildings are evaluated according to the principles of energy justice.

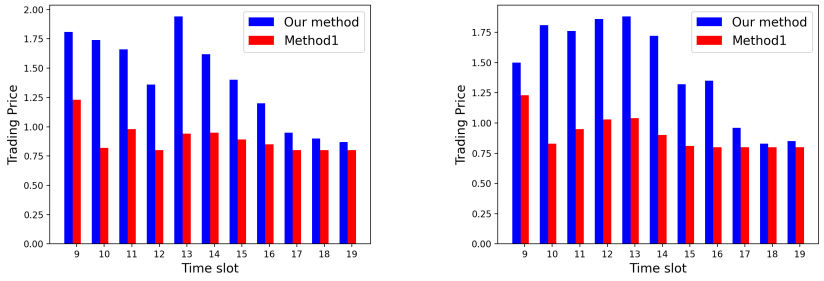



Figure III.3: (a) Energy trading prices in Building A, (b) Energy trading prices in Building B, which are computed by Method 1 and our method throughout the day.

From the perspective of recognition justice, Buildings A and B support different groups of residents with different preferences to enjoy the benefits of shared DRESs in their building. Given that each unit of Building A has already been allocated a specific share according to its unit characteristics, new residents (i.e., residents who just moved into the building) have the opportunity to use the shared DRESs of the building. Moreover, unit-owners and temporary residents (e.g., tenants) can lease the allocated share of PV panels/BESSs as long as they live in the building (e.g., units 1–4 as unit-owners and units 6–8 as tenants lease a share of PV panels from the owner of Building A), or can pay only for their energy consumption if they do not afford the lease cost (e.g., units 5, 9, and 10 in Building A pay only for their energy consumption). In the case of Building B, the building owner cooperates with the residents of the building by allowing them to install PV panels on the roof of the building. The sharing model in Building B enables residents to participate in the purchase of PV panels/BESSs either alone (e.g., units 1–5 whose owners separately buy a share of PV panels/BESSs) or in collaboration with other units (e.g., units 6, 7, and 8 whose owners collaborate in buying PV panels/BESSs). The sharing model in Building B also considers tenants whose unit owner owns a share of PV panels/BESSs and those tenants who wish to benefit from PV panels/BESSs. In this case, tenants can lease a part of the share from their unit owner (e.g., unit 4 in Building B) or just pay for their energy consumption (e.g., unit 5 in Building B).

From a distributive perspective, it should be seen how energy, profits, and costs are distributed among residents of Buildings A and B using the proposed sharing models. The sharing model of Building A enables the EMO of the building to allocate a specific share of PV panels and/or BESSs to the residents according to their unit characteristics. Accordingly, the amount of energy distributed among residents is based on the cost they pay for leasing the share of PV panels/BESSs or their energy consumption. In this sharing model, residents gain

financial profit by participating in energy trading in the building, and the EMO makes financial profit by leasing the share of PV panels/BESSs to each resident, selling energy to the residents who pay for their energy consumption, and selling excess energy available from residents who did not lease PV panels/BESSs share. The sharing model in Building B follows the distribution principle in distributing PV panels/BESSs costs among residents. This means that residents in Building B can either participate in buying PV panels/DRESs considering their ability to pay (e.g., Units 1–5 and Units 6–8 buy PV panels/BESSs separately and together, respectively) or lease a part of the share of PV panels/BESSs from their unit owner (e.g., units 4 lease the share from the unit owner). In this building, energy is distributed among residents according to their ownership factor. In relation to justice in the distribution of profits among residents in Building B, the sharing model in the building supports energy trading in which participants benefit by selling their excess energy available from their share of PV panels/BESSs or buying energy from their neighbors in the building.

With respect to procedural justice, the sharing model in Buildings A and B encourages resident participation in decision-making during energy allocation and trading processes. In the energy allocation process, residents in Building A can participate in decision-making to decide whether to lease the share of PV panels/BESSs from the building owner or pay only for their energy consumption. The residents of Building B can also make a decision on buying PV panels/BESSs separately or in collaboration with their neighbors. The sharing model in Buildings A and B also supports all stakeholders, such as sellers, buyers, and the EMO, in decision-making during energy trading. This means that sellers/buyers are given the opportunity to decide how much energy they should sell/buy to gain more profit. In addition to some factors like unit characteristics which are fixed, sellers/buyers are given the opportunity to increase the chance of selling/buying more energy by participating in previous energy trading in their building (i.e., they can increase their priority by participating in more energy trading). Moreover, the EMO of the building decides on the trading price and allocates energy to participants with the purpose of maximizing their profits.

## III.6 Conclusions

In this paper, a fair energy sharing framework (FESM) is proposed to enable fair and reliable energy allocation and trading in multi-unit buildings. Two different specializations of the framework, referred to as Buildings A and B, that followed different energy-sharing models, are presented. An energy management operator is used for each multi-unit building to coordinate the energy allocation and trading processes among all residents in the building. The processes of energy allocation and trading in our sharing model show that residents receive and trade energy fairly using the characteristics of a unit or ownership factor and priority. To certify fairness between buyers and sellers in all trading stages, this work gives both groups the opportunity to decide on their strategy by participating in a non-cooperative game to increase their financial profit. A simple trading price

mechanism is proposed to maximize the profits of sellers and buyers and simplify the trading stages. The efficiency of our method is verified in comparison with the baseline methods on real data from Austin, Texas. The results illustrate high financial profit for sellers and low costs for buyers during the day.

We also analyzed justice in the proposed energy allocation and trading processes for both cases of the framework with respect to the main principles of energy justice. From the recognition justice perspective, justice is achieved when the sharing models ensure the accessibility to the benefits of shared DRESs in the buildings for different groups of residents. For example, recognition justice is realized in the proposed sharing models by giving tenants and low-income families the opportunity to use the DRESs of their building via renting or investing in a share of PV panels/BESSs individually or in cooperation with neighbors or paying for their consumption. Justice as distribution in the sharing models results in fair distribution of cost, benefits, and energy. To reach distributive justice in the proposed sharing models, for example, some factors, such as the unit characteristics, ownership factor, and priority factor, are utilized to perform a fair distribution of energy and benefits among residents during both energy allocation and trading. Procedural justice enables all stakeholders in the sharing model to participate in making decisions on the distribution of cost/benefits, accessing the shared DRESs, etc. Procedural justice is achieved in the proposed sharing models by enabling residents to decide how to use the shared DRESs of their building (i.e., the residents can rent or invest in a share of the DRESs) and their buying or selling strategy. In sum, analyzing the main principles of energy justice in this work is useful in understanding that justice principles have to be applied in the design of energy-sharing models in the first step. These principles can be applied in different ways, and depending on the context or situation justice's definition can be different. Applying the energy justice principles in the proposed sharing models motivates the residents to use the shared DRESs of their building, which leads to high financial benefits for the building.

Future research could explore how to achieve trust among participants and how much information they should share during energy trading. Future research might also be to develop the proposed framework into an interactive tool for exploring and comparing the effects of different approaches to energy justice. It may also be relevant to study how errors in intraday (<1 h) forecasting of PV power generation may influence the trading results on seller profit and buyer cost.

Conceptualization, Sara Mohammadi, Frank Eliassen and Hans-Arno Jacobsen; Methodology, Sara Mohammadi, Frank Eliassen and Hans-Arno Jacobsen; Software, Sara Mohammadi; Validation, Sara Mohammadi, Frank Eliassen and Hans-Arno Jacobsen; Formal analysis, Sara Mohammadi; Investigation, Sara Mohammadi; Writing – original draft, Sara Mohammadi; Writing – review and editing, Sara Mohammadi, Frank Eliassen and Hans-Arno Jacobsen; Visualization, Sara Mohammadi; Supervision, Frank Eliassen and Hans-Arno Jacobsen; Funding acquisition, Frank Eliassen.

This research was funded by the Norwegian Research Council under the

SmartNEM project grant number 267967.

Data supporting reported results can be found on https://www.pecanstreet.org

The authors declare no conflict of interest.'

## Appendix .A

**Algorithm 2** Optimal strategy for buyers

1: *Input* :

- Energy demand of all buyers ($D_{i,t}$) and their priority factors ($Pr^b_{i,t}$) at time slot $t$.
- Two vectors, including buyers and their priority factors, sorted on the value of $\frac{D_{i,t}}{(Pr^b_{i,t})}$ in ascending order.

2: *Output* :

- The vector of the optimal strategy of buyers $S^b_t$ sorted in the original order.

3: *Initialization* :

- Filling index $j = 1$;
- $N_t$ = Number of buyers at time slot $t$, $M_t$ =set of buyers at time slot $t$;
- Filling width $\omega = \sum_{i \in M_t} (Pr^b_{i,t})$;
- $E^{ex}_t$ = total extra energy available from sellers at time slot $t$;
- Energy height $h = 0$;
- For exception handling $D_{N+1,t} = \infty$ and $Pr^b_{N+1,t} = 1$

4: $While(E^{ex}_t > 0)$
$if\ (\omega(\frac{D_{j,t}}{(Pr^b_{j,t})} - h) < E^{ex}_t)$:
$E^{ex}_t = E^{ex}_t - \omega(\frac{D_{j,t}}{(Pr^b_{j,t})} - h)$; $h = \frac{D_{j,t}}{(Pr^b_{j,t})}$;
$\omega = \omega - (Pr^b_{j,t})$; $S^b_{j,t} = D_{j,t}$; $j = j + 1$;
$else$
$h = h + \frac{E^{ex}_t}{\omega}$; $E^{ex}_t = 0$;
$for\ k = j : N$
$S^b_{k,t} = h(Pr^b_{k,t})$;
*End*

5: Sort the optimal strategy of buyers $S^b_t$ in original order.

**Algorithm 3** Allocating Energy to Buyers by EMO

1: *Input* :

- Strategies of all buyers ($S_t^b$) and their priority factors ($Pr_{i,t}^b$).
- Three vectors, including buyers, their strategies, and their priority factors sorted on the value of $\frac{S_{i,t}^b}{(Pr_{i,t}^b)}$ in ascending order.

2: *Output* :

- The vector of the allocated energy of buyers $AE_t^b$ sorted in the original order.

3: *Initialization* :

- Filling index $j = 1$ and $k = 2$;
- Filling width $\omega = (Pr_{1,t}^b)$;
- $E_t^{ex}$ = total extra energy available from sellers;
- Energy height $h = \frac{S_{1,t}^b}{(Pr_{1,t}^b)}$;
- The vector of all buyers' allocated energy $AE_t^b = 0$
- For exception handling $S_{N+1,t}^b = \infty$ and $Pr_{N+1,t}^b = \infty$

4: $While(E_t^{ex} > 0)$

$if\ (\frac{2S_{j,t}^b}{(Pr_{j,t}^b)} > \frac{S_{k,t}^b}{(Pr_{k,t}^b)})$ and $(\omega(\frac{S_{k,t}^b}{(Pr_{k,t}^b)} - h) < E_t^{ex})$:

$E_t^{ex} = E_t^{ex} - \omega(\frac{S_{k,t}^b}{(Pr_{k,t}^b)} - h)$; $h = \frac{S_{k,t}^b}{(Pr_{k,t}^b)}$;

$\omega = \omega + (Pr_{k,t}^b)$; $k = k + 1$;

$elseif\ (\frac{2S_{j,t}^b}{(Pr_{j,t}^b)} \leq \frac{S_{k,t}^b}{(Pr_{k,t}^b)})$ and $(\omega(\frac{2S_{j,t}^b}{(Pr_{j,t}^b)} - h) < E_t^{ex})$:

$E_t^{ex} = E_t^{ex} - \omega(\frac{2S_{j,t}^b}{(Pr_{j,t}^b)} - h)$;

$AE_{j,t}^b = S_{j,t}^b$; $\omega = \omega - (Pr_{j,t}^b)$;

$h = \frac{2S_{j,t}^b}{(Pr_{j,t}^b)}$; $j = j + 1$;

$else:\quad h = h + \frac{E_t^{ex}}{\omega}$; $E_t^{ex} = 0$;

$for\ i = j : k$

$AE_{i,t}^b = (Pr_{i,t}^b)(h - \frac{S_{i,t}^b}{(Pr_{i,t}^b)})$;

*End*

5: Sort the allocated energy $AE_t^b$ in original order.

**Algorithm 4** Optimal strategy for sellers

1: *Input* :

- Excess energy of all sellers ($E_{i,t}^{excess}$) and their priority factors ($Pr_{i,t}^{s}$) at time slot $t$.
- Two vectors, including sellers and their priority factors, sorted on the value of $\frac{E_{i,t}^{excess}}{(Pr_{i,t}^{s})}$ in ascending order.

2: *Output* :

- The vector of the optimal strategy of sellers $S_t^s$ sorted in the original order.

3: *Initialization* :

- Filling index $j = 1$;
- $N_t$ = Number of sellers at time slot $t$, $M_t$ =set of sellers at time slot $t$;
- Filling width $\omega = \sum_{i \in M_t} (Pr_{i,t}^{s})$;
- $D_t$ = total demand of buyers at time slot $t$;
- Energy height $h = 0$;
- For exception handling $E_{N+1,t}^{excess} = \infty$ and $Pr_{N+1,t}^{s} = 1$

4: $While(D_t > 0)$
$if\ (\omega(\frac{E_{j,t}^{excess}}{(Pr_{j,t}^{s})} - h) < D_t)$:
$D_t = D_t - \omega(\frac{E_{j,t}^{excess}}{(Pr_{j,t}^{s})} - h)$; $h = \frac{E_{j,t}^{excess}}{(Pr_{j,t}^{s})}$;
$\omega = \omega - (Pr_{j,t}^{s})$; $S_{j,t}^{s} = E_{j,t}^{excess}$; $j = j + 1$;
$else$
$h = h + \frac{D_t}{\omega}$; $D_t = 0$;
$for\ k = j : N$
$S_{k,t}^{s} = h(Pr_{k,t}^{s})$;
*End*

5: Sort the optimal strategy of sellers $S_t^s$ in original order.

**Algorithm 5** Determining energy for sale by EMO

1: *Input* :

- Strategies of all sellers ($S^s_t$) and their priority factors ($Pr^s_{i,t}$).
- Three vectors, including sellers, their strategies, and their priority factors sorted on the value of $\frac{S^s_{i,t}}{(Pr^s_{i,t})}$ in ascending order.

2: *Output* :

- The vector of the allocated energy of sellers $AE^s_t$ sorted in the original order.

3: *Initialization* :

- Filling index $j = 1$ and $k = 2$;
- Filling width $\omega = (Pr^s_{1,t})$;
- $D_t$ = total demand of buyers at time slot $t$;
- Energy height $h = \frac{S^s_{1,t}}{(Pr^s_{1,t})}$;
- The vector of all buyers' selling amount of energy $AE^s_t = 0$
- For exception handling $S^s_{N+1,t} = \infty$ and $Pr^s_{N+1,t} = \infty$

4: $While(D_t > 0)$

$if\ (\frac{2S^s_{j,t}}{(Pr^s_{j,t})} > \frac{S^s_{k,t}}{(Pr^s_{k,t})})$ and $(\omega(\frac{S^s_{k,t}}{(Pr^s_{k,t})} - h) < D_t)$:

$D_t = D_t - \omega(\frac{S^s_{k,t}}{(Pr^s_{k,t})} - h)$; $h = \frac{S^s_{k,t}}{(Pr^s_{k,t})}$;

$\omega = \omega + (Pr^s_{k,t})$; $k = k + 1$;

$elseif\ (\frac{2S^s_{j,t}}{(Pr^s_{j,t})} \leq \frac{S^s_{k,t}}{(Pr^s_{k,t})})$ and $(\omega(\frac{2S^s_{j,t}}{(Pr^s_{j,t})} - h) < D_t)$:

$D_t = D_t - \omega(\frac{2S^s_{j,t}}{(Pr^s_{j,t})} - h)$;

$AE^s_{j,t} = S^s_{j,t}$; $\omega = \omega - (Pr^s_{j,t})$;

$h = \frac{2S^s_{j,t}}{(Pr^s_{j,t})}$; $j = j + 1$;

$else:\quad h = h + \frac{D_t}{\omega}$; $D_t = 0$;

$for\ i = j : k$

$AE^s_{i,t} = (Pr^s_{i,t})(h - \frac{S^s_{i,t}}{(Pr^s_{i,t})})$;

*End*

5: Sort the vector of determined energy for sale $AE^s_t$ in the original order.

## References


[CBE17] Castellazzi, L., Bertoldi, P., and Economidou, M. "Overcoming the split incentive barrier in the building sector". In: *Publications Office of the European Union, Luxembourg* (2017).

[CBK20] Chakraborty, S., Baarslag, T., and Kaisers, M. "Automated peer-to-peer negotiation for energy contract settlements in residential cooperatives". In: *Applied Energy* vol. 259 (2020), p. 114173.

[Cic10] Cicero. *New study shows lack of government support for renewable energy communities*. 2021-05-10. URL: https://cicero.oslo.no/en/articles/new-study-shows-lack-of-government-support-for-renewable-energy-communities (visited on 11/10/2021).

[Com+15] Comodi, G. et al. "Multi-apartment residential microgrid with electrical and thermal storage devices: Experimental analysis and simulation of energy management strategies". In: *Applied Energy* vol. 137 (2015), pp. 854–866.

[Cui+20] Cui, S. et al. "A new and fair peer-to-peer energy sharing framework for energy buildings". In: *IEEE Transactions on Smart Grid* vol. 11, no. 5 (2020), pp. 3817–3826.

[Dat19] Dataport. *Dataport*. 2019. URL: https://www.pecanstreet.org (visited on 04/09/2020).

[Fin+18] Fina, B. et al. "Economic assessment and business models of rooftop photovoltaic systems in multiapartment buildings: case studies for Austria and Germany". In: *Journal of Renewable Energy* vol. 2018 (2018), pp. 1–16.

[GCG21] Gjorgievski, V. Z., Cundeva, S., and Georghiou, G. E. "Social arrangements, technical designs and impacts of energy communities: A review". In: *Renewable Energy* vol. 169 (2021), pp. 1138–1156.

[Har+17] Hart, W. E. et al. *Pyomo-optimization modeling in python*. Vol. 67. Springer, 2017.

[HL22] Huang, W. and Li, H. "Game theory applications in the electricity market and renewable energy trading: A critical survey". In: *Frontiers in Energy Research* (2022), p. 1387.

[Inê+20] Inês, C. et al. "Regulatory challenges and opportunities for collective renewable energy prosumers in the EU". In: *Energy Policy* vol. 138 (2020), p. 111212.

[Jaf+20] Jafari, A. et al. "A fair electricity market strategy for energy management and reliability enhancement of islanded multi-microgrids". In: *Applied Energy* vol. 270 (2020), p. 115170.

[JPG18] Jadhav, A. M., Patne, N. R., and Guerrero, J. M. "A novel approach to neighborhood fair energy trading in a distribution network of multiple microgrid clusters". In: *IEEE Transactions on Industrial Electronics* vol. 66, no. 2 (2018), pp. 1520–1531.

[LAG16] Lang, T., Ammann, D., and Girod, B. "Profitability in absence of subsidies: A techno-economic analysis of rooftop photovoltaic self-consumption in residential and commercial buildings". In: *Renewable Energy* vol. 87 (2016), pp. 77–87.

[Liu+14] Liu, N. et al. "A heuristic operation strategy for commercial building microgrids containing EVs and PV system". In: *IEEE Transactions on Industrial Electronics* vol. 62, no. 4 (2014), pp. 2560–2570.

[Liu+17] Liu, N. et al. “Energy sharing management for microgrids with PV prosumers: A Stackelberg game approach”. In: *IEEE Transactions on Industrial Informatics* vol. 13, no. 3 (2017), pp. 1088–1098.

[Lov+20] Lovati, M. et al. “Optimal simulation of three peer to peer (P2P) business models for individual PV prosumers in a local electricity market using agent-based modelling”. In: *Buildings* vol. 10, no. 8 (2020), p. 138.

[LZW19] Long, C., Zhou, Y., and Wu, J. “A game theoretic approach for peer to peer energy trading”. In: *Energy Procedia* vol. 159 (2019), pp. 454–459.

[McC+13] McCauley, D. A. et al. “Advancing energy justice: the triumvirate of tenets”. In: *International Energy Law Review* vol. 32, no. 3 (2013), pp. 107–110.

[Opt16] Optimization, G. “Gurobi optimizer reference manual; gurobi optimization”. In: *Inc.: Houston, TX, USA* (2016).

[Par+16] Park, S. et al. “Contribution-based energy-trading mechanism in microgrids for future smart grid: A game theoretic approach”. In: *IEEE Transactions on Industrial Electronics* vol. 63, no. 7 (2016), pp. 4255–4265.

[Pau+18] Paudel, A. et al. “Peer-to-peer energy trading in a prosumer-based community microgrid: A game-theoretic model”. In: *IEEE Transactions on Industrial electronics* vol. 66, no. 8 (2018), pp. 6087–6097.

[PC21] Pros, C. S. T. and Cons. *Community Solar: The Pros and Cons*. 2021-01-21. URL: https://www.paradisesolarenergy.com/blog/community-solar-the-pros-and-cons (visited on 12/15/2021).

[PD20] Pappalardo, M. and Debizet, G. “Understanding the governance of innovative energy sharing in multi-dwelling buildings through a spatial analysis of consumption practices”. In: *Global Transitions* vol. 2 (2020), pp. 221–229.

[Per+21] Perger, T. et al. “PV sharing in local communities: Peer-to-peer trading under consideration of the prosumers’ willingness-to-pay”. In: *Sustainable Cities and Society* vol. 66 (2021), p. 102634.

[PF05] Palomar, D. P. and Fonollosa, J. R. “Practical algorithms for a family of waterfilling solutions”. In: *IEEE transactions on Signal Processing* vol. 53, no. 2 (2005), pp. 686–695.

[Qad22] Qadourah, J. A. “Energy and economic potential for photovoltaic systems installed on the rooftop of apartment buildings in Jordan”. In: *Results in Engineering* vol. 16 (2022), p. 100642.

[RSM22] Roberts, M. B., Sharma, A., and MacGill, I. “Efficient, effective and fair allocation of costs and benefits in residential energy communities deploying shared photovoltaics”. In: *Applied Energy* vol. 305 (2022), p. 117935.

[Sar17] Sarı, R. "Energy justice-a social sciences and humanities cross-cutting theme report". In: (2017).

[SD15] Sovacool, B. K. and Dworkin, M. H. "Energy justice: Conceptual insights and practical applications". In: *Applied Energy* vol. 142 (2015), pp. 435–444.

[Sena] Sendy, A. *Find out how much it will cost to install solar panels on your home.* URL: https://www.solarreviews.com/solar-panel-cost#state (visited on 01/02/2022).

[Senb] Sendy, A. *How long does it take for solar panels to pay for themselves?* URL: https://www.solarreviews.com/blog/how-to-calculate-your-solar-payback-period (visited on 01/02/2022).

[TES] TESLA. *Powerwall.* URL: https://www.tesla.com/powerwall (visited on 01/02/2022).

[WMC22] Woo, J., Moon, S., and Choi, H. "Economic value and acceptability of advanced solar power systems for multi-unit residential buildings: The case of South Korea". In: *Applied Energy* vol. 324 (2022), p. 119671.

[Wu+16] Wu, X. et al. "Stochastic optimal energy management of smart home with PEV energy storage". In: *IEEE Transactions on Smart Grid* vol. 9, no. 3 (2016), pp. 2065–2075.

[WZ] Will, D. H. and Zuber, F. *GESCHÄFTSMODELLE MIT PV-MIETERSTROM.* URL: http://www.pv-financing.eu/wp-content/uploads/2016/11/D4.1_Germany.pdf (visited on 11/17/2021).

[Zha+19] Zhang, M. et al. "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)*. IEEE. 2019, pp. 1–6.