Understanding the Impacts of Data Integrity Attacks in the Context of Transactive Control Systems

Shuchismita Biswas

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Electrical Engineering

Virgilio A. Centeno, Chair
Vassilis Kekatos
Jaime De La Reelopez
Seemita Pal

December 11, 2018
Blacksburg, Virginia

Keywords: Smart grid, transactive energy, data integrity attacks, locational marginal price, impact metrics, reliability

Understanding the Impacts of Data Integrity Attacks in the Context of Transactive Control Systems

Shuchismita Biswas

Abstract

The rapid growth of internet-connected smart devices capable of exchanging energy price information and adaptively controlling the consumption of connected loads, has paved the way for transactive control to make inroads in the modern grid. Transactive control frameworks integrate the wholesale and retail energy markets, and enable active participation of end users, thereby playing a key role in managing the rising number of distributed assets. However, the use of internet for the communication of data among the building, distribution, and transmission levels makes the system susceptible to external intrusions. A skilled adversary can potentially manipulate the exchanged data with the intention to inflict damage to the system or increase financial gains. In this thesis, the effect of such data integrity attacks on information exchanged between the distribution systems operator and end-users is investigated. Impact on grid operations is evaluated using different categories like operational, financial, user comfort and reliability parameters. It is shown that attack impact depends on a number of factors like attack duration, time of attack, penetration rate etc besides the attack magnitude. The effect of an attack continues to persist for some time after its removal and hence effective detection and mitigation strategies will be required to ensure system resilience and robustness.

This work was supported by the U.S. Department of Energy as part of the Grid Modernization Laboratory Consortium (GMLC) program.

Understanding the Impacts of Data Integrity Attacks in the Context of Transactive Control Systems

Shuchismita Biswas

General audience abstract

Transactive energy is a framework where price-responsive loads adjust their energy consumption at a certain time according to the real-time energy price sent by the utility. Field demonstrations in recent years have shown that transactive control can effectively manage grid objectives and also monetarily benefit both the electric utility and end-users. Therefore, transactive energy is expected to make inroads into conventional grid operations in the next few years. As successful operation of such a market depends on the information exchanged among different stakeholders, a malicious adversary may try to inject false data and affect system operations. This thesis investigates how manipulating data in the transactive energy platform affects system operations and financial gains of different stakeholders. Understanding system behavior under attack conditions will help in formulating effective detection and mitigation strategies and enhancing system resilience.

Acknowledgments

I would like to express my heartfelt gratitude to my academic advisor and committee chair Dr. Virgilio Centeno, who has been a source of immense support and inspiration throughout my time at Virginia Tech. His encouragement has been instrumental in my decision to further continue my academic journey towards a doctoral degree.

I would also like to thank Dr. Vassilis Kekatos and Dr. Jaime De La Ree for the guidance I received as a graduate student and the nurturing ambience I have grown to enjoy in the Power Lab. Their classes have not only deepened my understanding of power systems but also sharpened my critical analysis skills.

I would like to thank Dr. Seemita Pal for her mentor-ship, research inputs and above all her friendship. Without her support and collaboration, my summer at PNNL would have been quite dull and this thesis would not have seen the light of day. I would also like to extend my gratitude to Dr. Siddharth Sridhar, whose inputs have been valuable in shaping up this thesis. My thanks go to the researchers at PNNL whose work provided the foundation that this thesis is built on.

I cherish the friendship of my fellow graduate students Manish, Aditie, Rounak, Lasya and Akshay. We started our journey together at Blacksburg and have since charted our different paths, but the first semester here continues to be some of my favorite memories. Also Manish, our coffee sessions always provide me fresh insights into Mathematics and life. Sherin, swapping stories has always been a pleasure.

My life in Blacksburg would have been quiet difficult without a bunch of wonderful people, who despite what a certain lady in Niagara thinks, I did not know from back home. Prosenjit Da, you are the life of any party. Ranit, Arit, Pal, GB and Sreeya Di- you are the best roommates and profound armchair philosophers I could have wished for. Lekha, thanks for getting us up to date on the thoughts and ways of the next generation. Srijan Da, your facebook updates are a source of much knowledge. Shreya Di and Abhijit Da, you are among the best people I have ever met and how you balance responsibilities and make time to enjoy the little joys of life is a lesson worth learning. Gubli always brightens up my day. Poorna Di and Gupta Da, thanks for being there. And Shantanab, you are integral to everything, thanking you would be sort of audacious.

My friends Sarika, Nikhil and Daksh have always been a support system I have always banked on. And though we live in different continents and cannot spend hours hanging out at Nescafe anymore, I know that they will always have my back. Pooja, Shubhada and Vasu, my friends and colleagues, are people I have shared a journey of self-discovery with and am thankful for the support and encouragement I have received.

And last but not the least, I would like to thank my family- Ma, Baba and Tuntai for letting me live life on my own terms and follow my dreams.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The power grid is evolving to accommodate advancements in renewable energy, changing user preferences and load growth due to increasing population and initiatives like the electrification of transportation. Traditionally, the electric utility had been a vertically integrated monopoly that managed generation, transmission as well as distribution of electricity. This utility could be owned by the government or by investors. In the mid 1990s, the electricity market in the United States was deregulated to facilitate entry of independent generators so that competitive forces could lower prices and increase system efficiency. At present, there are significant efforts to incentivize the integration of Distributed Energy Resources (DER) that can be leveraged to alleviate transmission congestion, meet local demand and also reduce dependency on fossil fuels. Advancements in the field of communication and automation has brought about a paradigm shift in the way utilities operate, paving way for the smart grid. The smart grid envisions better control, monitoring and protection of grid assets through near real-time information exchange and increased awareness.

One of the recent focus areas in energy research is transactive control of energy markets, where a highly coordinated self-optimizing performance of grid resources is desired. The aim is to unite suppliers, buyers and service providers under one market platform umbrella to address both local and regional grid objectives. Some advantages envisioned in the *Transactive Energy (TE)* ecosystem include better incentives for DER adoption, increased grid reliability, efficiency and flexibility as well as better utilization of controllable grid assets. However, the TE system is very complex and actions can potentially lead to unintended consequences. Therefore, any TE framework needs to be evaluated from both economic and control perspectives. Improper control can not only impact financial interests of the stakeholders, but also cause reliability and stability issues.

Since successful operation of a TE market is contingent on periodic information exchange among its different stakeholders, any attempt to manipulate this information can adversely affect the system performance both from an economic and operations perspective. It is well recognized that the introduction of network-connected devices and their communication in-

frastructure will introduce new vulnerabilities into the grid and the grid has to be resilient against attacks that seek to exploit these vulnerabilities. To formulate effective defense strategies, one must first understand how unauthorized cyber intrusions can affect the operation of TE. In this thesis, we focus specifically on understanding how attacks that target the energy prices sent from distribution system operators to end-users affect grid operations. Different data integrity attacks are simulated on a IEEE 14-bus model and their impact is analyzed using several parameters.

This chapter briefly discusses TE and its principal features. Motivations for present work and its contributions are also elaborated on.

1.1 What is transactive energy?

Transactive energy is defined as *"a system of economic and control mechanisms that allows the dynamic balance of supply and demand across the entire electrical infrastructure using value as a key operational parameter"* [1]. This value signal is price-like in that it does not necessarily have to be the actual price of electricity. It is a single shared signal that is formulated considering both local and regional operational objectives. Responsive demand assets i.e. devices which are capable of adjusting their consumption in response to real-time information can bid into and are controlled by this value signal. Typically, in a hierarchical TE framework, demand is communicated from the end-users towards generation in an upstream direction while value is communicated from generation towards end-users in a downstream direction. However, any node in the hierarchy can communicate both value and demand [2].

There have been a few TE pilot demonstration projects in the industry and hence its definitions are kept broad enough to accommodate diverse smart assets, loads, consumers, prosumers and communication technologies. Advanced Metering Infrastructure (AMI) that facilitates bidirectional communication among transmission and distribution system operators as well as end-users has been instrumental in the pilot demonstrations of TE. Targeted deployment of Home Energy Management (HEM) systems and enhanced Programmable Communicable Thermostats (ePCTs) have proved effective in achieving peak-shaving and actively adjusting residential cooling in response to energy prices [3]. In recent years, the effectiveness and feasibility of transactive control has been demonstrated through the Olympic Peninsula [4] and American Electric Power (AEP) Ohio gridSMART [3] projects. The gridSMART project designed, developed, deployed and evaluated a Real-Time Pricing scheme with a double auction mechanism (RTP_{da}) [3]. The Olympic Peninsula Project successfully demonstrated that transmission feeder constraints can be managed within a transactive control framework. The project also concluded that automation was effective in getting consistent responses from supply and demand resources [4]. Although both these projects used a hierarchical structure for implementing TE, peer-to-peer strategies for resilient transactive control have also been proposed in literature [5]. In this thesis, the TE architecture from the gridSMART project is used as reference.

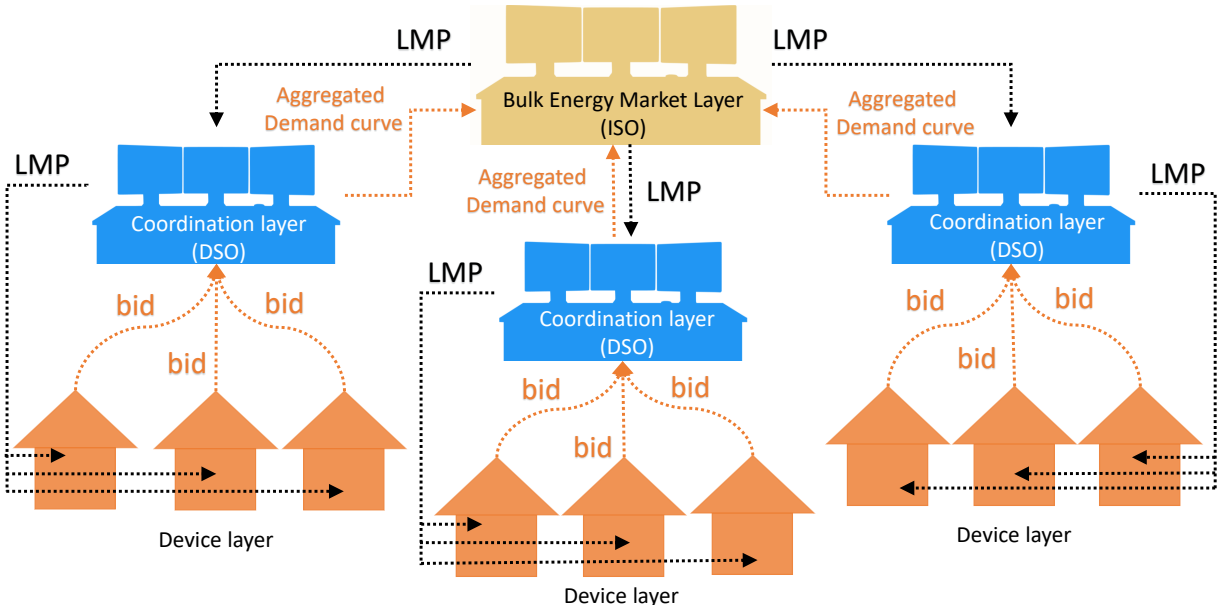


Figure 1.1: Hierarchical Transactive Energy Architecture

A schematic description of the hierarchical TE architecture used is shown in figure 1.1. There are three layers in the structure - i) the device layer, ii) the coordination layer, and iii) the bulk energy market layer. At the beginning of each market period, the bulk energy market layer calculates the Locational Marginal Price (LMP) for the period and communicates it to the coordination layer. The coordination layer sends the LMP to all downstream devices. Based on the received LMP, each device adjusts its energy consumption and sends a bid back to the coordination layer expressing their need for energy in the next market period. The coordination layer collects all the downstream bids to form an aggregated demand curve. This aggregated demand curve is then sent back to the bulk market. The LMP calculated for the next market period depends on aggregated demand curves received from the coordination layer. It can be assumed that the device layer is implemented at the end-user level, the coordination layer at the Distribution System Operator (DSO) level and the bulk market layer at the Independent System Operator (ISO) level. The TE architecture and market mechanism is explained in further detail in section 2.2.

1.2 Motivation of cyber attacks on power systems

The energy infrastructure is a critical asset for any nation. Its disruptions may lead to outages that impact several sectors and interrupt emergency services. In the United States, the energy sector has been identified as one of 16 critical infrastructure sectors by the Department of Homeland Security [6]. The other critical sectors also need reliable power supply for normal operation, making the power sector a prime target for malicious agents. At present,

the power grid assets consist of both legacy devices without internet connectivity and Intelligent Electronic Devices (IEDs) equipped with bidirectional communication that allow resources distributed over large geographic expanses to be controlled remotely. The grid is steadily evolving towards the vision of a 'smart' one which needs the conventional physical infrastructure to be rapidly overlaid with fast communication networks, network-connected sensors and control elements. As the proliferation of such communicable devices grows in the smart grid, so does its vulnerability to cyber intrusions.

An intruder who targets the power grid may have different motivations. *Hacktivists* (ideologically motivated hackers) might want to make socio-political statements. Hobbyist hackers might want to test their skills or expose security shortcomings. Disgruntled employees might want to cause nuisance. Financial gains (energy theft, DER fraud, financial extortion etc) and industrial espionage are other possible motivations that drive intruders. The large number of electric devices can also potentially attract intruders who want to use the grid as a launchpad for future multi-pronged internet attacks [7]. The worst threat is from highly motivated, well-funded and resourceful intruders who are capable of launching large scale coordinated attacks aiming to cause disruptions, physical destruction and prolonged outages. This class of intruders comprises of politically motivated enemy nation states or terrorist cells [8].

One of the first confirmed cyber attacks against the power grid occurred in Ukraine in December 2015. Intruders used a version of the BlackEnergy malware to gain access to the IT infrastructure [9] of a distribution utility and compromised the SCADA distribution management system (DMS) causing outages that lasted for 3-6 hours. At the same time, outage report calls were prevented from reaching call centers by Denial of Service (DoS) attacks. The Ukraine attack was a well-orchestrated intrusion and affected about 230,000 consumers [8]. Ukraine faced another cyber attack in 2016 when a transmission systems control center was compromised using the *Industroyer* or *Crash Overrride* malware [9]. The number of cyber events in the US grid including phishing campaigns to steal authentication credentials from authorized users has been on the rise in recent years. In view of the above, there has been substantial research and legislative efforts to increase the cyber resilience of the US power grid [9].

1.3 Why are cyber attacks likely in a transactive energy framework?

A successful implementation of transactive control depends on the information exchanged between its diverse stakeholders- utilities, aggregators, smart buildings, DERs, Virtual Power Plants (VPPs), Load Serving Entities (LSEs) etc. This requires large scale deployment of IEDs capable of bidirectional communication which expands the attack surface for the power grid. Till date, the threat of cyber intrusions is poorly understood by utilities and

manufacturers often add security measures to devices only as an afterthought, making them extremely vulnerable to unauthorized access. As much of the information (for example, bids from residential customers being sent to aggregators) may be exchanged over the internet, these devices can be potential candidates for manipulative attacks. Manipulating the demand or price even in small regions can be of interest to different agents. For example, a DER might benefit from artificially hiked LMP because it can sell energy at a higher price, thereby increasing its profit. Similarly an artificially lowered LMP can discourage DERs from injecting power into the grid, which in some cases might lead to generation shortage. A false low LMP can also lead to a sudden increase in load since responsive loads might increase their consumption in response to a price drop.

1.4 Need to study impact of cyber attacks in transactive control

Transactive energy is envisioned to accomplish a number of goals including integration of DER, flattening load profiles, peak shaving and improvement in reliability while ensuring monetary benefits for both utilities and end-users. However, in light of the cyber vulnerabilities present in such a system as discussed in the previous sections, it is apparent that substantial efforts must be invested in ensuring the cybersecurity of a TE ecosystem. In order to formulate effective defense and mitigation strategies, it is first necessary to fully understand how an attack can affect grid operations. To that end, this thesis studies the impact of data integrity attacks on the value signal in TE. Impact is evaluated using different operational, financial, user-comfort and reliability parameters.

1.5 Contributions of thesis

Present research efforts focus on designing effective value signals for TE and has not explicitly evaluated these control strategies from a cybersecurity perspective. This thesis presents the first step in comprehensively understanding how manipulating the value signal impacts the performance of a transactive market. To this end, this thesis makes the following contributions.

1. **Discusses the cyber attack surface and attack models**: The cyber-physical aspects of a transactive control system are discussed. It is envisioned that DSOs and ISOs will use dedicated communication channel to exchange information, making them more secure and harder to manipulate. However, the communication among residential smart controllers and DSOs will rely on the internet or cellular networks and hence, will be more susceptible to malicious attacks. This work focuses on attacks targeting

information exchange between DSO and residences, i.e. attacks aimed at manipulating bid prices and LMP. The attack models used in this work are explained.

2. **Evaluating impact of cyber-attacks in a transactive control market:** A TE market is implemented using MATPOWER, GridLAB-D and FNCS. Data integrity attacks are simulated by manipulating messages being exchanged through FNCS between the transmission and distribution system simulators. Impact observed is evaluated by looking at four categories- operational, financial, end-user comfort and reliability. It is shown that attack impact depends on a number of factors like attack duration, time of attack, penetration rate etc besides attack magnitude. We show that the effect of an attack continues to persist in the system for some time even after its removal and hence effective detection and mitigation strategies will be required to ensure system resilience against cyber attacks.

Chapter 2

The Big Picture

Although a majority of consumers in the United States are still a part of the fixed price energy market, price-responsiveness has been gradually gaining a foothold. Several states have introduced Time of Use (ToU) rates to achieve peak shaving. These pricing schemes are often aimed at large industrial or commercial customers [1]. Implementing ToU rates requires sophisticated interval meters that can distinguish between peak and off-peak hour usage. Increasing deployment of AMI, availability of metering devices with two-way communication capabilities and home energy management modules that can automate customer responses are some promising initiatives that are accelerating ToU adoption rate [4].

There have also been efforts to offer real-time-pricing contracts to large consumers. However, these schemes employ long time intervals and do not receive feedback from end-users in real time i.e. there is no visibility of the actual amount of controllable load present in the market at any given instant. Demand is aggregated from users in a slower day-ahead market. In fact, there is no uniform organized wholesale market that exists throughout the US; regional markets vary greatly from each other due to different deregulation policies and different bilateral contracts among key market players. Hence, there is a long way to go before we can expect a market completely driven by real time demand and price information.

Against this backdrop, researchers have undertaken various pilot projects to show how automation and communication technologies can be leveraged to convert passive loads and DERs to market driven resources that interact with each other to meet grid objectives and also increase economic and performance efficiency. This chapter describes some recent field demonstrations that show the effectiveness and feasibility of a transactive energy market. Previous work which have concentrated on cyber attacks within a TE ecosystem are also discussed.

2.1 Findings from transactive energy trials

2.1.1 Olympic Peninsula Project

The Olympic Peninsula Project (OPP) [4] was part of the larger Pacific Northwest GridWise Testbed Demonstration led by Pacific Northwest National Laboratory (PNNL) for the US Department of Energy (DOE) and Pacific Northwest GridWise^{TM} Testbed, a group comprising of Bonneville Power Authority (BPA), PNNL and several utilities in the Northwest region. The Olympic Peninsula region was chosen for the demonstration because it was being served by a radial transmission system and also experiencing a steady increase in population, placing stress on the transmission feeder. Planning for the project began in 2004 and field data was collected in the 2006-2007 period.

The primary objective of OPP was to test whether two way communication of price and demand information among the grid and distributed resources could be used for effectively dispatching power. Another goal was to check if conventionally passive loads at the user end and idle DERs could be actively engaged to manage power flow through a constrained feeder distribution circuit. In other words, the project checked if resources at user end could be leveraged to alleviate the stress on the distribution system during peak demand periods. OPP also checked the feasibility of reducing market clearing time interval to 5 minutes.

The project used commercial building space conditioning, municipal water pumping loads, diesel generators, microturbines, residential thermostats and water heaters as participants in the two-way market. Response of the resources to the market price was automated. The residential customers could choose a degree of their price responsiveness by selecting a comfort setting for their thermostats. In case of commercial and municipal entities, the degree of price responsiveness was pre-negotiated. Each participant also had the ability to temporarily override the automated response of their loads or generators. A shadow market was created for providing incentive signals that encouraged operating DER and demand-response (DR) resources to alleviate local distribution congestion.

Key Learnings

Some key observations made in course of the project are listed below [2, 4].

- The feeder constraint was successfully managed for the duration of a year. During each season a constraint was imposed limiting energy imports from an external wholesale energy provider to a certain value. The additional demand was successfully catered to by local distributed generation. For the entire project year, energy imports exceeded the preset limit for only one 5-minute interval.
- The project found that residential thermostatically controlled loads on real-time pricing

contracts shifted their peak consumption to early morning periods i.e. spaces were pre-cooled or pre-heated when energy was the least expensive. The thermostat controllers did not have any explicit in-built prediction mechanisms and were solely controlled by the price signal itself.

- The project reported a 5% reduction in peak load when energy import was capped at 750 kW. This reduction was 20% when the feeder constraint was 500 kW.
- Bid and price information were exchanged over the internet and the market was cleared centrally every 5 minutes at PNNL. Although communication between the distributed resources and the market headquarters were sporadic at times, the market operated without significant hindrance even when the field resources reverted to default operating options.
- The project concluded and asserted the fact that automation was effective in getting consistent response from supply and demand resources.

2.1.2 AEP Ohio gridSMART Demonstration Project

The AEP Ohio gridSMART Demonstration Project [3] showed how secure inter-operable smart grid technologies can be used to enhance distribution system efficiency, reliability and also reduce peak demand and fossil fuel requirements. One part of the gridSMART project was checking an experimental Real Time Pricing scheme with double auction (RTP_{da}) mechanism. The RTP_{da} program offered a complete demand response system where consumers could optimize their consumption according to real time energy prices and comfort settings on their thermostats. The project aimed to evaluate the economic and operational benefits to both consumers and utilities that such a pricing scheme could provide, whether the scheme was effective enough to manage distribution load during congestion events and also if the scheme was scalable.

Any consumer who participated in the RTP_{da} program needed to have an AMI meter, a Home Energy Manager (HEM) and an enhanced Programmable Communicating Thermostat (ePCT). The HEM managed communications among the ePCT, the AMI meter at customer premises and the Smart Grid Dispatch (SGD) system at AEP's control center. The ePCT settings were customizable and was used to control HVAC temperature setting in real time. Each ePCT also had a display where customers could view the estimated price for electricity at any given market interval. Auction process for the markets was managed within the SGD.

Double Auction Process

Double auction is a process where bids to buy and sell a commodity (power) are submitted to the auctioneer (SGD) simultaneously and the auctioneer determines the market clearing price

by the intersection of the supply and demand curves. In the gridSMART demonstration, the bids to buy energy were formulated by the residential HEMs. During each market period, the residential customer could indicate a desired, a maximum and a minimum temperature set-point. The 15 minute price of electricity was sent to the HEMs from the SGD at the beginning of each market period and accordingly the HEMs sent back a bid. The SGD aggregated bids from all households to form a demand curve. The supply curve was calculated considering different factors like the 5 minute wholesale electricity price provided by PJM. The market clearing price (prevailing energy price for the next 5 minutes) would be decided based on the intersection of the supply and demand curves thus formed. The market structure used in this thesis uses the gridSMART market architecture as reference.

Key Learnings

Key learnings from the gridSMART demonstration are summarized below [3].

- Double auction mechanism for TE was successfully demonstrated. It was seen that during congestion events, higher energy prices led to reduction in demand from RTP_{da} participants, thereby reducing peak load.
- Cellular technology was used for communicating bids and prices. Due to limited cellular coverage in some areas, consumers from those areas could not participate in the RTP_{da} program. Therefore, although cellular technology is arguably the easiest communication media, alternate options have to be evaluated for larger scale deployment.
- An overall positive satisfaction report was obtained from consumers who participated in the RTP_{da} program.

2.2 Standardized hierarchical TE architecture

Building on the findings of the OPP, a standardized hierarchical TE node structure is formalized in [2]. The nodes and the functional signal pathways between them are defined. The inputs, outputs, and functional responsibilities of each node are fully generalized and hence the proposed approach becomes applicable to a wide set of responsive assets and operational objectives. A node is defined as a physical point where demand maybe aggregated or predicted. The demand capacity is communicated from the end users towards generation in an upstream direction while the value signal propagates from the generation towards the end users. However, any node along the hierarchy can inject both demand and value information. Any node can manipulate the value signal to account for local objectives before passing it further downstream. For example, in anticipation of a congestion event, a substation node can increase the energy price to discourage consumption. In order to address all local objectives within the power grid, it is important to include all nodes between the generation

and end-users in the hierarchy. Skipping over or ignoring nodes within the hierarchy might result in control approaches that do not adequately address or even violate local operational constraints.

In addition to discussing TE in the context of a framework of regulatory and policy considerations, [1] also puts forth revenue and business models and elaborates on the general cyber-physical considerations important in implementing TE applications. Two different business models are identified- volume based (targeting larger number of customers for a large number transactions with small dollar-amounts) and customized solutions (targeting smaller number of customers for few high dollar-value transactions). Reliability and ancillary services that stakeholders might be interested in are also discussed. DSOs might want access to reactive power support and ISOs might want access to services from DERs during peak congestion events.

An important contribution of [1] is a discussion on those aspects of TE that operate in the cyber domain. Since the TE framework envisions a highly coordinated self-optimization platform involving information exchange among all stakeholders, the cyber-physical elements of the power grid need to be equipped with secure and flexible information gathering, exchange and processing capabilities. Evidently, the integration of Information Communications Technology (ICT) with the existing grid infrastructure introduces new vulnerabilities for cyber-attacks, which may potentially be exploited by malicious agents for financial gain or disrupting service. These vulnerabilities need to be investigated in order to devise effective detection mechanisms and counter-measures.

2.3 Previous work studying cyber attacks on a TE platform

Seamless operation of a transactive market needs a resilient cyber infrastructure. In the gridSMART demonstration, the HEMs used Secure Sockets Layer (SSL) encrypted communications to connect with the SGD via cellular networks. A unique security certificate was created for every HEM which had to be verified before any communication took place [3]. In the OPP, messages were exchanged over the internet [4]. Present research focuses on designing effective value signals for the TE framework and has not explicitly evaluated these control strategies from a cybersecurity perspective. There has been some work on modeling and analyzing different attacks for dynamic pricing schemes in smart grids. Scaling and delay attacks on pricing signal identified in [10] are extended to include arbitrary attacks devised by resourceful attackers trying to maximize their payoff functions in [11]. [12, 13, 14] discuss unobservable or stealth attacks, in which faulty data insertion within the system noise is considered. In [15], Pasqualetti et al consider a more generalized stealth, dynamic false data and replay attack scenarios. These results cannot be directly extended to TE as the closed feedback loop nature of TE is not accounted for.

In [16], the authors present some preliminary analysis of how cyber attacks can affect the operation of a simulated TE system. The security concerns discussed include data manipulation, centralized failure, breach of confidence and lack of availability. A 9-bus bulk power system with 4 generator units, 30 single-phase homes with controllable thermostats, a three-phase building load and a fixed unresponsive demand is simulated using TESP (Transactive Energy Simulation Platform), a simulation platform developed by PNNL. Three different attacks are simulated - a) manipulating price caps for bids placed by houses, b) manipulating bid price and quantity signals communicated by HVAC controllers and c) attack on circuit breaker between a generator and the grid. The effect of the attacks are observed with respect to the following quantities- a) system load, b) Locational Marginal Price (LMP) and c) cooling set point of HVAC controllers for attack type a). Impact on the actual temperature inside the houses which is correlated with occupant comfort level has not been analyzed. Manipulation of the pricing signal is also not studied.

The pricing or value signal is the central control signal in a TE system that forces grid resources to act in a desired manner. Hence, it is apparent that manipulating the value signal will have significant impact on the operation of TE. This thesis provides the first focused analysis of how manipulating the value signal can affect grid operations.

Chapter 3

Cyber Vulnerabilities in Transactive Energy

In this chapter we briefly discuss cyber vulnerabilities that are probable within a TE framework. An overview of the associated attack surface is provided. Different possible attack scenarios (with an emphasis on data integrity attacks) and their motivations are also elaborated on.

3.1 Attack surface

The attack surface of an environment can be described as the sum of its different points where an unauthorized user can try to enter or extract data [7]. Evidently, smaller the attack surface of a system, more is its resilience against cyber intrusions. However, implementation of TE requires wide deployment of communicable devices, which leads to a huge expansion in the attack surface. To understand the scale of the attack surface, it is first important to appreciate the cyber-physical nature of the TE infrastructure.

TE consists of two layers- *i*) the *physical* layer made up of interconnected electrical components and *ii*) the *cyber* layer made up of communication devices and channels superimposed on the physical layer. In the physical layer, commodities (power, ancillary services etc) are delivered. The cyber layer supports information exchange among different physical components, effectively monitoring and controlling them [1]. As TE continues to evolve and deployment grows, the cyber-physical elements of the grid have to evolve too. Legacy devices have to support operations they were not originally designed for and newly deployed sensors and meters have to be inter-operable with older field devices. This might lead to security challenges since older devices might not support improved security protocols.

One of the key advantages desired within TE is the inter-operability between different aggre-

gators, utilities, retailers and LSEs, where an operator at the highest level of the hierarchy can send control signals to different utilities and further down the line to individual customer premises and customer-programmed devices can decide whether or not to respond to the signal. This would require reliable end-to-end communication capable of supporting staged data filtering, asynchronous message exchange, distributed control and decision-making. A description of the roles of different nodes in the hierarchical communication layer within TE put forth in [1] is summarized below. The number of nodes present in the lower layers is much higher than the number of nodes in the upper ones. For the purpose of present discussion, it is assumed that messages originate at the highest level and propagate downstream.

- **Regional Nodes :** At the highest level of the hierarchy, the regional node would be responsible for operations within a large geographical area with a large number of customers and energy resources. A regional node can initiate wide area TE messages and also send targeted messages to a particular geographical area, for instance, to manage congestion. This node may be implemented at the ISO level.
- **Control Area Nodes :** A control area node would consist of a control center and its Automatic Generation Control (AGC) system. This node can receive TE messages from the regional node and translate the same to be passed onto generator units within the control area, distribution utilities and customers who might have demand-response contracts. There might be hundreds of control area nodes controlled by a single regional node.
- **Distribution Nodes :** Distribution nodes operate similarly to control area nodes but there might be multiple distribution operators within a control area. These nodes are responsible for receiving messages from the upstream nodes and passing them on to their customers. Different communication methods may be used, including AMI and text messages. Number of consumers served by a node at this level may range from several thousands to several millions.
- **Supply Nodes :** A supply node can be any point where supply can be injected in the distribution level. These nodes can signify generators who are registered and have contracts for services with the regional and/or control area node and must be able to provide assured supply at a known ramp rate.
- **Building Nodes :** All customers at the distribution level are essentially building nodes. They may or may not be price responsive and might also be capable of supplying electricity to the grid.

A malicious intruder can try to access data (in transit or at rest) at any of the nodes described above. The communication channels among the regional, control area and distribution nodes might be better protected because they are fewer in number. When it comes to the distribution side of things, the number of nodes may be in the range of millions. The communication

between the building and distribution nodes might be happening over the AMI infrastructure or the internet. The sheer number of messages being exchanged expands the attack surface available to an external intruder. Also, the attack surface for AMI becomes automatically applicable to TE. An overview of the attack surface for AMI is given in [7].

An attack downstream of the DSOs is more plausible even under encrypted communication scenarios considering low cost devices, limited security features, and poor patch management to new security vulnerabilities. However, a large-scale coordinated attack targeting a large number of communication links at this level would need to be carried out to cause any significant impact to the system. On the other hand, although it would be comparatively difficult to carry out an attack upstream of the DSO, compromising even one node would have a huge impact on the system. For example, manipulating the value signal being communicated to a distribution node would impact all its downstream customers.

3.2 Different possible attacks and their motivation

Attacks might target the power grid for causing disruptions or financially benefiting the threat attacker. In this section, we discuss three broad classes of plausible attacks in the TE framework- data integrity, data availability and data confidentiality.

1. **Data Integrity Attacks :** This class of attack seeks to manipulate transmitted messages. The attacker might manipulate energy price signals being sent to the distribution system or energy bids being sent by price-responsive loads. This can have both financial and operational impacts. For instance, a DER owner might want to artificially jack up energy prices for increasing their profits. Falsely decreasing energy price during high load conditions can prompt price responsive loads to suddenly increase their consumption, thereby causing a sudden spike in power.

   Attackers may also seek to manipulate control commands. For example, the attacker can gain unauthorized access to generator units, and switch them off, leading to generation shortage, thereby driving up energy prices.

2. **Data Availability Attacks :** Communication channels maybe flooded with bogus messages leading to actual TE messages being dropped. This can stop upstream nodes from receiving response from responsive loads or control messages from reaching downstream nodes (Denial of Service). This can affect voltage and current calculations and also stop certain equipment from operating properly.

3. **Data Confidentiality Attacks :** An unauthorized user can access or delete user information. Stolen data can be used to discover information about user behavior patterns, infer when they are not at home etc which leads to privacy concerns.

3.3 Attacks included in the scope of this work

Manipulating information exchanged between market participants in TE can lead to wrong control decisions being taken potentially impacting grid performance and reliability. Hence, this thesis focuses on data integrity attacks on the messages being transmitted between distribution utilities and their customers i.e. between the coordination and device layers. Such attacks can be carried out in the following ways.

- Firstly, the adversary could manipulate the bids originating from the consumers identifying the price of energy they are willing to pay over the next cycle. This would impact the calculation of the aggregated demand curve at the DSO, thereby affecting the market clearing price.
- Secondly, they could directly manipulate the energy price (LMP) dispatched by the bulk energy market to the devices via the DSO. This could result in sub-optimal setting of thermostat, and therefore lead to unexpected energy consumption.

Our preliminary investigations revealed that manipulating the LMP has a more pronounced impact on market operations than manipulating end-user bids. Therefore, the scope of the present work has been limited to investigating scaling and ramping attacks on LMP. These attack models are described next.

3.3.1 Scaling Attacks

As the name suggests, in this type of attack, the true value of a measurement or control signal is scaled by a factor of constant magnitude. Mathematical representation of such an attack is presented below.

$$y^*(t) = \begin{cases} y(t) & \text{for t} \notin \tau_a \\ (1+\lambda) * y(t) & \text{for t} \in \tau_a \end{cases}$$

During the attack period τ_a, the true value $y(t)$ is scaled by a factor of λ to form the attack value $y^*(t)$. If λ takes a positive value, it is called a scaling up attack, and if λ takes a negative value, it is called a scaling down attack. The magnitudes of impacts due to scaling attacks - in addition to the value of λ - would significantly depend on the time of execution. This can be demonstrated by the following two extreme scenarios.

- *Scaling down during peak load* - In this scenario the LMP communicated to the end use customers are scaled down to create a perception of low-cost energy. This will result in instantaneous increased power consumption from flexible loads, thereby driving the peak load-consumption even higher.

- *Scaling up of LMP during low load* - The scaling up of LMP during low load scenarios would force flexible load to reduce/stop energy consumption. In addition to causing service interruption to flexible loads, this scenario could also further lower demand during periods of low load.

3.3.2 Ramping Attacks

In ramping attacks the true value is slowly manipulated, i.e. the factor by which the base value is scaled is changed gradually. Such attacks are stealthier than scaling attacks and maybe able to circumvent detection mechanisms since they do not abruptly change any quantity. Mathematically, ramping attacks maybe expressed as follows.

$$y^*(t) = \begin{cases} y(t) & \text{for t} \notin \tau_a \\ (1 + \lambda t) * y(t) & \text{for t} \in \tau_a \end{cases}$$

Here, τ_a represents the attack period, $y(t)$ is the true value and $y^*(t)$ is the manipulated value. λ is the ramping rate and maybe both positive or negative.

Chapter 4

Simulation Set-up

The transactive energy simulation platform used for experiments in this thesis was developed at PNNL, using different simulators for transmission and distribution systems and a co-simulation platform for integrating the two. This chapter provides an overview of the transactive control methodology adopted, and also describes our experimental setup.

4.1 Transactive Control Methodology

The hierarchical TE architecture has already been introduced in section 1.1. In [17], the authors develop a multi-layer closed-loop control system for communicating price-responsiveness of end-user loads to the bulk market. Each flexible load is provided with a controller that constructs its utility curve and also actively controls its consumption [18]. The authors show that since the bulk market becomes aware of the exact amount of price-responsive load present in the system, the *'cobweb effect'* [19] and resultant price oscillations can be avoided. Each responsive load, at the same time, is able to maximize their utility. As stated in section 1.1, we assume that the TE market works in three hierarchical layers - a) device layer, b) coordination layer, and c) bulk market layer. The bulk market collects demand curves from the coordination layer and determines the clearing price (LMP) at the intersection of the demand and generator supply curves. This LMP is then communicated downstream. The operating mechanism for the coordination and device layers is explained in further detail in this section.

4.1.1 Device Layer

Each price-responsive (also referred to as *flexible* or *controllable*) load is provided with an intelligent controller which performs two primary tasks- a) it communicates the load's utility curve to the upstream coordination layer in the form of bids, and b) it

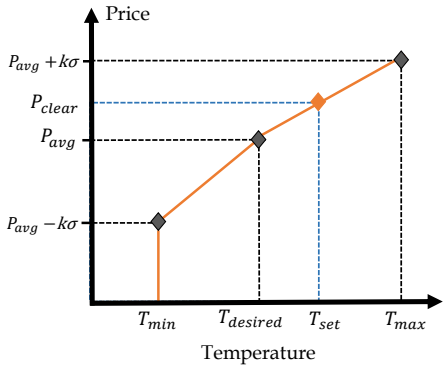


Figure 4.1: Example response curve for an air-conditioner unit. Adapted from [17]

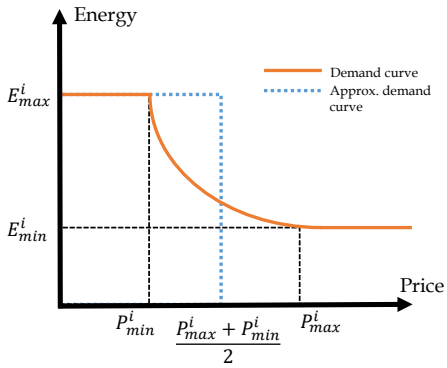


Figure 4.2: Example demand curve for an air-conditioner unit. Adapted from [17]

controls the load's energy usage by changing its settings in response to the market clearing price. In this work, the flexible loads modelled are thermostatically controlled residential air-conditioners. Therefore the intelligent controller is capable of adaptively adjusting the temperature set-point of the AC, thereby dictating its energy usage.

For each AC load, two curves are defined [17, 20]-

- **Response Curve:** This curve expresses the relationship between the local cooling set-point and marginal utility. The response curve helps in constructing the bid to be sent to the coordination layer and also determines the new temperature set-point once clearing price is received from the market.

  An example of a response curve for an AC unit is shown in figure 4.1. For a particular device, this curve is constructed using some user-defined parameters. The user defines a desired temperature for their space ($T_{desired}$) and the range that the set-point is allowed to vary in (T_{min}, T_{max}). In figure 4.1, P_{avg} and σ represent the mean and variance of market clearing price over a period of 24 hours. P_{clear} is the market clearing price or LMP for a period. k is determined by the user's relative preference for savings over comfort. If the user indicates preference for comfort over savings, the value of k is low and the response curve becomes increasingly vertical. Similarly, if the user prefers to maximize savings at the cost of comfort, the value of k is high and the curve tends to become horizontal. As is evident from figure 4.1, if the LMP for a period is higher than the average price over the last 24 hours, the controller raises the temperature set point over $t_{desired}$ and vice versa.
- **Demand Curve:** The demand curve expresses the relationship between a load's utility and its energy consumption and thereby determines how the controller constructs a bid for the next market period. To construct the demand curve, first the device's utility is mapped to its cooling set-point (response curve) and

then the indoor temperature is mapped to its energy consumption. This relationship between temperature and energy consumption can be determined using an Equivalent Thermal Parameter (ETP) model, as described in [21].

Figure 4.2 shows an example demand curve for an AC unit i. Theoretically, the unit i can consume some amount of energy in the range (E^i_{min} ,E^i_{max}). If the LMP is P^i_{min}, the unit would stay on for the entire market period and if the LMP is P^i_{max}, the unit would stay off for the entire market period. However, there is no closed form expression for the curve between P^i_{min} and P^i_{max}. Therefore the bid sent by unit i to the coordination layer is constructed using an approximate demand curve. The demand curve is approximated by a step function and E^i_{min} is assumed to be 0. The bid thus constructed has a demand quantity(Q^i_{bid}) and a price (P^i_{bid}) given by (E^i_{max} , ($P^i_{max} + P^i_{min}$)/2). This bid is then sent to the DSO in the coordination layer.

4.1.2 Coordination Layer

The coordination layer at the DSO level collects the individual bids from downstream loads and forms an aggregated demand curve to be sent to the bulk energy market. As explained in section 4.1.1, the bid received by the DSO at the beginning of each market period consists of a price and a quantity. The DSO first sums up all the received bids to form a marginal demand curve (Equation 4.1.)

$$P_{marginal}(Q) = \begin{cases} \sum_{n=0}^{n=N(Q)} P^i_{bid} & \text{if } P^i_{bid} < P_{cap} \\ P_{cap} & \text{if } P^i_{bid} \geq P_{cap} \end{cases} \tag{4.1}$$

Here $P_{marginal}(Q)$ represents the marginal price curve as a function of the demand quantity Q and P^i_{bid} represents the price bid submitted by controllable unit i. $N(Q)$ represents the number of bids submitted at demand Q. The market cap for bid prices is given by P_{cap}. The resultant demand curve (figure 4.3) shows how much each device is willing to pay to run for the next period. In this figure, the yellow region shows the devices which have bid at market cap i.e. devices which will stay on during the next period and are no longer controllable. The DSO then forms an adjusted marginal demand curve by removing the fixed loads. The marginal demand curve is subsequently converted to a demand curve $P(Q)$ by integrated over the marginal curve. Since in this case the bids are discrete quantities, a summation is taken as per equation 4.2. A quadratic curve is fit on this demand curve and this approximate demand curve is

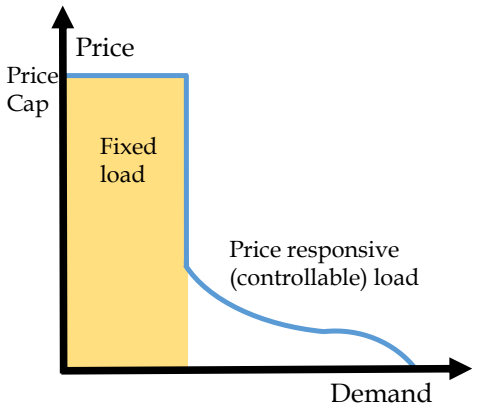


Figure 4.3: Marginal demand curve constructed by DSO after collecting individual bids from end users. Adapted from [17]

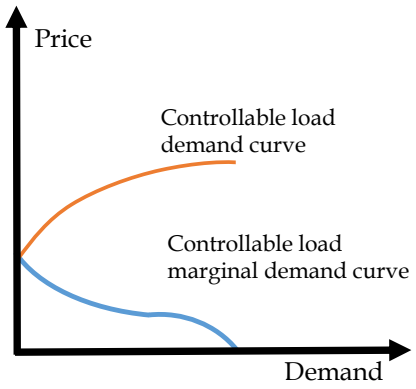


Figure 4.4: Marginal demand curve and corresponding demand curve for controllable loads. Adapted from [17]

submitted to the ISO as the price-responsive demand curve for the next market period.

$$P(Q) = \sum_{q=0}^{q=Q} P_{marginal}(Q) \tag{4.2}$$

However, it must be remembered that majority of the load present in each distribution circuit is not controllable and all fixed loads may not interact with the DSO through bids. The DSO estimates the amount of fixed load present in the system using current measurements. When being submitted to the wholesale market, this fixed load's price curve is a vertical line on the price- quantity plane where only the quantity must be defined.

4.2 Simulation Framework

The transactive control methodology discussed above is challenging to simulate since it spans both the transmission and distribution domains. In order to appreciate the electrical behavior of both the transmission and distribution systems operating together in an integrated retail market scenario, domain specific simulators have been used for transmission and distribution, which talk to each other in a co-simulation environment. The co-simulation platform used is FNCS (Framework for Network Co-Simulation) [22] which allows supported simulators to exchange messages in a synchronized manner. In this way, results obtained by one simulator affects the calculations of the other. This synchronized and uninterrupted exchange of information provides a comprehensive

view of the state of the interconnected electrical system that would be impractical to achieve by running the simulators independently.

Here, MATPOWER and GridLAB-D have been used as the transmission and distribution system simulators respectively. In addition to providing conventional distribution system functionality, GridLAB-D also supports residential thermodynamic models with integrated control and weather sensitivity, making it an ideal choice for this work. At an instant, MATPOWER solves a transmission power flow to produce a unique voltage for each node in the network. GridLAB-D simulators attached at these nodes use the voltages as substation input voltage. Each GridLAB-D simulator can now provide a new load value that MATPOWER uses during its next power flow solution. At the beginning of every market period, MATPOWER performs an AC OPF (Optimal Power Flow) based on generator cost functions and the demand curve provided by GridLAB-D simulators. The LMP thus determined is communicated to the buildings in GridLAB-D, and accordingly price-responsive air conditioning loads adjust their set-points. AC set-points may also be affected by changes in the modeled external environment, which lead to updating of the thermodynamic models of residences. In the case studies performed, MATPOWER sends GridLAB-D voltage information every 60 seconds and LMP is recalculated at the market every 5 minutes. Distribution power flows are solved by GridLAB-D every 15 seconds. The market operation cycle is run every 5 minutes of co-simulation time. Each price-responsive load formulates a bid and sends it to the DSO 30 seconds before market clearing. The DSO sends an aggregated demand curve to the transmission system 15 seconds prior to market clearing. This flexibility in load is accounted for by the transmission system as it formulates an AC OPF problem. The AC OPF is solved at the beginning of the next 5-minute market period. An updated set of LMPs for each node in the transmission network is calculated and communicated to the DSOs.

The transmission grid used is a modified version of the IEEE 14-bus model, as shown in figure 4.5. Bus voltages are specified to be 135 kV. Bus 1 is considered to be the swing bus. At each of the load buses, 7.2 kV R3-12.47-1 prototypical feeder models (GridLAB-D instances) are attached [23]. These models represent heavily populated urban areas with weather representative of arid regions of the U.S. Typical Meteorological Year 3 weather data have been integrated in the simulated distribution system environment to ensure realistic experiment conditions. Less than 10% of the loads on these feeders are price-responsive and represent residential air-conditioners. DERs have not been considered. The loads are price-takers i.e. if an individual load changes its behavior, the operation of the remaining system is not significantly impacted. In order to recreate realistic transmission level load, each of the load buses also has some fixed loads that follow typical distribution systems daily load profiles. Implementation of the hierarchical transactive control in the co-simulation framework is schematically represented in figure 4.6. Cyber attacks have been simulated in the experiments by manipulating data exchanged at FNCS ports. Experiments conducted and results

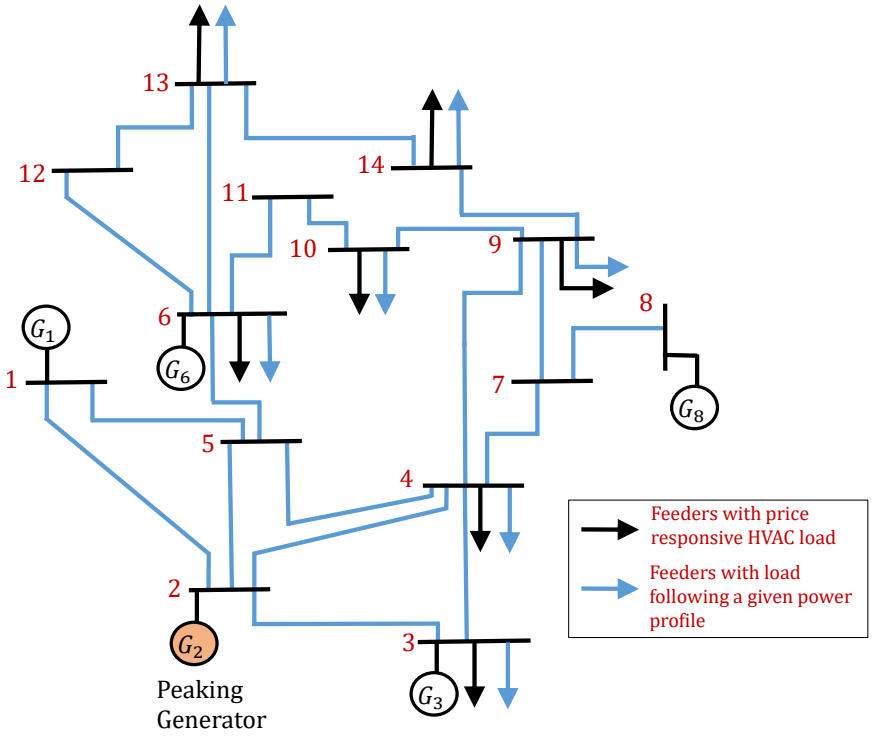


Figure 4.5: Modified IEEE 14-bus system used for simulation

obtained are explained in detail in chapter 5.

Of the generators present in the system, the quadratic cost coefficient of generator G_2 is high. The cost functions of the generators as function of energy produced (x) are given in equations 4.3-4.7. Startup and shutdown costs of generators have not been considered in the experiments.

$$C_{G_1}(x) = 0.02x^2 + 20x \tag{4.3}$$
$$C_{G_2}(x) = 0.25x^2 + 20x \tag{4.4}$$
$$C_{G_3}(x) = 0.01x^2 + 40x \tag{4.5}$$
$$C_{G_6}(x) = 0.01x^2 + 40x \tag{4.6}$$
$$C_{G_8}(x) = 0.01x^2 + 40x \tag{4.7}$$

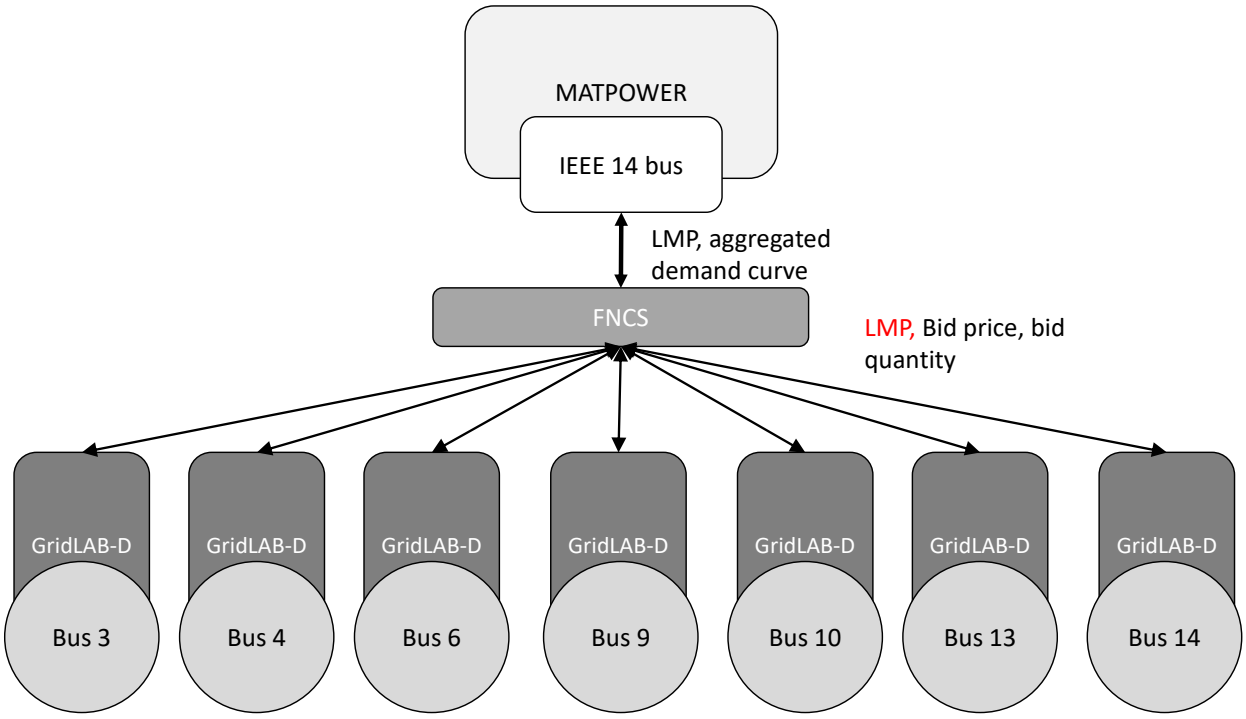


Figure 4.6: Hierarchical transactive control implemented in the co-simulation framework, using FNCS as an interface between transmission systems simulator MATPOWER and distribution systems simulator GridLAB-D

Chapter 5

Results and Discussions

The experimental set-up used for simulating data integrity attacks within a TE framework has been explained in chapter 4. This chapter describes the conducted experiments in detail and also presents an overview of our findings. The metric used for assessing impact of data integrity attacks on the simulated system is also discussed.

Weather data representative of a hot summer day (May 8, 2013) has been used for our study since the residential cooling load would be high for this day. The temperature and humidity data that each distribution circuit experiences in the simulation is shown in figure 5.1. Each simulation has been run for a 24 hour period.

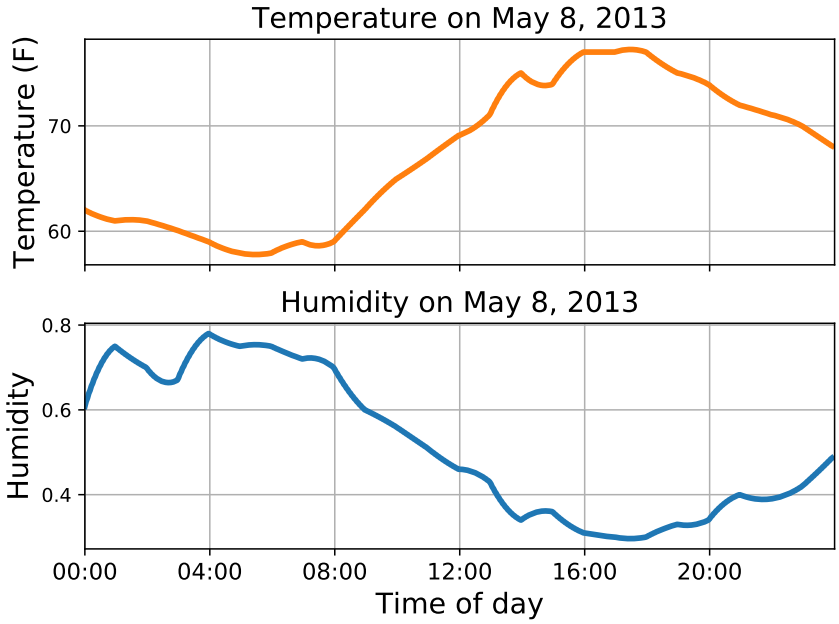


Figure 5.1: Weather data for day of experiment

5.1 Impact Assessment Metric

Four broad categories of metrics are earmarked for analyzing how data integrity attacks affect a TE system.

- **Operational:** The impacts on the underlying physical system can be estimated by comparing operational parameters (e.g. active powers, voltages) in normal and attack conditions. If during an attack an electrical component has to operate to avoid violating operation standards (for example, a voltage regulator might have to change tap positions to maintain bus voltages within the ANSI band), it also has a financial impact. This is because additional equipment operation shortens the equipment life and results in wear and tear.
- **Financial:** The impacts on the electricity bills of the households (or building owners), and the revenues of the DSO and the ISO will provide insight regarding the monetary gain or loss of each of these stakeholders.
- **Comfort:** The extent of shift from the optimal thermostat setting provides a measure of the discomfort (if any) faced by end users.
- **Reliability:** Coordinated attacks targeting a large percentage of the price-responsive loads can potentially lead to reliability impacts. Therefore, a few of the traditional reliability metrics like Momentary Average Interruption Frequency Index (MAIFI) and System Average Interruption Duration Index (SAIDI) can be used to capture reliability impacts [24]. If the attack results in damage to equipment or safety incidents, then cost of the damages should be taken into account.

5.2 Experiments

5.2.1 Case 1: Normal Conditions

To establish a baseline, electrical behavior of the system is first noted under normal conditions, i.e. when the LMP being transmitted to the end-users are not being manipulated. LMP at the load buses in normal conditions is shown in figure 5.2. It can be seen from the figure that the LMP at all buses follow similar trends but the absolute value may vary. Multiple factors dictate the LMP at a bus, including its distance from generator units, whether it is being supplied by peaking generators etc.

The active power consumption at load buses in normal conditions is shown in figure 5.3. Figure 5.4 shows the bus voltage A phase magnitudes and figure 5.5 shows the tap positions of the bus voltage regulators. It can be seen that the peak load in the system occurs at about 5 PM while the LMP is highest at about 4 PM. Evidently, the transactive control mechanism is successful in flattening the load profile to some

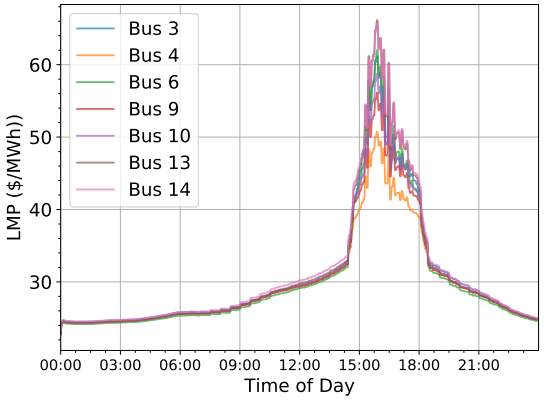


Figure 5.2: LMP at load buses under normal conditions

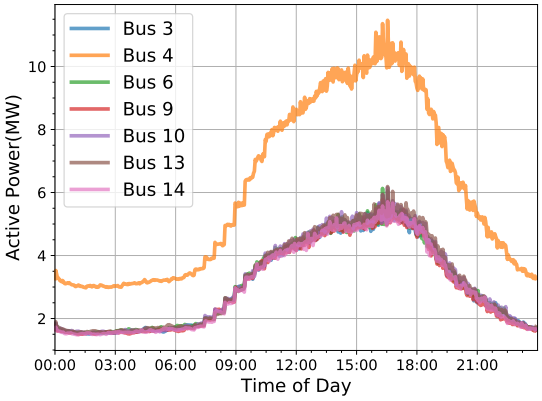


Figure 5.3: Active Power at load buses under normal conditions

extent, although the end user controllers are not prediction machines i.e. they are not able to predict future prices.

It is assumed that a DSO looks is in charge of operating the distribution circuits attached to each bus. In our study, the LMP sent from the DSO at bus 3 to its downstream loads are manipulated i.e. bus 3 is the bus being attacked. Also, at the feeder head, is the swing node, connected to a sub-station with a step-down 135 kV/7.2 kV, 10.8 MVA transformer, a voltage regulator (bandwidth = 120V, number of taps = 33) and a 0.4 MVar capacitor bank. The voltage magnitudes at user ends connected to bus 3 in normal conditions are plotted in figure 5.6. Voltage magnitudes remain within the ANSI band of 0.9-1.1 p.u.

5.2.2 Case 2: Scaling Attacks on LMP

The LMPs being broadcast from the DSO at bus 3 to the end-users connected to its distribution circuit have been manipulated to observe the effect on the behavior of the underlying physical system as well as the different market participants. It is intuitive that along with the scale of the attack, the time at which it is carried out also determines how the system behaves under attack. For instance, if the LMP during a congestion event is suddenly decreased, flexible loads respond by increasing their consumption placing further stress on the system. Similarly, if during a light load period preceding a congestion event, the LMP is increased, price-responsive loads further reduce their consumption and shift their consumption to a later period which might coincide with peak hours.

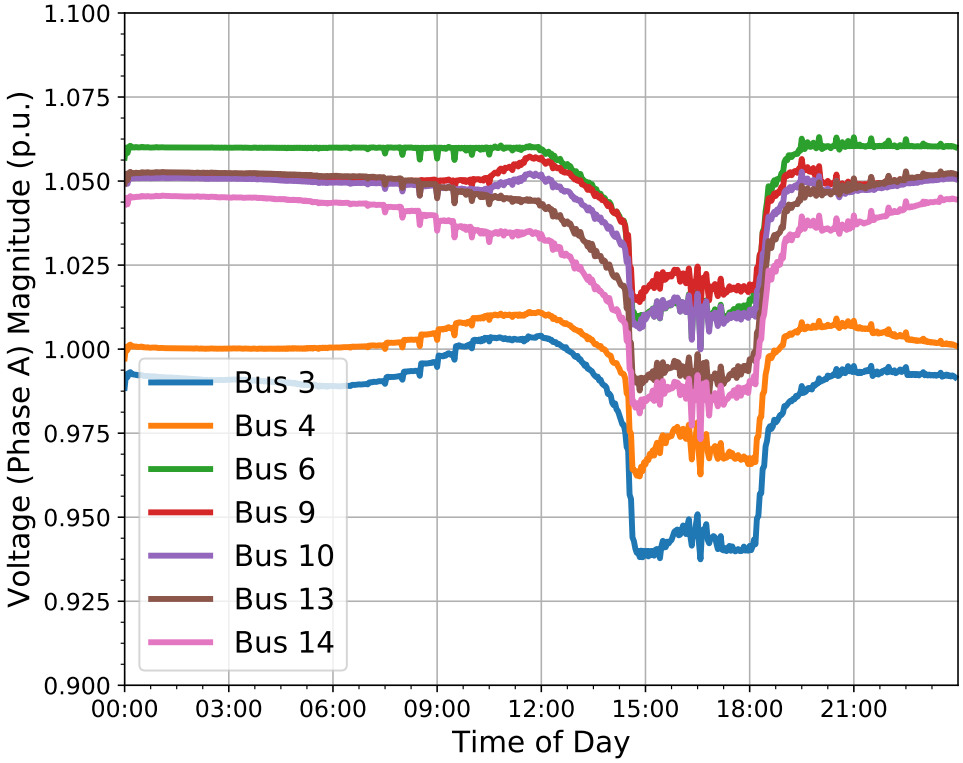


Figure 5.4: Voltage (Phase A) magnitude at load buses under normal conditions

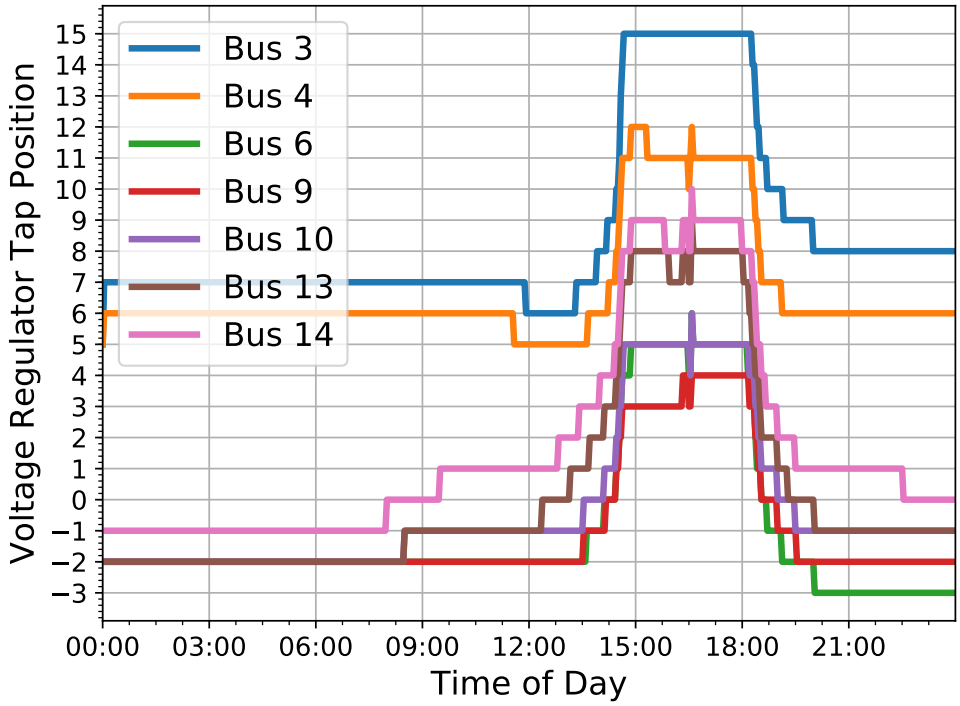


Figure 5.5: Voltage Regulator tap positions at load buses under normal conditions

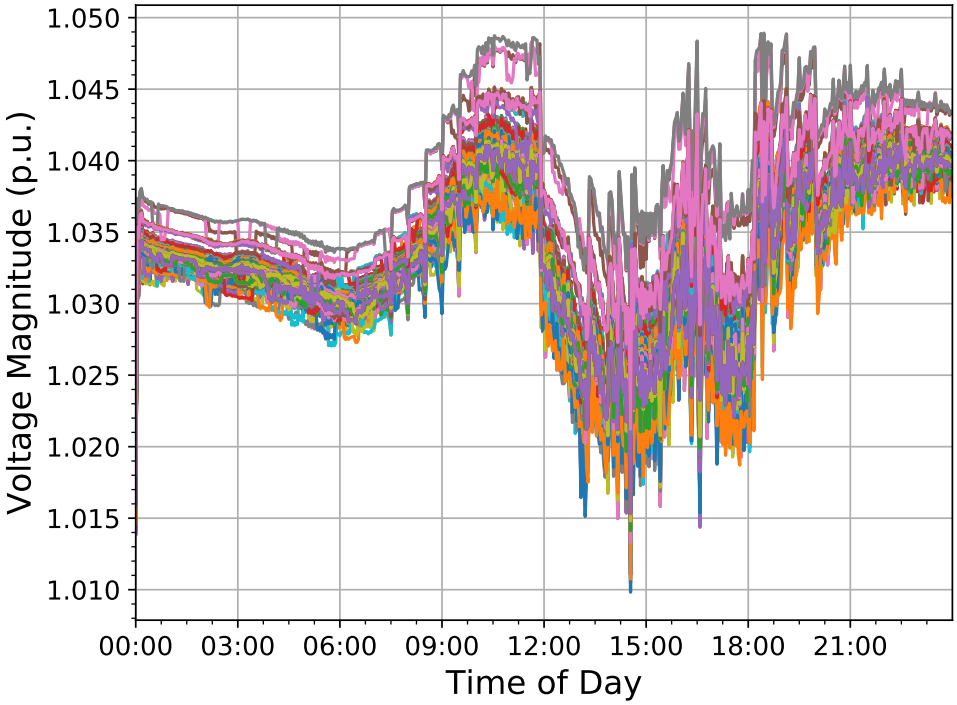


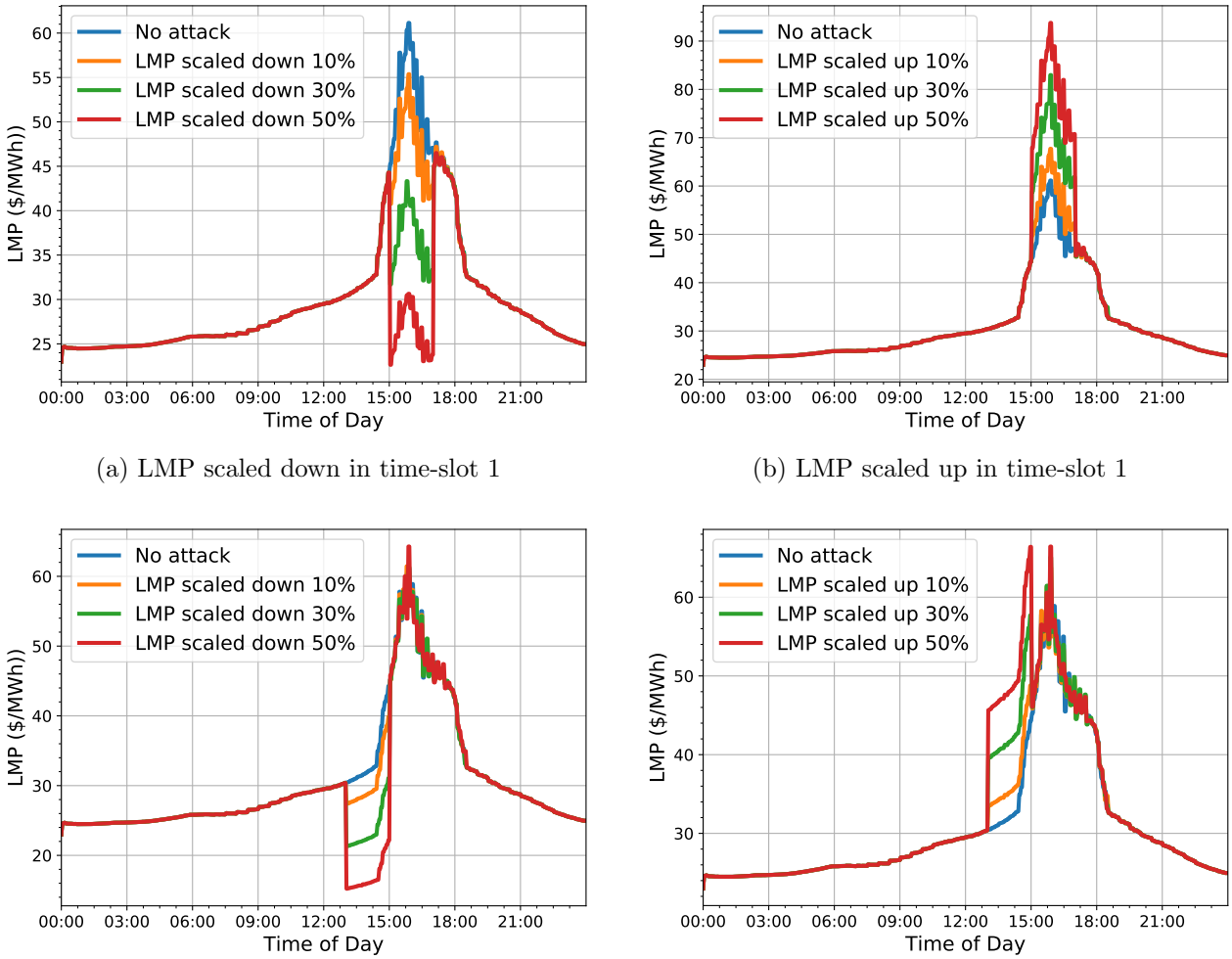
Figure 5.6: Voltage magnitude at end-users connected to bus 3 under normal conditions

Attack duration

In the present work, the effect of scaling attacks have been demonstrated with an attack duration of 2 hours. The effect of varying attack durations have not been investigated here. Two time-slots have been chosen for illustrating the attack impact :

1. **Time-slot 1: 3 PM - 5 PM :** This is the period corresponding to high LMP. Load fluctuations during this time results in larger price oscillations since the additional supply is provided by peaking generators with a higher incremental cost for providing energy.
2. **Time-slot 2: 1 PM - 3 PM :** This is the period with a low LMP just preceding the high LMP period. Load behavior during this period also impacts system behavior in the next hours corresponding to the high LMP period.

During both these time slots, the LMP has been both scaled up and down. Three different scaling factors are used - 10%, 30% and 50%. The LMP seen by end users connected to bus 3 as a result of the data integrity attacks is reproduced in figure 5.7.



(a) LMP scaled down in time-slot 1

(b) LMP scaled up in time-slot 1

(c) LMP scaled down in time-slot 2

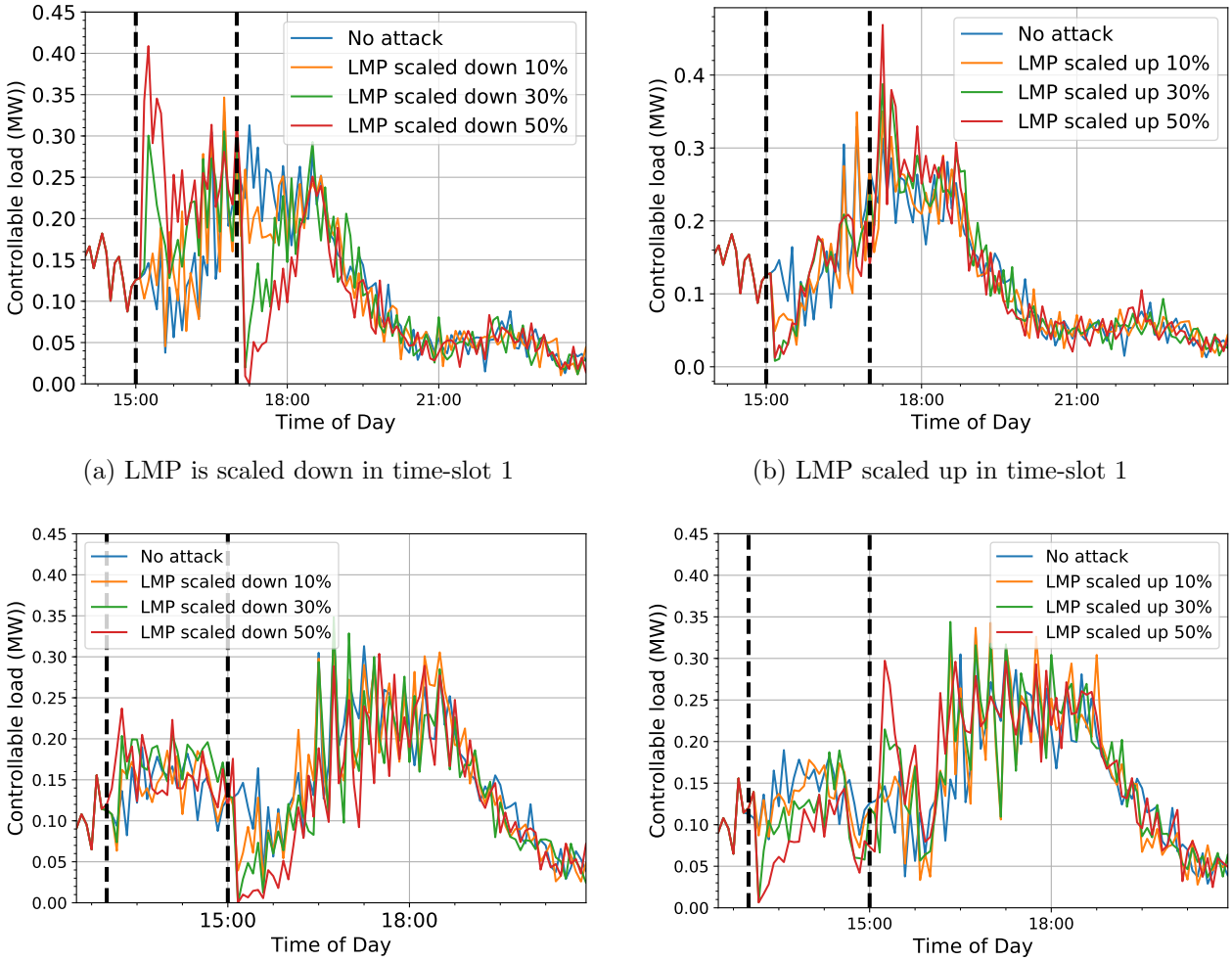
(d) LMP scaled up in time-slot 2

Figure 5.7: Scaling attacks on LMP at bus 3

Attack impact

Impact is estimated using the metric described in section 5.1. The simulated system does not have protection elements and the penetration of controllable load is too small to realistically observe any reliability impacts. Therefore, the reliability metric is not checked in the present work.

1. Operational: The operational impacts have been evaluated by looking at the changes in controllable residential cooling loads, total active power consumption and voltage magnitudes at bus 3. For the remaining buses we have only checked the variation in LMP as a result of the attack on bus 3. Changes in voltage regulator tap positions for bus 3 have been noted to account for equipment wear and tear.



(a) LMP is scaled down in time-slot 1

(b) LMP scaled up in time-slot 1

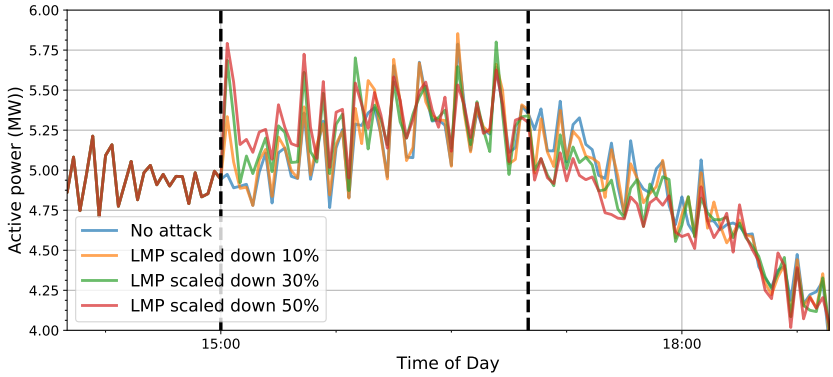
(c) LMP scaled down in time-slot 2

(d) LMP scaled up in time-slot 2

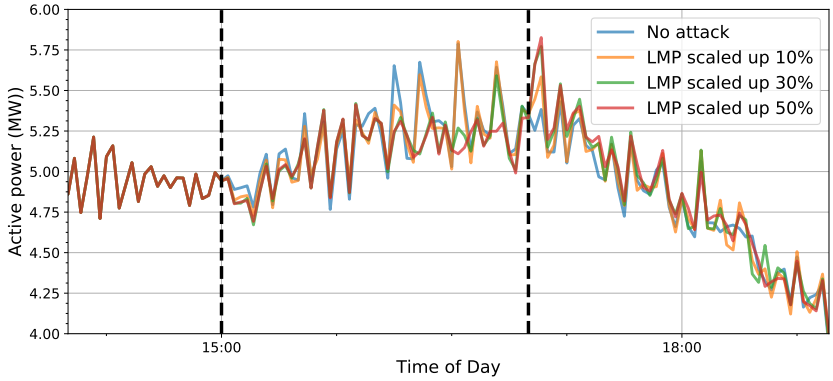
Figure 5.8: Change in controllable residential cooling load due to scaling attacks on LMP

Impact on controllable residential cooling load: Figure 5.8 shows variation in controllable residential cooling load at bus 3 due to scaling attacks. The black dotted lines indicate the time duration when the attack is live. When the system sees a sudden drop in LMP, there is an abrupt increase in controllable load. This spike appears right after a scale down attack goes live and after a scale up attack is removed. Similarly, a sudden jump in LMP causes a sharp decrease in controllable load. This effect appears when a scale up attack is initiated or a scale down attack is removed. The spike is positively correlated with scaling factors, but not necessarily proportional. It is interesting to note that as an attack continues to persist in the system, the controllable load tends to get closer to the value obtained in no-attack scenarios. Thus, intermittent attacks of shorter duration could prove more detrimental than a longer continuous attack.

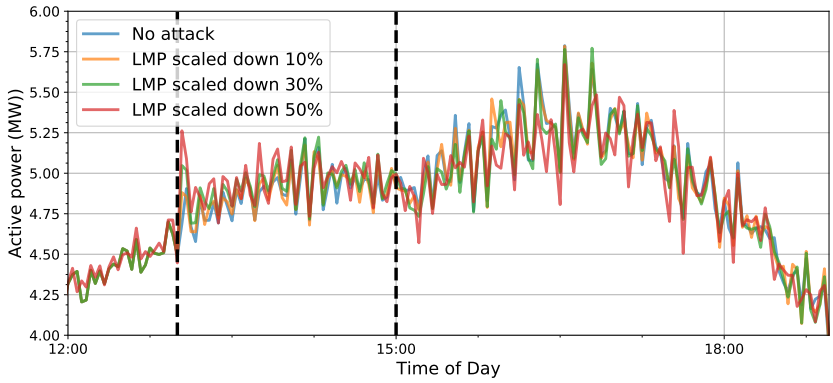
Some more conclusions can also be drawn from these results. It can be seen that



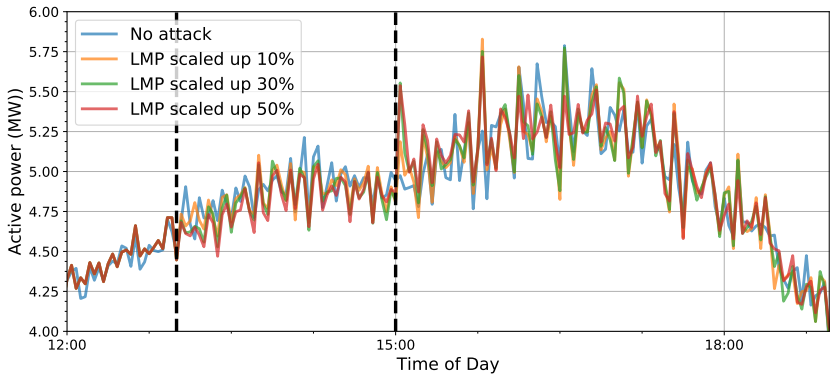
(a) LMP is scaled down in time-slot 1



(b) LMP scaled up in time-slot 1

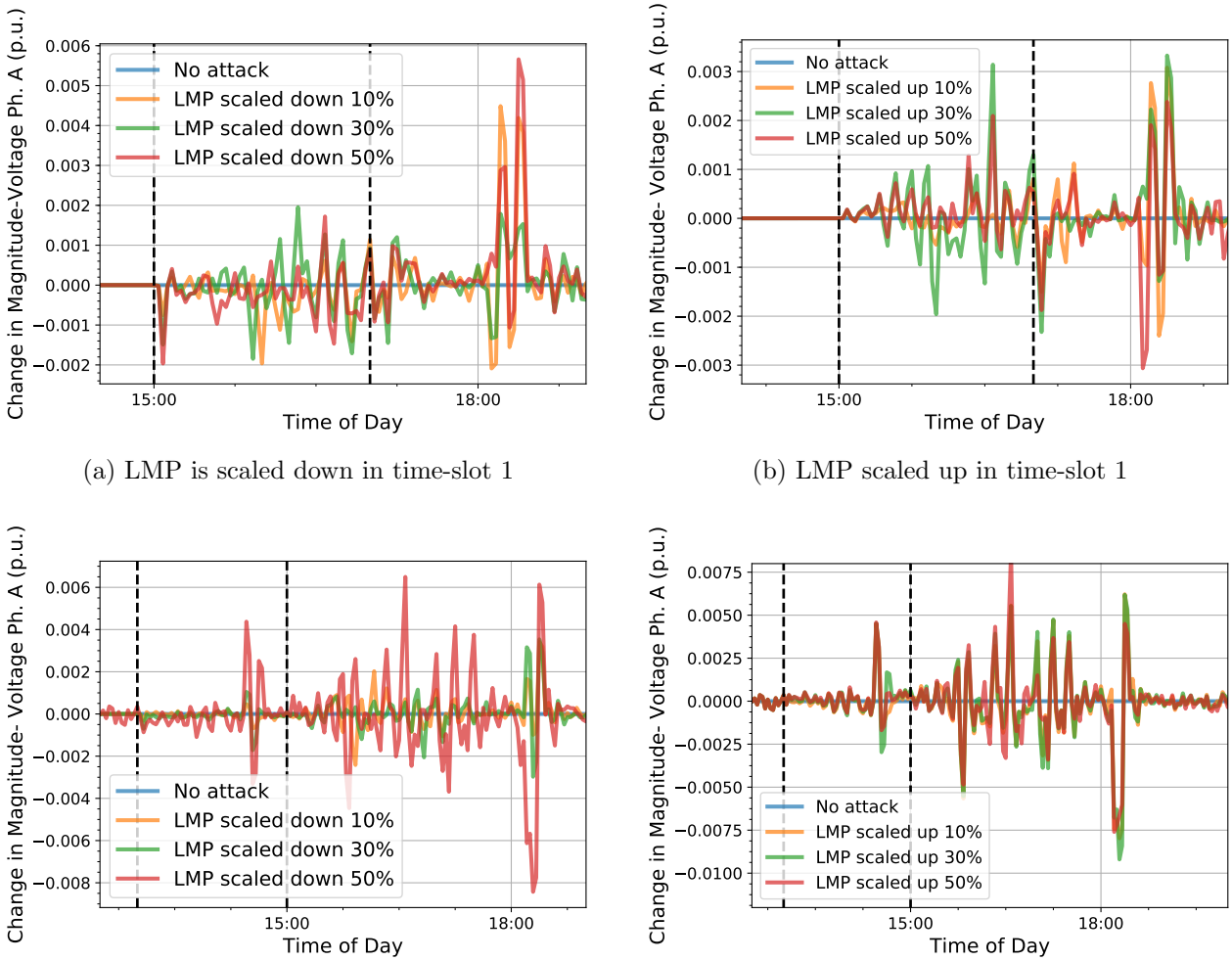


(c) LMP scaled down in time-slot 2



(d) LMP scaled up in time-slot 2

Figure 5.9: Change in active power due to scaling attacks on LMP



(a) LMP is scaled down in time-slot 1

(b) LMP scaled up in time-slot 1

(c) LMP scaled down in time-slot 2

(d) LMP scaled up in time-slot 2

Figure 5.10: Change in bus voltage magnitude (Phase A) due to scaling attacks on LMP

the load variations are more pronounced for scaling up attacks in time-slot 2 (deeper valleys) and scaling down attacks in time-slot 1 (sharper peaks). Also, when the scale up attack is conducted in time-slot 2, the residential price-responsive AC controllers raise their set-points. As a result, the indoor temperature of the residences rise, and there is a rebound effect once the scaling up attack is removed. As all controllable cooling loads lower their set-points simultaneously, there is a pronounced increase in system load.

Impact on active power consumption: The variation in active power consumption at bus 3 due to scaling attacks is visible from figure 5.9. The conclusions drawn looking at the variation in controllable load still hold true. We can also see that an apparent decrease in LMP seen by loads causes the active power at bus 3 to rise rapidly.

Depending on the protection settings of the feeder under attack, if this spike coincides with a high load period, the breaker/fuse protecting the feeder might be tripped/melted causing an outage and thereby affecting reliability of operation.

TE envisions the integration of multiple DERs and microgrids. These resources may have low fault current contributions and in order to deal with this issue, distance protection has been proposed as an alternative to conventional overcurrent protection in distribution systems [25, 26, 27]. A distance relay may interpret a sudden spike in power as a sign of abnormal operating conditions.

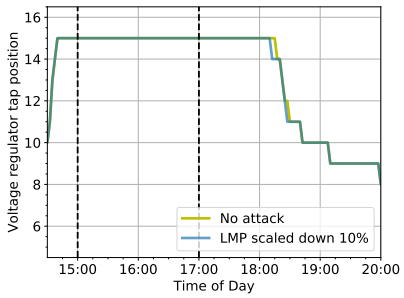
Impact on voltage magnitudes: We have checked the variation in voltage magnitude at phase A for bus 3 (figure 5.10). On the low voltage side, no ANSI violations were observed i.e. voltage magnitudes stayed within the suggested range of 0.9 and 1.1 p.u. It is interesting to observe that the variation in voltage magnitudes once an attack is removed is appreciable, especially when the attacks are conducted in time-slot 2.

At present, we have not investigated the variation in voltage angles. We have also not checked the contribution of capacitor banks in maintaining voltage magnitude within limits. However, the fact that the voltage regulator at bus 3 has to raise/lower taps to maintain normal operating conditions is evident from figure 5.11.

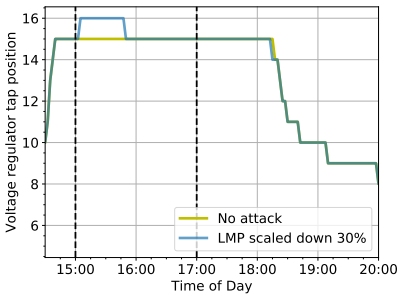
2. Financial: Due to the manipulation of the LMP values, the bid prices by responsive loads are affected. This causes the market clearing price at the next period to change. The variation in LMP at bus 3 due to the scaling attacks is shown in figure 5.12. The plotted value is the difference between LMPs in attack and normal conditions. We can see that in time-slot 1, scaling down the LMPs increase the LMP calculated by the ISO at the next market cycle. Interestingly, this trend continues for some time before it is reversed. The reverse effect is observed when LMPs are scaled up. Once the attack is removed, the LMP changes in the opposite direction but quickly stabilizes. That the increase/decrease in LMP due to attack is proportional to the scaling factor is pronounced only in the period immediately after the beginning/end of an attack. This observation leads us to conclude that it is difficult for an attacker to accurately estimate their financial gain/loss by manipulating LMP values.

When the attacks are carried out in time-slot 2, the price fluctuations are actually more pronounced in the period after the attack. This can be explained by the fact that the varying load is supplied by a peaking generator whose incremental cost of supplying power is high.

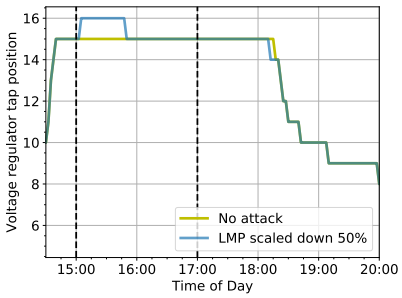
Since the LMP calculated at the bulk market changes, ISO earnings are impacted. The LMP communicated to load buses which are not under attack change as well (detailed results are included in appendix A). Although the magnitude of change is not equal for all buses, they follow similar trends. This difference in change depends on a number of factors, like proximity to the bus under attack, distance from generator units and whether the bus under consideration is supplied by a peaking generator unit. It is assumed that the DSO charges controllable loads a percentage of the bids placed



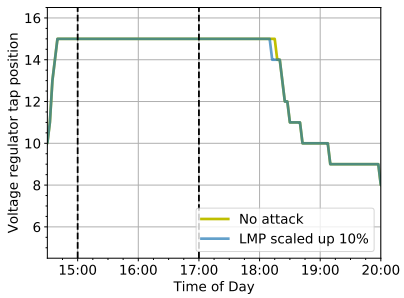
(a) Slot 1: LMP scaled down 10%



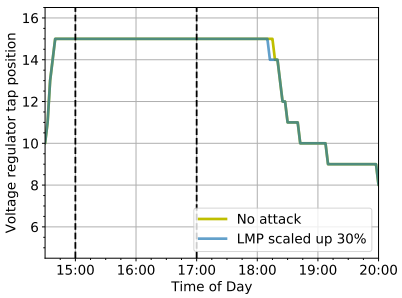
(b) Slot 1: LMP scaled down 30%



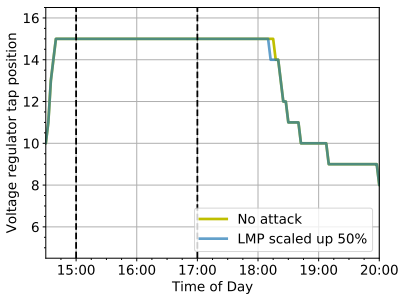
(c) Slot 1: LMP scaled down 50%



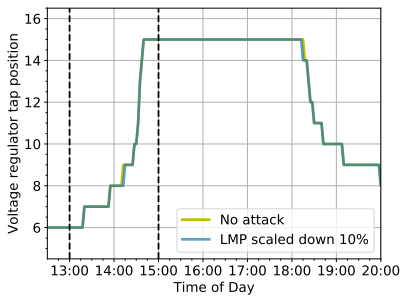
(d) Slot 1: LMP scaled up 10%



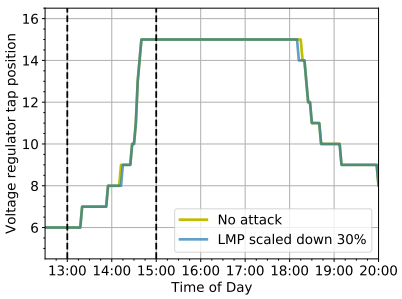
(e) Slot 1: LMP scaled up 30%



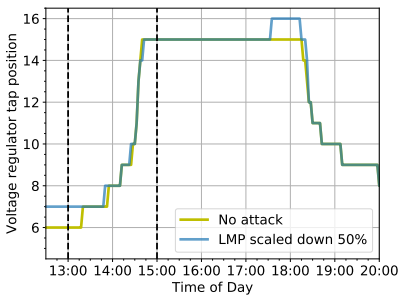
(f) Slot 1: LMP scaled up 50%



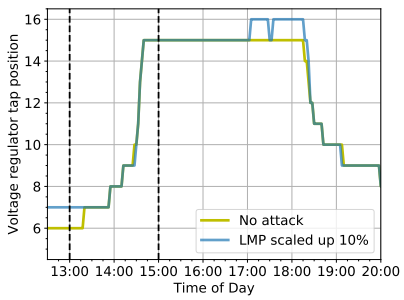
(g) Slot 2: LMP scaled down 10%



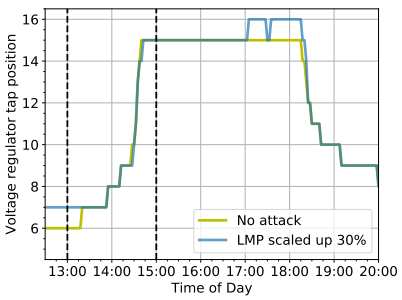
(h) Slot 2: LMP scaled down 30%



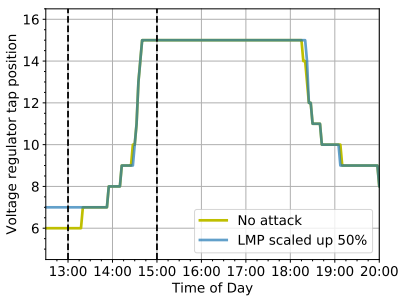
(i) Slot 2: LMP scaled down 50%



(j) Slot 2: LMP scaled up 10%

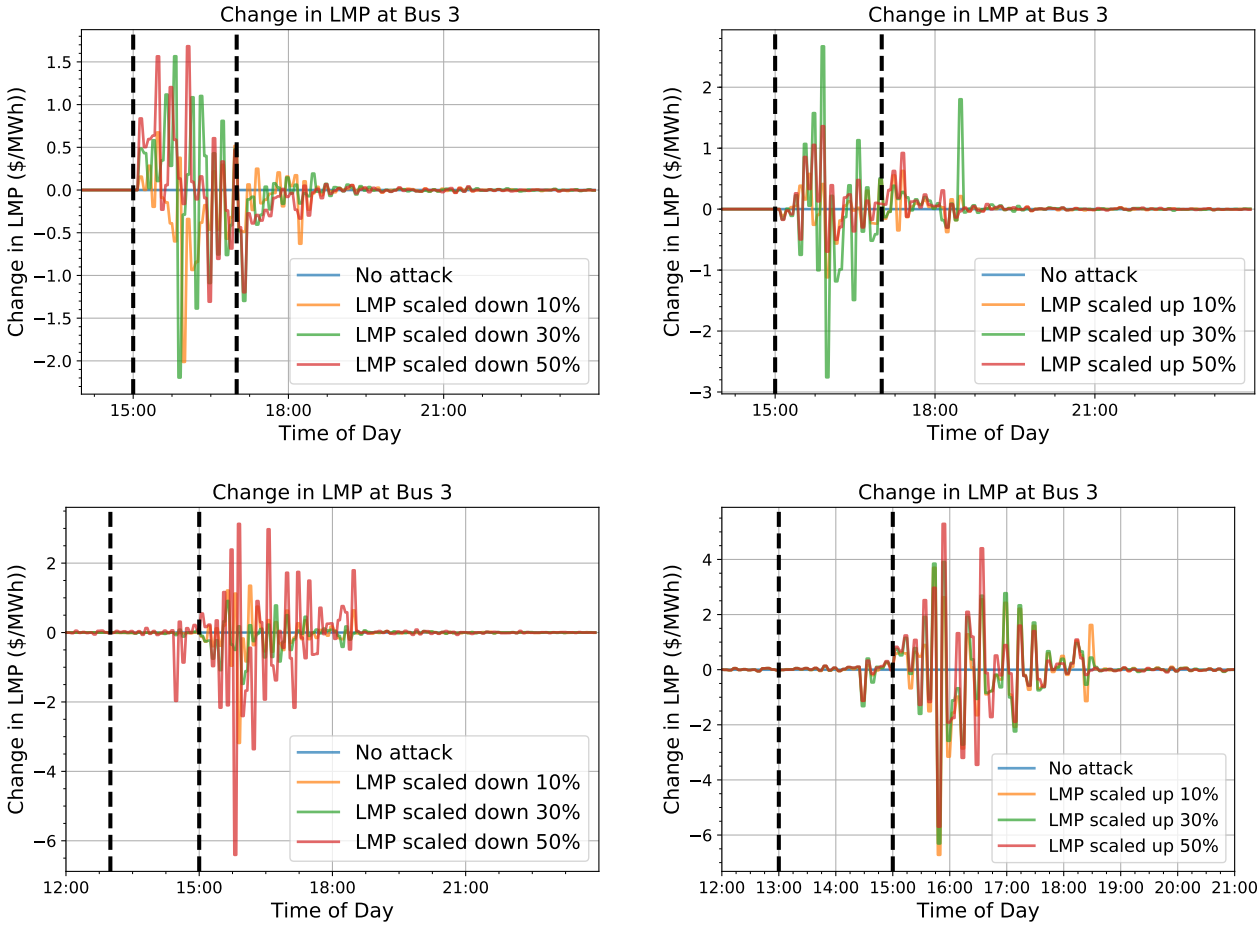


(k) Slot 2: LMP scaled up 30%



(l) Slot 2: LMP scaled up 50%

Figure 5.11: Change in voltage regulator tap positions due to scaling attacks on LMP



(c) LMP scaled down in time-slot 2

(d) LMP scaled up in time-slot 2

Figure 5.12: Change in bus 3 LMP calculated by bulk market due to scaling attacks on LMP

(much like services such as ebay and Paypal). Thus, changes in DSO earnings will be proportional to volumetric changes in controllable load.

Monetary impact will also be seen by individual houses. For example, when LMPs are scaled down, the buildings will assume the electricity expenditures to be less than normal but the bill provided by DSO will be comparatively higher (since the DSO continues to charge at the non-manipulated LMP). Impact observed by DERs is interesting to analyze. If storage units are manipulated to see a low LMP during peak-periods, they might chose to buy power from the grid to sell at a later period. Not only will this cause the storage units to make a financial loss, but also place stress on the feeder load. Similarly, if DERs see a high LMP during a low load period, they may choose to inject power to the grid, leading to potential generation excess, over-voltage and over-frequency issues. Also, the DER units will lose money.

The above discussion leads us to deduce potential motivations for DER owners to

launch data integrity attacks within a TE framework. For example, a dishonest DER owner can seek to artificially increase demand on a feeder by scaling down the LMPs being communicated from the DSO to end-users. Since other DERs on the same feeder will see a low price, they may choose to not inject power into the grid and/or buy power from the grid for storage at an apparent low cost. Also, the LMP calculated by the bulk energy market layer will increase, thereby helping the dishonest DER to maximize their revenue. In this work, automated DERs have not been modeled but analyzing the impact of data integrity attacks with DERs included in the system can be an avenue for future exploration.

3. Comfort: It is assumed that end-user comfort is correlated with the deviation of the thermostat set-point from the desired value. Higher the deviation, more is the discomfort faced. In this work, we have checked the mean and maximum absolute deviation of thermostat set points of price responsive ACs under different conditions from their no-attack values (shown in figures 5.13 and 5.14 respectively).

As expected, the set-points are higher when LMPs are scaled up and lower when LMPs are scaled down. The median values of set-point differences under attack conditions are also marked in the figure.

Some impact measures for scaling attacks on LMP are summarized in tables 5.1 and 5.2.

5.2.3 Case 3: Ramping Attacks on LMP

Attack duration

The attack durations are maintained at two hours for ramping attacks as well. LMP is ramped up during time-slot 1 and ramped down during time-slot 2. Three different ramping rates have been used- 1%, 5% and 10%. When the LMPs are being reduced, the minimum value that the manipulated LMP can reach has been defined to be 0. Manipulated LMP values as seen by end-users connected to bus 3 are shown in figure 5.15.

Attack Impact

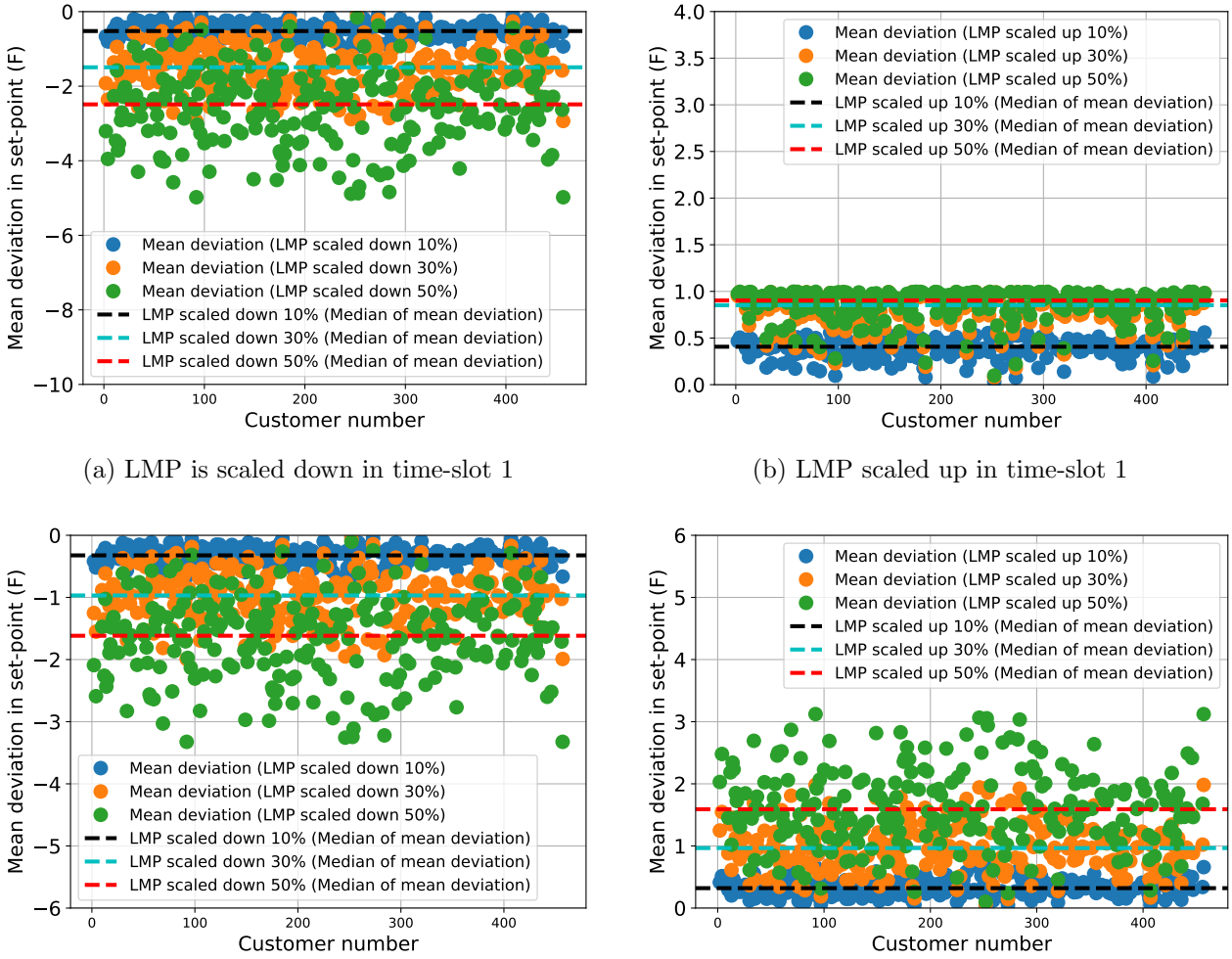
Ramping attacks agree with results obtained during scaling attacks. We have checked variation in controllable residential cooling load (figure 5.16, active power consumption at bus 3 (figure 5.17), variation in phase A voltage magnitude (figure 5.18), voltage regulator tap positions (figure 5.19) and deviation in thermostat set points during the attack duration (figure 5.20-5.21). Variation in LMP at buses other than 3 is included in appendix A. As expected, the impact on the system increases gradually. For instance, we can see from figure 5.16 that the controllable load increases/decreases

Table 5.1: Impact of LMP scaling attacks in time-slot 1

	Scaling down			**Scaling up**		
Scaling factor	10%	30%	50%	10%	30%	50%
Spike in active power when attack starts(%)	7.24	14.3	16.44	-4.3	-9.98	-11.7
Spike in active power when attack ends(%)	-5.16	-5.8	-8.63	4.24	7.83	8.24
Extra voltage regulator tap operations	0	2	2	0	0	0
Mean dev. in temp. set-pt (Median)(F)	-0.52	-1.49	-2.49	0.4	0.85	0.9
Mean dev. in temp. set-pt (Std. Dev.)	0.196	0.592	0.998	0.102	0.186	0.168
Max. abs. dev. in temp. set-pt (Median)(F)	-0.75	-1.96	-2.99	0.551	1.43	1.66
Max. abs. dev. in temp. set-pt (Std. Dev.)	0.287	0.687	1.129	0.199	0.519	0.445

Table 5.2: Impact of LMP scaling attacks in time-slot 2

	Scaling down			**Scaling up**		
Scaling factor	10%	30%	50%	10%	30%	50%
Spike in active power when attack starts(%)	4.13	7.68	12.25	-5.02	-5.89	-5.98
Spike in active power when attack ends(%)	-1.77	-2.85	-4.38	4.97	11.66	11.32
Extra voltage regulator tap operations	0	0	2	4	4	0
Mean dev. in temp. set-pt (Median)(F)	-0.32	-0.97	-1.61	0.32	0.96	1.59
Mean dev. in temp. set-pt (Std. Dev.)	0.132	0.395	0.660	0.130	0.394	0.619
Max. abs. dev. in temp. set-pt (Median)(F)	-0.42	-1.26	-2.10	0.44	1.28	1.97
Max. abs. dev. in temp. set-pt (Std. Dev.)	0.172	0.514	0.859	0.178	0.520	0.703



(a) LMP is scaled down in time-slot 1

(b) LMP scaled up in time-slot 1

(c) LMP scaled down in time-slot 2

(d) LMP scaled up in time-slot 2

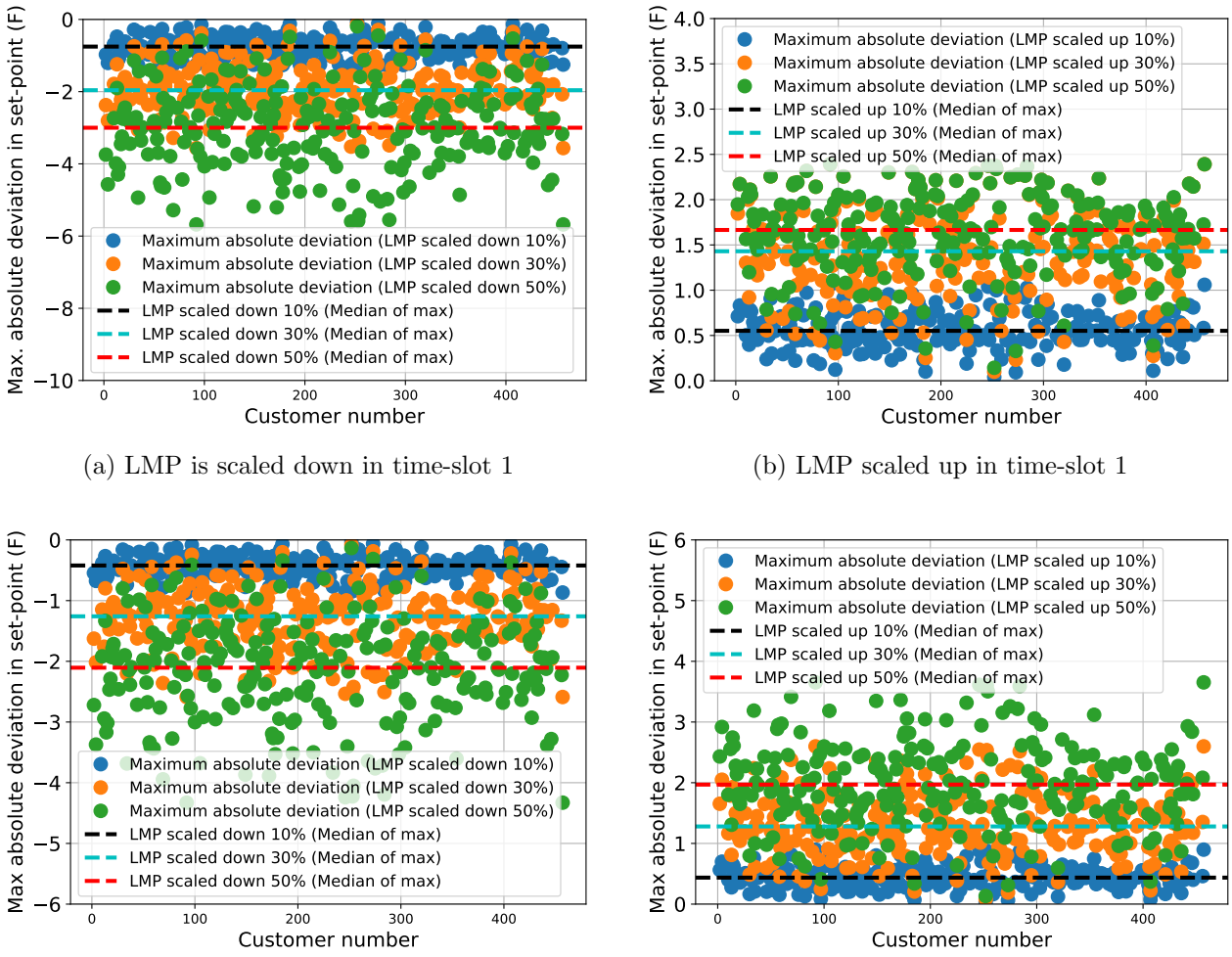
Figure 5.13: Mean change in thermostat set points for price-responsive AC units due to scaling attacks on LMP

slowly in the system as the attack is initiated. However, the change in load is abrupt once the attack is removed from the system.

5.3 Discussions

5.3.1 Limitations

The simulated system considers only residential cooling loads as price-responsive loads present in the system. Other responsive assets like washing machines, dryers etc have not been considered. Start-up and shutdown costs of generating units and the behavior



(a) LMP is scaled down in time-slot 1

(b) LMP scaled up in time-slot 1

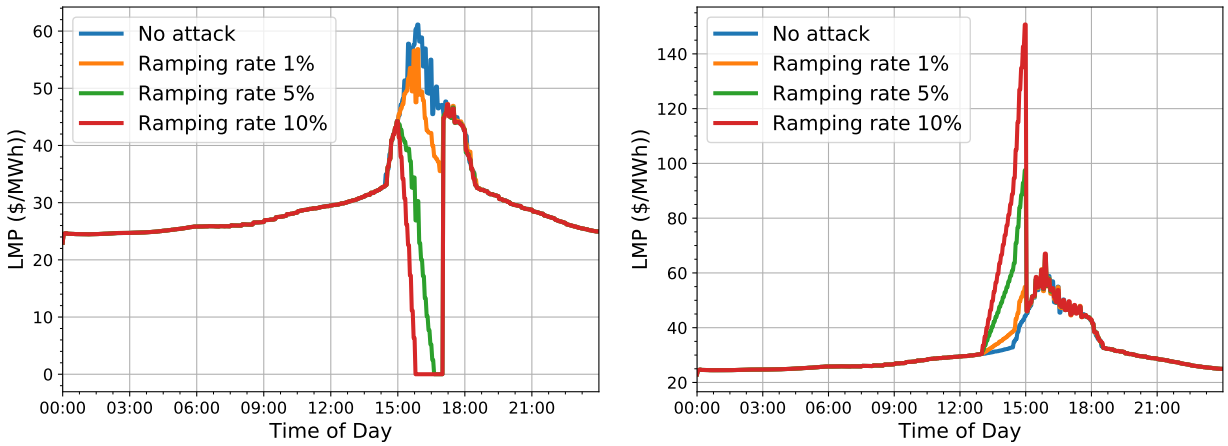
(c) LMP scaled down in time-slot 2

(d) LMP scaled up in time-slot 2

Figure 5.14: Maximum absolute change in thermostat set points for price-responsive AC units due to scaling attacks on LMP

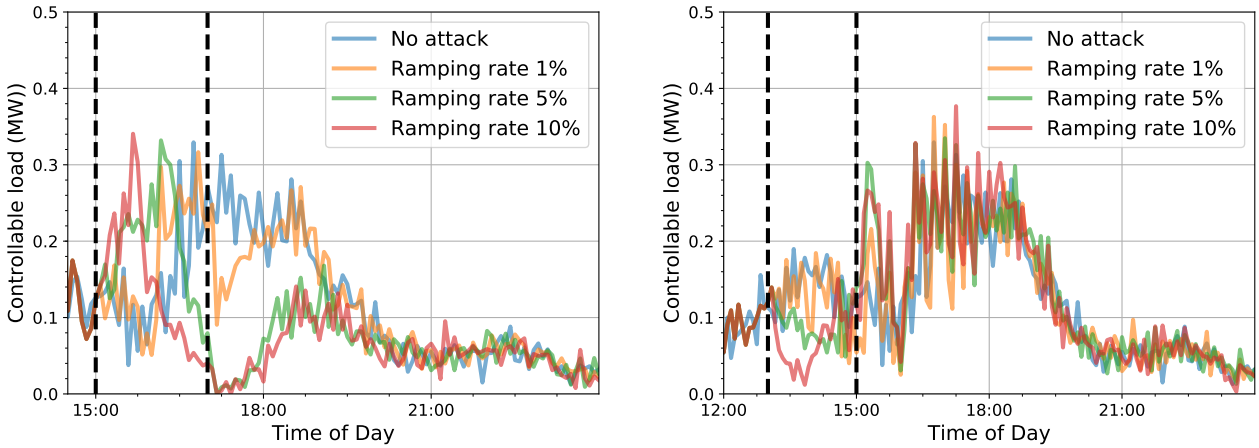
of DERs integrated within the distribution system have not been included in the scope of this study. We have also not considered the scenario where automated response of AC units can be overridden manually by end-users. Moreover, the responsive loads are not aware of and cannot predict future LMP values.

In view of the above limitations of the simulation framework as well as the relatively low penetration of price-responsive loads in the market, the results we have observed in present research are general and more work is needed to fully understand how malicious external intrusions impact different stakeholders in the emerging transactive energy markets.



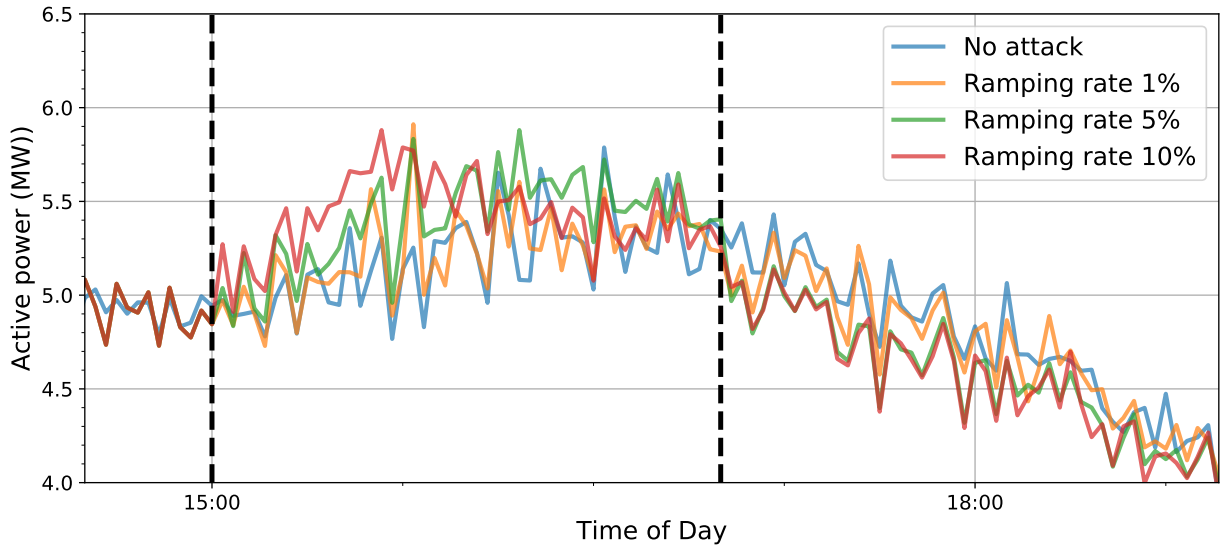
(a) LMP being ramped down in time-slot 1 (b) LMP being ramped up in time-slot 2

Figure 5.15: Ramping attacks on LMP at bus 3

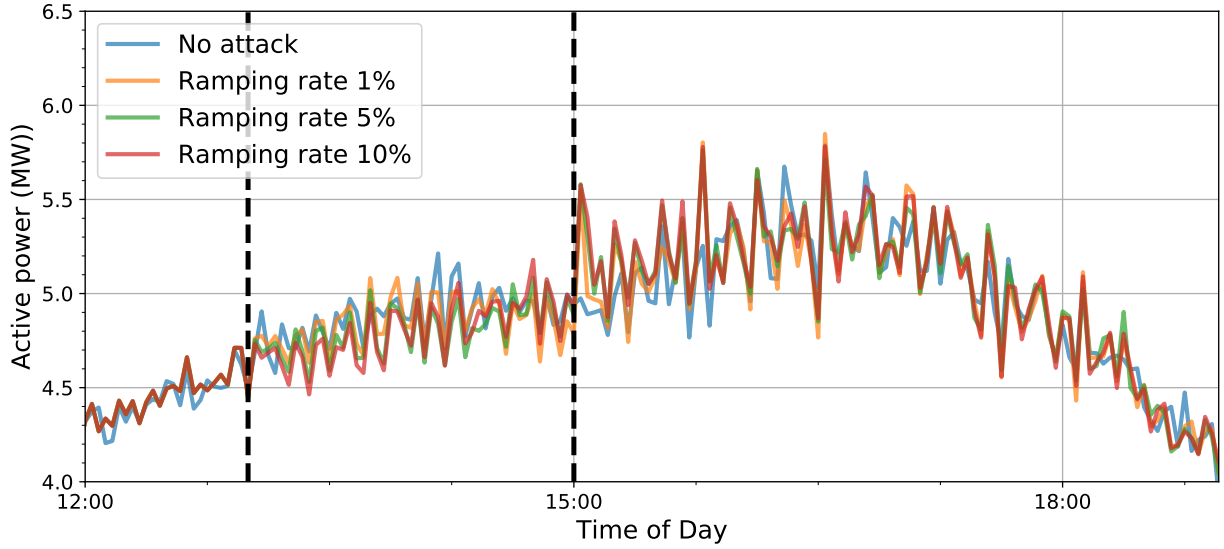


(a) LMP being ramped down in time-slot 1 (b) LMP being ramped up in time-slot 2

Figure 5.16: Controllable residential cooling load at bus 3 during to ramping attacks on LMP at bus 3

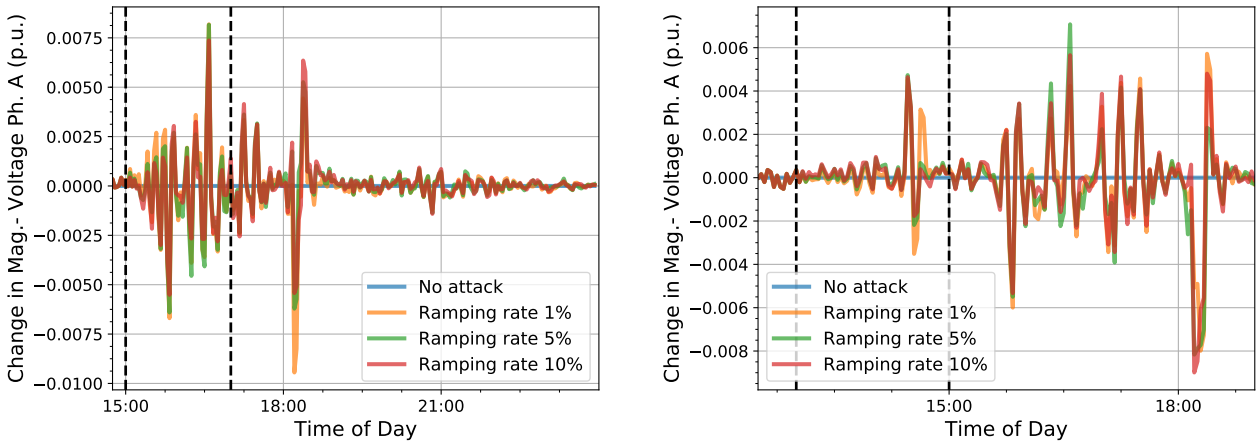


(a) LMP being ramped down in time-slot 1



(b) LMP being ramped up in time-slot 2

Figure 5.17: Active power consumption at bus 3 during to ramping attacks on LMP



(a) LMP being ramped down in time-slot 1

(b) LMP being ramped up in time-slot 2

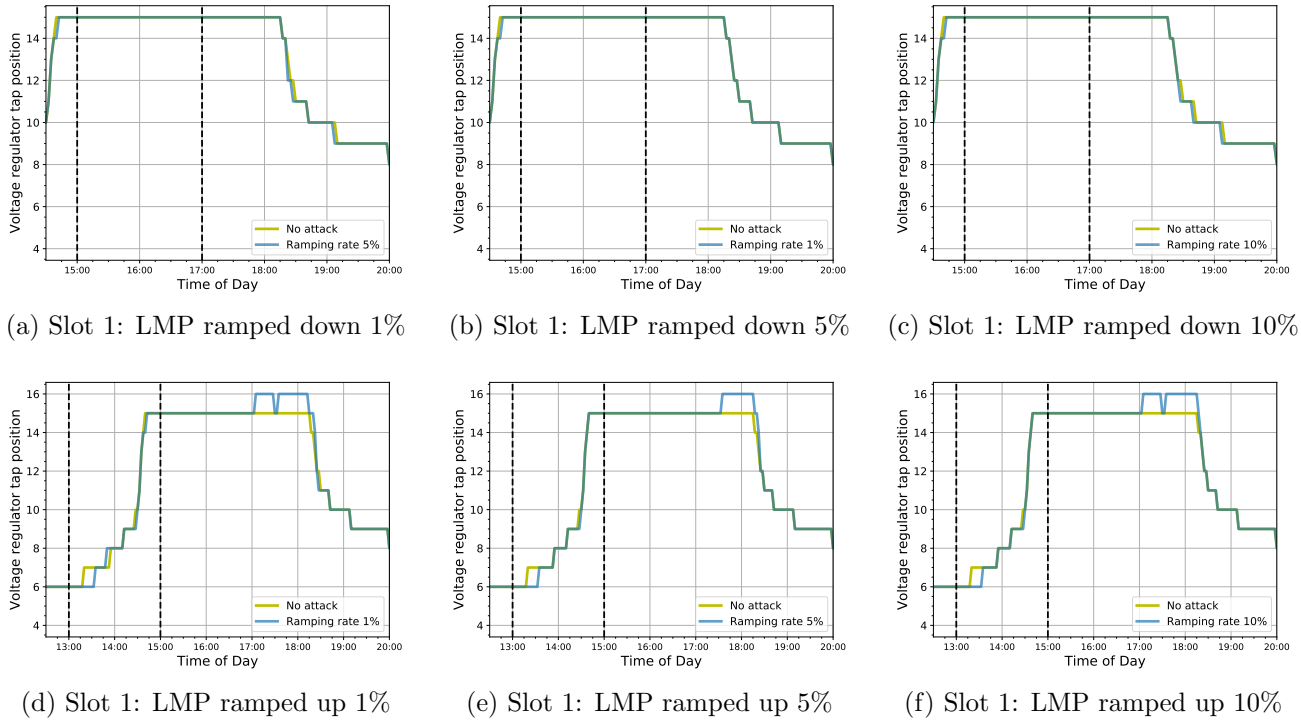
Figure 5.18: Variation in Phase A voltage magnitude at bus 3 during to ramping attacks on LMP at bus 3

5.3.2 Key Learnings

Despite the limitations discussed in the previous section, this thesis forms the first step in understanding the impact of data integrity attacks on emerging transactive control systems and illustrates some associated interesting phenomena. Some key learnings are summarized below.

1. Reducing energy price is more detrimental to the grid when the load is already high. Similarly, increasing energy price is more detrimental in the period immediately preceding peak hours. There are more fluctuations in the market when change in load causes a peaking generator to be switched on/off repeatedly.
2. The impact of attacks continue to persist in the system for some time even after an attack is removed. Therefore, for quantifying the impact of an intrusion, it is necessary to also consider system behavior in the period after an attack removal. This effect is more pronounced when LMPs are increased in a time-slot preceding the high-LMP period.

   In our work, responsive loads are not aware of future energy prices. However, ACs can be incentivized to shift a bulk of their consumption to lean load periods, if they are aware of future LMPs i.e. they pre-cool premises when energy prices are low [4]. If this pre-cooling can be prevented by artificially increasing LMP, the rebound effect where all ACs reduce their cooling set-points simultaneously once the attack is removed will be exacerbated.
3. Since the system sees significant impact after an attack removal, efficient mitigation strategies are needed along with effective attack detection mechanisms in a TE ecosystem.

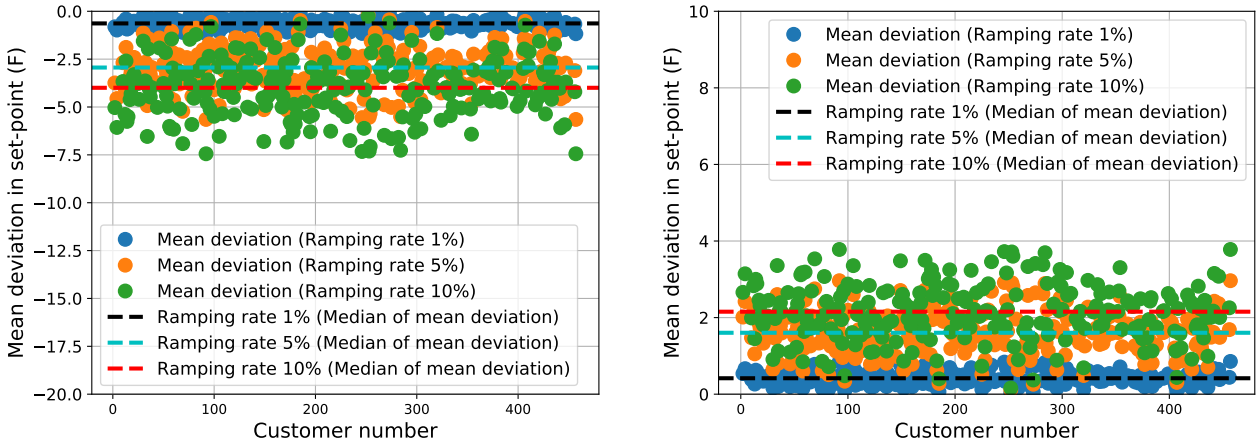


(a) Slot 1: LMP ramped down 1% (b) Slot 1: LMP ramped down 5% (c) Slot 1: LMP ramped down 10%

(d) Slot 1: LMP ramped up 1% (e) Slot 1: LMP ramped up 5% (f) Slot 1: LMP ramped up 10%

Figure 5.19: Change in voltage regulator tap positions due to ramping attacks on LMP

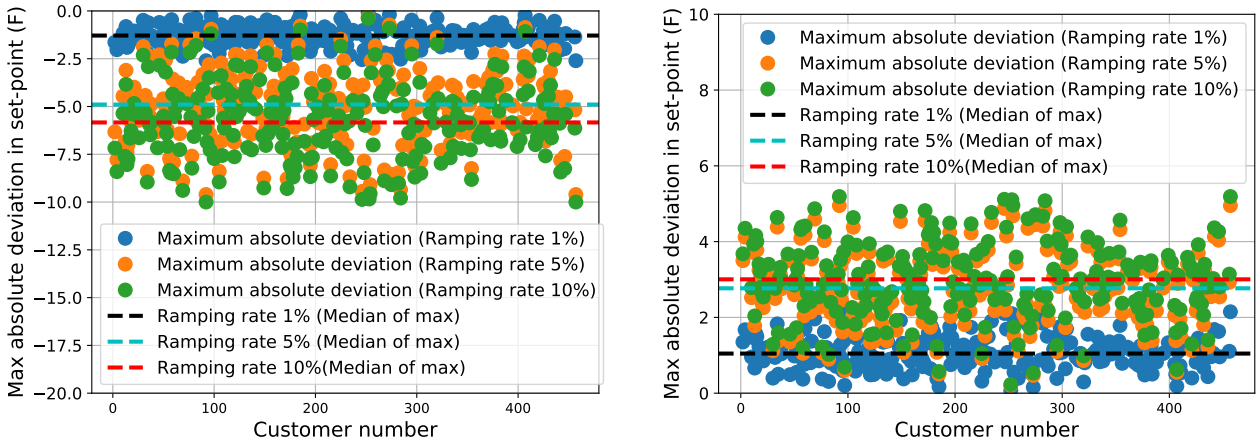
4. Results show that even when only one bus is attacked, the LMP calculated at the bulk energy market for the next market period changes considerably. The LMP thus calculated is propagated to the remaining buses in the system which then act according to the change in LMP. Therefore, manipulating the LMP sent by one DSO to its customers has a wide impact on the entire transactive market.
5. Our results show that as an attack continues to persist, the system tends to get closer to no-attack conditions. Hence, intermediate attacks of shorter duration could prove to be more disruptive than a single attack of a longer duration.
6. It can be seen from the simulation results that as attack durations increase, the increase/decrease in loads, prices etc do not necessarily show similar trends as exhibited right at the beginning of the attack duration. This is because different houses may need different times to reach their desired temperature, depending on size, initial temperature etc. Therefore, it will be very difficult for an attacker to accurately estimate their financial gains/losses.



(a) LMP being ramped down in time-slot 1

(b) LMP being ramped up in time-slot 2

Figure 5.20: Mean change in thermostat set points for price-responsive AC units due to scaling attacks on LMP



(a) LMP being ramped down in time-slot 1

(b) LMP being ramped up in time-slot 2

Figure 5.21: Maximum absolute change in thermostat set points for price-responsive AC units due to scaling attacks on LMP

Chapter 6

Future Work

Further work is needed to better understand how data manipulation affects a transactive market and which attacks are more detrimental to grid operations. In our present work, we have formed a preliminary understanding of how different grid assets respond to data integrity attacks with the help of a modified IEEE 14-bus transmission system. The next step is to validate our results using a larger system like the WECC (Western Electricity Coordinating Council) 240-bus model. We will explore the system behavior when recurring undetected attacks occur at the same time in the day over a longer span of time. Validating our hypothesis that multiple attacks of shorter duration is more detrimental than a single long attack will also be pursued.

Future research will involve investigating how manipulating bid prices and quantities sent from price-responsive loads to the DSO impacts system operation. Attacks of different durations and varying penetration rates will be examined. Impact of data availability attacks will also be explored. An interesting direction of research will be understanding how DER owners respond to manipulated price signals and how these actions subsequently affect the power grid.

Chapter 7

Conclusion

As the penetration of consumer level internet-connected smart devices participating and interacting with the utilities in transactive control approaches increases, performing a thorough analysis of the impact of various cyber-attacks on these interactions becomes important. In this thesis, we have analyzed the impact of data integrity attacks on energy prices being exchanged between the DSO and end-users, and concluded that such attacks can result in significant impacts on the operations of the system. Coordinated attacks targeting multiple buses can potentially result in reliability issues under stressed operating conditions.

We observe noticeable impacts on different stakeholders of the TE system although the scale of the attack and the amount of price-responsive load present in the system is small. These impacts continue to persist in the system for some time even after the attack is removed, which leads us to conclude that along with attack detection strategies, efficient mitigation mechanisms will also be needed in a resilient TE framework. This thesis forms a first step in quantifying the impacts of cyber-attacks on emerging transactive control approaches and highlights the need for incorporating appropriate attack detection and mitigation techniques at multiple levels to make them robust and resilient.

Bibliography

[1] The GridWise Architecture Council, "GridWise Transactive Energy Framework Version 1.0," The GridWise Architecture Council, Richland, WA, Tech. Rep. PNNL-22946 Ver1.0, Jan. 2015.

[2] D. Hammerstrom, T. Oliver, R. Melton, and R. Ambrosio, "Standardization of a hierarchical transactive control system," in *In Grid Interop*, 2009.

[3] PNNL, "AEP Ohio gridSMART Demonstration Project Real-Time Pricing Demonstration Analysis," Pacific Northwest National Laboratory, Richland WA, Tech. Rep. PNNL-23192, Feb. 2014.

[4] PNNL, "Pacific Northwest GridWise Testbed Demonstration Projects: Part I. Olympic Peninsula Project," Pacific Northwest National Laboratory, Richland WA, Tech. Rep. PNNL-17167, Oct. 2007.

[5] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *2017 Resilience Week (RWS)*, Sept 2017, pp. 18–23.

[6] D. of Homeland Security. (2018) Critical infrastructure sectors. [Online]. Available: https://www.dhs.gov/critical-infrastructure-sectors

[7] J. C. Foreman and D. Gurugubelli, "Identifying the cyber attack surface of the advanced metering infrastructure," *The Electricity Journal*, vol. 28, no. 1, pp. 94 – 103, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1040619014002899

[8] INL, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," Idaho National Laboratory, Tech. Rep. INL/EXT-16-40692, Aug. 2016.

[9] Congressional Research Service, "Electric Grid Cybersecurity," Congressional Research Service, Tech. Rep. R45312, Sep. 2018.

[10] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13, 2013, pp. 439–450.

[11] J. Giraldo, A. Crdenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: Impact and countermeasures," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249–2257, Sept 2017.

[12] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2011, pp. 232–237.

[13] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," *2010 First IEEE International Conference on Smart Grid Communications*, pp. 220–225, 2010.

[14] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *2010 First IEEE International Conference on Smart Grid Communications*, Oct 2010, pp. 214–219.

[15] F. Pasqualetti, F. Dörfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," *IEEE Conference on Decision and Control and European Control Conference*, pp. 2195–2201, 2011.

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

[17] J. Hansen, T. Hardy, and L. Marinovici, "Transactive energy: Stabilizing oscillations in integrated wholesale-retail energy markets," *Manuscript Submitted*, 2018.

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

[19] M. Ezekiel, "The cobweb theorem," *The Quarterly Journal of Economics*, vol. 52, no. 2, pp. 255–280, 1938. [Online]. Available: http://www.jstor.org/stable/1881734

[20] S. Li, W. Zhang, J. Lian, and K. Kalsi, "Market-based coordination of thermostatically controlled loadspart i: A mechanism design formulation," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1170–1178, March 2016.

[21] Residential module user's guide. [Online]. Available: http://gridlab-d.shoutwiki.com/wiki/Residential_module_user%27s_guide

[22] S. Ciraci, J. Daily, J. Fuller, A. Fisher, L. Marinovici, and K. Agarwal, "FNCS: a framework for power system and communication networks co-simulation," *Proceedings of the Symposium on Theory of Modeling and Simulation - DEVS Integrative*, p. 36, Apr. 2014.

[23] Feeder taxonomy. [Online]. Available: https://github.com/gridlab-d/Taxonomy_Feeders

[24] IEEE, "Common T&D Reliability Metrics." [Online]. Available: http://www.ewh.ieee.org/r6/san_francisco/pes/pes_pdf/Reliability_and_Artificial_Intelligence/Common_T&D_Reliability_Indices.pdf

[25] S. Voima and K. Kauhaniemi, "Using distance protection in smart grid environment," in *IEEE PES Innovative Smart Grid Technologies, Europe*, Oct 2014, pp. 1–6.

[26] A. Sinclair, D. Finney, D. Martin, and P. Sharma, "Distance protection in distribution systems: How it assists with integrating distributed resources," *IEEE Transactions on Industry Applications*, vol. 50, no. 3, pp. 2186–2196, May 2014.

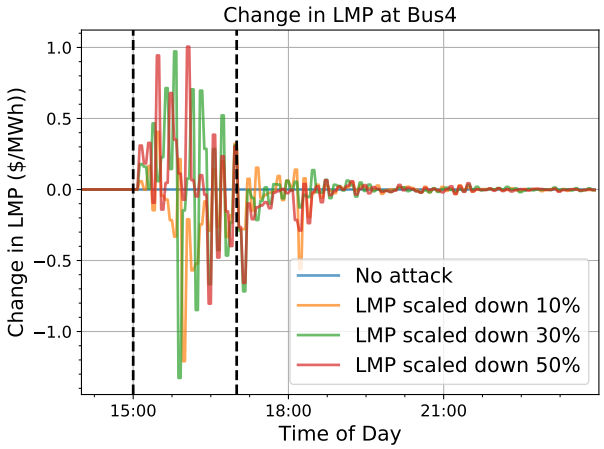
[27] S. Biswas and V. Centeno, "A communication based infeed correction method for distance protection in distribution systems," in *2017 North American Power Symposium (NAPS)*, Sept 2017, pp. 1–5.

Appendices

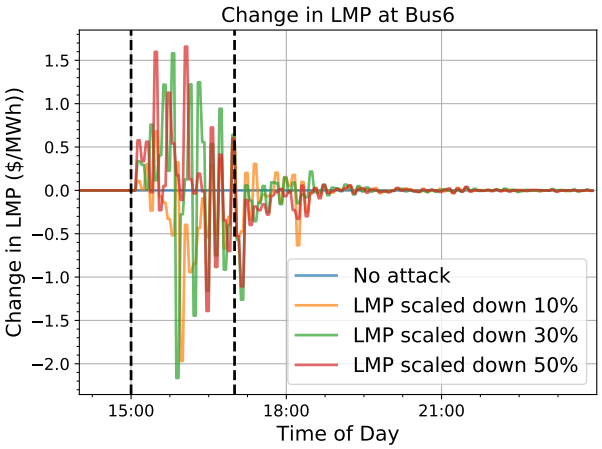
Appendix A

Change in LMP

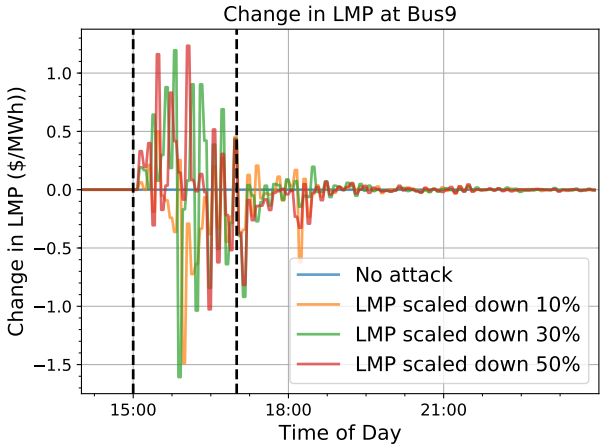
It is observed that manipulating LMPs at one bus affects the LMP calculated in the bulk energy market for the next iteration, which is then transmitted to other buses of the transmission system. Therefore manipulating values at even one bus can have a significant impact on other buses in the grid. Impact on LMP sent to load buses in the IEEE 14-bus transmission system due to data integrity attacks simulated in this work are shown in figures A.1 - A.6.



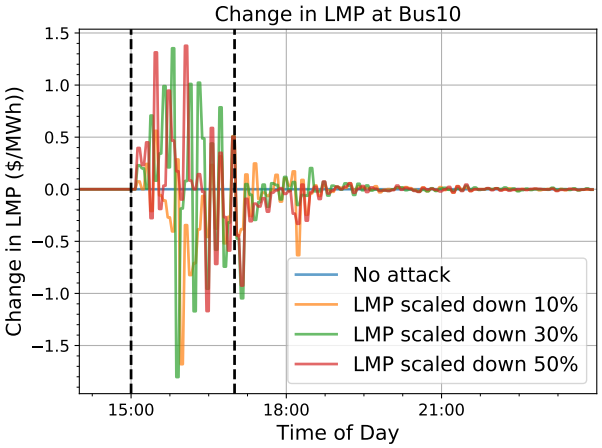
(a) Change at bus 4



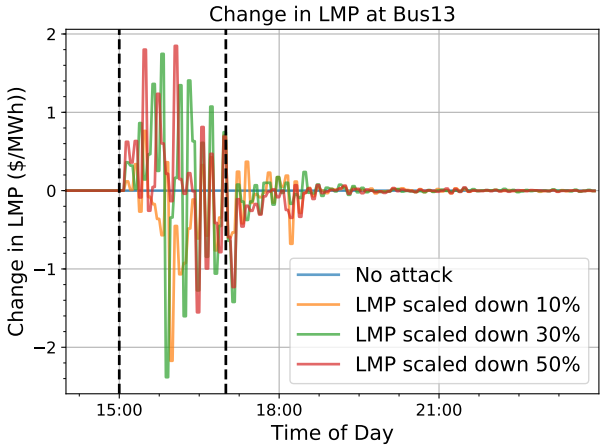
(b) Change at bus 6



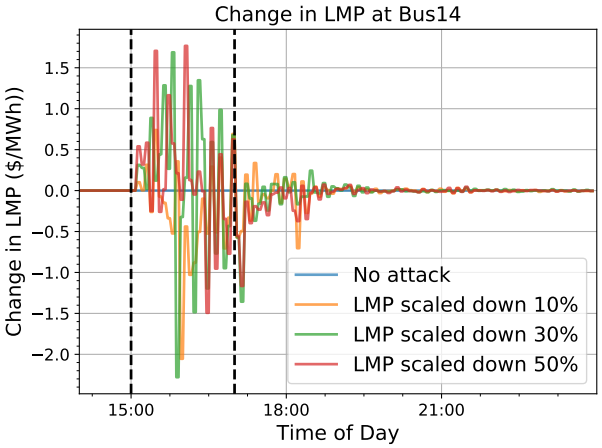
(c) Change at bus 9



(d) Change at bus 10

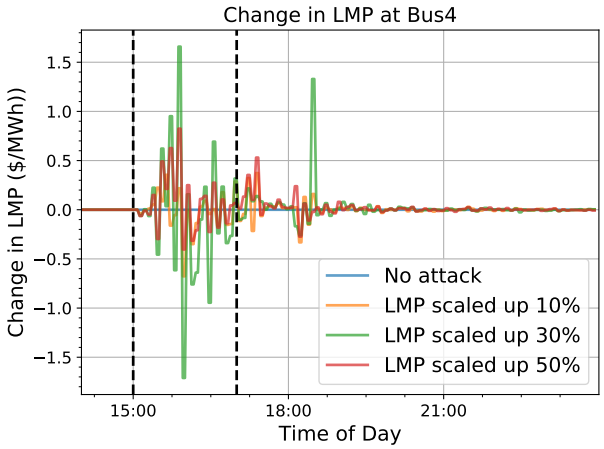


(e) Change at bus 13

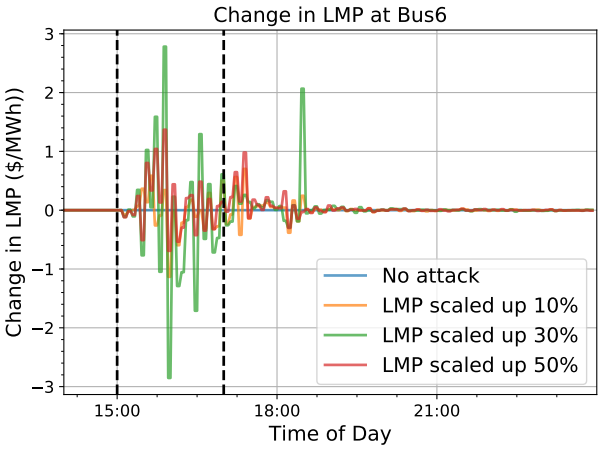


(f) Change at bus 14

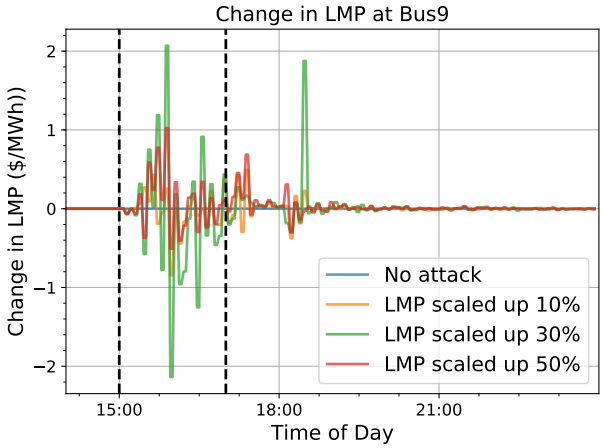
Figure A.1: Change in LMP at load buses when LMPs are scaled down in time-slot 1



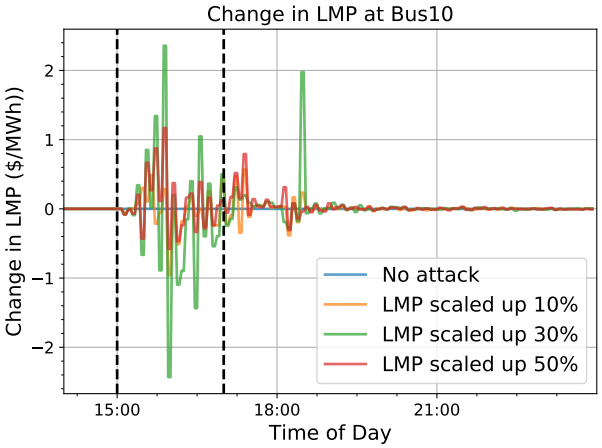
(a) Change at bus 4



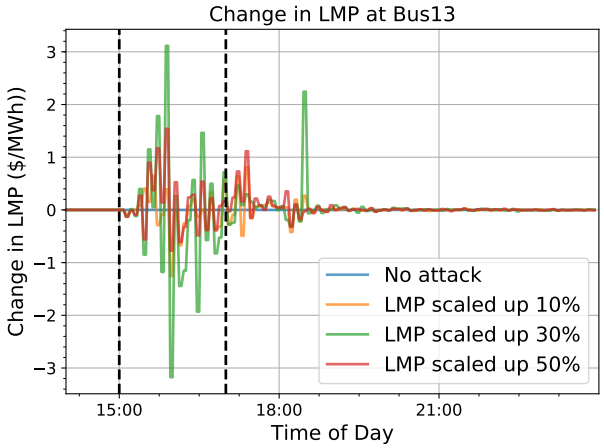
(b) Change at bus 6



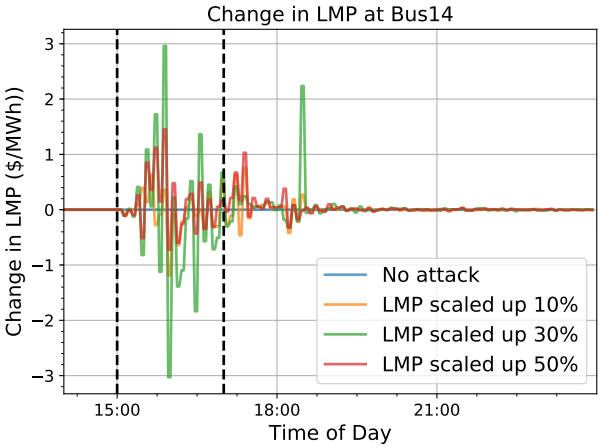
(c) Change at bus 9



(d) Change at bus 10

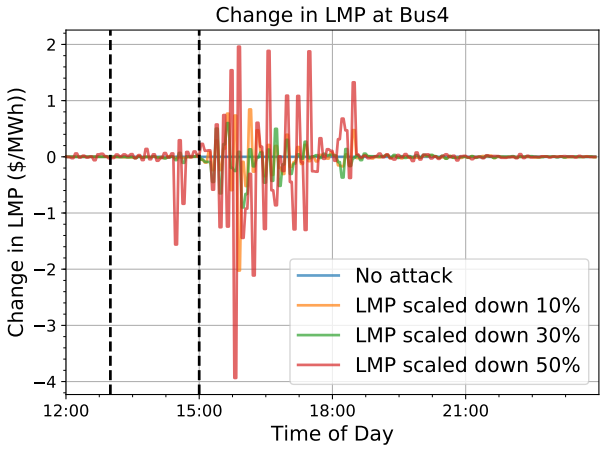


(e) Change at bus 13

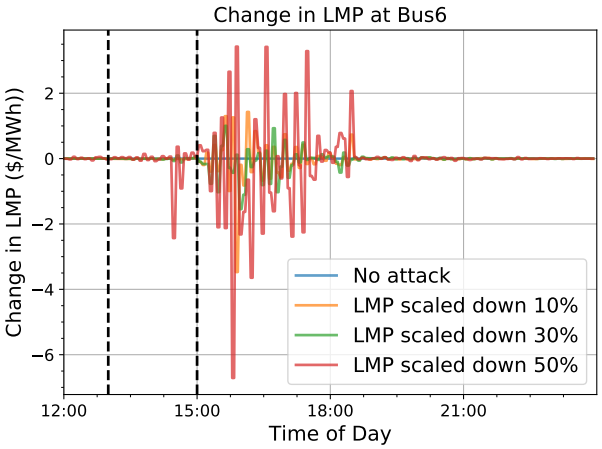


(f) Change at bus 14

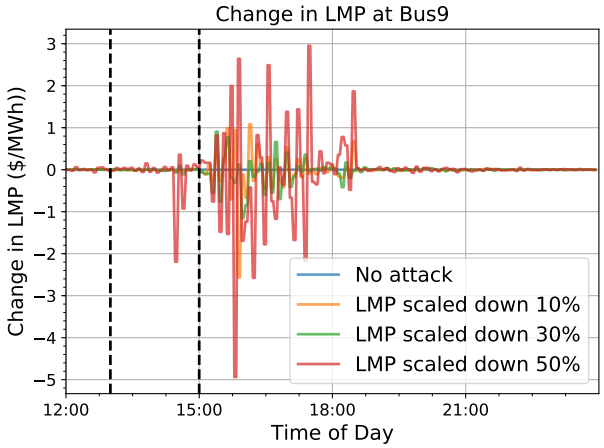
Figure A.2: Change in LMP at load buses when LMPs are scaled up in time-slot 1



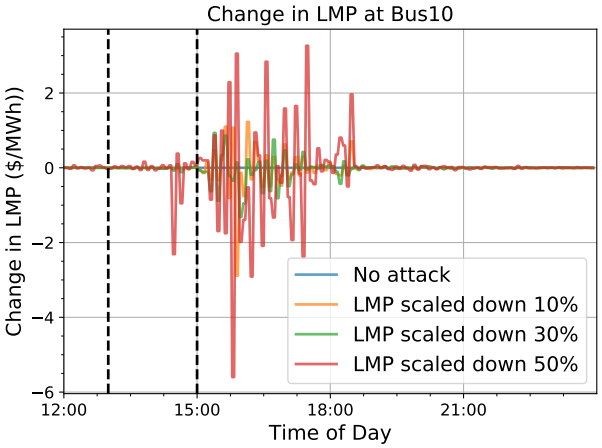
(a) Change at bus 4



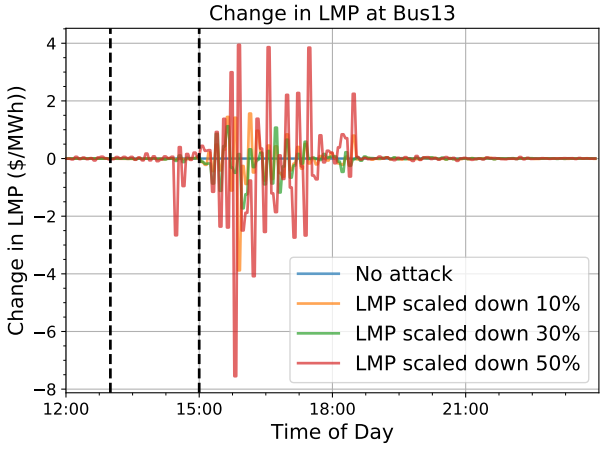
(b) Change at bus 6



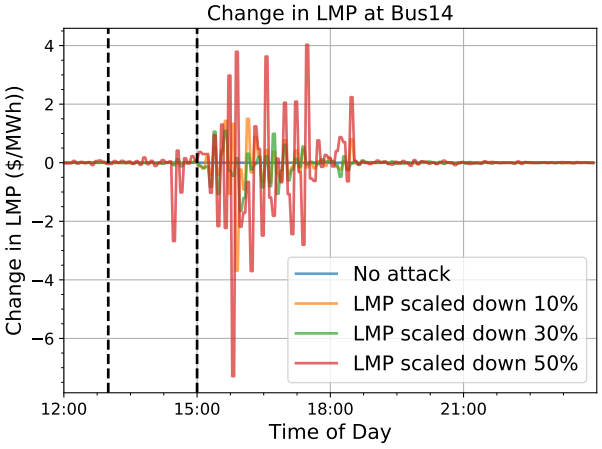
(c) Change at bus 9



(d) Change at bus 10

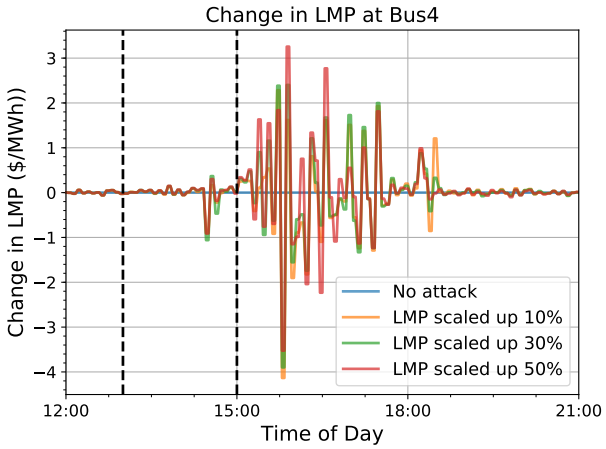


(e) Change at bus 13

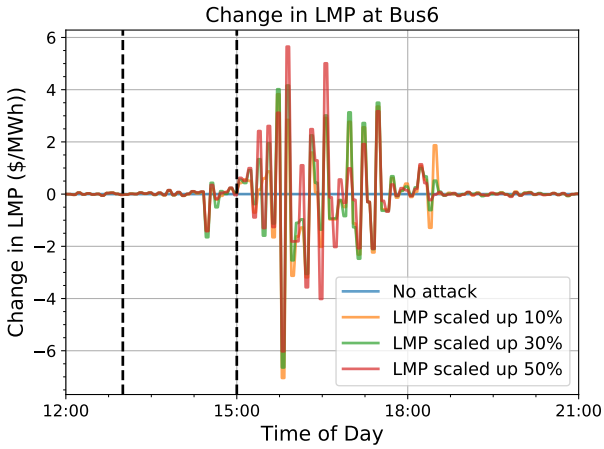


(f) Change at bus 14

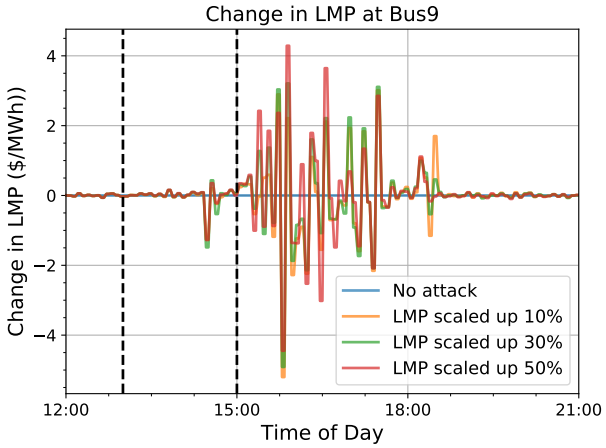
Figure A.3: Change in LMP at load buses when LMPs are scaled down in time-slot 2



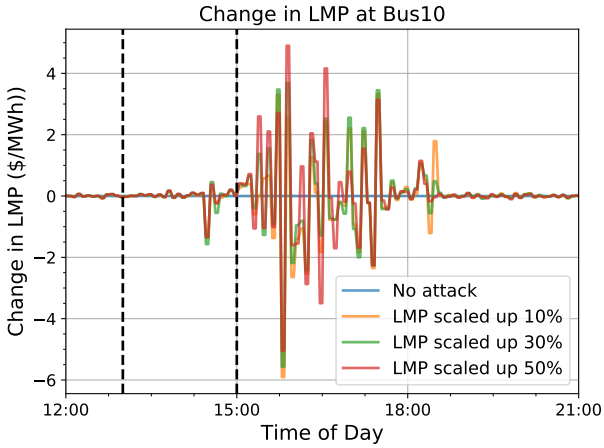
(a) Change at bus 4



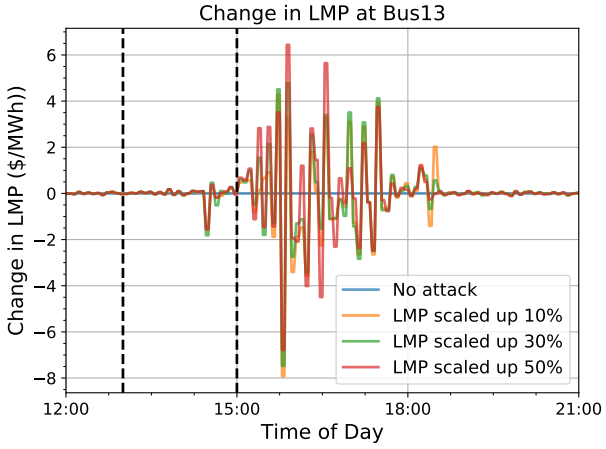
(b) Change at bus 6



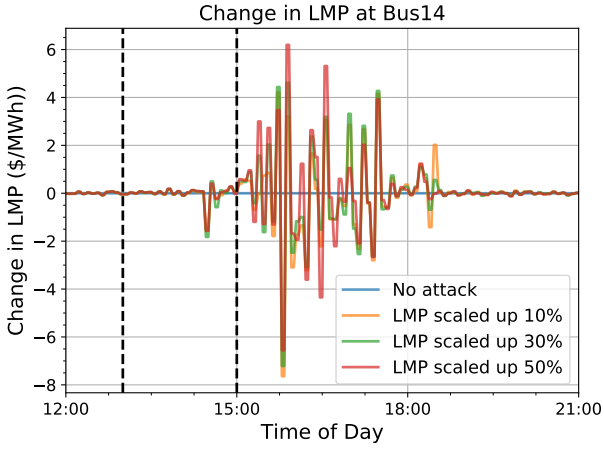
(c) Change at bus 9



(d) Change at bus 10

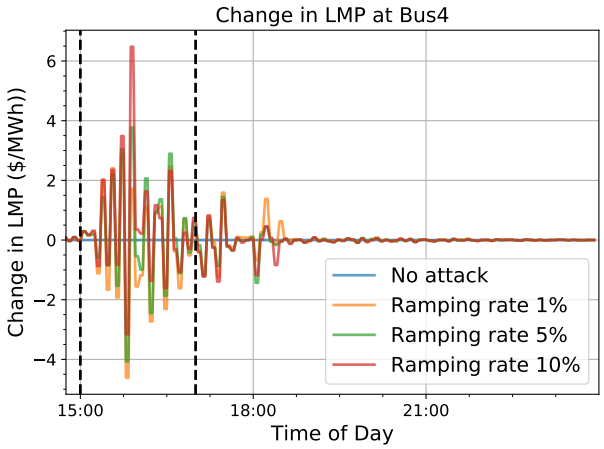


(e) Change at bus 13

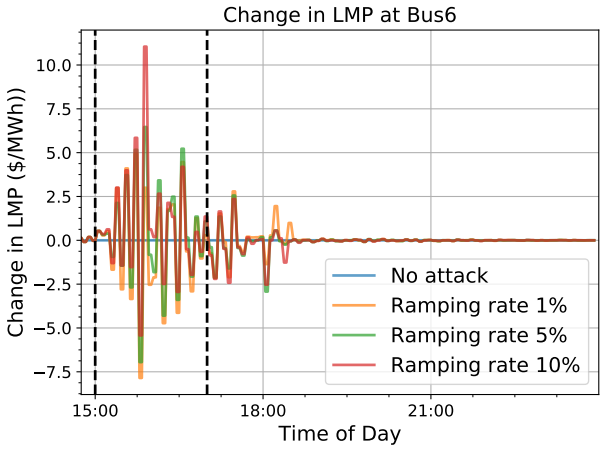


(f) Change at bus 14

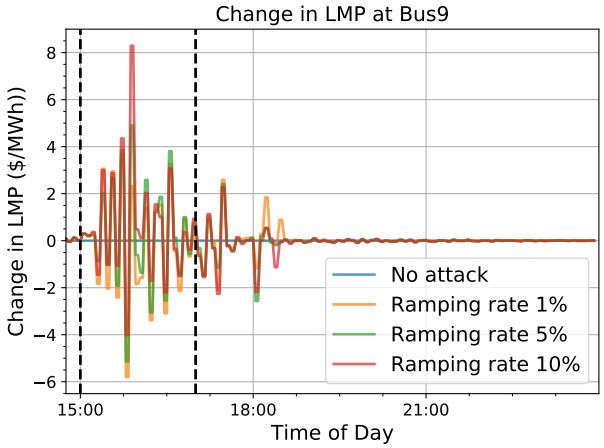
Figure A.4: Change in LMP at load buses when LMPs are scaled up in time-slot 2



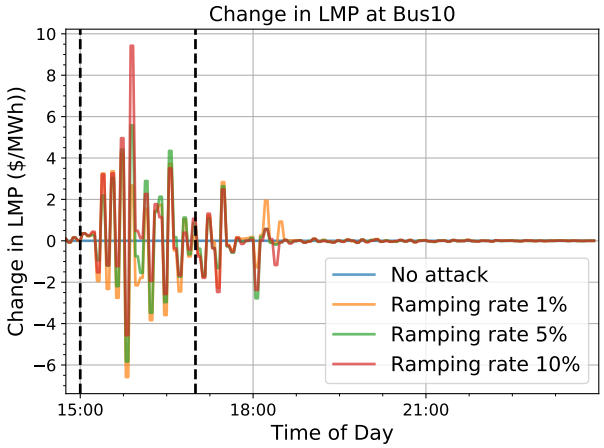
(a) Change at bus 4



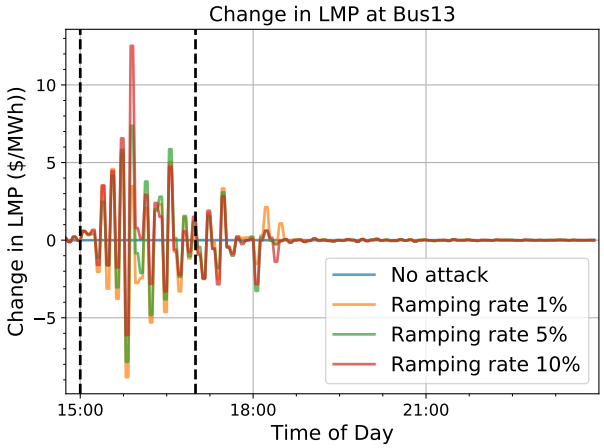
(b) Change at bus 6



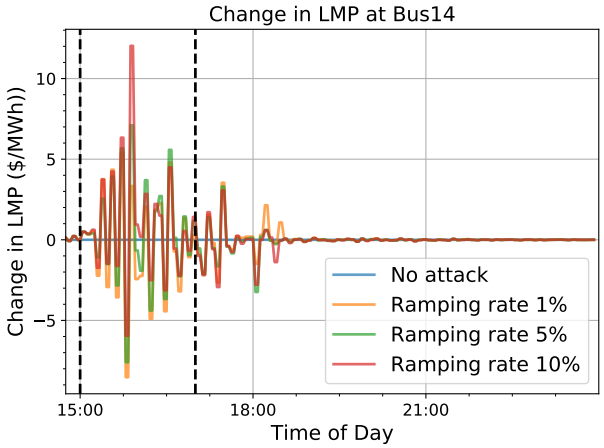
(c) Change at bus 9



(d) Change at bus 10

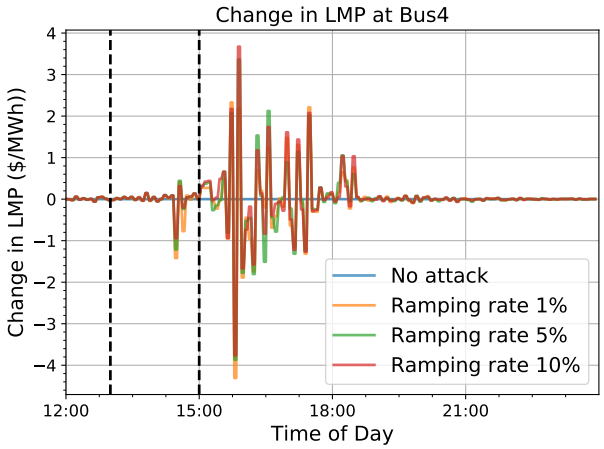


(e) Change at bus 13

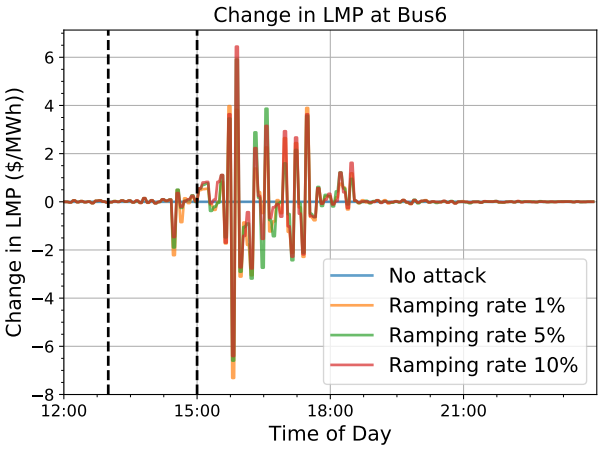


(f) Change at bus 14

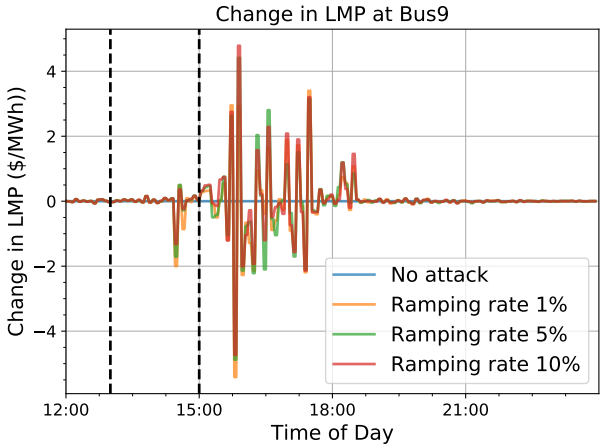
Figure A.5: Change in LMP at load buses when LMPs are ramped down in time-slot 1



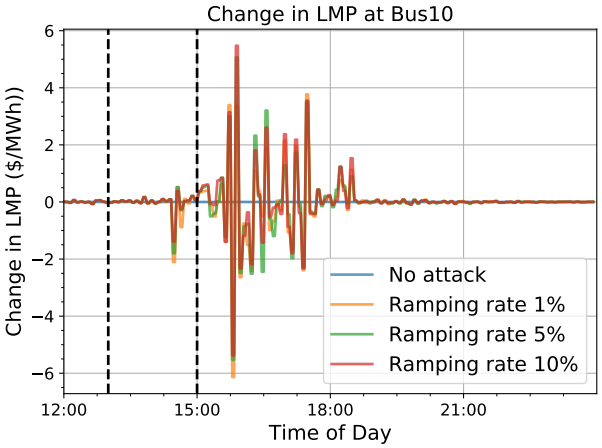
(a) Change at bus 4



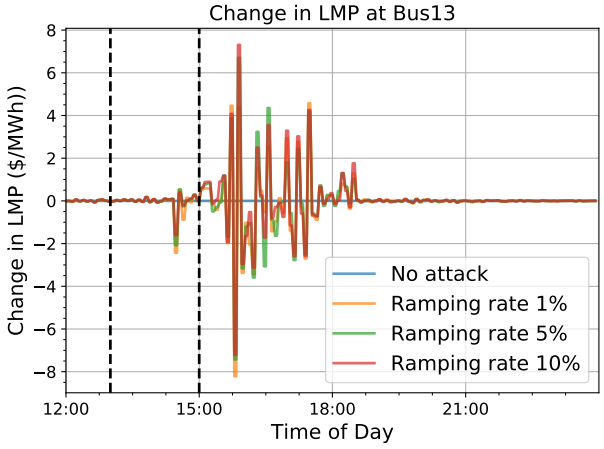
(b) Change at bus 6



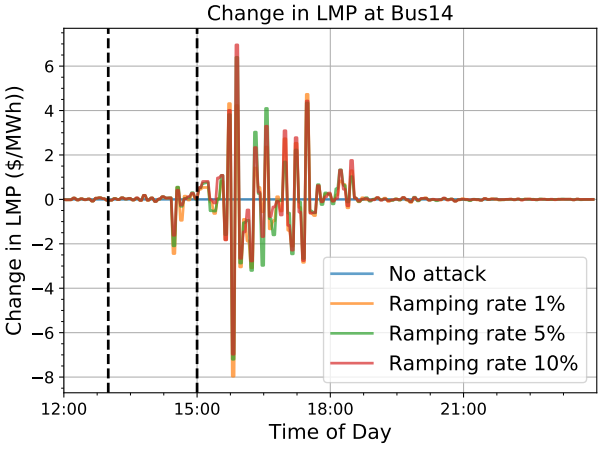
(c) Change at bus 9



(d) Change at bus 10



(e) Change at bus 13



(f) Change at bus 14

Figure A.6: Change in LMP at load buses when LMPs are ramped up in time-slot 2