METHODS TO ATTACK AND SECURE THE POWER GRIDS AND ENERGY MARKETS

A Dissertation
Presented to
The Academic Faculty

By

Tohid Shekari

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical and Computer Engineering

Georgia Institute of Technology

August 2021

METHODS TO ATTACK AND SECURE THE POWER GRIDS AND ENERGY MARKETS

Thesis committee:

Dr. Raheem Beyah, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Morris Cohen, Co-Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Lukas Graber
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Brendan Saltaformaggio
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Alvaro Cardenas
Department of Computer Science and Engineering
University of California, Santa Cruz

Dr. Saman Zonouz
School of Engineering
Rutgers University

Date approved: July 22, 2021

If you can’t fly then run, if you can’t run then walk, if you can’t walk then crawl, but whatever you do you have to keep moving forward.

Martin Luther King Jr.

To the bravest soul I have ever seen in my life, my little brother Mahdi, who has been courageously fighting with cancer for almost three years!

ACKNOWLEDGMENTS

I truly believe that this PhD degree is the direct result of my resilience, perseverance, creativity, and knowledge along with the kind help and support that I have received from other individuals. It is really hard to clearly pinpoint and duly acknowledge these individuals. One can only try!

First and foremost, I would like to express my deep appreciation to Dr. Raheem Beyah for serving as my advisor for the past four years at Georgia Tech. He is smart, kind, sharp in grasping ideas, and a truly wonderful presenter and speaker. I really enjoyed our regular discussions about the research and life challenges I have faced during this period. Without his kindness, generosity, support, and insightful comments/suggestions, I would not have been able to finish this work. During the rather long time I spent in the U.S. and was deprived of face-to-face interaction with my family, he was indeed a great friend and mentor whose advice and guidance greatly contributed to my transformation from an awkward PhD student to a (hopefully reasonably) professional researcher and colleague. I would also like to sincerely thank his wife Kali for her kindness and hospitality over the years, and wish their children all the very best.

Next, I would like to thank Dr. Morris Cohen for serving as my co-advisor and for first getting me interested in VLF receivers and their applications in security. His guidance and direct collaboration were crucial to the progress and completion of this thesis. His deep curiosity about problems of science and particularly in the VLF domain, and his ability to break problems down to simple tractable pieces, amenable to a researcher's interrogation, were truly instructive. It happened a lot that I raised a question and he, by asking clarifying questions, narrowed the problem down and guided me to the answer. I also learned a lot from his wise amiable character about how to collaborate effectively and how to extend one's network of long-term collaborators in academic circles.

I would like to thank other members of my thesis reading committee, Dr. Lukas Graber, Dr. Brendan Saltaformaggio, Dr. Alvaro Cardenas, and Dr. Saman Zonouz for serving as the other members of my committee, and for all of the support and guidance they provided. I have wonderful memories from working as a lab TA for Dr. Graber in ECE 3072 in Summer 2017. I would like to specially thank Dr. Saltaformaggio for introducing me to the fascinating world of the binary analysis and reverse engineering in his software vulnerability and security course. I also learned a lot from Dr. Cardenas during our collaborations in the last year.

One of the Georgia Tech faculty who has my utmost respect and gratitude is Dr. Maryam Saeedifard. I got to know her early on in graduate school by taking her power electronics class in Fall 2016. She is very kind and supportive, and helped me a lot find the best research area I could focus on during my PhD studies.

This dissertation could also not have been possible without the direct and indirect support from all of my labmates over the years. I was lucky to be a part of two amazing research labs at Georgia Tech: communication assurance and performance (CAP) and low frequency radio groups. From the CAP group, I would like to sincerely thank David Formby, Qinchen Gu, Sizhuang Liang, Celine Irvene, Anni Zhou, and Binbin Zhao for their kind help and support. I experienced the best moments of my life in the CAP group with them. Special thanks goes to Dr. Qinchen Gu from whom I learned a lot about computer security and programming topics. From the low frequency radio group, I appreciate the help and support from Gebreab K. Zewdie, Jackson McCormick, Nathan Opalinski, Nikhil Pailoor, Ted Slevin, Roderick Gray, Charles Topliff, David Richardson, Shweta Dutta, Liam Smith, Kevin Whitmore, Baris Gurses, Nick Gross, Marc Higginson-Rollins, and Parker Singletary. I specially appreciate Ted and Kevin for their patience in answering my questions about the AWESOME receiver and lightning sferics.

I was blessed by the friendship of few others, outside of these research groups. Mohammadreza Miranbeigi is a great friend that I had wonderful memories with in the past five years. I also consider myself a lucky person who got to know (soon to be Dr.) Amin

Gholami since 2009. We have been studying and working together since my undergraduate studies until now and I consider him as my closest friend. I have learnt so many things from him about social life, mathematics, and science. He is a truly wise, smart, hardworking, and kind-hearted person, and a highly-regarded scientist, and I am deeply indebted to him for the countless hours he has spent helping me progress in my academic and social life.

I must give tremendous thanks to my wonderful family. Without their love, support, and encouragement, I would not be able to finish my PhD and become the person I am now. My parents, Akbar and Sakineh, are the heroes of my life and the best role models I could have possibly asked for. My younger brother, Mahdi, has been so inspiring to me, especially in the past few years. He is one of the main people who has encouraged me to pursue higher academic education, and also, one of the few people that always listens to the complaints and frustrations related to my research, despite having tremendous challenges in his daily life. I deeply appreciate him and wish him the best in his life. Last but not least, I would like to thank the love of my life, Shima, for her patience, support, and kindness during the past few years. She is the one that always makes me happy and I really feel blessed to have her in my life.

This work has been partially funded by the National Science Foundation (NSF), under the following award number: 1929580.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

The power grid is a highly complex control system and one of the most impressive engineering feats of the modern era. Nearly every facet of modern society critically relies on the proper operation of the power grid such that long or even short interruptions can impose significant economic and social hardship on society. The current power grid is undergoing a transformation to a Smart Grid, that seeks to monitor and track diagnostic and operational information so as to enable a more efficient and resilient system. This significant transformation, however, has made the grid more susceptible to attacks by cybercriminals, as highlighted by several recent attacks on power grids that have exposed the vulnerabilities in modern power systems. Motivated by this, this thesis aims at analyzing the effect of three classes of emerging cyberattacks on smart grids and a set of possible defense mechanisms to prevent them or at least reduce their damaging consequences in the grid.

In the first part of the thesis, we analyze the security of the power grid against the attacks targeting the supervisory control and data acquisition (SCADA) network. We show that the existing techniques require some level of trust from components on SCADA system, rendering them vulnerable to sophisticated attacks that could compromise the entire SCADA system. As a viable solution to this issue, we present a radio frequency-based distributed intrusion detection system (RFDIDS) that remains reliable even when the entire SCADA system is considered untrusted.

In the second part of the thesis, we analyze the performance of the existing high-wattage IoT botnet attacks (Manipulation of Demand IoT (MaDIoT)) on power grids and show they are ineffective in most of the cases because of the existence of legacy protection schemes and the randomness of the attacks. We discuss how an attacker can launch more sophisticated attacks in this category which can cause a total collapse of the power system. We illustrate that by computing voltage instability indices, an attacker can find the appropriate time and locations to activate the high-wattage bots, causing (with very high probability) a complete voltage collapse and blackout in the bulk power system; we call these new attacks MaDIoT 2.0. We also propose novel effective defenses against MaDIoT 2.0 attacks by modifying the way classical protection algorithms work in the power networks.

In the third part of the thesis, we discuss how an smart attacker with access to high-wattage IoT botnet can indirectly manipulate the energy prices in the electricity markets. We name this attack as Manipulation of Market via IoT (MaMIoT). MaMIoT is the first energy market manipulation cyberattack that leverages high-wattage IoT botnets to slightly change the total demand of the power grid with the aim of affecting the electricity prices in the favor of specific market players. Using real-world data obtained from two major energy markets, we show that MaMIoT can significantly increase the profit of particular market players or financially damage a group of players depending on the motivation of the attacker. We discuss a set of effective countermeasures to reduce the possibility and effect of such attacks.

CHAPTER 1
INTRODUCTION

1.1 Motivation

The electricity grids were introduced and developed in early 1880s and their structures have changed significantly since then. The early grids were mostly small and localized while the modern ones are big and interconnected systems. Power grids were traditionally operated with a monopoly structure in which the utilities control every aspect of the grid, from generation to distribution to end users. In the traditional structure, the price of the energy was inefficiently determined by the utilities subject to the limits placed by state governments [1]. Following the occurrence of energy crisis in 1970s, the U.S. Congress decided to change the monopoly structure to allow competition in electricity production with the aim of providing better energy production efficiency and cheaper energy for the customers [2]. In the new structure, facilities that produced power more efficiently or used renewable energy along with the big energy consumers could enter the marketplace, while the transmission operators (independent system operators (ISOs) and regional transmission organizations (RTOs)) still maintained a monopoly over the management of the grid to consistently guarantee its secure operation [3].

Modern power grids are one of the most important critical infrastructures in every country, and hence, their secure and reliable operation plays a vital role in different aspects of our daily life [4–6]. Because there are strong interdependencies between the power grid and other critical infrastructures, attacks against power networks can significantly affect a vast number of industries and infrastructures [7]. Examples of critical infrastructure interdependencies are illustrated in Figure 1.1 [8]. According to this figure, it is evident that widespread and/or long-lasting blackouts in the power grid can be catastrophic. There are a

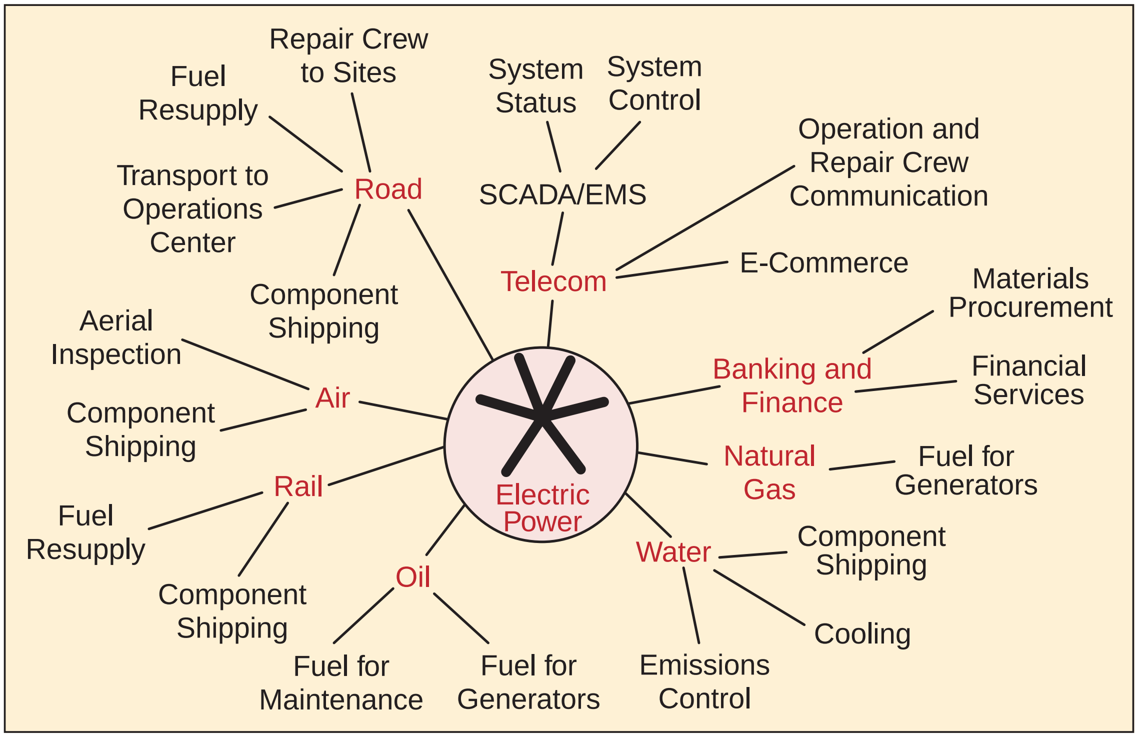


Figure 1.1: Electric power infrastructure dependencies [8].

number of threats to the reliability of the electric grid, including space weather, aging, accidents, and random failures. In this thesis, we focus on the growing threat from cyberattacks to power grids.

In recent years, security experts have raised serious concerns about the fact that the quickly evolving cyberthreat landscape is outpacing existing protection and defense mechanisms in the energy sector, especially in the power grid domain [9]. Technically speaking, there are no easy ways to address the cybersecurity issues in power grids. The reason is that power grids naturally have a very complex structure that are far more than power plants, high voltage transmission lines, transformers, and distribution lines. To understand the cybersecurity challenges in power systems, we first need to understand their general architecture. The overall architecture of a power grid can be represented with seven different component groups. These component groups can be leveraged to determine how a power grid can address the technical, operational, cybersecurity, market, regulatory, or end-customer requirements. These components are [10]:

1. **Electric Component:** This group includes the high power equipment of every power grid such as power generators, power transformers, circuit breakers (switches), and transmission/distribution lines.

2. **Industry Component:** This group represents a large number of the utilities and private-party generation units interacting with each other through the grid operation, planning, and energy markets. Note that the structure of the markets are different in every region.

3. **Control Component:** This group consists of the system control and protection schemes which are essential to the grid's continuous and optimal operation. The goal of this component is to ensure the delivery of the electric energy with high quality to the end users.

4. **Digital Component:** This group includes the devices associated with the information and communication technology (ICT) in the power grid, which are a part of its supervisory control and data acquisition (SCADA) system. This component is vital for the optimal operation and control of the grid.

5. **Convergent Networks:** This group represents the other networks which have indirect interactions with the power grid. For example, the fossil fuel and natural gas distribution pipelines are both very important in a reliable operation of every power grid.

6. **Regulatory Component:** This group denotes the state regulations on different levels of the power grid operation. The regulations vary significantly from region to region, and can significantly affect the cybersecurity aspect of the power grid operation.

7. **Coordination Framework:** This group represents the framework in which all the coordination between different groups can be done for the optimal operation of the

power grid. This task is usually done by independent system operators (ISOs) in the control centers of the SCADA system.

As it can be seen, the overall architecture of the power grid is very complex and there are so many pieces that are interacting with each other for the continuous and reliable operation of the grid [11]. The key point is that the current architecture of the power system has been designed few decades ago, when there was no cybersecurity consideration in its design. The concept of smart grid has been recently introduced and was a great improvement over the legacy power infrastructure. Smart grid was aimed at using the state-of-the-art communication and computation technologies in power grids to improve its efficiency, reliability, and economics. However, this massive increased digitization and connectivity came with a huge price of growing attack vector to cybercriminals around the world.

To discuss the key security requirements and challenges in the smart grid, we first need to take a closer look at the architecture of it. Smart grid can be technically divided into four different layers [10]:

1. **Physical Layer:** This layer represents the high voltage components of the smart grid including the traditional generation units, renewable energy resources, transmission/distribution lines, and the energy storage devices.

2. **Communication Layer:** This layer includes all the devices that are a part of the smart grid communication network, which is called the SCADA system. This network is mostly air-gapped from the Internet and can mainly be accessed internally.

3. **System Integration Platform:** This layer consists of all the components associated with the computing infrastructure, networks and security management, and data integration, which are concentrated in the control centers.

4. **Software Layer:** The software associated with meter data analysis, customer billing management, outage management, load control, etc. are categorized in this layer.

Similar to the information technology (IT) domain, the security requirements for the smart grid can be covered through the confidentiality, integrity, and availability (CIA) triad.

1. **Availability:** This security attribute, which is the most important one in the smart grid, means that information and services should be consistently and readily accessible for authorized parties at every instant. As an example, the customers should have a consistent access to the electric energy without any interruptions.

2. **Integrity:** This security attribute means that the communication data in the smart grid and the SCADA system must always be intact and unaltered. As an example, the control commands sent by the control center and the meter readings must always be accurate to have a secure and reliable grid operation.

3. **Confidentiality:** This security attribute refers to preventing unauthorized access to private information in the smart grid. This attribute is thought to be less important in the SCADA system but is absolutely critical in the end user related matters such as their billing information.

All things considered, it is obvious that cybersecurity challenges in the smart grid domain can be studied from different perspectives. One of the main security challenges in power grids is the vulnerability of the SCADA system against recent sophisticated attacks. The existing solutions are based on traditional network monitoring methods which are totally ineffective when the entire SCADA system is compromised. Also, there are a set of emerging threats in the smart grid that exploit the lack of data confidentiality in the SCADA system for different malicious purposes. This thesis studies the emerging threats caused by the aforementioned major challenges and proposes a set of real-world solutions to mitigate them or at least reduce their damaging consequences.

1.2 Research Scope and Thesis Outline

This thesis focuses on studying three major cybersecurity challenges in smart grids which are briefly outlined as follows:

1.2.1 RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid

The widespread blackout in Ukrainian power grid on December 2015 was a wakeup call that modern power systems have numerous vulnerabilities, especially in power substations which form the backbone of electricity networks. There have been significant efforts among researchers to develop effective intrusion detection systems (IDSs) in order to prevent such attacks or at least reduce their damaging consequences. However, all of the existing techniques require some level of trust from components on the SCADA network; hence, they are still vulnerable to sophisticated attacks that can compromise the SCADA system completely. The first part of this thesis presents a radio frequency-based distributed intrusion detection system (RFDIDS) which remains reliable even when the entire SCADA system is considered untrusted. The proposed system uses radio frequency (RF) emissions to monitor the power grid substation activities. Indeed, it utilizes a radio receiver as a diagnostic tool to provide air-gapped, independent, and verifiable information about the radio emissions from substation components, particularly at low frequencies (LF, 0.05−50 kHz, or $>$20 μs period). The simulation and experimental results verified that four types of diagnostic information can be extracted from radio emissions of power system substation circuits: i) harmonic content of the circuit current, ii) fundamental frequency of the circuit current, iii) impulsive signals from rapid circuit current changes, and iv) sferics from global lightning strokes. Each or a combination of the first three diagnostics can be effectively leveraged to directly detect specific types of power grid attacks. Meanwhile, the last diagnostic is utilized to check the integrity of the receiver's signal as it is encoded with the quasi-random distribution of the global lightning strokes. The simulation and real-world experimental results verified the effectiveness of RFDIDS in protecting the power grid against sophisticated attacks.

1.2.2 MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses in the Power Grid

The widespread availability of vulnerable IoT devices has been traditionally exploited to form giant IoT botnets. A particularly concerning IoT botnet is the one that can be built around high-wattage IoT devices such as EV chargers and water heaters because in large numbers they can be leveraged to abruptly change the electricity consumption in the power grid. These attacks are called Manipulation of Demand via IoT (MaDIoT) attacks, and while concerning, previous research has shown that the existing power grid protection mechanisms prevent any large-scale negative consequences to the grid. In the third part of this thesis, we deeply analyze this assumption and show that a smart attacker can launch more sophisticated attacks which can cause a total collapse of the power system. We illustrate that by computing voltage instability indices, an attacker can find the appropriate time and locations to activate the high-wattage bots, causing (with very high probability) a complete voltage collapse and blackout in the bulk power system; we call these new attacks MaDIoT 2.0. We also propose novel effective defenses against MaDIoT 2.0 attacks by modifying the way classical protection algorithms work in the power networks.

1.2.3 MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets

If a trader could predict small price changes in the stock market better than any other trader, she would make a fortune. Similarly, in the electricity market, a trader that could predict small changes in the electricity load, and thus electricity prices, would be able to make large profits. Predicting price changes in the electricity market better than other market participants is hard, but in the second part of this thesis we show that attackers can manipulate the electricity prices in small but predictable ways, giving them a competitive advantage in the market. Our attack is possible thanks to recent research that has shown how high-wattage devices such as EV chargers are able to abruptly change the total demand of the power grid. Such attacks are called MaDIoT attacks. In this thesis, we present a new variant of MaDIoT and name it Manipulation of Market via IoT (MaMIoT). MaMIoT is the first energy market manipulation cyberattack that leverages high-wattage IoT botnets to slightly change the total demand of the power grid with the aim of affecting the electricity prices in the favor of specific market players. Using real-world data obtained from two major energy markets, we show that MaMIoT can significantly increase the profit of particular market players or financially damage a group of players depending on the motivation of the attacker.

The rest of this thesis is organized as follows. The related work and literature review are discussed in Chapter 2. Chapter 3 presents RFDIDS, the air-gapped IDS for power substations and its main challenges. In Chapter 4, we will study MaMIoT, explaining how an adversary can exploit the lack of data confidentiality in the SCADA system to manipulate the electricity market prices through high-wattage IoT botnets. In Chapter 5, we will discuss MaDIoT 2.0, where the same attack vector in MaMIoT can be used for causing blackout in the target power grid. Eventually, The conclusions and possible future directions are given in Chapter 6.

CHAPTER 2

RELATED WORK

Previous work related to this research, while limited, can be divided into four broad categories of: i) IoT device security, ii) SCADA system security, iii) attacks on financial markets and historical electricity market manipulation cases, and iv) power system security.

2.1 IoT Device Security

The vulnerability and security issues associated with IoT devices have been widely investigated in [12–23]. The comprehensive study presented in [12] demonstrated that the Mirai botnet compromised around six hundred thousand vulnerable devices such as cameras, digital video recorders (DVRs), and routers in a very short period of time. Most of the devices targeted by Mirai suffered from the "poor default password policy" vulnerability. Prior to this study, it was revealed that Honeywell home controllers such as thermostats have two major vulnerabilities: an authentication bypass bug and a cross-site request forgery flaw. The former of which can be potentially leveraged to get around the authentication mechanism in the targeted device [24].

Similarly, the lack of sufficient hardware protections in Nest products can be used by an attacker to install malicious software on these devices [25]. Even older IoT devices, in which Arduino Yun microcontrollers were used, are vulnerable to cyberattacks [26]. Several papers have shown that even in modern architectures, where appliances are controlled via home assistants or mobile applications, adversaries are able to control IoT devices. By exploiting vulnerabilities in the home assistants and mobile applications, [13, 14, 27] showed that attackers can penetrate through the most unlikely channels. For example in [27], it was shown that by injecting inaudible voice commands to home assistants, attackers can control nearby connected IoT devices. In another interesting research, it was illustrated that a worm is capable of compromising Zigbee-based smart lights within a city and relinquishing control to the attacker [28]. Despite the existing extensive studies in the IoT security domain, it is obvious that these devices are still vulnerable to different types of attacks, and as a result, the emergence of large high wattage IoT botnets are a serious threat in the near future.

2.2 SCADA System Security

Attacks on the power grid SCADA system can be classified into four groups based on the end goal of the attackers: i) false data injection [29], ii) malicious command injection [30], iii) communication delay attack [31], and iv) impersonation of control center [32]. The first two groups are common and were implemented during the Ukrainian power grid blackout in 2015 [32]. In this event, the attacker opened the substation circuit breakers and cut the power to customers while feigning normal operating condition to the control center.

To secure ICSs, defense mechanisms have been developed at network and controller device levels [33, 34]. Promising recent efforts tried to ensure the satisfaction of plant integrity requirements through behavioral controller profiling [35], hardware-assisted execution monitoring [36], and formal control logic verification [37]. In the firmware level, the integrity of the control flow graph of the controller device can be checked for any possible infections [38]. In addition, the use of hypervisor architecture for controllers is an effective way to protect the device firmware against zero-day vulnerabilities [39].

Power system cyber security has been traditionally handled using network security and Internet technology (IT) practices [40–53]. The common features of these works include: i) they obtain the SCADA system measurements as an input, and ii) they leverage machine learning methods that look for statistical anomalies in a feature space (often heuristic and require significant training). For instance, the authors of [45] proposed a hybrid IDS that learns temporal state-based specifications for different possible scenarios in the system (disturbances, normal control operations, and cyberattacks). A data mining approach is then adopted to learn patterns for various scenarios.

While there are a variety of companies selling industrial control system (ICS)-specific IDSs and intrusion prevention systems (IPSs), Snort [54] is a popular free and open-source solution for power grid applications. Using Snort, researchers can define rules to detect various types of attacks. For instance, specific rules can be defined to alert operators of attackers performing reconnaissance by detecting suspected SSH password guessing, network scanning, and Modbus scanning.

However, the challenge is that power system security goals differ from traditional IT security ones due to additional requirements and conditions of operation [55]. The interconnection of the physical world and cyber world is a unique feature of modern power grids compared to traditional IT infrastructures. Therefore, most of the aforementioned solutions are still vulnerable because they: i) rely on the very components of the grid they seek to protect (e.g., sensors that monitor power grid equipment), ii) are directly connected to the power grid (and thus are “in the line of fire”), and iii) rely on the network being monitored to transport authentic security alerts. Accordingly, it is still theoretically possible that the solutions themselves can be compromised. This partially motivates the need for security solutions that are completely decoupled from the system they monitor.

Purely cyber processes can be monitored directly through physical channels, since they emit physical emanations of different modalities. Past efforts using physical channels (decoupled from the systems being monitored) illustrate the feasibility of targeted secret information disclosure (e.g., cryptographic keys) and signal probes [56–58]. These works explore technologies to associate the running state of a physical device with its involuntary analog emissions across different physical modalities. Electromagnetic emissions, acoustic emanations, power fluctuations, and thermal output variations are the main physical modalities used in previous works. In this chapter, we will use the RF emissions of the substation circuits to detect malicious activities of attackers. The machine learning-based studies presented in [59–61] have leveraged high frequency electromagnetic emissions emanated from processors of computers and embedded devices to monitor the program execution path.

2.3 Attacks on Financial Markets and Historical Electricity Market Manipulation Cases

Financial markets have been recently a popular target for cybercriminals around the world. In this line, hackers have leveraged the concept of market manipulation to affect the specific market players or the entire market with the aim of gaining monetary profits or causing financial damage to the market players. Market manipulation can be defined as the deliberate and malicious interference with the market values to create an artificial price for a tradable entity [62]. One of the main ways employed by cybercriminals to implement the market manipulation attack in financial markets is the DDoS attack. In this attack the adversary deliberately reduces the availability of products and/or services from a targeted company or even an entire financial exchange platform, to affect the associated stock prices. Many companies which deliver services to their clients via online or web applications could fall victim. In this type of attack, while the victim does not experience physical loss, they could be severely affected by the negative consequences of service unavailability and reduced investor confidence.

The biggest market manipulation attack campaign which leveraged the DDoS attack against U.S. financial markets to date was the Operation Digital Tornado campaign organized by a group called L0ngWave99. Between February and April 2012, this campaign launched over six DDoS attacks against U.S. securities and commodities exchange [62]. The Al-Qassam Cyber Fighters, known as QCF, was an attack campaign supported by anti-Western rhetoric group Hamas that claimed responsibility for Operation Ababil, a series of DDoS attacks against U.S. financial institutions between 2012 and 2013 [62]. The full list and detailed explanation of attacks in this category can be found in [62].

In the electricity market domain, since the passage of the Energy Policy Act of 2005, fraud and market manipulation have been the top enforcement priority of the Federal Energy Regulatory Commission (FERC). For fiscal year 2018, FERC reported 16 potential market manipulation cases, 14 of which were closed with no action [63]. The reason for most of these no action closures was that no evidence was discovered on the detail and mechanism of the attacks which greatly undermined the credibility of allegations. From this we see that market manipulation attack in electricity markets is an emerging field which needs significant research and investigation.

2.4 Power Grid Security

Power system cyber security issues have been widely studied in the past few years [5, 29, 30, 32, 64–84]. Attacks on power systems can be classified into three main groups based on the ultimate goal of the attacker: i) attacks targeting the power grid communication infrastructure, ii) attacks targeting the power grid stand-alone components, and iii) attacks targeting the power grid indirectly.

In the first group, the adversaries' main goal is to compromise the supervisory control and data acquisition (SCADA) system, which is a communication network to remotely monitor and control the power grid. The notable attacks in this category are: i) false data injection, ii) malicious command injection, iii) communication delay, and iv) denial of service (DoS) attacks [64–67]. False data injection attacks are used for manipulating the measurements in the SCADA system to cause false evaluation on the system status in the control center [29]. This can lead to erroneous or inaccurate control decisions, and eventually result in widespread blackouts. In the case of malicious command injection attacks, attackers send inaccurate commands to system actuators such as circuit breakers to cause widespread outage in the grid [66]. Since the power grid is monitored and controlled in a real-time manner, communication delay attacks can cause inaccurate control decisions and instability of the entire system [66]. Finally, attackers can launch DoS attacks on the SCADA system. In this attack, the system actuators do not accept control commands from the control center [67], which could eventually make the entire system unstable. In order to detect the aforementioned four types of attacks and defend against them, secure state estimation (SE) algorithms have been proposed in the literature[29, 68–72]. These methods are able to estimate the true state of the power grid despite being fed with inaccurate and delayed measurements.

In the second group (attacks targeting the power grid stand-alone components), attackers compromise the local controllers such as programmable logic controllers (PLCs) and remote terminal units (RTUs) with various types of malware to cause damage in the power system components. Although these malware can damage stand-alone equipment in the system, extensive propagation of them can affect the entire grid severely and cause regional or nation-wide blackouts. As the first malware in this category, the Aurora attack was introduced and tested by the Idaho National Laboratory in 2007 [73]. Aurora mainly targeted power generators by forcing them to get out of a synchronous state. First, the malware would disconnect the targeted generator from the grid, and then, wait for the generator to slip out of sync, and quickly reconnect it back to the grid [74]. This series of operations can cause extreme mechanical stress on the generator's rotor and eventually lead to explosion. The effect on the generator is akin to getting your car up to 90 mph on the highway and then suddenly shifting to reverse. The Aurora attack can be detected and prevented by incorporating the synchronism checking functionality to protective relays of the generator [75].

Dragonfly was a Russian group that used a set of Trojans and worms to infect the equipment controllers of the power grid generation sector and cause sabotage in major power plants [76]. They targeted several energy generation facilities in the U.S., Canada, Turkey, and Switzerland between 2013 and 2017 [77]. General defense mechanisms such as employing the defense-in-depth strategy were used to mitigate the risk of Dragonfly malware. Following the Dragonfly campaign, Blackenergy emerged as a powerful Trojan which targeted power substations. Blackenergy's main functionality was to open the substation's circuit breakers and cut the power to customers. This malware was the primary reason for the Ukrianian power blackouts that occurred on December 2015 and 2016, in which more than 230,000 people were left without power for over six hours [30, 32, 78]. Most recently, a group of researchers from the U.S. and Germany have introduced Harvey, a PLC rootkit which launches a physics-aware stealthy attack on power grid components such as power generators [79]. Harvey infects the firmware of the PLC and replaces the legitimate control commands by malicious ones before they are sent out by the PLC's output ports to the physical actuators. It also simulates the physical process to calculate the values of the benign sensor readings. Sending these fake sensor values to the monitoring system allows Harvey to keep the attack stealthy. As explained in [79], power grid components can be reliably protected against Harvey by implementing remote attestation and secure boot mechanisms.

In the third group of power grid attacks (attacks targeting the power grid indirectly), the adversaries try to indirectly affect the normal operation of the system and cause sabotage in stand-alone components or blackout in the entire grid [5, 80–84]. This class of attacks was first introduced in [80] where the system total demand was altered by the intruders to cause overflow in the power transmission lines and other system components to push the grid towards instability. The basic mechanism of the attack stems from compromising the load control signals associated with big industrial loads and data centers. By securing the communication channels between the control center and controllable loads, the risk of this attack is greatly reduced. The possibility of load altering to attack big data centers with the aim of causing power outage in them was studied in [81]. The paper showed that exploiting the attack vectors in cloud environments (platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS)) can be effectively used for taking down big data centers. According to this paper, defense and prevention mechanisms for such attacks are either impractical or extremely expensive.

The authors in [82] developed a software-based protection scheme to detect and protect against the load altering attacks introduced in [80]. This protection system is purely software and does not require any changes in the traditional communication channels/protocols.

In [5, 83, 84], the authors studied the possibility of exploiting compromised IoT devices to alter the total demand of the power grid and cause instability in the system. More specifically, the method developed in [83] is an optimization-based approach which requires a complete knowledge about the power grid (topology of the grid, detailed parameters of the transmission lines/generators, and real-time regional generation/demand). However, implementation of this attack is very challenging in practice as the required information may not be readily available to attackers. To overcome this challenge, Dabrowski et al. proposed a new method to increase the total system demand through remotely activating CPUs, GPUs, hard disks, screen brightness, and printers to cause frequency instability in the European power grid [84]. Although the new approach did not require as much detailed information about the system components, the number of compromised IoT devices needed for a successful attack is quite high because the devices do not consume a lot of power. Soltan et al. proposed the use of high wattage IoT devices to launch various types of attacks (frequency instability, power line cascade tripping, and black start restoration interruption) on a power grid to cause blackouts in the entire system [5]. This novel attack, called Manipulation of demand via IoT (MadIoT), was further analyzed by Huang et. al. [6] and it was shown that the introduced attack is not as effective as it was illustrated in [5]. The new analysis in [6] revealed that while MaDIoT attacks could have negative effects on the power grid operation, it is extremely hard to cause a widespread blackout in the system through this attack. According to these analysis, the existence of conventional protection schemes in the grid can effectively protect the system against random MadIoT attacks. However, these protection schemes were mainly designed to help the power grid withstand against credible contingencies and there was no consideration of the manipulation of demand attacks in their configurations [85, 86].

CHAPTER 3

RFDIDS: RADIO FREQUENCY-BASED DISTRIBUTED INTRUSION DETECTION SYSTEM FOR THE POWER GRID

3.1 Introduction

3.1.1 Aim and Motivation

The electricity grid is a highly complex control system and is one of the most impressive engineering feats of the modern era. Modern societies critically rely on the proper operation of power delivery systems in nearly every facet [87–89]. There are a number of threats to the reliability and security of the electric grid, including space weather, aging, accidents, and random failures. In this chapter, we focused on the growing threat from cyberattacks to power grid substations.

The world's first known successful cyberattack on a power system is the Ukrainian power grid attack which took place on December 23, 2015. During this event, the attackers used spearphishing in order to gain access to the SCADA system of multiple substations by posing as a trusted entity [32]. Following the attack, circuit breakers in 30 substations were switched off, and more than 230,000 residents were left without power [30, 78]. At the same time, the attackers spoofed the SCADA network traffic and reported a normal operating condition to the control center. A key aspect of the incident was a distributed denial of service (DDoS) attack on the call centers so that customer complaints could not be received by the power company. Between this and the spoofing of network traffic, the company was unaware of the attack until it was too late. By this point, the substations were shut off and would not accept commands from the power company to come back online [32].

After this attack, the number of power outages due to cyberattacks has increased dramatically. Ukrainian power grid blackout in 2016 as well as the discovery of Dragonfly 2.0 as a root cause for a set of outages in the U.S., Turkey, and Switzerland are testimonies to this claim [30, 76, 78, 90]. Prior to 2013, Dragonfly targeted defense and aviation companies in the U.S. and Canada. Additionally, the recent attacks on the U.S. power grid by Russia are a sobering wake-up call that the power grid needs securing [91–93]. The aforementioned attacks on power systems mainly focused on substations, which form the backbone of electricity networks. Substations offer a large attack surface as they are widely distributed throughout the power networks. As an illustrative example, there are $\sim$70,000 substations across the U.S. [94].

Industrial facilities and individual customers can and do utilize backup power generation, typically with several hours of available backup. For some foreseeable events such as hurricanes, fuel can be stored to allow several days of backup power. But, this cannot be relied on for unpredictable events like cyberattacks, or months-long outages that may result from severe damage. Therefore, we need a reliable and robust intrusion detection system (IDS) for the power grid to detect attacks early and potentially reduce their damaging consequences.

To detect attacks early and potentially reduce their damaging consequences, we need a reliable and robust IDS for the power grid. The existing IDSs focused on securing power substations through monitoring the network traffic of the SCADA system. Accordingly, if the attacker can compromise the SCADA network entirely, the IDS will not be able to detect his malicious activities in the substation. Motivated by this fact, the aim of this chapter is to propose an air-gapped distributed IDS which monitors the substation activities by radio frequency (RF) measurements (as a side channel) to verify the correctness of the SCADA network traffic. With this approach, the SCADA system is assumed to be an untrusted entity.

3.1.2 Contributions

A radio frequency-based distributed intrusion detection system (RFDIDS) is proposed in this chapter to quickly detect cyberattacks in power system substations. The basic idea behind the novel approach is that any AC circuit in a substation invariably emits a magnetic field which our receiver can very easily detect. Our antenna setup reliably captures four useful attributes of the magnetic field in power substations: i) magnetic field harmonic content (circuit current harmonic content), ii) magnetic field fundamental frequency (system fundamental frequency), iii) magnetic field impulsive emissions (impulses in the circuit current caused by switching actions), and iv) lightning sferics. The useful information that can be extracted from each of the first three attributes were mentioned inside the parenthesis. The first three quantities measured by our system will be compared to the SCADA network traffic, hence providing an air-gapped and redundant mechanism to power system monitoring and diagnostics. Circuit breaker malicious switching, transformer malicious tap changing, false data injection to protective relays, and control center are the most important attacks which can be detected by RFDIDS. We also utilize a unique and novel method to authenticate the collected data using the quasi-random sequence of global lightning encoded into the magnetic field data (last mentioned attribute), meaning that low frequency (LF) magnetic field data cannot be spoofed/played back by an attacker. As the proposed system is non-invasive, it can be easily augmented onto existing substations. This system can be realized as an extension of an existing open source IDS such as Snort. Indeed, it can act as a complementary physical signal-based diagnostic and can be codified as a Snort module. The salient features of the proposed methodology are summarized as follows:

- RFDIDS is air-gapped from the power system substation components and uses a side channel (RF emissions) to estimate the operating status of the substation;
- The developed methodology can protect the power grid against attacks that can compromise the entire grid and all of its attached components;

- The measured signal from the side channel cannot be spoofed/played back as it is encoded with the impulses from lightning strokes occurred in far distances.

These features make RFDIDS robust and resilient against advanced types of attacks in which the attackers can simultaneously compromise the SCADA and RF measurement systems.

The rest of this chapter is organized as follows. The threat model and the overview of the proposed scheme is given in section 3.2. Then, section 3.3 presents the background information about the power grid, RF measurements, and lightning authentication scheme. The detailed methods to extract useful data from RF measurements in substations will be explained in section 3.4. Next, section 3.5 represents simulation and experimental results to verify the effectiveness of the proposed approach. The robustness and resilience of the new method in challenging situations are thoroughly discussed in section 3.6. Finally, the conclusion and possible directions are given in section 3.7.

3.2 Threat Model and Scheme Overview

An overview of the considered threat model and RFDIDS structure is illustrated in Figure 3.1. As shown in this figure, RFDIDS has four inputs: i) magnetic field data from the LF receiver (located inside the substation fences), ii) lightning database signal, iii) lightning signals from the receivers located in nearby substations, and iv) measurements from the SCADA system and direct sensors. Also, the global positioning system (GPS) signal is used to synchronize the inputs of RFDIDS with each other. In the first step, the integrity of the LF antenna signal is checked using first three inputs and the method described in subsection 3.3.3. If the signal integrity is verified, the second step will be executed; otherwise, an alarm, as a sign of intrusion, is sent to the control center via a secure mobile backchannel separate from the SCADA communications, and the substation control changes to manual mode. In the second step, RFDIDS extracts the substation measurements and control actions from the SCADA network traffic and antenna signal (i.e., the method described in

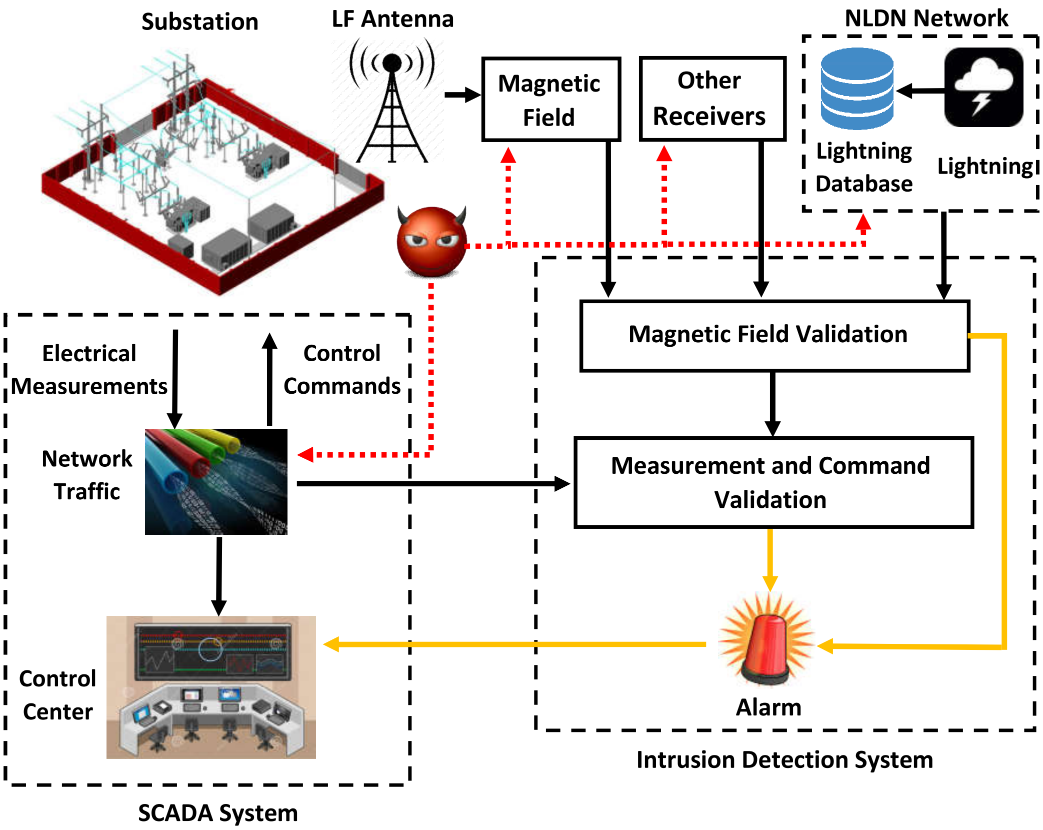


Figure 3.1: The overall structure of RFDIDS.

section 3.4). If there is any inconsistency between these two, RFDIDS will set the alarm signal and changes the substation control to manual mode to prevent further potential adversary actions.

The main assumptions of the threat model are: i) the SCADA system is totally compromised by the attacker, and hence, is untrusted, ii) a knowledgeable attacker will be fully aware of the substation configuration, its control mechanisms, and even our algorithm, and iii) GPS is a secure and trusted entity[1]. In this chapter, the possible attacker is classified into four main groups:

- Attacker level 1: This attacker has background in ICS/SCADA security but he has no knowledge on electromagnetic analysis;

[1] Even if the GPS signal is considered untrusted, the attacker needs to spoof $\lfloor \frac{n}{2} \rfloor + 1$ of the receivers to cause a false negative in RFDIDS. Meanwhile, spoofed GPS signals cannot cause false positives.

- Attacker level 2: This attacker has background in both ICS/SCADA security and electromagnetic analysis;
- Attacker level 3: This attacker has background in both ICS/SCADA security and electromagnetic analysis as well as complete knowledge of and access to the lightning database;
- Attacker level 4: This attacker has background in both ICS/SCADA security and electromagnetic analysis as well as complete knowledge of and access to the lightning database and geographical information about the power grid.

Each of these attackers and possible defense mechanisms are discussed in below.

3.2.1 Attacker Level 1

This attacker can only compromise the SCADA system. Therefore, the SCADA system is assumed to be completely untrusted. However, the magnetic field measurement signal from the LF antenna, the global lightning database, and sferics detected from other LF antennas remain trusted entities. The attack is carried out such that the substation equipment behaves maliciously despite sending legitimate measurements to the control center. For instance, the attacker opens a distribution line circuit breaker to cut the electricity to customers while sending the circuit breaker close status to the control center. The attacker can launch a DDoS attack on the call centers so that customer complaints do not reach the power company (as was done during the Ukrainian power grid blackout in 2015 [30, 78]). Consequently, the power company is unaware of the attack until it is too late. Substations are therefore shut off and do not respond to commands to come back online. Accordingly, the system operator in the control center observes normal operating conditions while customers have no electricity.

In this type of attack, the antenna signal can be authenticated successfully using the method described in subsection 3.3.3. In the next step, to defend against the attack, our methodology infers substation measurements and control actions from the magnetic field signal and compares the results with the SCADA network traffic to identify the malicious activities in the substation. In this step, the RF signal will show the circuit breaker opening action while there is no circuit breaker operation report in the SCADA system. Therefore, the control center will be able to intervene before the attacker can impart long-term damage.

3.2.2 Attacker Level 2

This attacker can go one layer deeper and compromise both the SCADA and the LF magnetic field measurement systems simultaneously. Accordingly, in this type of attacker, we also cannot trust any data from the LF magnetic field measurement system. However, the lightning database and sferics data from other receivers are still trusted entities. Lightning database is formed by a network of LF receivers, and includes the location, occurrence time, and intensity of lightning strokes in each time instant. As it will be discussed in subsection 3.3.3, by extracting the sferics from the LF measurement signal and comparing them with the presumed arrival times based on current lightning locations, we can check the integrity of the antenna's signal in real time. Should the LF data fail the authentication test, the control center may intervene to prevent significant damage. After the validation of magnetic field signal, the rest of the algorithm is similar to the one that we used for attacker level 1. Note that in this case, the attacker needs to entirely compromise two air-gapped systems (i.e., SCADA and LF measurement systems) at the same time, which is an extremely hard task.

3.2.3 Attacker Level 3

This attacker can completely compromise the SCADA system, antenna measurement system, and global lightning database. Hence, the only trusted entity in the case of such attacker is the sferics data from other receivers located in nearby substations. In this situation, the only way to authenticate the antenna signal is to leverage the sferics data from other receivers using the method described in subsection 3.3.3. If the signal authentication test fails in the first step, an intrusion alarm will be set in the control center; otherwise, the SCADA system validation test will be executed to find any sign of intrusions in the SCADA system. It should be noted that the attacker would have to compromise three separate, air-gapped systems in this type of attack, and yet his malicious activities will be detected by RFDIDS.

3.2.4 Attacker Level 4

This attacker can compromise the SCADA system, antenna measurement system, lightning database, and a portion of the other RF receivers in nearby substations. As we will describe later in subsection 3.3.3, even in this situation, if only one LF receiver works correctly, it will cause inconsistency in the lightning authentication scheme, illustrating a sign of an attack. The attacker compromising three air-gapped systems plus additional receivers' signals in nearby substations is an unlikely scenario, if not impossible.

3.3 Background

3.3.1 Power Grid Overview

The power grid is defined as an interconnected electricity network which aims to deliver electricity from producers to consumers [95]. A system-level view of a power grid and its different sectors are shown in Figure 4.3. The grid consists of three main sectors, i.e., generation, transmission, and distribution, which are connected together through substations [89]. In the generation sector, much of the required energy is produced in large scale power plants at medium voltage (e.g., 13.8 kV). Then, the generated power is stepped up to a higher voltage (e.g., 345 kV) and is connected to the bulk power transmission network through substations to be transmitted over long distances. Finally, the electricity is stepped back down to the medium voltage level by substations as it nears consumers. The distribution sector feeds the consumers within a limited geographical area with medium

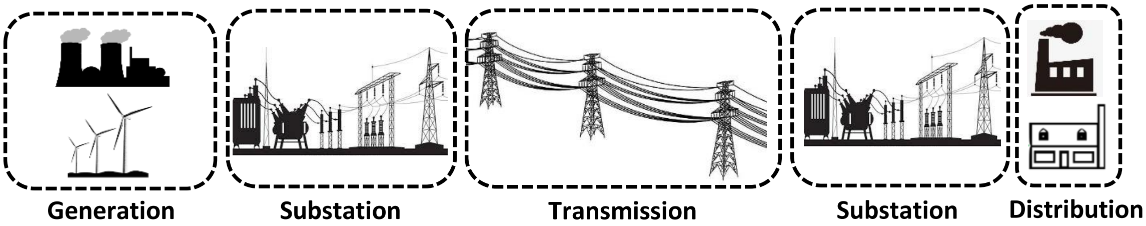


Figure 3.2: The overall view of a power grid and its different sectors.

voltage.

Inside the substations, there are measurement devices (e.g., current transformers (CTs) and voltage transformers (VTs)), which are responsible for measuring the electrical attributes of the substation circuits to monitor the condition of the whole substation. These measurements are polled periodically (every few seconds) in remote terminal units (RTUs) to be transmitted to the control center, where the goal is to monitor and control the entire power grid. The collection of RTUs from different substations along with the control center form a meshed communication network called SCADA system [11]. In the control center, energy management system (EMS) uses the gathered data to perform state estimation (SE). Doing so, the state variables (e.g., bus voltage magnitudes and their corresponding angles) of the power grid are calculated. The results of the SE are used in EMS applications such as system security assessment, optimal power flow (OPF), and reactive power control. EMS applications perform different calculations in order to specify control decisions to be implemented in the substations or power plants. The main control actions that can be implemented in power system substations are circuit switching (to change the topology of the grid) and transformer tap changing (to keep the system voltage level within its acceptable range). Since wide-area control of the power grid is based on remote measurements from substations, if the SCADA system is compromised by an attack, substations can be critically damaged. Alternatively, falsified data can trick the operator into making damaging erroneous changes, causing long-lasting widespread power blackouts.

Owing to the key role of substations in power systems, they have been a popular target for attackers to cause widespread blackouts [30, 96]. New technologies including microprocessor-based intelligent electronic devices (IEDs) and standardized networking protocols (e.g., TCP/IP) over wide area networks (WANs) are widely adopted in the substations. Remote access to IEDs or user interfaces in a substation for maintenance purposes is common. Further, there are many potential system vulnerabilities in substation components, e.g., unsecured standard protocols, remotely controllable IEDs, and unauthorized remote access to substation IEDs [97–101]. In addition, some substation IEDs have web servers which open them up to malicious remote configuration changes. The fact is, the power grid has a vast attack surface with many components that are insecure. Thus, it is critical that we provide novel ways to protect this vital system.

It is worth mentioning that even if firewalls and cryptography schemes are used for cybersecurity, weak security key management cryptography and misconfigured firewalls are still exposed to intruders. From the IT point of view, cybersecurity issues are well known and new security technologies are available. However, security research on the integration of IT and physical power systems, as an important critical infrastructure, is still an emerging area.

3.3.2 Radio Frequency (RF) Measurements and AWESOME Receiver

RF measurement of the magnetic field refers to capturing the magnetic field oscillations in the frequency range of <300 GHz [102]. Since the fundamental frequency of the power grid is 60 Hz, in our proposed method, we focused on the LF range (<100 kHz) signals, which are within the range of the RF emissions generated directly by power lines. The LF radio receiver to collect the magnetic field emissions, known as atmospheric weather electromagnetic system for observation, modeling, and education (AWESOME) [103], was completed in 2010 and then upgraded in 2015. The distinguishing features of this receiver are extremely good sensitivity, frequency and phase response, timing accuracy, and dynamic range. Accordingly, we used this receiver in our method to capture the magnetic fields of substation circuits. The detailed explanation about AWESOME receiver can be

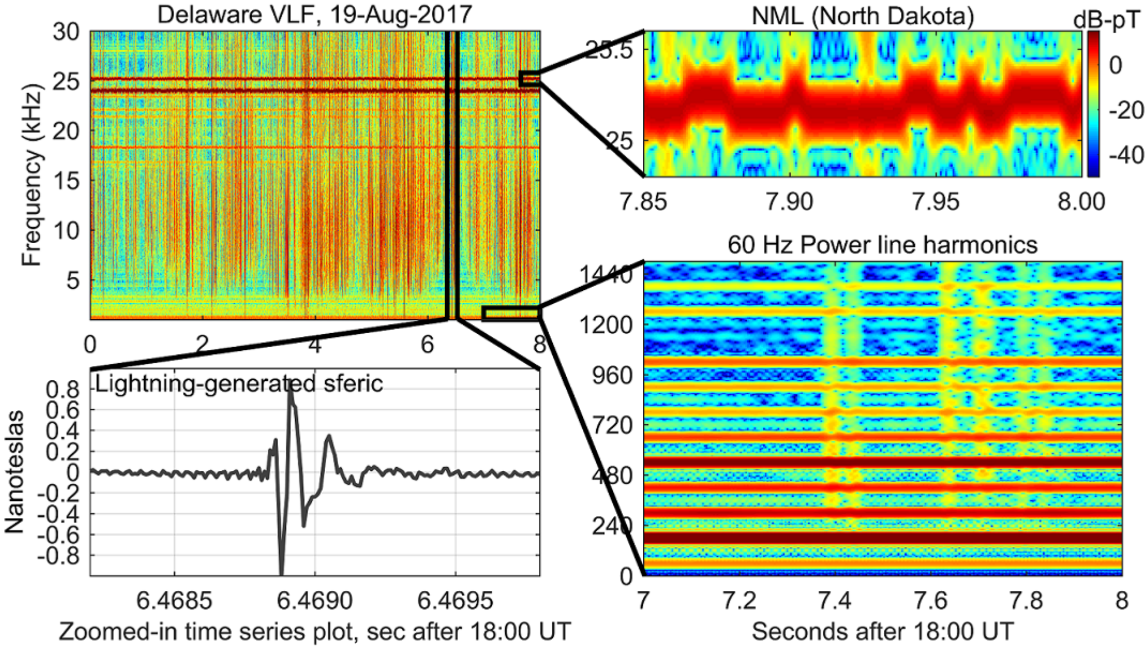


Figure 3.3: Sample of an LF radio signal and its different components.

found in [103].

An example of LF radio data recorded by AWESOME receiver is shown in Figure 3.3. These data are taken from a receiver in Dover, Delaware, recording magnetic field as a function of time. The top left panel shows a spectrogram of the data, with horizontal axis in seconds, vertical axis in frequency, and color indicating the strength of each frequency at each time instant. The horizontal lines in the top left spectrogram are radio stations used by the U.S. Navy for submarine communications. A zoom-in in the top right panel shows one in particular known as NML, at 25.2 kHz, which broadcast from North Dakota, very far away from the receiver. The vertical lines in the spectrogram show radio atmospherics, or ‘sferics’. These may originate from lightning strokes many thousands of miles away, so could be from almost anywhere around the world. Since a lightning flash occurs roughly 40 times per second on average, and the sferic travels to global distance, there are numerous sferics in the data, as is clearly evident in this example. The arrival times and amplitudes of the sferics are determined by the quasi-random distribution of global lightning at that moment. One selected sferic is shown in the lower left thumbnail. The characteristics of this sferic are complex and depend on the type of lightning, the distance from the lightning stroke to the receiver, and the propagation conditions in the upper atmosphere. As such, each sferic looks unique. Roughly speaking, this is a random natural phenomenon. Indeed, it is almost impossible to get a similar lightning signals in two different time instants. Technically a lightning sferic lasts roughly 1 ms. If there is exactly 1 sferic randomly inserted each second, and conservatively assuming we have only 1 ms arrival time accuracy then, the probability of two 1-second segments having the same impulse location would therefore be 1/1000. In practice, we have many sferics per second which reduces this probability to be exceedingly small. The interesting point is that the AWESOME receiver can detect sferics regardless of weather conditions. The bottom right panel of Figure 3.3 shows the harmonics of 60 Hz observed in the receiver. This particular receiver is located at an educational museum not near a substation, and yet many harmonics of 60 Hz are clearly detected due to the high sensitivity of the receiver.

3.3.3 Lightning Watermark and Global Lightning Detection Database

A critical differentiator of our approach is a novel scheme to authenticate the measured RF signal. While many smart grid cybersecurity efforts involve setting up a new sensor, they all share the same issue that if a capable hacker gains access to the SCADA system, all these sensor data can be faked. However, our LF data diagnostic does not suffer from this limitation, and thus, is more secure against spoofing/replay attacks.

Typical LF data contains not only the power line harmonic radiation and impulses, but also the sferics from global lightning strokes as described in subsection 3.3.2. An example of LF data detected at multiple sites is shown in Figure 3.4. The top three panels show magnetic field signatures in a single second at three sites in Georgia, USA. The bottom three panels show a close-up of a 12-ms segment. There are a huge number of impulsive sferics from lightning all over the world at any time, many of which are detected by GLD360 (i.e., a network of RF receivers to detect lightning strokes around the globe), as shown in the

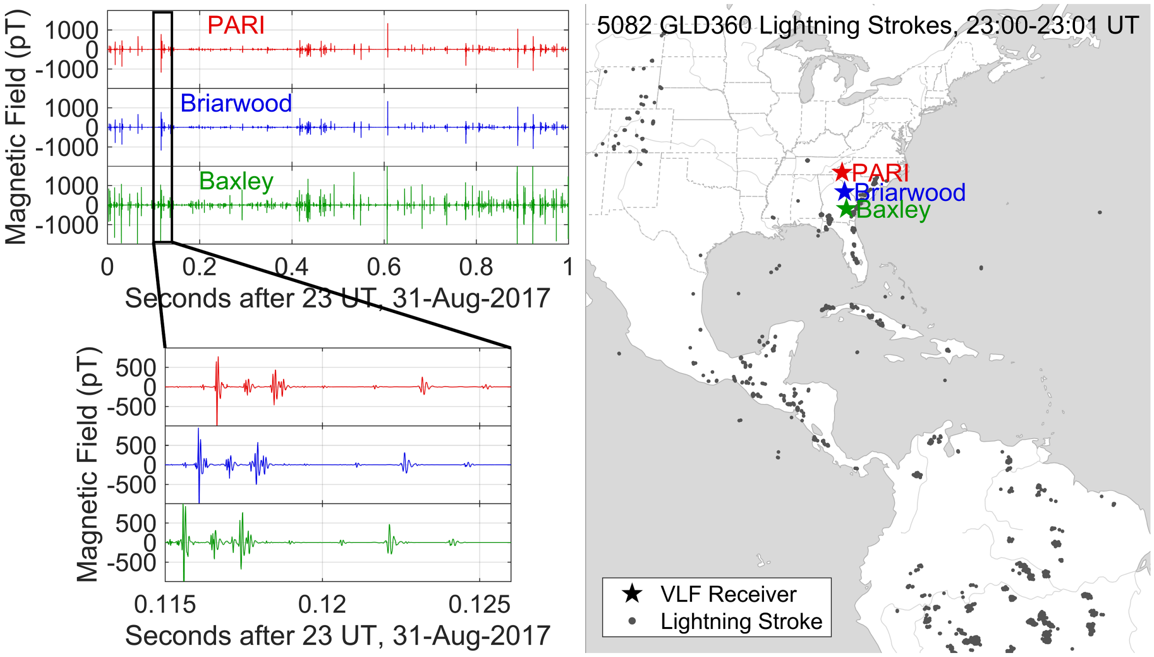


Figure 3.4: Lightning impulses (sferics) at multiple LF radio receivers.

map on the right. As an interesting observation, this quasi-random distribution of impulses acts as a watermark/nonce.

With the knowledge of lightning times and locations detected by GLD360, one could easily check that the impulse arrival times are consistent with the global constellation of lightning, by simply accounting for propagation delays around the world at close to the speed of light, calculating the expected arrival times of sferics, and then verifying that impulses do indeed appear, thus authenticating the data.

Interestingly, however, even if perfect knowledge of global lightning activity did in fact exist and were available to a hacker, it would still be extremely difficult, if not impossible, to synthesize LF data. As the shape of a sferic evolves with distance and as a function of time of day, season, and other factors, synthesizing accurate LF data would require computationally intense physical models of propagation between the Earth and ionosphere that cannot be run anywhere near real time [104]. As such, the quasi-random distribution of global lightning makes for a one-way function that allows easy authentication but is practically impossible to synthesize. We will later discuss in subsubsection 3.6.1 that only

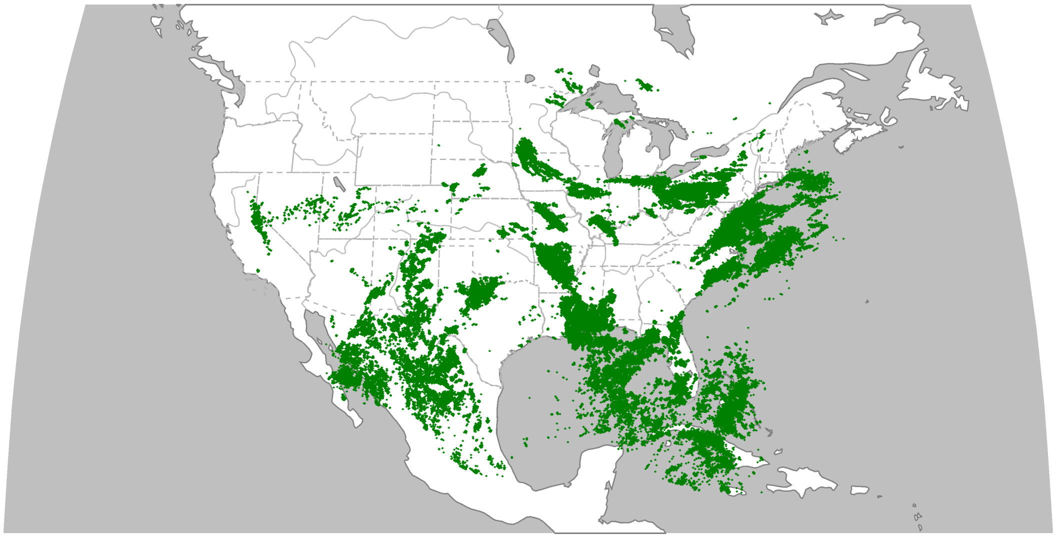


Figure 3.5: Lightning locations within the continental USA on 19-Aug. 2017.

replay attack is possible (not feasible) to be implemented on RFDIDS.

The lightning data are available from the Global Lightning Detection 360 (GLD360) network, which provides precise time (μs accuracy), location (km accuracy), and intensity of the vast majority ($\sim$80%) of lightning strokes around the globe. GLD360 uses an earlier version of the AWESOME receiver, licensed to a company called Vaisala [105]. Figure 3.5 shows an example of lightning locations within the continental USA on 19-Aug. 2017. Using this precise database of lightning locations and times, it is straightforward to predict arrival times of impulsive sferics that should be seen by an LF receiver at any location. In fact, by having the GPS coordinates of the lightning strokes and the substation, we can calculate how long it takes a lightning signal to travel to the substation location. The accuracy of this prediction depends on the time accuracy of the GPS signal ($< 1\mu$s). As an example, Figure 3.6 shows the occurrence time of lightning strokes and their corresponding expected arrival time to a substation located in Atlanta, GA, USA within a 200 ms time window. In this chapter, we use the national lightning detection network (NLDN) database, which has the functionality similar to GLD360. However, NLDN captures the lightning sferics in the continental USA and is more precise than GLD360, meaning that in a constant time window, NLDN can capture more sferics than GLD360.

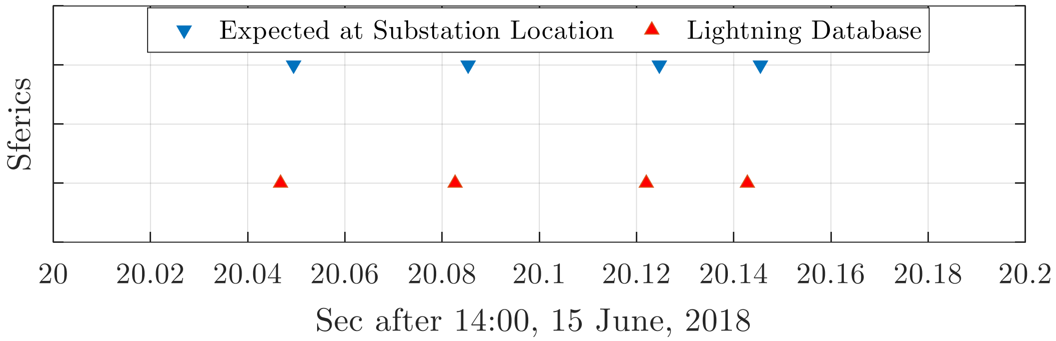


Figure 3.6: The occurrence time of lightning strokes and their corresponding expected arrival time to the substation location (located in Midtown Atlanta).

The general structure of the lightning authentication scheme is shown in Figure 3.7. As can be seen, this scheme has three inputs: i) LF antenna signal which includes the magnetic field of the substation circuit, ii) lightning database which is acquired from a network of RF receivers, and iii) the detected sferics from the receivers located in nearby (e.g., $<$100 km) substations. The lightning authentication scheme leverages the correlation between these three inputs to identify any attacks on any one of them. The algorithm extracts the sferics from the first input by removing the signal caused by power line current, as formulated in Equation 3.1 [106]. The resulting signal consists of a small noise with some impulses (sferics) (see top left corner in Figure 3.4). We can define a threshold to detect the time of these sferics and identify their occurrence time.

$$B_{sferics}(t) = B(t) - B_{power}(t), \tag{3.1}$$

where $B(t)$ is the measured magnetic field signal (first input), and $Bpower(t)$ is the magnetic field signal caused by power line current which can be determined by a mathematical process expressed in section 3.4.

The second input (i.e., lightning database) has three attributes including lightning location, its occurrence time, and its current intensity. Given the location of a lightning strike and a substation, also occurrence time of that lightning, we can easily calculate the expected arrival time of sferics at the substation location. The reason is that the impulsive

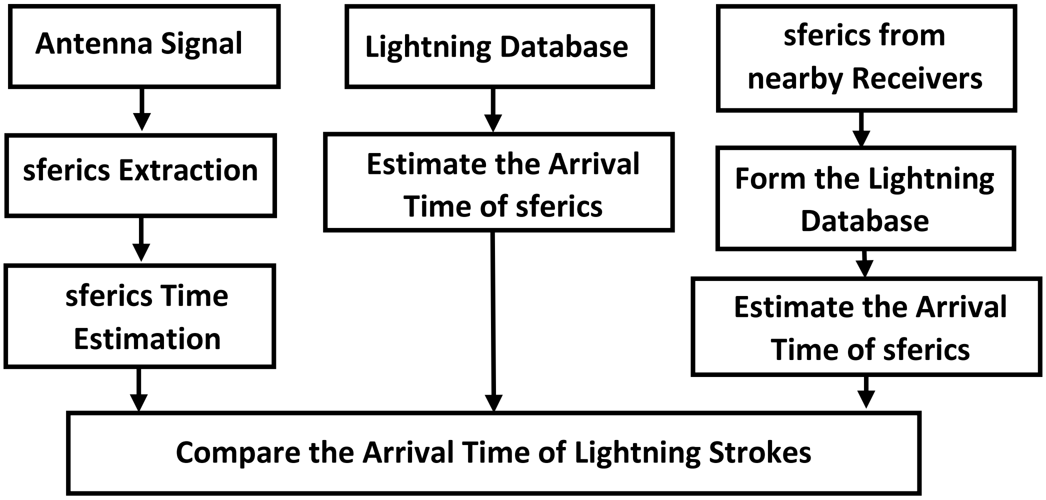

Antenna Signal
Lightning Database
sferics from nearby Receivers
sferics Extraction
Estimate the Arrival Time of sferics
Form the Lightning Database
sferics Time Estimation
Estimate the Arrival Time of sferics
Compare the Arrival Time of Lightning Strokes

Figure 3.7: The general structure of the lightning authentication scheme.

electromagnetic signals from the lightning strokes travel at the speed of light in vacuum. The bottom left corner of Figure 3.4 illustrates the sferics detected from three receivers at different locations. As can be seen, the sferics have the same shape with various detection time which results from their different distances from the lightning locations.

To improve the security of the lightning authentication method, we used the third input which is sferics from nearby substations. Since each utility owns a large number of substations (e.g., 50), this input can be used to form a secondary lightning database. To explain in more details, the time and location of the lightning strokes can be determined by three receivers forming a triangle. Suppose that our algorithm gets the sferics arrival time from three different substations (i.e., t_1, t_2, and t_3) as shown in Figure 3.8. In this figure, t_0, x_0, and y_0 are three parameters which identify the lightning occurrence time and its location. For t_1, one can write the following equation:

$$t_1 = t_0 + \frac{\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2}}{c}, \tag{3.2}$$

where c is the speed of light in vacuum. This equation means that the arrival time of a lightning sferic to a substation is a function of its occurrence time and the distance between the lightning location and the substation. By writing two other equations for t_2 and t_3

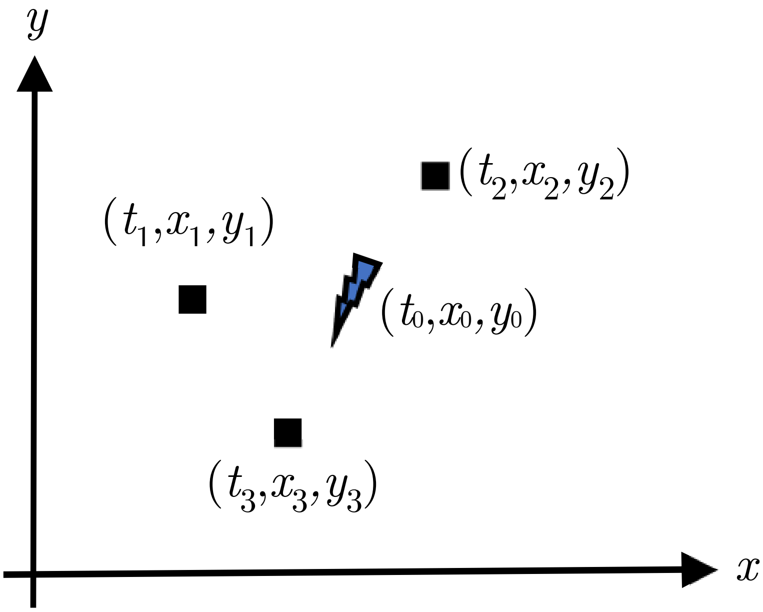


Figure 3.8: Three different substations with LF receivers and a lightning strike between them.

similarly, we will have three independent equations with three variables (i.e., t_0, x_0, and y_0). Solving this system of equations will form the secondary lightning database with lightning locations and occurrence time. Similar to the second input, this new database can be used to authenticate the first input signal.

Considering the above mentioned inputs in each substation, we can obtain three sequence of sferics within the specified time window. Any inconsistency between the arrival time of the sferics in these three inputs will likely be a sign of intrusion. Axiomatically, the existence of the third input increases the reliability of the RFDIDS by improving its data redundancy. In fact, even if the attacker can compromise the lightning database (second input) or it is not available at all, our method can still reliably authenticate the receiver's signal via the third input. In this condition, at least three other receivers from nearby substations are needed. In the other case, if only one substation deploys the receiver, the lightning database (the second input) can be leveraged to authenticate the measured LF signal.

3.4 Radio Frequency (RF) Measurements in Power System Substations

As mentioned in subsection 3.1.2, at least four types of diagnostics can be extracted from the measured magnetic field signal: current signal harmonic content, power system fundamental frequency, impulses from sudden changes in the current signal, and sferics. The method for obtaining the last attribute (i.e., sferics) was explained in subsection 3.3.3. In the following sections, we will explain how we can extract the other three attributes. To do so, first, we need to find the relationship between the current flowing through a three-phase circuit and the corresponding measured magnetic field by our receiver. Technically, the magnetic field emission from a current density in the three-dimensional space can be calculated from the magnetic retarded vector potential. To explain in the mathematical format, the magnetic retarded vector potential, $\overrightarrow{A}$, for a given point source in the space can be calculated as [104]:

$$\vec{A}\left(\vec{r}\right) = \frac{\mu_0}{4\pi}\overrightarrow{I_i}\frac{e^{-jk\left|\vec{r}-\overrightarrow{r_i}\right|}}{\left|\vec{r}-\overrightarrow{r_i}\right|}, \tag{3.3}$$

where $\overrightarrow{I_i}$ and $\overrightarrow{r_i}$ are the current (as a phasor) and location of the i^{th} point source, respectively, with respect to the origin, k is the free space wavenumber, and $\overrightarrow{r}$ is the location of the receiver (i.e., the location where the magnetic field of the source point is measured). It should be noted that the free space wavenumber can be calculated as $k = 2\pi f/c$, where f denotes the frequency of the current flowing in the source point. Considering the fact that one can split each power line to small pieces of source points, the total magnetic retarded vector potential from the source points can be written as:

$$\vec{A}\left(\vec{r}\right) = \frac{\mu_0}{4\pi}\sum_i \overrightarrow{I_i}\frac{e^{-jk\left|\vec{r}-\overrightarrow{r_i}\right|}}{\left|\vec{r}-\overrightarrow{r_i}\right|}. \tag{3.4}$$

In addition, the method of images is used to account for the ground plane, allowing the entire problem to be treated as homogeneous free space. Therefore, every current element is accompanied by an image current, at the opposite location on the other side of the ground plane, with horizontal current magnitude in the opposite direction. All things considered, the magnetic field at a given location (i.e., $\overrightarrow{B}(\overrightarrow{r})$) can be calculated through Equation 3.5.

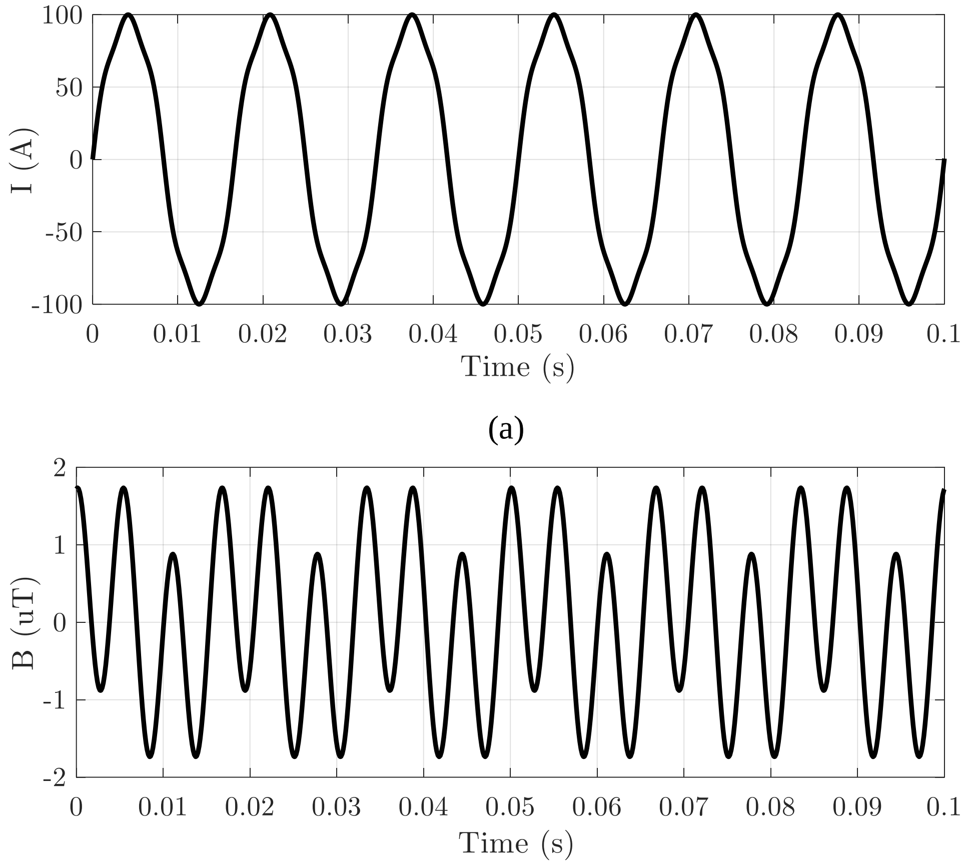
$$\overrightarrow{B}(\overrightarrow{r}) = \nabla \times \overrightarrow{A}(\overrightarrow{r}), \tag{3.5}$$

where ∇ is the curl operation on the given vector. Assuming the balanced three-phase condition in the circuit, one can calculate the magnetic field resulting from the three lines of the circuit in terms of the current flowing in one of the phases. Accordingly, in a fixed location for the receiver, the magnetic field of a three-phase line in each frequency can be expressed as follows:

$$B_f(I_f) = K_f I_f, \tag{3.6}$$

where B_f, K_f, and I_f denote magnetic field, constant coefficient, and current amplitude of the circuit at a certain frequency (f), respectively. Therefore, by analyzing the magnetic field measurements at each frequency, one can simply estimate the features of the circuit current (i.e., harmonic content, fundamental frequency, and impulses). Figure 3.9 illustrates the current signal of a typical three-phase circuit and its corresponding magnetic field which can be seen from a 4 m distance below the circuit in the ground. Although the shapes of the waveforms look totally different, they have relatively definable relationship. The reason for this difference is that K_f is not the same in different frequencies. For this specific example, $K_f = 5.89 \times 10^{-9}$ for all of the harmonics except those of multiples of three (e.g., 60×6 Hz). In the case that the current has a harmonic of a multiple of three, $K_f = 2.88 \times 10^{-7}$. In practice, we can calculate K_f in the location of our receiver inside the substation and hence, by measuring the magnetic field of the substation circuits, we can reconstruct the current signal of different circuits.

Note that the magnetic field signal that can be seen by the AWESOME receiver is slightly different than what is shown in Figure 3.9, because this receiver has an inherent



(a)

(b)

Figure 3.9: Typical waveform of: (a) Line current of a three-phase circuit, (b) Corresponding magnetic field.

high pass filter inside that which further affects the measured signal. To explain in more details, Figure 3.10 depicts the harmonic content of typical three-phase circuit current. The black solid line shows the frequency response of the AWESOME receiver filter. Finally, the harmonic content of the measured magnetic field signal by AWESOME receiver is illustrated in Figure 3.10(b). Since we already know the behavior of the receiver's filter and the value of K_f in different frequencies, by analyzing the harmonic contents of the LF signal, we can estimate the useful information about the actual current signal of the substation circuits, which are leveraged in the proposed IDS.

3.4.1 Harmonic Content and Fundamental Frequency of the RF Signal

The aim of this section is to present the mathematical method for estimating the harmonic content and fundamental frequency of the measured magnetic field signal. As shown earlier in section 3.4, the magnetic field signal is a periodical one with different harmonics. Accordingly, the general form of the antenna signal ($B(t)$) can be represented as follows:

$$B\left(t\right) = B_0 + \sum_{n=1}^{m} B_n \sin\left(n\omega_0 t + \phi_n\right), \tag{3.7}$$

where B_n and ϕ_n denote the amplitude and phase of the n^{th} harmonic, respectively. Also, ω_0 stands for the fundamental angular frequency and can be defined as $\omega_0 = 2\pi f_0$. Finally, B_0 is the DC component of the receiver's signal. In Equation 3.7, there are $2m+2$ variables (i.e., $B_0, ..., B_m$, $\phi_1, ..., \phi_m$, and f_0) which should be determined by our algorithm. In this chapter, we use the nonlinear least-square algorithm to estimate the aforementioned parameters of the antenna signal [107]. This algorithm finds the best fit of the measured signal to the specified mathematical form of that (i.e., Equation 3.7). Suppose that we have a data window with $N > 2m+2$ samples. Therefore, for k^{th} data sample, we can write the following equation:

$$\begin{gathered} B\left[k\right] = B_0 + \sum_{n=1}^{m} B_n \sin\left(n\omega_0 \Delta T k + \phi_n\right), \\ \forall k = 0, 1, .., N-1 \end{gathered} \tag{3.8}$$

where ΔT denotes the sampling time period. Now, let's define $\boldsymbol{x}$ and $\boldsymbol{B}$ as the vector of variables and data samples, and f as the function which represents the right hand side of Equation 3.8. The dimensions of $\boldsymbol{x}$ and $\boldsymbol{B}$ are $(2m+2) \times 1$ and $N \times 1$, respectively. Accordingly, we can rewrite Equation 3.8 as:

$$\boldsymbol{B} = f(\boldsymbol{x}). \tag{3.9}$$

With some mathematical manipulations [107], it can be proven that we can estimate the value of $\boldsymbol{x}$ iteratively as:

$$\boldsymbol{x}_{i+1} = \boldsymbol{x}_i + \left(f'^T(\boldsymbol{x}_i)f'(\boldsymbol{x}_i)\right)^{-1} f'^T(\boldsymbol{x}_i)(\boldsymbol{B} - f(\boldsymbol{x}_i)), \tag{3.10}$$

where $f'(\boldsymbol{x})$ stands for the first derivative of f with respect to $\boldsymbol{x}$. We continue this process until we get to the convergence point, that is:

$$|\boldsymbol{x}_{i+1} - \boldsymbol{x}_i| < \varepsilon \tag{3.11}$$

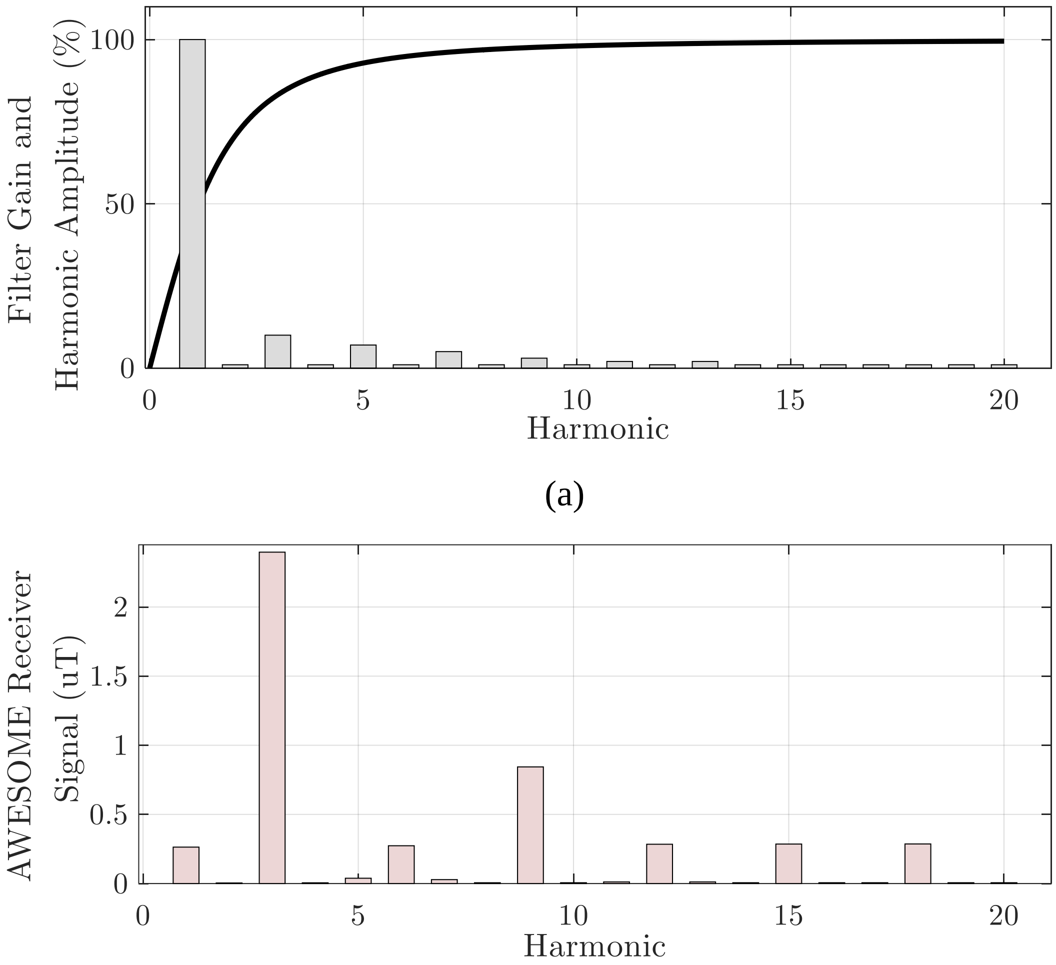
3.4.2 Impulses in the RF Signal

The aim of this section is to extract the impulses from the receiver's signal. These impulses stem from either the circuit breaker switching actions or lightning strokes. However, there are distinguishing features that allows us to differentiate between the impulses from lightning strokes and circuit breaker operation. The main difference is that the circuit breaker operation impulse is always accompanied by a sudden drop/increase of the first harmonic (e.g. 60 Hz) in the circuit current, and hence, the magnetic field emission from that circuit. Moreover, the resulting impulse from a circuit switching causes higher electromagnetic overshoot than that of a lightning sferic. In this chapter, we used the equation stated in Equation 3.1 to extract the impulses from magnetic field signal.

3.5 Numerical Validation and Case Studies

3.5.1 Measurement Setup

In order to have comprehensive analysis, we will present a set of experimental results as well as simulation ones in the following sections. The experimental results come from the measurements inside multiple power substations. The first two substations are owned by



(a)

(b)

Figure 3.10: Illustration of: (a) Harmonic content of a typical circuit current and AWESOME receiver filter response (100 A = 100%), (b) Harmonic content of the corresponding receiver signal.

Choptank Electric, A Touchstone Energy Cooperative, which is a not-for-profit, member-owned, electric distribution Co-op serving approximately 54,000 residential, commercial, and industrial members in all 9 counties on Maryland's Eastern Shore (over 6,264 miles) [108]. Another substation is located in an urban area in Atlanta, Georgia, USA and is owned by Georgia Power, which is the largest utility that is operated by Southern Company. Georgia Power is an investor-owned, tax-paying public utility that serves more than 2.4 million customers in 155 counties of Georgia [109]. We have built an LF antenna, which consists of 20 AWG copper wire wrapped around a 23-cm-diameter circle in 42 turns, to

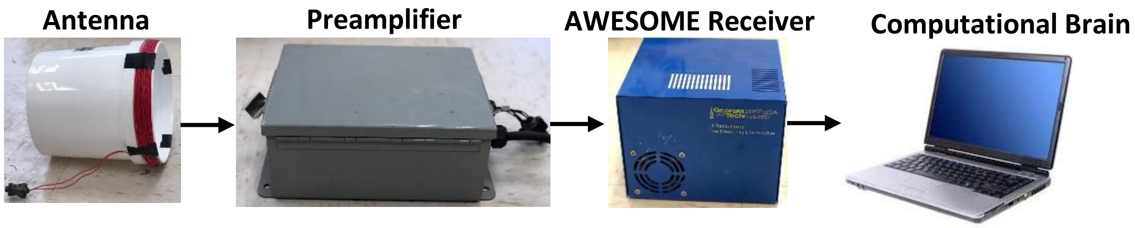


Figure 3.11: Different components of the measurement setup.

capture the magnetic field emissions from these substations. In order to gain a good signal quality, have the impedance matching, and capture a suitable bandwidth, we designed the antenna such that its resistance and inductance are 1.0 Ω and 1.0 mH, respectively. The antenna placed right below the AC circuits on the ground with 10 ft distance, such that its surface is perpendicular to the circuit current. The general view of the measurement setup is shown in Figure 3.11. In our setup, we used 1 MHz as a sampling frequency for capturing the LF data. In some cases, we did not have access to experimental results because of the attacks considerable economic consequences (several million dollars). In such cases, we illustrated the RFDIDS's performance through simulation results. In the simulations, we considered worst case operating conditions and scenarios to assure the promising performance of RFDIDS. For instance, to model the measurement noise, 10% (or 20 dB SNR) Gaussian noise is superimposed onto the magnetic field measurement signal [110, 111].

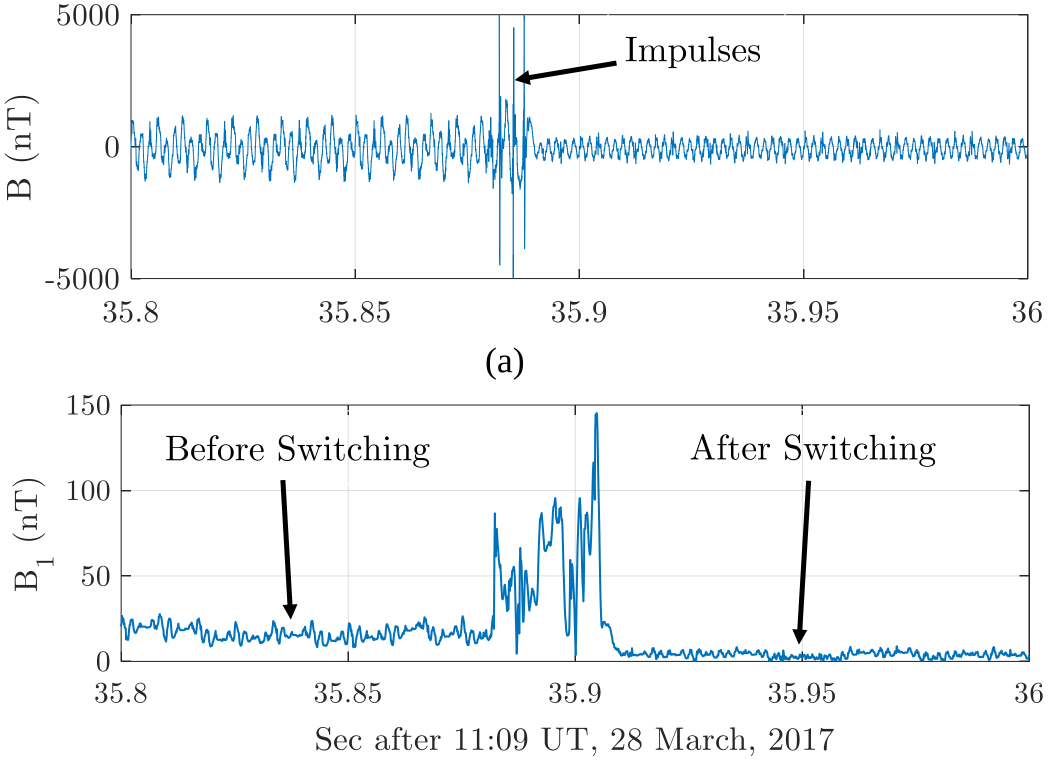
3.5.2 Attack Scenarios on Substations

The air-gapped IDS described above can be applied in a variety of situations to secure power system substations against cyberattacks. Some important applications of our method are explained in the following subsections. Note that the applicability of the proposed structure is not limited to the mentioned cases. In fact, any attack that changes the current waveform of a power circuit has the potential to be detected by RFDIDS.

Circuit Breaker Malicious Switching

The opening or closing of circuit breakers by an attacker can lead to large-scale power outages such as the Ukrainian power grid blackouts in 2015 and 2016 [30, 32, 78]. The circuit breaker operation is accompanied by a sudden decrease/increase in the line current. This generates a radiated magnetic field impulse along with a reduced/increased 60 Hz magnetic field around the power line. Accordingly, the impulsive signals and amplitude of the 60 Hz component of the magnetic field are two diagnostic tools that are leveraged for detecting switching events. Note that these two conditions should occur at the same time to represent the circuit switching event as there are other normal conditions which can cause one of the aforementioned situations. For example, in the case of load increase/decrease, the amplitude of the 60 Hz component will increase/decrease without the presence of any impulses. Also, the presence of impulse without the change in the 60 Hz component implies the lightning sferics.

To evaluate the developed theory, we recorded the magnetic field of substation circuits during several switching events using our measurement setup. Since planned switching actions rarely (e.g., every six months for maintenance purposes) occur in power substations, we only had a chance to record the magnetic field of substation circuits during several (i.e., three opening and three closing) switching actions in three substations mentioned in subsection 3.5.1. From the multiple switching incidents, two general cases are chosen to be illustrated in this section. However, the following explanations hold true for all of the recorded cases. Figure 3.12 illustrates the magnetic field signal and its 60 Hz component as a function of time. As can be seen, the circuit breaker opening occurs at 11:09:35 since there are three impulse signals (corresponding to three phases of the circuit breaker) with reduced 60 Hz magnetic field (drops to zero) after the circuit transient. Because this event was a legitimate circuit breaker operation, the magnetic field signal is consistent with the network traffic which is shown in Figure 3.13. According to this figure, the trip command is sent to the circuit breaker at 11:09:35 utilizing the *Select then Operate* function code in



(a)

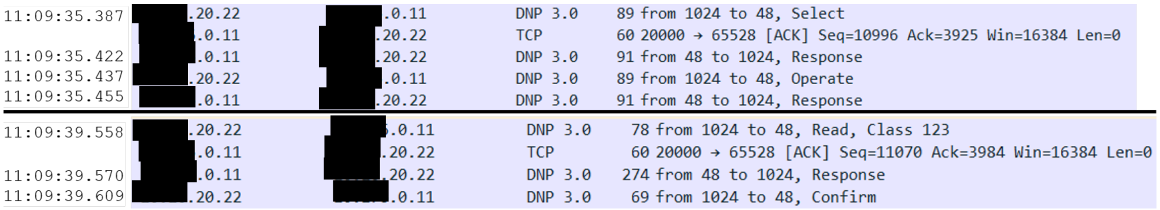
(b)

Figure 3.12: Measured magnetic field in a real-world substation during a circuit breaker opening event: (a) Magnetic field, (b) 60 Hz component of the magnetic field.

DNP 3.0 protocol. Four seconds after the operation of the circuit breaker, the master controller reads the status of the breaker to make sure the trip command has been implemented successfully. In the case of an attack, we will see the normal operating condition (no sign of switching) in the network traffic as the attacker tries to hide his malicious activity. In contrast to the circuit opening event, Figure 3.14 shows the magnetic field signal and its 60 Hz component as a function of time during a circuit closing incident. The impulses along with the increase in the 60 Hz harmonic (suddenly increases from zero) at 11:47:44 implies a circuit breaker closing event.

Transformer Malicious Tap Changing

A transformer is a critical and expensive piece of equipment in power system substations that transfers electrical power between two circuits through electromagnetic induction.

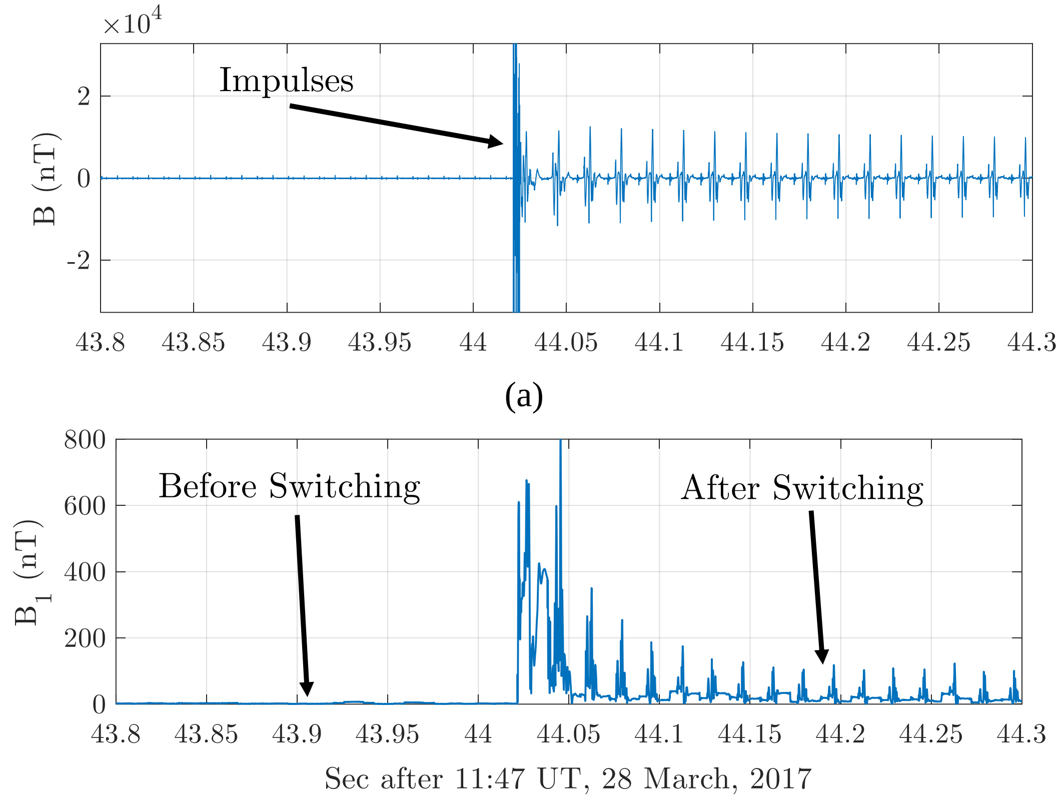


```
11:09:35.387 [redacted].20.22   [redacted].0.11    DNP 3.0    89 from 1024 to 48, Select
             [redacted].0.11    [redacted].20.22   TCP        60 20000 → 65528 [ACK] Seq=10996 Ack=3925 Win=16384 Len=0
11:09:35.422 [redacted].0.11    [redacted].20.22   DNP 3.0    91 from 48 to 1024, Response
11:09:35.437 [redacted].20.22   [redacted].0.11    DNP 3.0    89 from 1024 to 48, Operate
11:09:35.455 [redacted].0.11    [redacted].20.22   DNP 3.0    91 from 48 to 1024, Response
11:09:39.558 [redacted].20.22   [redacted].0.11     DNP 3.0    78 from 1024 to 48, Read, Class 123
             [redacted].0.11    [redacted].20.22    TCP        60 20000 → 65528 [ACK] Seq=11070 Ack=3984 Win=16384 Len=0
11:09:39.570 [redacted].0.11    [redacted].20.22    DNP 3.0   274 from 48 to 1024, Response
11:09:39.609 [redacted].20.22   [redacted].0.11     DNP 3.0    69 from 1024 to 48, Confirm
```

Figure 3.13: Network traffic associated with the circuit breaker opening event.

Transformers are used to increase or decrease the voltage levels in power grids. Distribution substations are usually equipped with on load tap changers (OLTCs). OLTCs help transformers hold the secondary voltage level in the nominal value regardless of load current. Although transformers have not been a direct target of cyberattacks so far, we will show in the following paragraph that if an attacker gets access to the substation network, he will be able to cause significant damage to them. Recovering from such an attack needs a significant amount of time. For example, a physical attack on a substation in California on April 16, 2013 resulted in damage to 17 giant transformers and 27 days of repair time [112]. This attack resulted in over 15 million USD worth of damage.

If a hacker gets access to the controller of the transformer OLTC, he can cause substantial damage to the substation. Let us assume that hackers have gained full control of a substation. Assuming the typical configuration of two parallel transformers in power substations, the attacker could change the OLTC setting of one transformer. Meanwhile, they can send the spoofed current and temperature readings so that the utility does not detect the wrong OLTC settings. An incorrect OLTC setting can result in circulating current flowing through the parallel transformers, which increases losses in power transformers. The increased load leads to overheating of the affected transformers, which contain thousands of liters of oil. The rising oil temperature deteriorates the dielectric properties and results in an electrical breakdown, and the transformer can catch fire. The substation may be completely destroyed and the fire may spread to nearby neighborhoods. Recovering from such an event may take weeks or months. In fact, The substation will require substantial refurbishment including decontamination of the soil, rebuilding the foundation and grounding system,



(a)

(b)

Figure 3.14: Measured magnetic field in a real-world substation during a circuit breaker closing event: (a) Magnetic field, (b) 60 Hz component of the magnetic field.

acquisition and installation of a replacement transformer as well as all other primary and secondary equipment affected by the fire. This attack can also occur in bulk transformers, which have been identified as a major vulnerability of power grids. Incorrect tap changing transformer operation can even lead to voltage problems and voltage collapse.

This stealth attack takes 10s of minutes to reach a catastrophic state, whereas RFDIDS can detect the problem within seconds. Our algorithm is able to estimate the flowing current in power circuits within an acceptable level of error. By monitoring the amplitude of the 60 Hz component of the transformer current, we can detect such attacks and prevent widespread damage to the substation transformer. To further illustrate this attack with simulation results, let's consider a simple substation configuration with two identical parallel transformers supplying a single distribution feeder with a constant current load ($I_{load} = 1$

p.u.), Figure 3.15. In normal conditions, each transformer supplies half the feeder's load. In this figure, V_{th} and Z_{th} represent the voltage and impedance of the Thevenin equivalent circuit of the transmission system, respectively. Assume that the attacker alters the tap changer settings of T$_1$ ($\varepsilon_1 = 0.1$) and T$_2$ ($\varepsilon_2 = 0$). In this circumstance, considering typical values $V_2 = 1$ p.u., $n = 1$, and $X = X_1 = X_2 = 0.01$ p.u., we can write the following equations:

$$V_1 = \frac{V_2}{(n\,(1+\varepsilon_1))} + I_1 \times jX_1, \tag{3.12}$$

$$V_1 = \frac{V_2}{(n\,(1+\varepsilon_2))} + I_2 \times jX_2. \tag{3.13}$$

With some mathematical manipulations, we can omit V_1 from Equation 3.12 and Equation 3.13 and write the relation between I_1 and I_2 as:

$$I_1 - I_2 = \frac{V_2}{jX}\left(\frac{1}{n\,(1+\varepsilon_2)} - \frac{1}{n\,(1+\varepsilon_1)}\right). \tag{3.14}$$

On the other hand, we know that the summation of transformer currents equals the load current:

$$\frac{I_1}{n\,(1+\varepsilon_1)} + \frac{I_2}{n\,(1+\varepsilon_2)} = I_{load}. \tag{3.15}$$

Given the typical parameters in this example, the set of linear Equation 3.14–Equation 3.15 is solved and the transformer currents are calculated as $I_1 = 4.790\angle-83.7°$ p.u. and $I_2 = 4.360\angle 83.1°$ p.u. Notice that $|I_1|$ and $|I_2|$ are much larger than $|I_{load}|$. The physical interpretation is that there is a large component of the current that circulates from one transformer to the other without entering the load. This circulating current serves no useful purpose. In fact, it is harmful, wasting energy and possibly overheating the transformers. Another subtle point is that even if the load current is zero ($I_{load} = 0$), we still get a large circulating current [113].

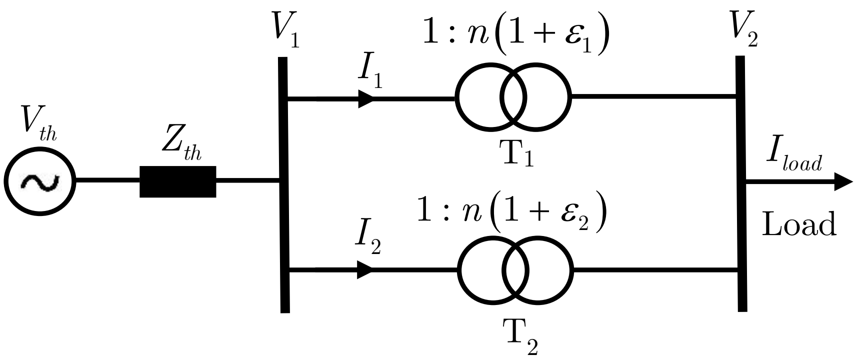


Figure 3.15: Substation configuration with two identical parallel transformers.

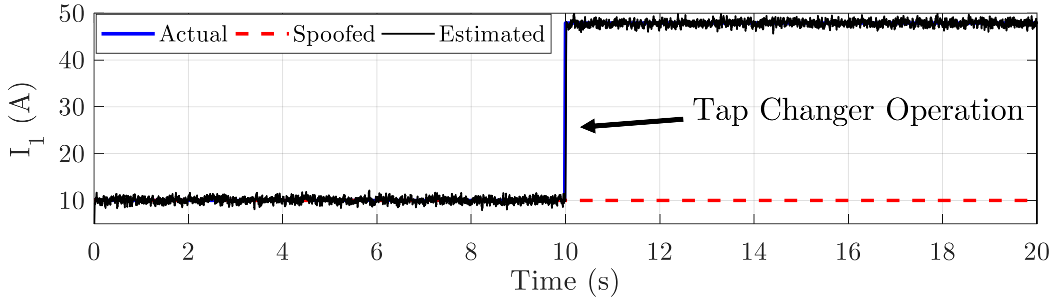


Figure 3.16: Illustration of malicious tap changing attack on a power transformer and its detection by RFDIDS.

We simulated the previously described scenario in which the malicious tap changer operation by the attacker causes a significant circulating current in both of the transformers. Figure 3.16 shows the amplitudes of the actual, spoofed, and estimated currents associated with the first transformer (T_1). To consider the worst case measurement scenario, we added 20 dB noise to the measured signal. As shown in the figure, RFDIDS can successfully track the current change in the transformer and detect the malicious tap changing attack on that in the presence of 20 dB measurement noise.

False Data Injection to Substation RTUs

This is one of the most common cyberattacks in power system substations. In this attack, the attacker tries to manipulate the information in RTUs and report false data to the control center. As mentioned in subsection 3.4.1, our proposed algorithm is able to estimate the

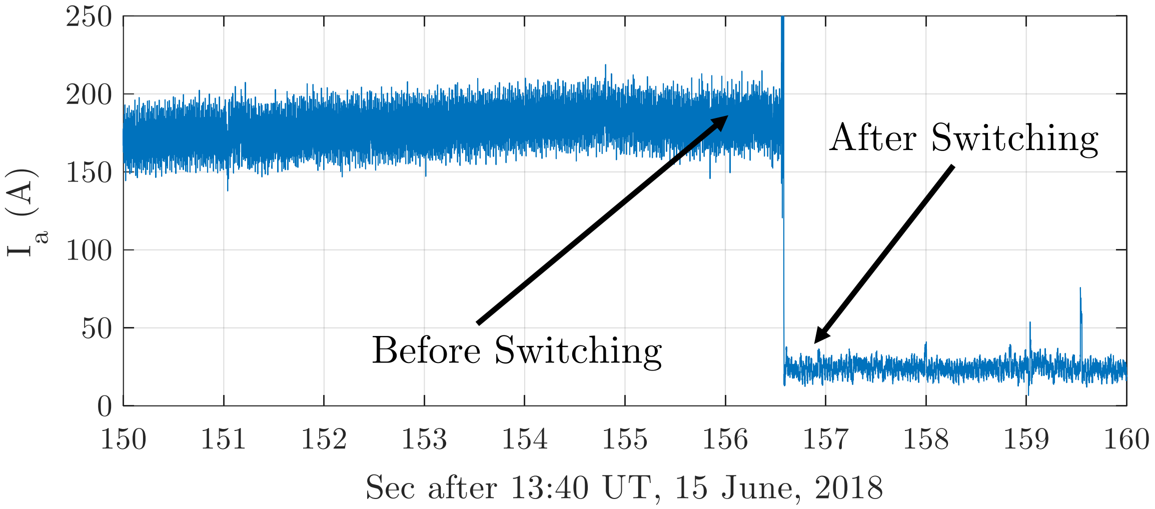


Figure 3.17: Estimated amplitude of the circuit current from RF measurements during a circuit opening event.

amplitude and fundamental frequency of the circuit current with a reasonable error. Since the values of these two variables are periodically reported to the control center, our algorithm can check the reported values and compare with the values obtained from the RF receiver to detect any false data injection attack. In the case of attack, we will see a considerable difference between the reported value of the parameters and their estimated values from RF measurements.

To show the effectiveness of the RFDIDS in this type of attack, we recorded the magnetic field of a substation circuit as a function of time during a switching event. The goal is to estimate the circuit current before and after the switching event and compare it with the output of direct measurement devices in the SCADA system. To evaluate the proposed algorithm in the worst case (in terms of noise), a substation is chosen which is located in a metropolitan area (i.e., Midtown) in Atlanta, GA, USA. Figure 3.17 depicts the estimated amplitude of the circuit current before and after the switching incident. In this event, the other side of the circuit was opened at 13:42:36 through the operation of the circuit breaker while our side was still connected to the Midtown substation. In the estimation algorithm, we assumed that the circuit is operated in the balanced condition, meaning that all of the three phases has the same current amplitude with 120 degrees phase shift with respect to each other. According to Figure 3.17, the estimation algorithm reveals the following values for the amplitude of the phase current before and after the switching incident, respectively: 175 A and 25 A. It should be noted that this 25 A is indeed the charging current of the circuit which is supplied by the substation.

The actual three phase current values before and after the switching event that are obtained from the SCADA system measurements, are summarized in Table 3.1. As can be seen, the estimation error in such a noisy area is still reasonable and is almost 10% in the worst condition. Note that this error partially stems from the assumption of three phase balanced operation. By deploying three receivers, we can easily eliminate the error causing by unbalanced operation of the circuit. All things considered, it is obvious that RFDIDS can successfully detect any false data injection attack on the circuit current amplitude by defining a threshold of 12%. If there is a deviation greater than 12% between the reported value of the current and its estimated value, one can claim that it is a false data injection attack. This means that if the attacker spoofs the reported value of the current amplitude with less than 12%, the proposed method will return a false positive (normal operation) for that attack. However, such a small spoofing attack can hardly cause damage or erroneous decisions in the power grid.

Regarding the threshold for the frequency estimation algorithm, we did not have access to the value reported by the SCADA system to make a fair comparison. Instead, we performed an illustrative simulation, which will be discussed in subsubsection 3.6.2. According to our simulations, a suitable threshold for the system frequency is 0.05 Hz. By estimating the aforementioned attributes from RF measurements and considering the determined thresholds, we can detect false data injection attack to protective relays as well. We omitted the results associated with this attack due to the lack of space.

Table 3.1: Current amplitude of the circuit before and after the circuit opening event obtained from SCADA measurements and the corresponding estimation error of RFDIDS.

Phase	I_{pre}^{SCADA} (A)	Error(%)	I_{post}^{SCADA} (A)	Error(%)
A	174	0.57	26	3.84
B	182	3.84	27	7.40
C	158	10.75	24	4.16

False Data Injection to Protective Relays

Protective relays, which are located in substations, detect faults in power grids and isolate the faulty area by sending the trip command to the circuit breakers. These relays, depending on their functionalities, monitor the circuit voltage, and current waveforms to make their decisions. A possible attack on a power system substation is to feed these protective relays with spoofed signals (representing the faulty condition) to cause unnecessary circuit breaker operations leading to massive load curtailments. Using the presented method in this manuscript (see section 3.4), we can detect the false data injection attacks on the protective relays which primarily rely on the current and frequency measurements in their decision-making process. Distance, overcurrent, and under-frequency load shedding (UFLS) relays are examples of the relays that are using the circuit current amplitude and frequency in their decision-making process [114].

As an illustration, we simulated a false data injection attack on the UFLS relays in a typical power substation to evaluate the efficiency of our algorithm. Technically speaking, these relays measure the frequency decline of the system from its nominal value (i.e., 60 Hz) and disconnect a predefined amount of customers loads in multiple steps once the frequency hits the pre-specified thresholds. This is done to recover the frequency of the system to its nominal value. The typical setting of the UFLS relays in the U.S. power grid is given in Table 3.2 [115]. The attacker feeds the relay with falsified measurement signal to cause unnecessary load shedding in the substation (see Figure 3.18). Note that the system frequency cannot change abruptly since it is coupled with the mechanical speed

Table 3.2: Typical setting of UFLS relays [115].

Step	Frequency Threshold (Hz)	Load Curtailment (%)
1	59.4	30
2	59	40
3	58.8	30

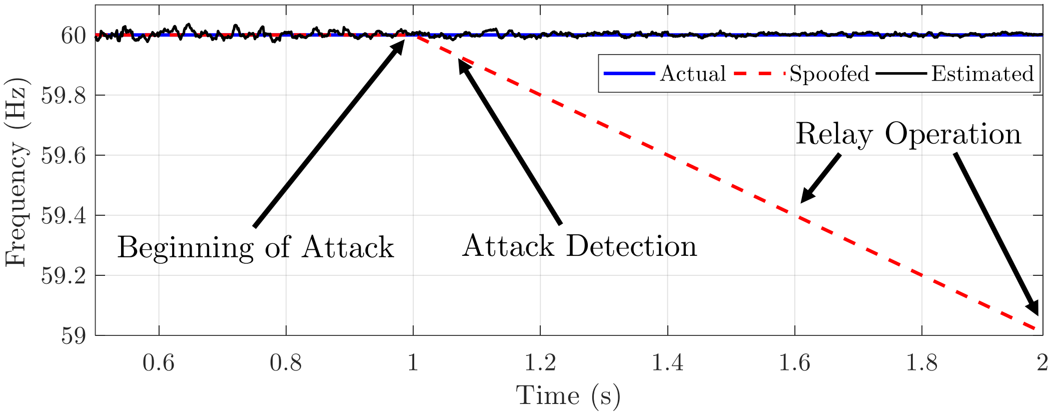


Figure 3.18: Illustration of false data injection attack on an UFLS relay and its detection by the proposed method.

of the grid generators. To consider the worst case possible scenario for our algorithm, we assumed that the frequency changes as fast as possible and there is 20 dB measurement noise in the antenna signal. According to Figure 3.18 and considering 0.05 Hz as the frequency checking threshold, the proposed scheme is able to detect the attack 100 ms after the attacker starts to inject the spoofed signal and 500 ms before the operation of the first step of the UFLS relay. This means that even in the worst case operation and measurement conditions, RFDIDS can successfully prevent such attacks with 100% successful rate.

3.6 Robustness and Resiliency of RFDIDS

Our proposed algorithm has two general stages: i) magnetic field validation (lightning authentication) stage, and ii) measurement and command validation stage. The aim of this section is to discuss the robustness and resiliency of these two stages in different challenging situations.

3.6.1 Magnetic Field Validation (Lightning Authentication) Stage

In this stage, the integrity of the measured magnetic field signal is checked for any possible manipulations. According to subsection 3.3.3, the lightning authentication scheme can check the integrity of the measured signal by comparing the arrival time of the lightning sferics obtained from three different inputs: lightning database, secondary lightning database formed by the receivers at nearby substations, and the receiver in the current substation. The following challenges can be discussed for the algorithm of this stage.

The Length of Moving Time Window

As mentioned before, the lightning authentication scheme checks the signal's integrity in a moving time window. Here a fundamental question arises: what is the optimal length of this time window? There are two main challenges in answering this question. If the length of the time window is too short, there is a possibility that no lightning sferic is detected in some time windows, and thus, the authentication scheme becomes vulnerable or conservative (depending on the type of decision in the case of no lightning in the current data window). On the other hand, if the length of the data window is too long, the proposed IDS will experience too much delay in identifying the malicious activities in the substations. Accordingly, a reasonable trade-off should be made between the number of sferics in the current time window and the length of that. To determine this, we performed a statistical analysis on the recorded magnetic field signal from multiple substations as well as the lightning database. The analyzed data includes the signal of AWESOME receiver obtained from three substations and in two different seasons and hours (2 hours in total). Also, the lightning database of the corresponding days are analyzed for 24 hours. As shown in Figure 3.19, two consecutive sferics can be detected by the AWESOME receiver and lightning database in a time window with the length of two seconds (with the probability of %99.99). Therefore, by considering a moving data window with the length of greater than two seconds, if the attacker feeds the algorithm with a spoofed signal without any sferics, he will

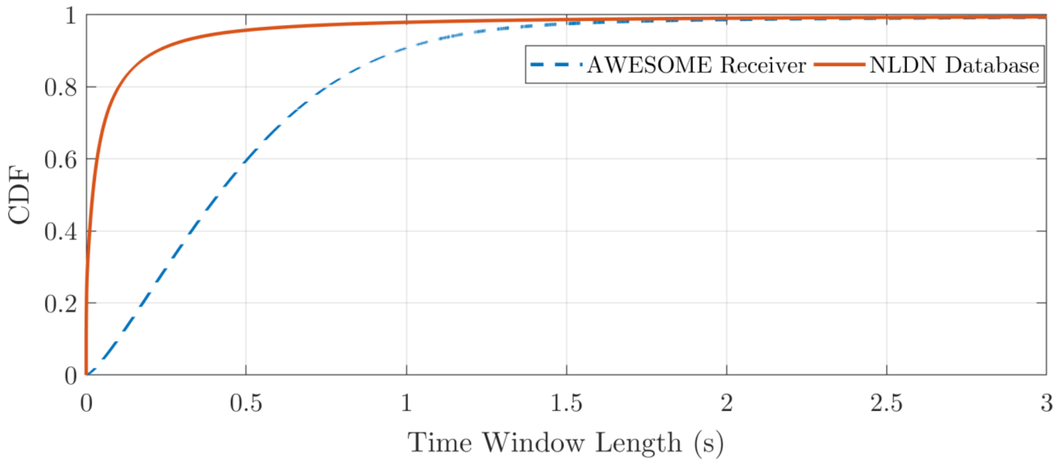


Figure 3.19: Cumulative distribution function (CDF) of the appearance of two consecutive sferics in terms of time window length.

succeed with the probability of 10^{-4}. In the case that he feeds the RFDIDS with sferics included signal, the successful rate is zero. Note that the brute force attacks cannot be implemented in power substations, as with the first sign of intrusion, the substation control changes to manual mode.

The Level of Consistency between the Inputs

Our statistical analysis (see Figure 3.19) shows that a network of receivers can pick up a major portion of the lightning sferics in each time window while our fabricated receivers are able to pick up a subset of those sferics. With a similar reasoning, the probability that a sferic shows up in the secondary database formed by the network of receivers in nearby substations is more than that of a single receiver and less than that of the lightning database. The reason is that the number of receivers used in the lightning database is much higher than that of the secondary lightning database.

Figure 3.20 shows the typical arrival time of lightning sferics obtained from: lightning database, secondary lightning database, and the receiver located in the current substation. In this specific time window, it is expected that four sferics are detected by the AWESOME receiver. Also, the secondary lightning database misses one of those sferics and detects the other three one. Finally, the AWESOME receiver detects two sferics. Considering this point, the proposed scheme compares the arrival time of the sferics from bottom to the top. This means that our method extracts the lightning sferics from the antenna signal, and then, sees that if all of these sferics are expected according to the primary and secondary lightning database. There is a possibility that a sferic is detected by the AWESOME receiver and its corresponding data does not exist in the primary and secondary lightning databases. Therefore, we need to define a suitable threshold for the number of inconsistencies in each time window. To find the appropriate threshold, we performed a statistical analysis on 1.5 hours of the recorded data with different data window lengths and thresholds. As shown in Table 3.3, with the time window length of 4 seconds and the threshold of 3, we will have 99.99% true positive rate (normal conditions). By choosing the mentioned parameters as the settings of the lightning authentication method, we tested the proposed algorithm with another 30 minutes of LF signal that we did not consider in our statistical analysis. The result of this test is 100% true positive rate and 0% false negative rate. We also tested our algorithm with the determined parameters and by feeding it with a 15 minutes replayed (fake) signal. In this experiment, the true negative (attack) rate is acquired 99.99% and the false positive rate is obtained 0.01%, which show the effectiveness of RFDIDS in authenticating the LF signal. Figure 3.21 depicts the extracted lightning sferics from the antenna signal during a switching event and the corresponding lightning database sferics. In this 10 seconds window, there is only one sferic in the receiver's signal that its corresponding sferic does not exist in the lightning database.

Feasibility of Attacks

The difficulties associated with launching various levels of attacks on the lightning authentication scheme were mentioned in section 3.2. As discussed, the attacker needs to compromise all of the three inputs of the first stage algorithm to be able to circumvent the authentication scheme. However, even if the attacker can compromise all of the three

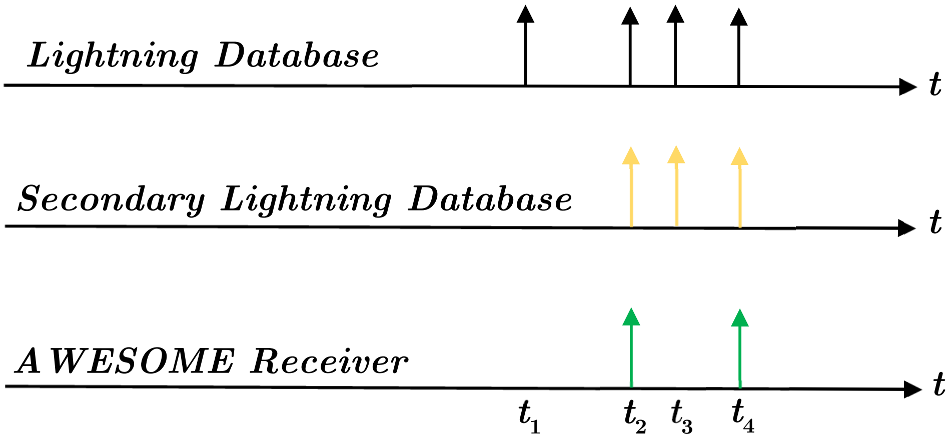


Figure 3.20: A typical illustration of the arrival time of lightning sferics obtained from: lightning database, secondary lightning database, and the receiver located in the current substation (the order is from top to below).

Table 3.3: Statistical analysis of the LF signal.

Win. Length (s)	Threshold (#)	True Pos. (%)	False Neg. (%)
3	0	51.65	48.35
	1	76.14	23.86
	2	87.29	12.71
	3	96.85	3.15
4	0	63.31	36.69
	1	82.58	17.42
	2	93.74	6.26
	3	99.99	0.01

stages, he still needs to synthesize the LF data to implement malicious activities in the substation. As the shape of a sferic evolves with distance and as a function of time of day, season, and other factors, synthesizing accurate LF data would require computationally intense physical models of propagation between the Earth and ionosphere that cannot be run in real time [104]. Indeed, the quasi-random distribution of global lightning makes a one-way function that allows easy authentication but is practically impossible to synthesize. In addition to this, to synthesize an accurate LF signal, the attacker needs to know the exact geographic distances between all of the substations in the system which is not easily accessible.

The only way to circumvent the first stage of RFDIDS is to launch a replay attack. This

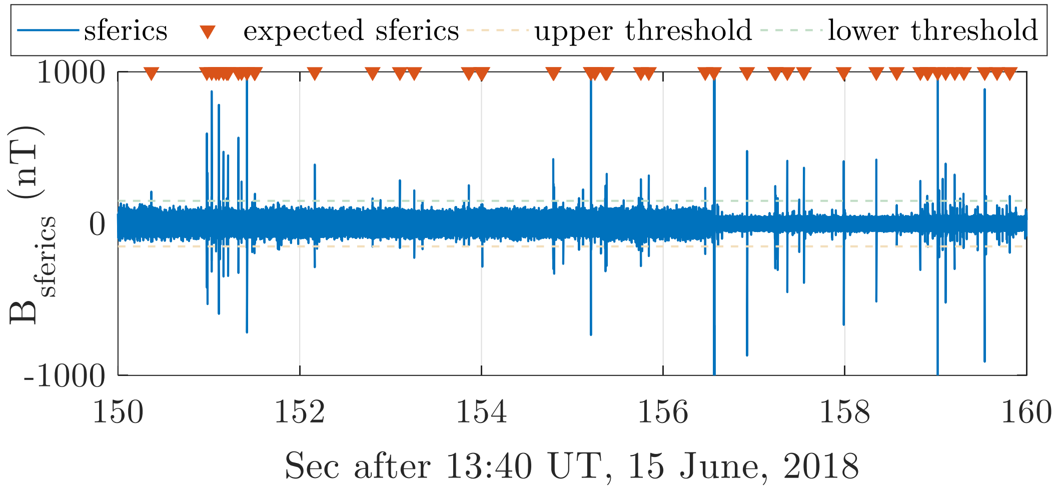


Figure 3.21: The extracted lightning sferics from the antenna signal during the switching event and the corresponding expected sferics obtained from lightning database.

means that the attacker needs to record the signals of the three inputs and replay them to the proposed scheme. In order to successfully defeat the whole IDS, the attacker should also replay the relevant SCADA network traffic to the control center. Needless to say, recording and spoofing the mentioned four signals are extremely hard, if not impossible.

3.6.2 Measurement and Command Validation Stage

As mentioned earlier, this stage of the proposed algorithm is responsible for extracting the harmonic content, fundamental frequency, and impulses (caused by switching actions) of the measured magnetic field signal. According to Equation 3.1, the accuracy of the impulse detection approach directly depends on the accuracy and robustness of the harmonic content and fundamental frequency estimation algorithms, which are analyzed in the following subsections. To test the proposed algorithm, we simulated a set of illustrative case studies which represent the worst case operation condition of power substations that can rarely occur in practice.

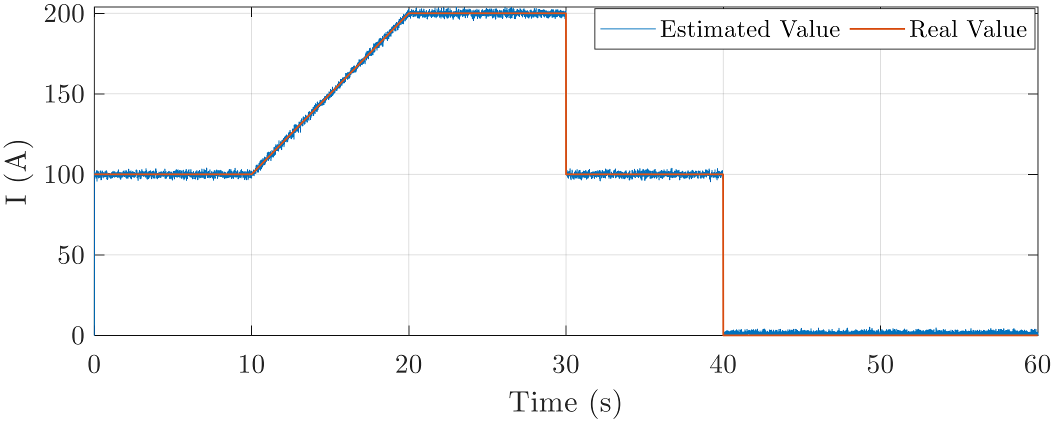


Figure 3.22: Illustration of the robustness of the harmonic estimation algorithm in the presence of 10% noise.

Performance of the Harmonic Content Estimation Algorithm

To evaluate the performance of this algorithm, we simulated a signal representing the worst case operating conditions of power substations. The generated signal starts with a constant amplitude, then, increases with a ramp rate, and finally, suddenly decreases twice. Also, to model the measurement noise, %10 (or 20 dB SNR) Gaussian noise is superimposed onto the reference input signal [110, 111]. The general view of the test signal is shown in Figure 3.22. Also, the actual and estimated amplitude of the signal's first harmonic is depicted in this figure with red and blue colors, respectively. A robust algorithm should be able to track the voltage amplitude of the circuit with negligible error. As can be seen in Figure 3.22, the adopted algorithm is robust against noise and abnormal operating conditions even in the worst cases, which implies the practical merits of the proposed approach in real-world applications.

Performance of the Fundamental Frequency Estimation Algorithm

Similar to the previous section, we simulated a signal for the worst case operating condition associated with the system frequency. The generated signal starts with a constant frequency, and then, its frequency increases with a ramp rate. Also, to model the measure-

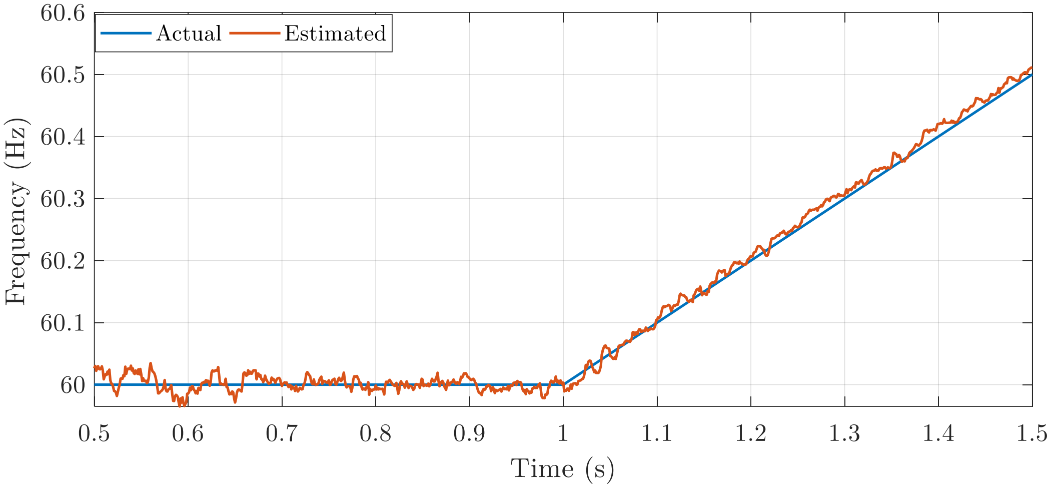


Figure 3.23: Illustration of the robustness of the fundamental frequency estimation algorithm in the presence of 10% noise.

ment noise, 10% (or 20 dB SNR) Gaussian noise is superimposed onto the reference input signal. Note that the fundamental frequency of the power system cannot change suddenly as it directly depends on the rotating speed of the synchronous generators [115]. The actual and estimated values of the system fundamental frequency is shown in Figure 3.23. As can be seen, the frequency estimation algorithm can successfully track the actual fundamental frequency of the magnetic field signal with negligible amount of error even in the worst condition.

3.7 Conclusion and Possible Directions

Recent widespread blackouts throughout the world caused by cyberattacks have shed light on the fact that the electric power networks require reliable and robust defense mechanisms to prevent such attacks and reduce their damaging consequences. With this aim in mind, this chapter proposed an air-gapped physical signal-based distributed intrusion detection system (i.e., RFDIDS) to protect power substations (as the most critical part of power networks) against advanced types of cyberattacks. Although in the proposed IDS, the SCADA system and even the side channel measurements are considered untrusted entities, it still can provide high level of security to protect substations against advanced types of attacks. In fact, the RF signal is encoded with the quasi-random sequence of lightning strokes around the globe, which acts as a watermark/nonce and this is an effective feature to authenticate the signal. Once the RF signal's integrity is verified, we can estimate the substation measurement and control actions from the magnetic field measurements with high accuracy. This allows us to check the integrity of the SCADA system traffic. The simulation and real-world experimental results revealed the effectiveness of RFDIDS in authenticating the magnetic field signal and estimating the SCADA system measurements and commands with an acceptable level of resiliency and robustness.

Despite the progress made in this chapter, there are still a set of challenges in the proposed scheme. Our future studies will focus on the following existing issues:

- In the lightning authentication scheme, we used the location and occurrence time of lightning strokes as diagnostic tools. Future studies can include the shape and intensity of sferics in the authentication scheme with machine learning methods in order to increase the security of this approach.

- The proposed effort in this chapter analyzed the utilization of RF receivers placed inside the substation fences. We noticed that some of the circuit current attributes can be detected from the receivers located at distant locations. One possible future study is to investigate and formulate the use of remote LF antennas to monitor the substation activities.

- In this chapter, we assumed that there is one antenna for securing each of the substation circuits. Future studies can focus on finding the optimal number and location of LF receivers to reduce the implementation cost.

- Another existing challenge is the lack of secure wide-area monitoring system for the power grid. Owing to the fact that the current SCADA system is highly unreliable and vulnerable, one can study the use of proposed substation monitoring system to quickly detect and defend against system level attacks (on multiple substations at the same time).

CHAPTER 4

MADIOT 2.0: MODERN HIGH-WATTAGE IOT BOTNET ATTACKS AND DEFENSES IN THE POWER GRID

4.1 Introduction

Most attacks on power systems (e.g., Ukrainian power grid blackout, Dragonfly 2.0, and Aurora [32, 75, 77, 78]) target the central control systems of the electrical grid through phishing. While targeting control systems is a direct attack, power systems can also be attacked indirectly through the consumer side. Given the proliferation of IoT vulnerabilities and the growing availability of high-energy wattage devices with Internet connectivity, a new research community has begun studying Manipulation of Demand via IoT (MaDIoT) attacks [5, 6]. In a MaDIoT attack, a botnet consisting of high-wattage IoT devices is used to abruptly change the load of the power system; these attacks might cause frequency instabilities, line failures, and increased operating costs [5].

A followup-work by Huang et. al. [6] argued that a missing piece in Soltan's analysis was a model of the protection mechanisms already in place in the power grid to prevent problems caused by natural events (e.g., sudden loss of generation due to technical reasons). They then showed how these protections (e.g., under-frequency load shedding or the time delay before disconnecting an overloaded transmission line) will significantly reduce the impact of MaDIoT attacks. In particular, Huang et. al. argue that the embedded protection systems in the power grid will prevent widespread blackouts through MaDIoT attacks.

In this chapter, we revisit this problem by taking an adversarial look at how protection mechanisms can be fooled by sophisticated MaDIoT attacks. Previous work has launched MaDIoT attacks as an all-or-nothing effort (e.g., turning on all bots at the same time, or turning them all off) [5, 6] and this spreads the attack throughout the power system equally;

however, in this chapter, we show that sometimes “less” is better. In particular, we show that by carefully turning on devices in specific geographical locations, we can target the system more methodically and use the existing protection schemes to exacerbate the problem.

In particular, we propose MaDIoT 2.0; our new attack looks at voltage stability indices and then targets the geographical areas where the system is more vulnerable from the stability perspective. In addition, we show that while protection mechanisms help the stability of the power grid when the MaDIoT attacks spread over the system, under our attack scenario, these protections are not effective in preventing the system collapse. Finally, we design new power grid protections that take into account MaDIoT 2.0 attacks, and show that they are effective for limiting the impact of these attacks.

In summary, our contributions include the following:

- In order to have realistic results, we considered a more comprehensive model for the power grid relative to that used in [5, 6] including the high order models for the standalone devices (e.g., generators, transmission lines, and loads), protective relays, and the controllers of standalone devices. This higher fidelity model helps us have a more realistic result of the behavior of the power grid against MaDIoT 2.0.

- Unlike previous works [5, 6], MaDIoT 2.0 does not attack the system randomly from arbitrary geographical locations. Instead, the adversary takes down the power grid by launching the attack in specific geographical locations that have the riskiest voltage stability conditions.

- We show that MaDIoT 2.0 has a significantly better success rate compared to the previous attacks (i.e., [5, 6]) while requiring a fewer number of compromised IoT devices, which makes it more feasible in practical situations.

- We conduct extensive numerical studies to investigate the effectiveness of MaDIoT 2.0 with real-world data obtained from crawling the websites of ISOs and the Bloomberg Terminal.

- We propose a set of short-term and long-term practical countermeasures to minimize the damaging consequences and severity of MaDIoT 2.0.

The rest of this chapter is organized as follows. The threat model, attack feasibility, and its effect on the end-users are presented in section 4.2. Then, section 4.3 explains the basic structure of the bulk power system and its main control and protection schemes. The detailed formulation and mechanism of the attack model are given in section 4.4. Next, section 4.5 evaluates the performance of the proposed approach with real-world case studies and shows its better performance over the previous works. A set of practical countermeasures are given in section 4.6. We discuss the limitations of the proposed attack and future arms race in section 4.7. Finally, we conclude and discuss the possible future works in section 4.8.

4.2 Threat Model

4.2.1 Overview of MaDIoT 2.0

The main assumption of this attack (as was assumed in [5, 6]) is that vulnerable high-wattage IoT devices have been already compromised and are part of the botnet which can be directly controlled by the attacker (C2 server). We discuss this assumption in subsection 4.2.2. Before executing the attack stages in real-time, the adversary needs to obtain the graph of the targeted grid through reconnaissance, phishing, or available automatic tools. This is a one-time analysis for each given power grid and can be done with offline analysis. A detailed explanation of how an attacker can obtain the grid graph is given in subsection 4.4.1.

A MaDIoT 2.0 attack has two main real-time stages: in the first stage the attacker obtains basic information about the targeted power grid, and in the second phase the attacker analyzes the data to find the right time and place to launch the attack. Figure 5.2 shows the threat model and overview of the new MaDIoT 2.0 attack. We now describe in more detail

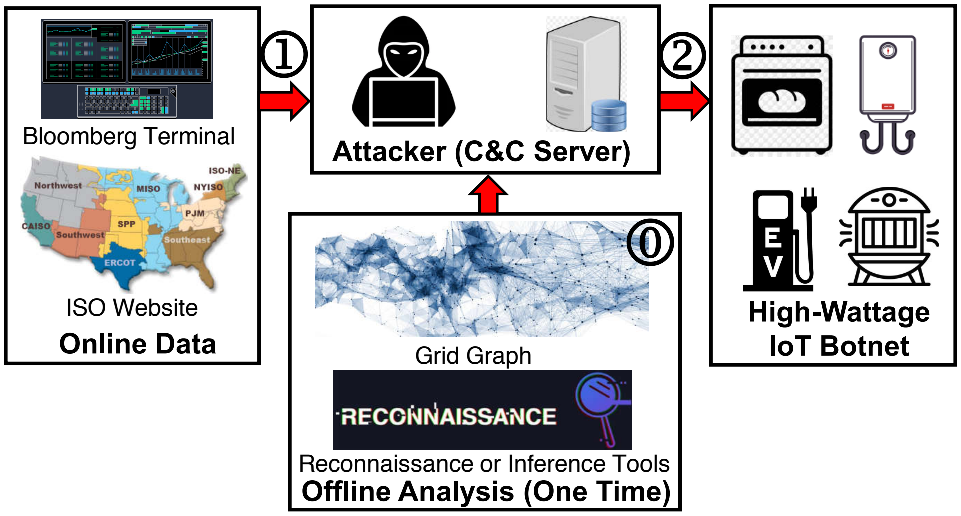


Figure 4.1: Overview of MaDIoT 2.0 attacks. ⓪ Preliminary offline analysis: the attacker obtains the grid graph through reconnaissance and inference tools, ① Data acquisition stage: the attacker collects the real-time operation information about the current operating point of the grid by crawling the online websites of ISOs and Bloomberg Terminal, ② System analysis stage: the attacker analyzes the raw data and determines the weakest points of the grid from the stability perspective. Finally, the attacker assesses the feasibility of the attack with the available high-wattage IoT botnet and implements it if it is feasible.

these steps.

Data Acquisition Stage

In this stage, the goal of the attacker is to obtain real-time information on the state of the power grid. With the emergence of deregulated electricity markets in recent years, real-time information is publicly available through the ISO websites or stock trading tools like Bloomberg Terminal [116]. Three examples of online data sharing in ISOs websites are given in [117–119]. This data is openly available so traders and market players can monitor the changes in the underlying system and quickly adapt their bids in the market for obtaining maximum profit. Since the power grid is controlled through an isolated network from the Internet called the SCADA system, it was believed that such data sharing would not help adversaries. MaDIoT attack showed that even when the attacker has not penetrated the SCADA system, they can use this information to indirectly launch successful high-wattage botnet attacks.

By crawling ISO websites and the Bloomberg Terminal, an attacker can learn the power production and consumption of the system in different nodes[1] and estimates the stability margin of the grid in various geographical regions. In particular, the attacker can obtain the integrated power generation/consumption of each node, which is explicitly shared via the methods outlined above.

System Analysis Stage

After learning the state of each node, the next step for the attacker is to identify the most vulnerable nodes based on voltage stability analysis. The motivation to conduct this study is the fact that one of the most common root causes of big blackouts is the voltage instability following severe technical incidents such as big imbalances between energy generation and consumption (e.g., caused by the outage of critical power plants due to technical faults) [86, 87, 120].

A classical way to identify vulnerable nodes is through voltage stability indices. There are multiple voltage stability indices in the literature, and they can help the attacker rank the nodes and determine the most vulnerable ones in real-time. We will give a detailed explanation of these indices along with their performance in section 4.4 and section 4.5.

Once the attacker ranks nodes according to their vulnerability margin, the attacker needs to evaluate the likelihood that an attack on the top nodes (e.g., the top 5 most vulnerable nodes) will bring the power system down. If the attack is feasible, the adversary sends the attack command to the relevant bots located in critical nodes. According to the numerical results presented in section 4.5, the attack's success[2] rate can be as high as 91%. If the attack is not feasible, the attacker will wait until the beginning of next scanning cycle (e.g., five minutes mainly depending on the refresh rate of the public information) and start again from the first stage. As we will discuss in section 4.5, MaDIoT 2.0 attacks have

[1] The terms nodes and buses are interchangeably used in power systems. Each node represents a relatively wide geographical area (e.g., a metropolitan city such as Atlanta or a big power plant).

[2] Success is defined as a complete blackout in the entire grid, and failure is defined as the recovery of the grid from the attack.

two advantages: i) the attack is executed only when there is a good chance for success (so the existence of the botnet is not discovered because of failed attacks), and ii) a successful attack to bring down the power grid requires less IoT bots than in previous work because it only targets the weakest nodes of the system.

4.2.2 Attack Feasibility

From the IoT Botnet Perspective

One of the main questions about manipulation of demand attacks is how feasible it is to gain control of a botnet of high-wattage devices within a limited geographical area. Historically, the number of IoT botnets in recent years has increased dramatically, with famous IoT botnets including Mirai, LuaBot, Hajime, and BrickerBot [121–124]. Similar to previous work [5, 6], we assume that the attacker has access to a high-wattage IoT botnet.

One of the requirements for MaDIoT 2.0 attacks is that the botnet should have enough devices in various power grid nodes. While high-wattage IoT devices are just starting to become commonplace, we can take a look at historical IoT botnets to get an idea of their distribution. Figure 4.2 shows the geographical distribution of the compromised devices in the case of Mirai botnet [125]. We can see that a high-wattage botnet with a distribution similar to Mirai can be used to attack the power grid in various countries such as the U.S., Japan, and European-Union countries. One might ask here: how an attacker can activate the compromised IoT devices located in a specific node (limited geographical area such as a city)? The differentiation between the location of the compromised bots can be trivially done by classifying and using their IP addresses. There are various research efforts providing IP location with median errors of just 3.4 km [126], and free and commercial IP geolocation databases claiming to locate cities (the nodes we are interested in for our study) with an accuracy of over 85% [127].

Compared to previous work [5, 6], MaDIoT 2.0 attack requires fewer IoT bots to be successful. The reason is that MaDIoT 2.0 attacks target the most vulnerable nodes of

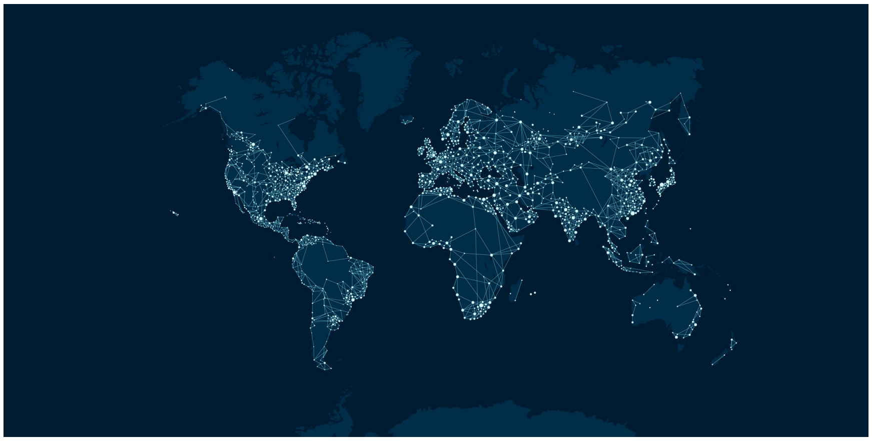


Figure 4.2: Geographical distribution of the bots in the case of Mirai botnet [125].

the grid instead of launching attacks spread over all nodes. As shown in section 4.5, an adversary with 150,000 bots can effectively take down a typical power grid with MaDIoT 2.0 attacks. Considering IoT botnets such as Mirai had over six hundred thousand compromised devices [121], the future existence of a high-wattage IoT botnet with 150,000 bots is not unlikely.

Entrepreneurial attackers can compromise high-wattage devices and then offer them for rent. This practice is common in current botnets [128–133]. The available botnet rental services provide clients with the capability to launch a limited or unlimited (for premium users) number of attacks per day with a guaranteed minimum duration from minutes to hours. Since MaDIoT 2.0 attacks take less than a minute, all of the currently available botnets satisfy this time requirement. The cost of renting a typical IoT botnet is negligible compared with the cost of a typical blackout. For example, Anderson Economic Group (AEG) estimates the likely total cost of the 2003 northeast U.S. blackout to be between $4.5 and $8.2 billion [134].

From the End User's Perspective

In order to make the attack repeatable, the adversary should try to keep it as stealthy as possible. From the end user's perspective, we discuss i) the effect of the attack on the billing statement of the homeowners, and ii) the possibility of attack detection and prevention in each home/building. The financial effect of the MaDIoT 2.0 attack on each of the homeowners depends on the duty cycle of the attack as well as the total power consumption at home. As mentioned earlier, MaDIoT 2.0 attacks use the compromised high-wattage devices for less than one minute. Therefore, even if the adversary launches this attack multiple times each month, its effect in the household is minimal. According to the energy information administration (EIA), the average electricity consumption of Americans is approximately 914 kWh per month. Tennessee has the highest electricity consumption at 1,282 kWh per residential customer, and Hawaii has the lowest at 517.75 kWh per residential customer [135]. Assuming that each of the high-wattage IoT bots consumes 3 kW of electricity and considering the duration of multiple typical attacks in each month (30 minutes), each compromised home will pay 0.11%-0.28% additional payment for electricity bills, which we believe is unnoticeable. To answer the second question, the possibility of the MaDIoT 2.0 attack is detected by home or device owners is almost negligible because the duration of the attack is very short (e.g., 10 seconds) to raise any suspicions. In addition to this, even if the home owner notices the unwanted activation/deactivation of the compromised high-wattage devices, he would likely think that it is happening because of a software bug in the device and a simple restart would resolve the issue but it is already too late and the blackout has already occurred (the attack usually takes less 30 seconds to cause a blackout in the entire system). Note that in the worst case, individual bot detection and losing few bots would not thwart the entire attack.

4.3 Background

A typical power grid is divided into different sections illustrated in Figure 4.3 [136]. Generation, transmission, and distribution are connected together through substations [89]. Each substation includes high voltage equipment such as power transformers (to change the voltage level of the circuits) and circuit breakers (switches for connecting/disconnecting lines), and also control and protection devices such as protective relays (to detect faults), voltage

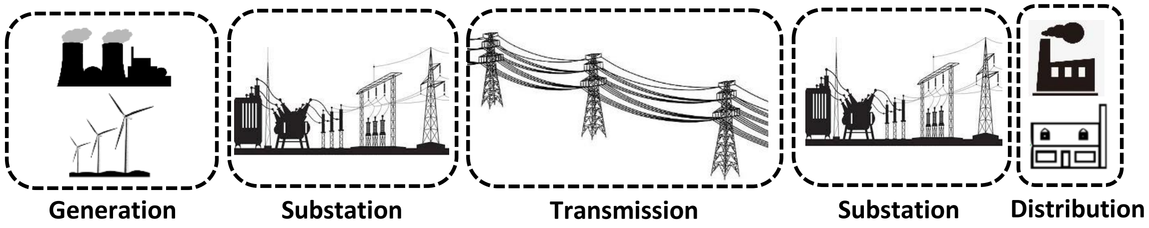


Figure 4.3: A system-level view of a typical power grid and its different sectors.

and current measurement sensors, and remote terminal units (RTU) to communicate with the control center via the SCADA system [11].

Most of the energy is produced by power plants in the generation sector. The voltage at generators is originally medium voltage (e.g., 13.8 kV), and this generated power is then stepped up to a higher voltage level (e.g., 500 kV) so that it can be transmitted over long distances. This voltage level change is performed to reduce energy losses in transmission lines (higher voltage levels imply smaller currents, which lead to lower transmission losses). Eventually, the electricity is stepped back down to a medium voltage level by distribution substations as it nears end users. The distribution sector generally feeds the consumers within a limited geographical area with medium voltage [136].

4.3.1 Control of Power Systems

The total demand of the power grid is continuously changing. To preserve system stability and avoid any large-scale blackouts, the output power of generators must match the demand in real-time [87]. These variations change the load of the transmission lines, some of them might even work while being overloaded, depending on the grid operating point [6]. Therefore, to relieve overloaded transmission lines, the configuration of the system is modified (by switching the transmission lines) so that the energy be transmitted to the end-users via different routes. These strategies are a part of the power system control mechanism. Power system control is defined as the set of local and wide-area algorithms which help the system operator maintain grid stability. The main goal of operators is to ensure that the grid is continuously delivering electric energy to consumers at the nominal voltage and frequency with an acceptable error (i.e., 120 ± 20 V and 60 ± 0.5 Hz in the U.S.) while keeping the generation-demand balance. The most important power system control schemes are i) primary frequency control (governor), ii) automatic voltage control (AVR), and iii) automatic generation control (AGC). These controllers have either local or wide-area mechanisms.

The primary frequency controller is locally installed in each generator, and it changes (increases/decreases) the output power of the generator in response to any frequency change in the system which is a sign of load-generation imbalance in the grid. As a rule of thumb, whenever the generation exceeds the demand in the grid, the system frequency becomes greater than the nominal value, and whenever the demand exceeds the generation, it drops below the nominal frequency [11].

The AVR is similarly installed in each generator with the goal of maintaining the voltage level of the generator within allowable ranges; it achieves this by changing the reactive power output of the generator [87].

Finally, AGC is a wide-area controller that changes the output power of the system generators to recover the frequency to its nominal value if the primary frequency controllers are not able to fully recover the system frequency change to the allowable range [87]. Wide-area controllers gather and analyze the data from the entire grid and make decisions and issue commands to multiple components throughout the system. These controllers use a private network for receiving data and sending commands; this network is called the SCADA system.

4.3.2 Protection of Power Systems

When a severe fault or incident occurs in the system (e.g., short circuit fault in a transmission line, sudden outage of a big power plant, etc.) and the physical damage to the grid components or a widespread blackout is inevitable, power system protection schemes will intervene to isolate the faulty area while keeping as much of the transmission network still in operation [11]. This means that there may be localized outages that can be easily repaired, and these are caused to prevent the interconnected bulk system from going down.

These protection schemes can be categorized into local and wide-area methods. The local protection schemes usually detect and isolate the faulty component in the system to prevent damage to the equipment and preventing the fault from spreading to the entire grid. On the other hand, wide-area protection schemes gather and process data from different parts of the grid through the SCADA system to detect any faults and react to them accordingly. From the technical perspective, wide-area protection schemes employ more sophisticated data analysis methods and are able to detect and resolve more complex faults in the system [11]. Table 4.1 lists the most common protection schemes used in the bulk power system.

Table 4.1: The most common protection schemes used in power grids.

Name of the Protection Scheme	Local or Wide-Area	Aim
Distance [137]	Local	Short circuit detection in transmission lines
Overcurrent [138]	Local	Overload detection in transmission lines
Overvoltage Load Shedding (OVLS) [11]	Local/Wide-Area	Overvoltage detection in grid nodes
Undervoltage Load Shedding (UVLS) [139]	Local/Wide-Area	Undervoltage detection in grid node
Under-Frequency Load Shedding (UFLS) [86, 120]	Local/Wide-Area	Underfrequency detection in grid nodes
Over-Frequency Generation Rejection (OFGR) [140]	Local/Wide-Area	Overfrequency detection in generation nodes
Differential [141, 142]	Local	Fault detection in power transformers and transmission lines
Out-of-Step [143]	Local	Out of synchronous detection in power generators
Loss-of-Excitation [144]	Local	Excitation system fault detection in power generators

These protection schemes play an important role in keeping the grid stable following severe natural events or accidents, and as shown by Huang et al. [6], they can even protect the grid from basic MaDIoT attacks. However, basic MaDIoT attacks and natural events have not taken an adversarial look at protection mechanisms. In the next section, we discuss what types of attacks can bypass and even use the existing protection mechanisms against the grid.

4.4 MaDIoT 2.0

4.4.1 Preliminary Offline Analysis

Before we describe the online tasks of MaDIoT 2.0, we discuss a preliminary offline step. To launch successful attacks, the attacker needs to gather some basic information about the architecture of the power grid. This architecture does not change over long periods of time (years) and we only need to obtain them once for every target grid. Although the power companies and ISOs do not explicitly share this type of information, the attackers can acquire them with indirect methods such as phishing or social engineering [145]. In addition to this, researchers have shown that there is enough openly available information to infer in great detail the topology and configuration of power grids [146].

Because all of the transmission lines and substations in the bulk power grid are outdoors, they can be identified with online mapping services such as Google Maps [147]. The attacker can easily follow transmission lines from the power plants to the distribution substations and obtain the graph of the entire system. The size and shape of the tower reveal the voltage level of the respective transmission line and the attacker can estimate the technical parameters of the line by multiplying the length of the line to the per-unit values of the relevant tower. Although this process might take some time if the attacker does it manually, the processing time here is not important because it is a one-time analysis for every system. In addition, the attacker can develop computer vision algorithms to automatically (or semi-automatically) generate the graph of a given system using Google Maps satellite pictures

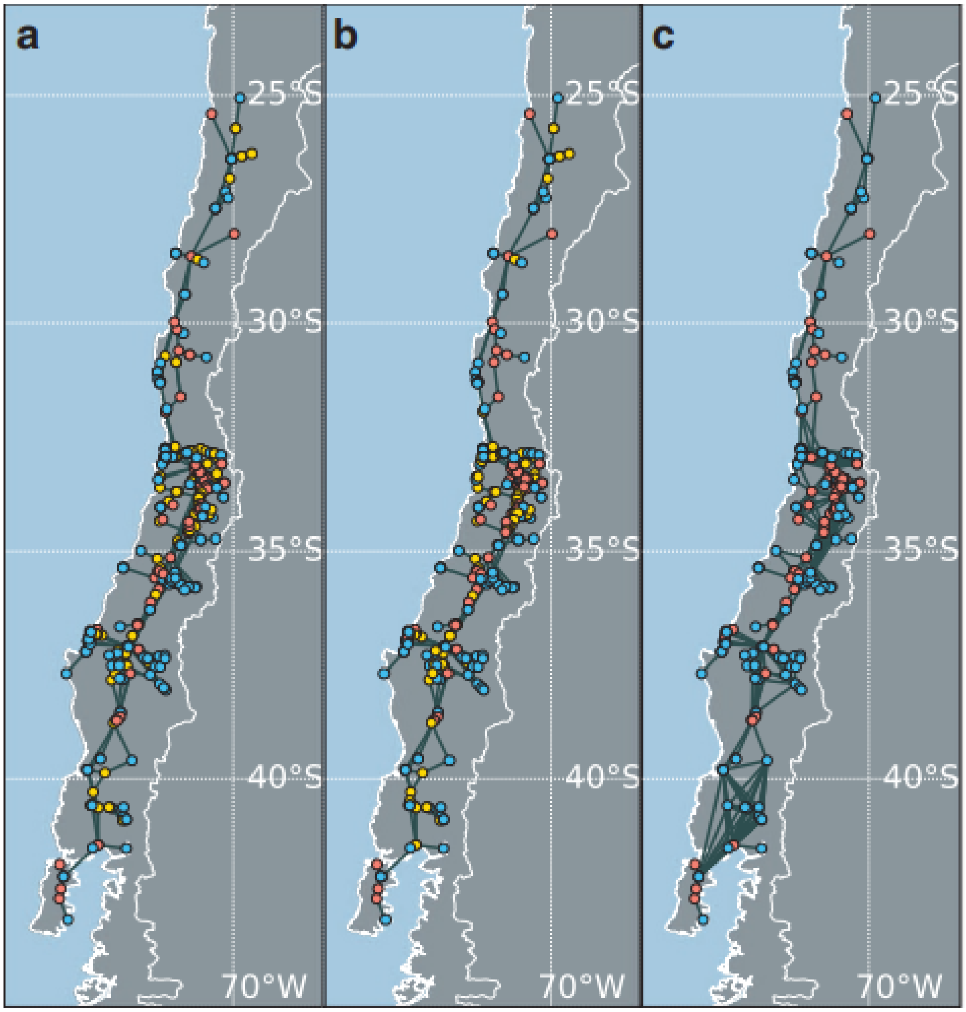


Figure 4.4: The graph representation of Chilean power grid on the map of Chile: a) Detailed network graph without any simplifications, b) Reduced network graph with the elimination of intermediate nodes, and c) Minimum network graph with the minimum independent number of nodes [149].

[148–150]. Figure 4.4 illustrates how the graph of the Chilean power grid can be inferred by an open-source tool [149]. In this figure, power plants, substations, and junctions are represented with red, blue, and yellow dots, respectively. Also, the transmission lines are visualized with black lines.

4.4.2 Data Acquisition Stage

As we briefly explained in subsection 4.2.1, once the attacker has some basic information of the topology of the grid, the next step is to start monitoring the state of the system and find vulnerable nodes in real-time. As explained before, this data (power generation and consumption in each node) of the power grid is released on the website of ISOs (e.g., NYISO and CAISO) and is updated every 5 minutes [117, 118]. In addition to this, this data can also be accessed through an advanced stock trading tool called Bloomberg Terminal [116]. To extract the operation data, the attacker uses a crawler. To verify this, we collected all the system operation data of the California and New York power grids from January 2020 to January 2021.

4.4.3 System Analysis Stage

Once the attacker has information about the state of the system, the next step is to determine the weakest nodes of the grid from the voltage stability perspective. Note that since the power generation and consumption in different nodes of the system change constantly, the weakest points of the target grid will change accordingly. In particular, we want to exploit voltage instability as changing voltages in multiple nodes is easier than attempting to change the frequency of the grid.

We can create voltage instabilities when the load increases in nodes where the *voltage stability margin* is at its critical point [139]. Therefore to find vulnerable nodes, we need to compute the voltage stability margin. While finding the exact stability margin is computationally expensive and cannot be solved in real-time, the power grid community has developed a set of voltage stability indices that approximately rank the system nodes based on their voltage stability margins. We now introduce two candidate options for estimating this quantity.

Voltage Magnitude of Nodes (Index 1)

During the normal operation of the power grid, the operators want to keep the voltage magnitude of system nodes constant, and only allow deviations between 0.95 and 1.05 per unit (p.u.). Undervoltage protection schemes use the voltage magnitude of the system nodes as an indication of their stability margin [139]. In these schemes, a lower voltage magnitude implies a lower stability margin in the node, and hence, during emergency conditions when the voltage magnitude is too low, the protection scheme drops a portion of the loads that are fed through the critical nodes to keep the system stability and recover the voltage value to its nominal range.

This index is very easy to compute, and therefore our first candidate to identify the most vulnerable nodes is the voltage magnitude of nodes. We will show later that if the attacker increases the system demand in several critical nodes where the voltage magnitude is in the minimum range, it then further drops it below the normal range and causes cascading outages in the power grid.

Modal Analysis (Index 2)

One of the most efficient methods to calculate the voltage stability margin of the system nodes is the modal analysis based on the Jacobian matrix [151–153]. To calculate this index for different nodes, the relationship between the system states and the active and reactive power of system nodes can be written as:

$$\begin{bmatrix} \Delta P \\ \Delta Q \end{bmatrix} = \begin{bmatrix} J_{P\theta} & J_{PV} \\ J_{Q\theta} & J_{QV} \end{bmatrix} \begin{bmatrix} \Delta \theta \\ \Delta V \end{bmatrix}, \tag{4.1}$$

where ΔP, ΔQ, $\Delta\theta$, and ΔV are the vectors representing active and reactive power changes and voltage magnitude and angle change in the system nodes. The elements of the Jacobian matrix (i.e., $J_{P\theta}$, J_{PV}, $J_{Q\theta}$, and J_{QV}) are calculated based on the results of the load flow analysis performed in the previous stage (the data acquisition stage helps us perform this analysis easily). Since the reactive power and voltage changes have strong relationships with each other, it is reasonable to assume $\Delta P = 0$ [151]. Therefore, we can write:

$$\Delta Q = [J_{QV} - J_{Q\theta} J_{P\theta}^{-1} J_{PV}] \Delta V = J_R \Delta V. \tag{4.2}$$

Reversing the matrix above equation, one can rewrite it as:

$$\Delta V = J_R^{-1} \Delta Q. \tag{4.3}$$

In order to simplify the calculations, a decomposition can be used to calculate J_R^{-1} as:

$$J_R^{-1} = E_R \xi^{-1} E_L. \tag{4.4}$$

Hence, Equation 4.3 can be transformed into:

$$\Delta V = E_R \xi^{-1} E_L \Delta Q = \sum_l \frac{E_{R,l} E_{L,l}}{\lambda_l} \Delta Q, \tag{4.5}$$

where E_R and E_L are the right and left eigenvector matrices of J_R and ξ is the diagonal eigenvalue matrix of J_R. Also, $E_{R,l}$ and $E_{L,l}$ denote the lth column and lth row of E_R and E_L and λ_l stands for lth eigenvalue of J_R. All things considered, the V-Q sensitivity of node k can can be computed through:

$$VQS_k = \frac{\partial V_k}{\partial Q_k} = \sum_l \frac{\mu_{kl} \eta_{lk}}{\lambda_l}, \tag{4.6}$$

in which μ_{kl} and η_{lk} are the kth element of $E_{R,l}$ and $E_{L,l}$. The negative value of VQS_k implies the voltage instability in the node k in the grid. During the normal operation of the power system, VQS_k will be positive for all of the system nodes which means that the system is stable from the voltage stability perspective; however, we can use this index to rank the system nodes and see which one of them are more prone to the instability point. The lower value for the VQS_k index implies that the kth node of the system is closer to the voltage instability and a small load shock can make it unstable.

Checking the Feasibility of an Attack

After the attackers find the most vulnerable nodes in the grid, they need to evaluate the feasibility of the attack before its implementation. To do so, the adversary can use modal analysis to determine whether the grid will be unstable following the implementation of load alteration attack in the weakest nodes of the system. In the first step, the attackers update the power consumption in the weakest nodes of the power grid based on the available potential of the high-wattage botnet. Then, they compute AC load flow analysis and recalculate $J_{P\theta}$, J_{PV}, $J_{Q\theta}$, and J_{QV} based on the new updates. Finally, the voltage stability index of different nodes can be obtained through Equation 4.6. If following the attack implementation, the index VQS of weak nodes becomes negative, this implies that the grid will be unstable; otherwise, the available botnet is not strong enough to take down the power grid and the attack scenario is not feasible in the current operating point.

If the attack does not succeed with the current state, the attacker needs to wait for at least five minutes so that the operating point of the grid and power consumption in different nodes change. Then, the adversaries will repeat the previous analysis until they find an attack with a high success likelihood. The accuracy of this evaluation is numerically evaluated in section 4.5. We will show that by using a suitable voltage stability index, the success rate of the attack can be as high as 90%.

4.5 Experiments and Discussion

Due to the irreparable economic and social damages caused by the real-world implementation of MaDIoT 2.0, we use simulation results to show the performance of the proposed attack (as was done in previous work [5, 6]). In this line, instead of adopting simplified models and simulations, we leveraged an advanced, commercial power system simulation software called DIgSILENT PowerFactory [154].

Table 4.2: Generator parameters for the New England power grid.

G	H	x'_d	x'_q	x_d	x_q	T'_{do}	T'_{qo}	x_l
G1	500	0.006	0.008	0.02	0.019	7.0	0.7	0.003
G2	30.3	0.0697	0.170	0.295	0.282	6.56	1.5	0.035
G3	35.8	0.0531	0.0876	0.2495	0.237	5.7	1.5	0.0304
G4	28.6	0.0436	0.166	0.262	0.258	5.69	1.5	0.0295
G5	26.0	0.132	0.166	0.67	0.62	5.4	0.44	0.054
G6	34.8	0.05	0.0814	0.254	0.241	7.3	0.4	0.0224
G7	26.4	0.049	0.186	0.295	0.292	5.66	1.5	0.0322
G8	24.3	0.057	0.0911	0.290	0.280	6.7	0.41	0.028
G9	34.5	0.057	0.0587	0.2106	0.205	4.79	1.96	0.0298
G10	42.0	0.031	0.008	0.1	0.069	10.2	0.0	0.0125

4.5.1 Test Case and Component Modeling

To evaluate the performance of the proposed attack, we use a standard test power grid, called the New England power system—this is also known as the IEEE 39-bus test system. The New England power system includes 39 buses (nodes), 32 transmission lines, 24 power transformers, and 10 generators. The total base load of the system is 6097.1 MW (active load) and 1408.9 MVAr (reactive load) [155]. We will also use a smaller test case (IEEE 9-bus test system) which has been used in the previous relevant works [5, 6]. The IEEE 9-bus test system has 6 transmission lines, 2 power transformers, 3 generators with a total active and reactive power generation of 350 MW and 244 MVAr. The single-line diagram of the New England power grid is shown in Figure 4.5 [155]. The New England power system includes 39 buses (nodes), 32 transmission lines, 12 power transformers, and 10 generators. This test system has been widely used in the literature in power grid security and stability studies. The total base load of the system is 6097.1 MW (active load) and 1408.9 MVAr (reactive load). To expand the base load, we used a daily load profile in the grid meaning that at every minute, the load of the grid nodes changes similar to the real-world cases. The daily load profile we consider is illustrated in Figure 4.6 for the New England power grid. The dynamic and static parameters of the system generators are outlined in Table 4.2.

The grid graph or the single-line diagram of the IEEE 9-bus test system is illustrated in

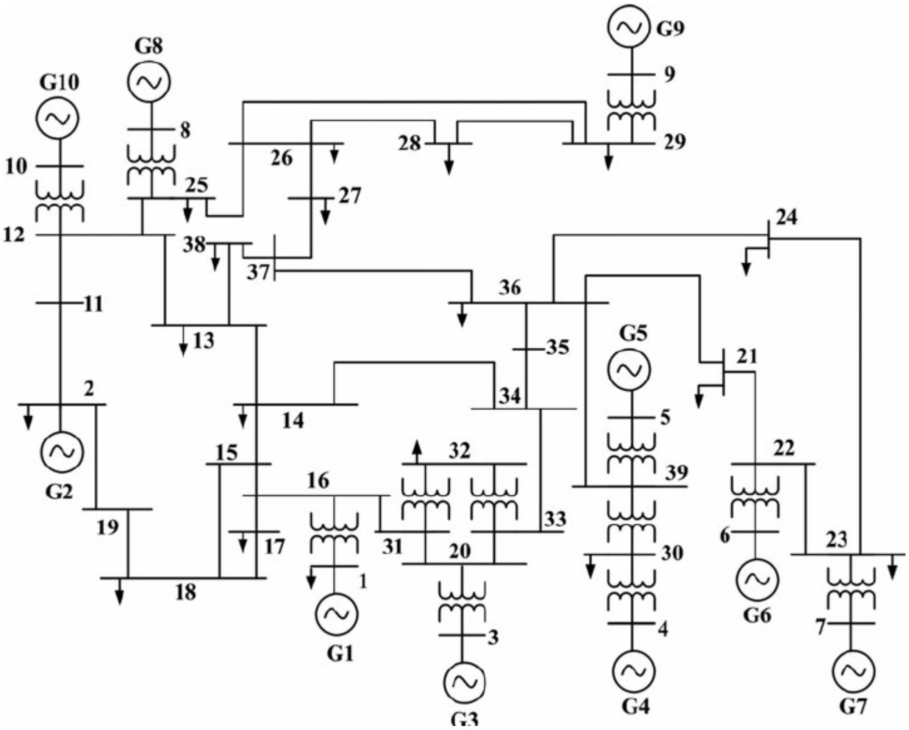


Figure 4.5: The single-line diagram of the New England power grid (IEEE 39-bus test system) [155].

Table 4.3: Generator parameters for the IEEE 9-Node system.

G	H	x'_d	x'_q	x_d	x_q	T'_{do}	T'_{qo}	x_l
G1	0	0.0608	0.0969	0.146	0.0969	8.96	0	0.0032
G2	0	0.1198	0.1969	0.8958	0.8645	6.0	0.535	0.026
G3	0	0.1813	0.25	1.3125	1.2578	5.89	0.6	0.036

Figure 4.7 [156]. This system has 6 transmission lines, 2 power transformers, 3 generators with a total base active and reactive power generation of 350 MW and 244 MVAr. For the IEEE 9-bus system, we used a relatively similar load curve shown in Figure 4.8. Also, the dynamic and static parameters of the system generators in this system are outlined in Table 4.3.

To capture the system dynamics and minimize the simulation errors, an eighth-order model is used for representing the dynamics of generators. In this model, the mechanical part of the generator is formulated by a second-order state-space equation and the electrical part by a sixth-order system [87]. Furthermore, the IEEE-type DC1A excitation system for

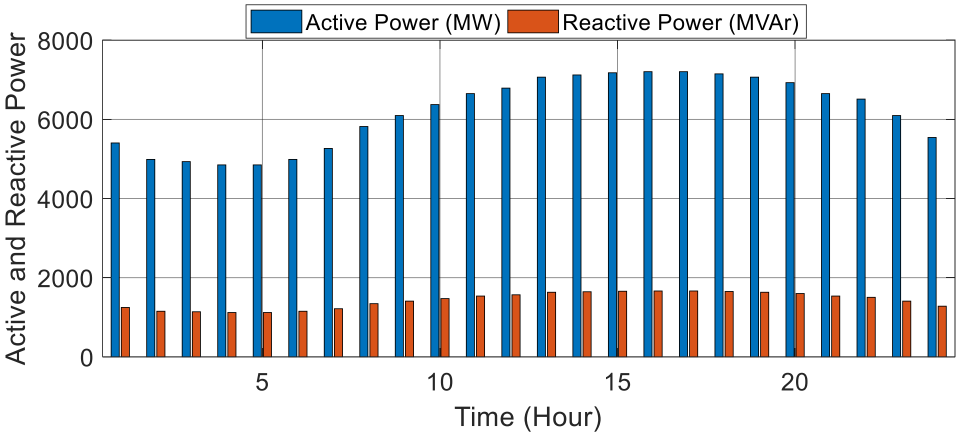


Figure 4.6: The active and reactive powers of the New England power grid during the evaluation period.

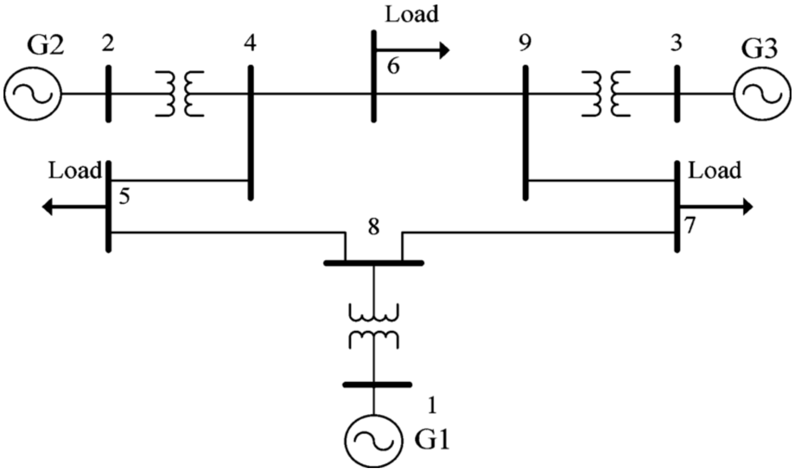


Figure 4.7: The single-line diagram of the IEEE 9-bus test system [156].

modeling the AVRs of generators and an appropriate governor model are employed in our simulations [87].

We also adopt a combinational load model in our simulations, where the static and dynamic parts of the composite model are represented by a polynomial model (i.e., a mixture of power constant, current constant, and impedance constant loads) and a third-order induction motor, respectively [86, 120]. This model of the system allows us to study the dynamic behavior of the power grid in response to MaDIoT 2.0 attacks with minimal errors.

We model the system for 24 hours. We chose 24 hours because the daily load curve of each power grid is similar and we can reasonably extrapolate the analyzed results to longer

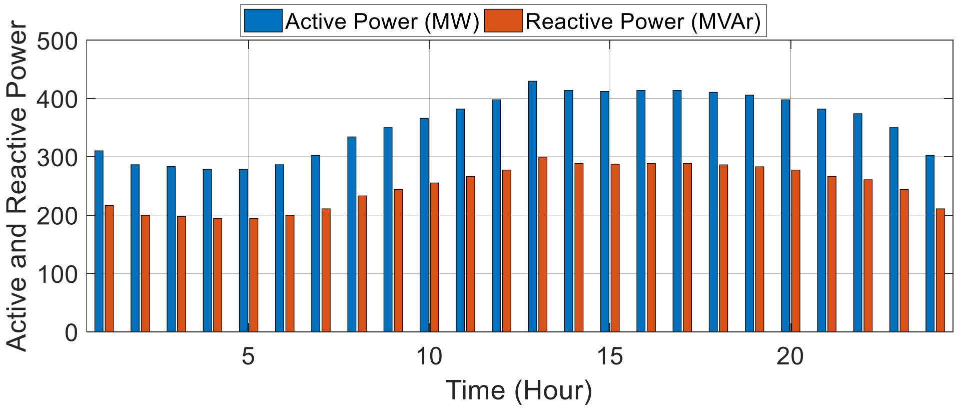


Figure 4.8: The active and reactive powers of the IEEE 9-bus test system during the evaluation period.

periods of time such as one year. Previous works have studied the power grid behavior during the non-strategic MaDIoT botnet attacks only in one snapshot (e.g., 5 minutes) [5, 6]. Therefore, previous results cannot be reliably extrapolated to longer time periods.

Table 4.4 summarizes the list of new models and simulation contributions of the current work over the recent related works. Our work presents the most comprehensive and high-fidelity modeling of real-world power systems when compared to previous works. Our improved models are highly important because of three main reasons:

1. Ignoring the detailed modeling of the system controllers (i.e., governor, AVR, AGC) in the time domain simulations can lead to considerably erroneous results compared with practical situations because these controllers contribute to the system recovery when a severe incident occurs in the grid [87].

2. When a big disturbance happens in the grid, system protection schemes (i.e., distance, overcurrent, OVLS, UVLS, UFLS, OFGR, differential, out-of-step, and loss-of-excitation) seek to locate and isolate the faulty area to limit the damaging consequences of the widespread outages and area of the blackout. Hence, overlooking these schemes in the simulations will lead to erroneous results [85].

3. The detailed modeling of the system components (i.e., generators, static, and dynamic loads) play an important role in the power system dynamic studies. During

Table 4.4: Modeling and simulation contributions of the current work over the recent related works.

Element	Our Work	Soltan et. al. [5]	Huang et. al. [6]
Governor	✓	✗	✓
AVR	✓	✗	✗
AGC	✓	✗	✗
Distance	✓	✗	✗
Overcurrent	✓	✓	✓
OVLS	✓	✗	✗
UVLS	✓	✗	✓
UFLS	✓	✓	✓
OFGR	✓	✗	✗
Differential	✓	✗	✗
Out-of-Step	✓	✗	✗
Loss-of-Excitation	✓	✗	✗
Static Load	✓	✓	✓
Dynamic Load	✓	✗	✗
Generator Model	✓	✗	✗

unstable conditions, the dynamic behavior of the loads and system generators makes the situation worse and pushes the grid towards a more unstable point where recovery is hard [86].

This comprehensive system modeling approach can be used in future studies as the benchmark.

4.5.2 Evaluation of MaDIoT 2.0

We first consider the New England power grid for 24 hours. We assume that the attacker obtains the power consumption of the simulated power grid every 5 minutes. Therefore, there are 288-time intervals in which the available high-wattage IoT botnet can be used to take down the power grid. For our initial evaluation, we assume that the attacker has access to a botnet with 150,000 bots, each of which is consuming 3 kW of electrical power.

Figure 4.9 illustrates the precision, recall, and the F-1 score of the proposed attack methods along with the approaches developed in the most recent works obtained from

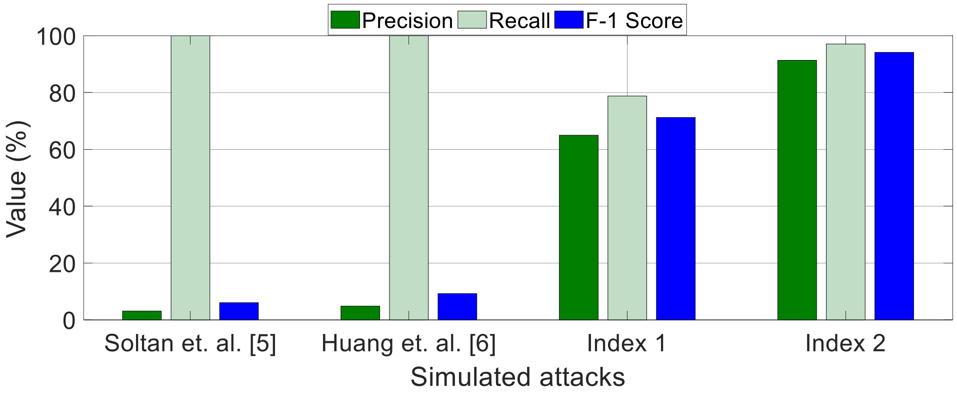


Figure 4.9: The performance of the proposed attack methods along with the approaches developed in the most recent works obtained from the New England power grid [5, 6].

the New England power grid [5, 6]. Here, the precision or recall alone are not suitable to judge the performance of the studied attack methods. Since the methods proposed in [5, 6] have zero false negatives, their recall is 100%. However, they have a high false-positive rate, and hence, low performance. Accordingly, we use the F-1 score to judge the overall performance of the simulated attack scenarios because it represents a combination of both precision and recall. As can be seen in Figure 4.9, the proposed MaDIoT 2.0 attacks outperform the previous methods with a relatively large margin. As previously reported by Huang et al. [6], we confirm that in most of the cases the conventional protection schemes are able to control the disturbance caused by ***random attacks*** and keep the system stability following the IoT botnet attack. However, MaDIoT 2.0 attacks can bypass these protections and create a cascading failure of the bulk power system. The reason behind this observation is that we target the weakest nodes of the grid while the proposed attack scenarios in [5, 6] are uniformly spread over the grid.

Simulating the IEEE 9-bus test system reveals similar results with 0%, 0%, 61%, and 93% F-1 scores that are associated with Soltan et. al. [5], Huang et. al. [6], Index 1 and Index 2, respectively (see Figure 4.10).

The other interesting observation is that Index 2 for the voltage stability margin indicator performs much better than Index 1 for launching MaDIoT 2.0 attacks. Based on this

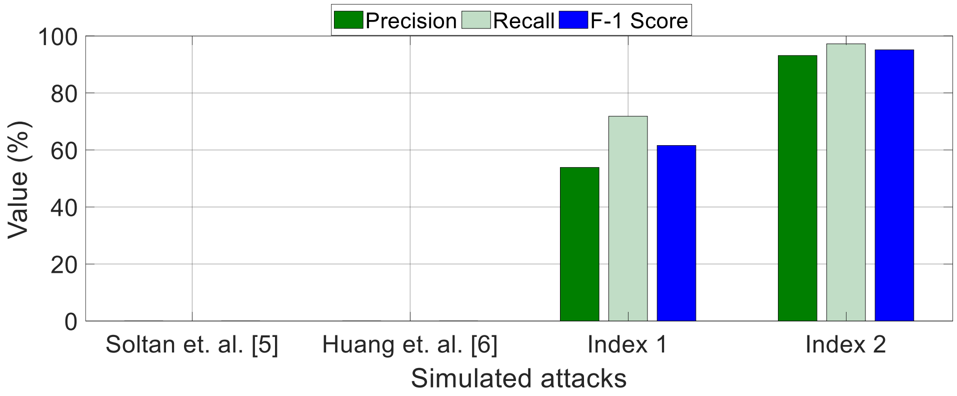


Figure 4.10: The performance of the proposed attack methods along with the approaches developed in the most recent works obtained from the IEEE 9-bus test system [5, 6].

observation, it is apparent that Index 2 is a better indicator for determining the voltage stability margin in system nodes. To validate this claim, we solved the exact model of the system equations in all of the 288-time intervals and obtained the error-free ranking of the system nodes in terms of their voltage stability margins. Figure 4.11 depicts the normalized accuracy of Index 1 and Index 2 compared with the ground truth which was acquired through performing the computationally intensive calculations (that cannot be performed in real-time) on the New England power grid. According to this figure, Index 2 represents the ranking of the grid nodes based on their voltage stability margins with lower errors and this justifies the results we observed in Figure 4.9. It should be noted that the exact equations of the entire grid took longer than 24 hours to calculate (for all 288 time intervals) and this is why we cannot use the exact model in the real-time attack mechanism. On the other hand, the calculation of the proposed indices in each of the time intervals took less than 5 sec (24 minutes for all 288-time intervals) and this makes the MaDIoT 2.0 attack feasible in practice. Again, simulation of the IEEE 9-bus system returns the same similar pattern where the normalized accuracy of Index 2 is much higher than that of Index 1. This is aligned with the aforementioned performance metrics discussed in the previous paragraph.

We also considered how the size of the botnet changed the effectiveness of all attacks. Figure 4.12 shows the F-1 score of different attack methods versus the number of compro-

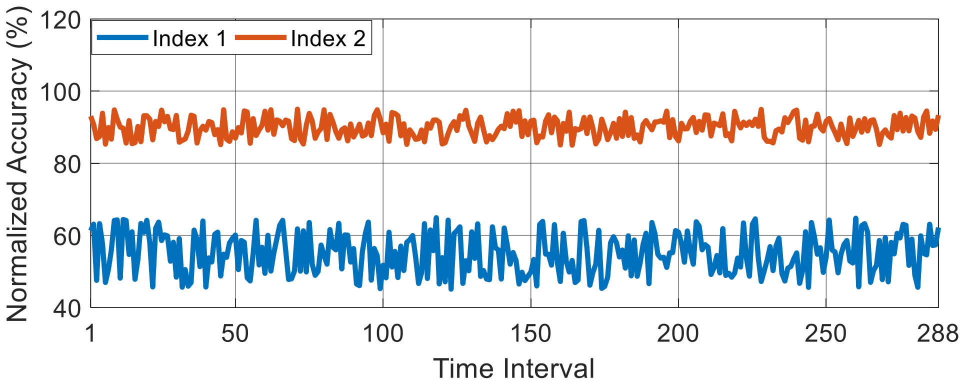


Figure 4.11: The accuracy of the proposed Index 1 and Index 2 compared with the exact calculations (ground truth).

mised high-wattage IoT devices that the attacker can control in the new England power grid. As can be seen, not only the proposed attack methods have a higher F-1 score compared to the previous attack mechanisms in the literature, but also they require smaller botnets to cause a large-scale blackout of the bulk power system. In addition to this, as the size of the available botnet increases, the success rate of the proposed attacks increases as well. However, after a certain point (150,000 bots) the increase in the attack success rate saturates and it does not respond to an increase in the size of the available botnet. In the IEEE 9-bus test system, the optimal success rate for the MaDIoT 2.0 attack is achieved when the size of the botnet is 5,500 bots. The reason for this observation and its difference with the New England power grid is that the IEEE 9-bus test system is much smaller than the New England power grid. Based on this, one can reasonably infer that for smaller power grids, we will need smaller botnets to achieve the highest attack success rate.

It is interesting to see how the proposed attack causes a system collapse. To do so, we illustrate the voltage profile of the system nodes and the grid frequency during different attacks in the New England power grid. Figure 4.13 shows the system frequency and the voltage profile of the New England power grid during one of the simulated time intervals. In this Figure, ⓪, ①, ②, and ③ denote the attack time, protection and control involvement time, system recovery to the normal condition, and wide-area blackout (voltage collapse), respectively. As we can see, the system controllers and the protection schemes are able

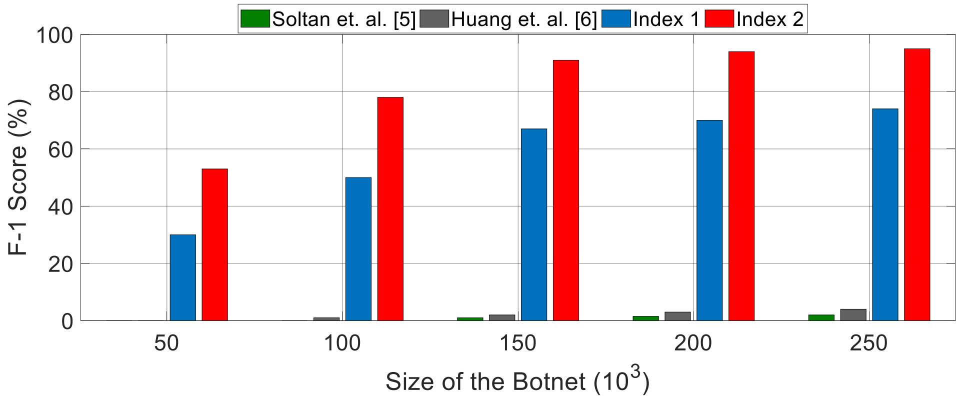
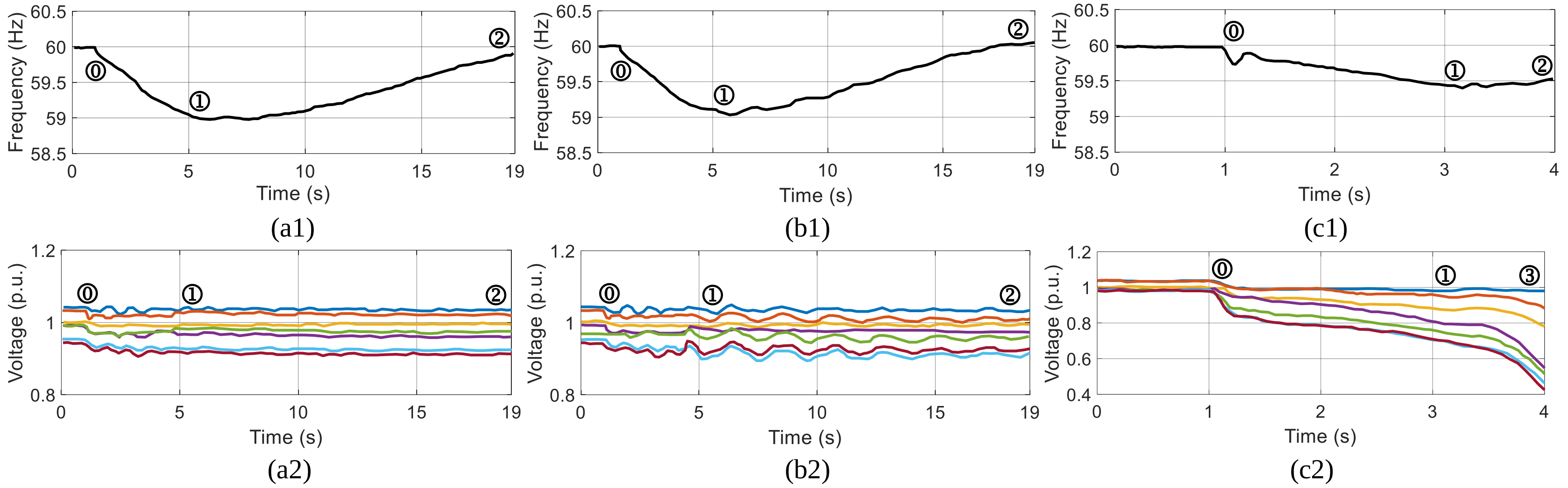


Figure 4.12: The success rates of different IoT botnet attacks versus the size of the available high-wattage IoT botnet in the New England power grid.

to recover the grid to the normal operating state following the attack scenarios proposed in [5, 6]. However, since our attack targeted the weak nodes of the system, power grid controllers and protection schemes are unable to handle the emergency conditions following the attack, and a system-wide voltage collapse becomes inevitable. More specifically, the voltage magnitude of the system nodes collapses after a few seconds of starting the MaDIoT 2.0 attacks.



(a1) (b1) (c1)

(a2) (b2) (c2)

Figure 4.13: The system frequency and voltage profile of the New England power grid during one of the simulated time intervals following the implementation of different attacks: a) Soltan et. al. [5], b) Huang et. al. [6], and c) Proposed approach using Index 2. Note: ⓪, ①, ②, and ③ represent the attack time, protection and control involvement time, system recovery to the normal condition, and wide-area blackout (voltage collapse), respectively.

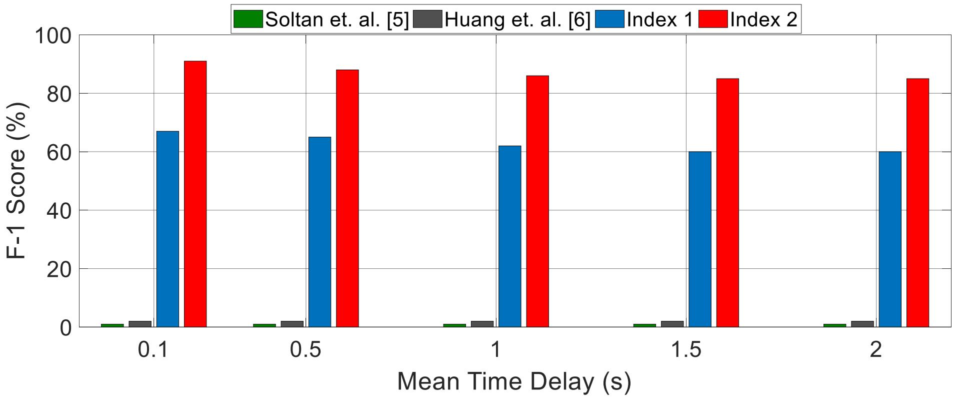


Figure 4.14: The performance of the different IoT botnet attacks in the New England power grid versus the mean value of the normal pdf used for modeling the network latency.

An important factor that has not been studied in the previous works is the network delay of the bots' activation during the manipulation of demand attacks. Practically speaking, the attacker cannot simultaneously activate/deactivate the bots in the botnet because of the latency and randomness in the underlying communication network. To model the network latency associated with different bots, we considered a normal probability distribution function (pdf) for the network latency. Considering the standard deviation of 100 msec, Figure 4.14 depicts the successful rate of different attack methods versus various values for the mean of the normal pdf in the New England power grid. As can be seen, the latency of the communication network does not have significant effects on the proposed and previous attack methods. The MaDIoT 2.0 attacks still have a very high chance to cause a system-wide blackout in the studied power system. Simulating this delay in the IEEE 9-bus test system resulted in a similar pattern where no notable change was observed during the increase of the botnet delay.

4.6 Countermeasures

The countermeasures for dealing with MaDIoT 2.0 attacks can be categorized as data-driven, and hardware-driven. Each of these countermeasures has its own advantages and disadvantages. In order to get the best results and limit the attack probability and consequences, we need to implement a combination of them.

4.6.1 Data-Driven Countermeasures

The first strategy which will significantly reduce the possibility and effectiveness of the MaDIoT 2.0 attack is to limit the real-time information shared by ISOs and market participants. This is clearly a data privacy issue. Publicly available system data is one of the main contributing factors which makes MaDIoT 2.0 attacks practical. To eliminate the risk of such attacks, the ISOs and system operators must share the real-time operation data of the power grid only with trusted parties. Without this data, the attacker cannot identify the weakest nodes of the power grid in the current operating point and other crucial parameters required to launch a successful attack on the grid.

While restricting access to system real-time data will thwart many attackers, it will also prevent researchers and energy market analysts from performing their analyses. To avoid this, a more practical solution would be releasing redacted or altered versions of the system data or even delaying the release of full datasets, such that they cannot be used in real-time. This would significantly reduce the effectiveness of MaDIoT 2.0 attacks as they require real-time information from the grid to launch a successful attack.

Another possible countermeasure could be to ask top IoT device vendors, or even consumers to register a fraction of their IoT products in an online database. This database can anonymously monitor the power consumption of registered devices (and even consider adding local differential privacy to the traces shared to the database). IoT device vendors can advertise this functionality as a security program. Even if 1% of the IoT devices are registered in the database, the market operator can potentially detect MaDIoT 2.0 attacks by monitoring the statistical behavior of registered devices over time. For example, if 5% of the registered IoT devices in the database are turning on/off simultaneously in a specific geographical area, this can be interpreted as an indicator that a MaDIoT 2.0 attack is happening in the system. The effectiveness of this countermeasure depends on the number of compromised IoT devices in the database. Our analysis shows that registering 1% of the high wattage IoT devices in the online database could almost completely mitigate the risk of MaDIoT 2.0 attacks. Nevertheless, the practical implementation of this countermeasure might have some challenges due to the privacy concerns of high-wattage IoT device users even if it is advertised as a security feature.

4.6.2 Hardware-Driven Countermeasures

The most effective way to prevent MaDIoT 2.0 attacks is to update the protection schemes of the power grid so that they can recover system stability following any unpredictable shocks caused by similar attacks. In our experiments, we saw that UFLS and UVLS are the two main protection schemes involved during MaDIoT 2.0 attacks.

Conventional UFLS and UVLS schemes drop a predetermined amount of the power grid loads when the system frequency and voltage drop severely following a technical event such as the outage of a power plant or a heavy transmission line. However, system operators do not consider the situations such as MaDIoT 2.0 attacks when they are configuring them. The current protection schemes drop the system loads that are evenly distributed in the entire grid. However, as shown in subsection 4.5.2, this strategy is unable to protect the grid and recover it following the proposed IoT botnet attack. While one possible way to fix this issue is to drop the loads where the attack was launched, it is hard to detect and identify the location of the MaDIoT 2.0 attack in the grid.

One of the effective indicators which could be leveraged to detect the region of the manipulation of demand attacks is to use the voltage falling rate of grid nodes [157]. We observed that during the IoT botnet attacks, the voltage falling rate in the nodes that are close to the attacked nodes is much higher than that of the far nodes. Therefore, we revised the setting of the existing protection schemes so that they will first drop loads of the system in the nodes where the voltage falling rate is bigger than the other nodes. This adaptive protection scheme will shed some loads in the area of the attack and will help the system recover from the attack.

Figure 4.15 illustrates the performance of different manipulation of demand attacks after the modification of UFLS and UVLS schemes with the explained logic in the New England power grid. As we can see, the F-1 score of the studied attack mechanisms significantly drops with this modification. The high recall occurs because we have zero false negatives in the test cases. Figure 4.16 depicts the system frequency and voltage profile following the implementation of a MaDIoT 2.0 attack considering the modified adaptive protection scheme in the New England power grid. We can see that the system was going to become unstable following the attack; however, the modified adaptive protection scheme is able to identify the region of the attack and drop the loads accordingly. This eventually helps the grid to fully recover from the attack and prevent a system-wide blackout.

This is just an improvement to existing protection schemes against IoT botnet attacks. However, we also need to check that our modified protection scheme also works against natural incidents and compare it with the existing protection schemes. Figure 4.17 illustrates the performance of the conventional and modified UFLS methods during one week of the operation of the New England power grid. As can be seen, the performance of the modified protection scheme is roughly equal to the conventional one during natural technical events. Therefore, it is feasible to redesign the power grid protection schemes to withstand against MaDIoT 2.0 attacks while keeping their satisfactory performance during natural technical incidents. Figure 4.17, is the result of considering a set of contingencies, including natural faults to evaluate both conventional and our suggested protections during the events. The contingency analysis was done through well-known methods explained in [158].

4.7 Limitations

Although MaDIoT 2.0 attacks have excellent performance in causing system-wide blackouts in power grids, they have their own limitations. While MaDIoT 2.0 requires fewer

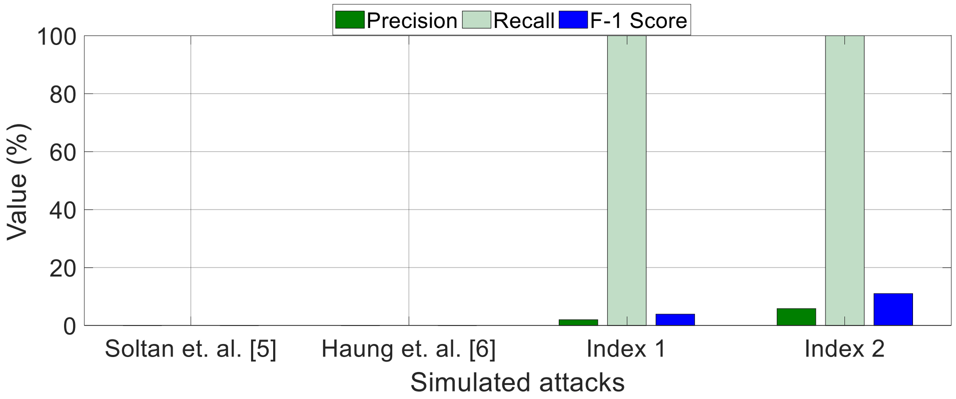
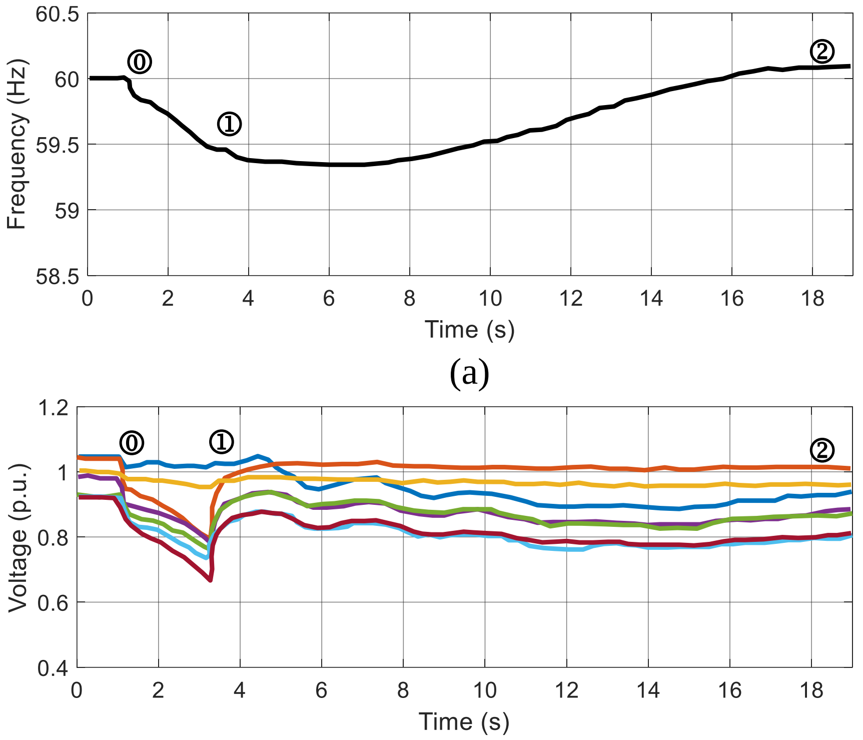


Figure 4.15: The performance of different manipulation of demand attacks after the modification of UFLS and UVLS schemes in the New England power grid.

bots, it also requires the attacker to have a presence in all nodes. This is a direct factor in the botnet operator's success, i.e., if the operator does not have enough bots in a location that is a "weak point", the adversary might not be able to launch a successful attack sometimes. It should be noted that the weak points of the power grid change as the loading of different nodes change around the clock. Accordingly, even if the adversary has compromised few bots in certain nodes, he still should be able to cause a blackout in the target grid at certain times. To verify these explanations, we did an experiment in the New England power grid. Figure 4.18 shows the performance of the MaDIoT 2.0 attacks with different coverage of nodes that consist of high-wattage bots. As expected, although the attack performance declines following the decrease in the number of nodes having high-wattage bots, the performances of the proposed MaDIoT 2.0 attacks are still much higher than that of the previous methods [5, 6].

The maximum amount of time the attacker will have to wait so that a feasible attack scenario occurs depends on the operating point of the grid and its general stability margin. Modern grids are often operated near to their stability limits to use the maximum capacity of the grid components and to postpone expensive grid expansion plannings. For this reason, a typical power grid such as the New England test system forces the attacker to wait roughly 3 hours. While impractical, (due to the high operational cost of non-optimal grid operation), operating a grid with a higher stability margin would increase the time the attacker would



(a)

(b)

Figure 4.16: The system frequency (a) and voltage profile (b) of the New England power grid during one of the time intervals following the implementation of MaDIoT 2.0 attack considering the modified adaptive protection scheme. Note: ⓪, ①, and ② represent the attack time, protection and control involvement time, and system recovery to the normal condition, respectively.

have to wait to launch a successful attack.

The other important aspect of the MaDIoT 2.0 attacks is their performance sensitivity to estimation errors by the attacker. To analyze this in detail, we performed two different experiments in the New England power grid. In the first experiment, we assumed that the line parameters of the grid transmission lines which are obtained through offline analysis have some errors. Figure 4.19 depicts the performance of the MaDIoT 2.0 attacks versus the mean error in the New England power grid line parameters. According to this figure, the attack performance decreases as the error becomes bigger. However, this performance reduction is not that significant and the MaDIoT 2.0 attacks are still relatively effective in the presence of reasonable errors in the transmission line parameters.

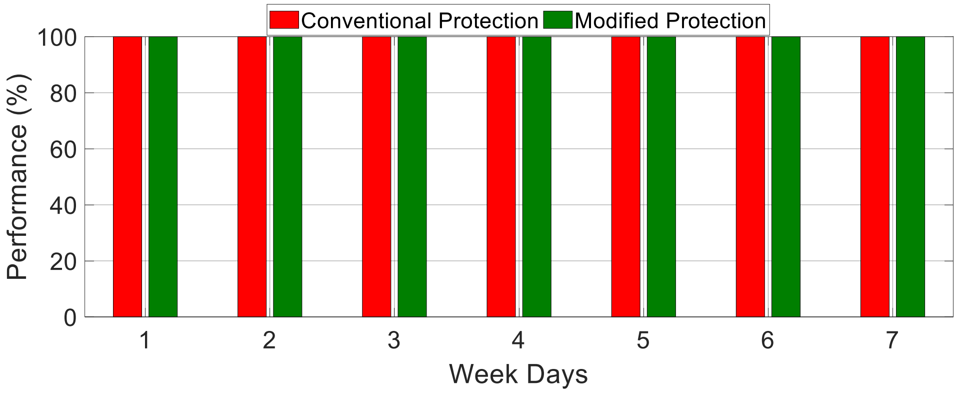


Figure 4.17: The performance of the conventional and modified UFLS schemes against the technical natural events during one week of the operation of the New England power grid.

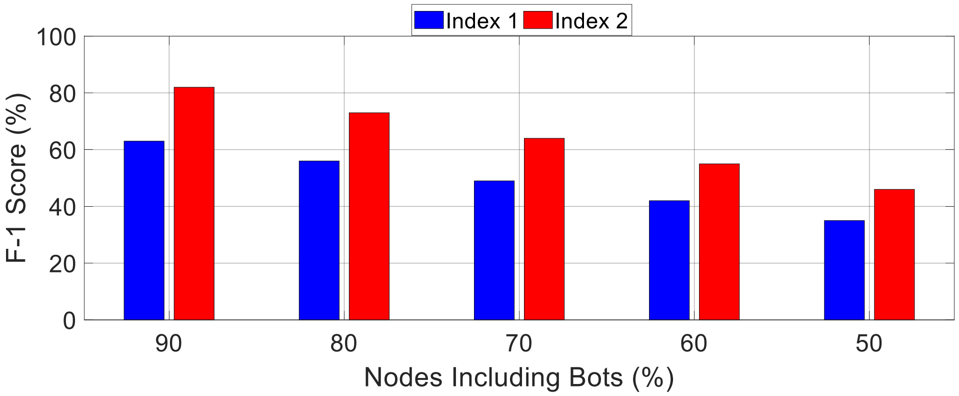


Figure 4.18: The performance of the MaDIoT 2.0 attacks versus the percent of the nodes including high-wattage IoT bots.

In a final experiment, we considered the effectiveness of our data-driven countermeasure, so we assumed that the data associated with the power generation/consumption in different nodes is publicly released with some errors. Figure 4.20 shows the performance of the MaDIoT 2.0 attacks versus the mean error in the New England power grid nodes' power generation/consumption. As it was expected, the performance of the MaDIoT 2.0 attacks drastically declines with the increased error in the grid nodes' power generation/consumption. This performance reduction is more severe than that of the previous experiment shown in Figure 4.19. It is worth mentioning that Figure 4.20 implies that the first data-driven countermeasure (limiting the online data sharing) cannot be alone used for eliminating the risk of MaDIoT 2.0 attacks. However, it definitely reduces (∼26% performance reduction for

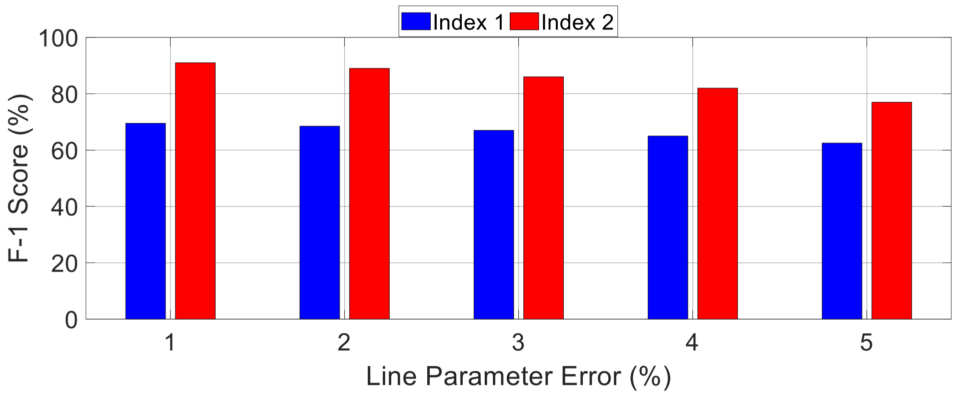


Figure 4.19: The performance of the MaDIoT 2.0 attacks versus the mean error in the New England power grid line parameters.

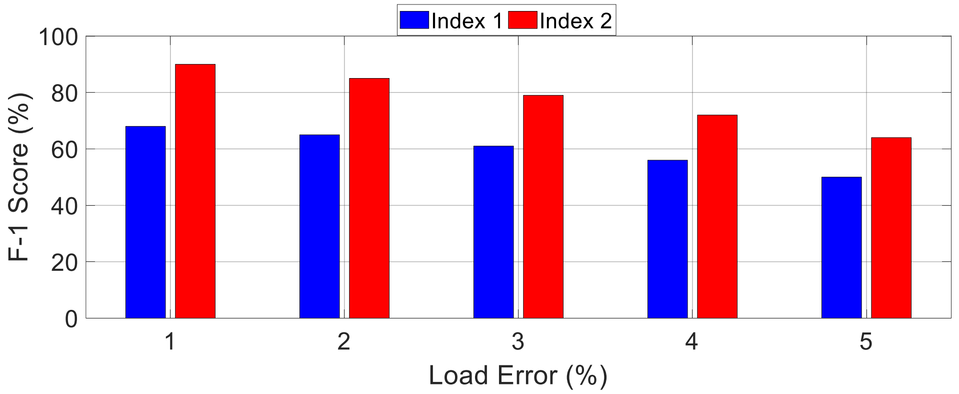


Figure 4.20: The performance of the MaDIoT 2.0 attacks versus the mean error in the New England power grid nodes' power generation/consumption.

index 2 in the presence of 5% error) the attacker chance of launching a successful attack to cause blackout in the entire grid.

4.8 Conclusion and Possible Directions

In this chapter, we introduced MaDIoT 2.0: a hierarchical two-stage attack mechanism that leverages the potential of high-wattage IoT botnets to attack the power grid and cause a widespread blackout in the entire system. The performance of the developed attack methods is evaluated using extensive simulations and the results showed the superiority of MaDIoT 2.0 over the previously studied attack mechanisms. More specifically, the success rates of the new IoT botnet attack were 91% and 67% for voltage stability Index 1 and

Index 2, respectively. In addition, MaDIoT 2.0 requires a smaller number of bots involved in the attacks, since it targets the weakest nodes of the system in the current operating state. Finally, we discussed and showed the effectiveness of proposed countermeasures to mitigate or reduce the damaging consequences of the studied attacks.

We hope that this chapter raises awareness of system operators, ISOs, IoT manufacturers, and system security experts to make the electricity grid more secure against IoT botnet attacks. In the near future, this problem will be even more critical as the number of smart appliances with Internet connectivity continues to grow. In closing, we recommend the following next directions:

- System operators should reconsider the current unnecessary online data sharing mechanisms and policies. As it was shown in the chapter, access to historical and real-time system data can be easily leveraged for malicious purposes.

- Further research is required to develop additional MadIoT attacks and effective protection schemes to help the power grid withstand emerging high-wattage botnet attacks.

CHAPTER 5

MAMIOT: MANIPULATION OF ENERGY MARKET LEVERAGING HIGH WATTAGE IOT BOTNETS

5.1 Introduction

In recent years, real-world attacks, as well as demonstration projects, have shown the effectiveness of cyberattacks against the power grid [32, 75, 77, 78]. These are *direct* attacks, meaning that they directly target the critical components (e.g., generators) or the supervision and control system of the power grids. Recent work, however, has shown how to attack the power grid *indirectly*, by compromising consumer devices (and not devices in the grid) [5, 6]. In particular, the adversary creates or rents a botnet of high-wattage IoT devices (e.g., an Internet-connected EV charger or water heater), and then, collectively and abruptly changes the electricity demand of thousands of these devices (via simultaneously turning them on/off), creating an unanticipated sudden power surge which can potentially result in local or regional blackouts [5, 6].

In this chapter, we analyze a new unexplored threat from high-wattage IoT botnets: attacks to the deregulated wholesale electricity market [159]. According to the U.S. Energy Information Administration (EIA), the average price of electricity and total energy consumption in the U.S. was 75 USD/MWh and 2.935×10^9 MWh, respectively [160, 161], with approximately 220 billion USD transactions. Such markets can be attractive targets for cybercriminals around the world and selfish traders who are willing to manipulate the market.

Market manipulation (creating artificial prices) is not a new problem. In the U.S., the primary purpose of the Securities and Exchange Commission (SEC) is to enforce the law against stock market manipulation. Recently, security researchers started to study how botnets can facilitate stock market manipulation [162]. In this chapter, we attempt to do a similar study but in the electricity market.

In a role similar to that of the SEC for the stock market, the Federal Energy Regulatory Commission (FERC) has oversight on electricity markets in the U.S. and can impose penalties on entities that manipulate the prices. While there have been multiple electricity market manipulation cases over the years, none of the discovered cases so far have been caused by cyberattacks [63]. The most visible case of manipulation of the electricity market is the case of Enron [163], but there are several other traders that have been fined for manipulating the market over the years, including JPMorgan [164, 165], and Barclays [166].

Our empirical observations on historical market data verified the research findings that there is a meaningful relationship between the power grid real-time demand and energy price fluctuations in electricity markets [167]. Our proposed attack, which we call Manipulation of Market via IoT (MaMIoT), exploits this relationship and manipulates the market prices by slightly altering the total power consumption of the grid through a high-wattage IoT botnet. This botnet can give a huge advantage to the malicious participants in the market, as they can predict sudden (but small) changes in the demand for electricity (changes created by the botnet). A similar analogy would be a stockbroker who could predict small fluctuations of the stock prices in advance.

The market manipulation through MaMIoT can be implemented in two general ways based on the ultimate goal and motivation of the attacker: i) to provide additional financial profits for one of the market players (i.e., the attacker is one of the market players such as the previously discovered market manipulation cases by FERC), ii) to cause economic damage to the entire market (i.e., attacker is a nation-state actor who is doing this as a part of a trade/cold war). For each of the cases, we develop an optimization model to maximize the profit (or damage) of a specific market player (or to the entire market) while keeping the attack as stealthy as possible. The input data for the optimization models are obtained by crawling and processing publicly available datasets from official electricity market websites (they can be similarly obtained through a trading tool called Bloomberg terminal or similar trading software).

The main contributions of this chapter are summarized as follows:

- This is the first research in the literature that identifies and analyzes the emerging threat from the high-wattage IoT botnets to the wholesale electricity markets.
- In order to develop successful attacks, we develop optimization algorithms to decide when and how to attack, subject to the constraints of the market, and the power constraints of the system.
- We evaluate and test the effectiveness of the attacks with real-world traces.
- We propose a set of practical countermeasures to considerably limit the damaging consequences and severity of the studied attacks.

The rest of this chapter is organized as follows. In section 5.2 we explain the basic structure of electricity markets and their various players. We then present the threat model and attack feasibility in section 5.3. The stealth strategies and the evidence for the presence of high wattage IoT botnets are presented in section 5.4 and **??**. We develop a formulation of the attack model for different attackers in section 5.5. In section 5.6 we evaluate the performance of the proposed approach with real-world case studies. We then propose a set of practical countermeasures in section 5.7. Finally, we conclude and discuss open research questions in section 5.8.

5.2 Background

5.2.1 Structure of the Electricity Market

There are two main markets for electricity. The wholesale market operates in bulk, while the retail market is where individual consumers (e.g., homeowners) interact with electric utilities. In this chapter, we focus on the wholesale market.

Before deregulation in the 1980s and 90s, the electricity industry operated as a monopoly, which meant that generators, transmission lines, substations, and distribution lines were owned and operated by monopolistic (sometimes government-owned) utilities. For several decades, the amount of energy consumed by their customers doubled about every eight years, and because of the lack of an efficient market, producers had significant costs for the expansion, planning, and real-time operations. Eventually, these costs were transferred to individual consumers.

With deregulation, electric utilities had to sell most of their generation plants and became wholesale consumers, bidding for electricity from power producers or other traders of electricity. Deregulated markets also allowed new participants to join the electricity markets such as energy firms, investment banks, and smaller traders, in fact, regulators of the electricity market encourage traders to join these markets in the hopes of making them more efficient. Deregulated electricity markets allowed the participation and competition of multiple energy producers and utilities in the market providing customers with efficient, cheap, and more reliable energy [168]. There are in general four major players in the market: producers (generators), consumers (retailers), a market operator, and a regulator.

Producers

Generation companies such as nuclear or coal power plants, hydropower plants, and wind farms mainly fall into this category where their basic goal is to produce and sell electric energy. They may also sell services such as frequency regulation, voltage control, and reserves to help the system operators maintain the reliability of the power grid. A generation company can own a single generator or a portfolio of generators with different technologies [159, 169]. In some cases, financial companies such as JPMorgan rent a power plant with multiple generators to participate in the market and make profits from their trading strategies [165, 166]. Other traders can also buy electricity from producers and then sell them in the wholesale market [163]. Electricity prices on the supply side are highly affected by fuel prices.

Retailers

Retailers buy electrical energy from the wholesale energy markets and resell it to consumers (e.g., homeowners). Electric utilities and electric vehicle (EV) aggregators[1] are two examples of such retailers [169, 170], but again, other traders can join the market and purchase electricity [163]. Consumer prices are highly affected by weather and economic activity.

Market Operator (MO) or Independent System Operator (ISO)

Market operators (MO), also known as independent system operators (ISO), run a computer program to match the bids and offers submitted by producers and retailers [169]. The second main responsibility of the ISO is to clear the market in such a way that it preserves the reliability of the power grid. For example, if all producers of electricity are in one geographical area and all consumers in another, the ISO has to make sure that the power transmission lines have the capacity to transfer the amount of energy. Therefore, specific bids and offers that violate the limitations of the power grid, will be removed from the market to maintain grid stability [169].

Regulator

A regulator is a government organization responsible for ensuring the fair and efficient operation of market players. This organization monitors the market, studies its environment, and determines a set of rules to prevent abuse, manipulation, and fraud by the market players. The regulator also sets the prices for the products and services that are provided by monopolies or single parties to preserve fairness in the market [169]. FERC is the main regulator in the U.S.

[1] An EV aggregator is a market player who participates in the wholesale market on behalf of a certain number of EVs and charges the batteries of these EVs based on a signed contract.

5.2.2 Day-Ahead and Real-Time Markets

The wholesale market is different than various other markets in that the products cannot be stored, so the production of electricity has to match the demand for electricity at every point in time, which in turn can lead to high volatility of electricity prices. To hedge this price volatility, the market is divided into two: a day-ahead market (which helps stabilize the prices of electricity) and a real-time market [159].

In the day-ahead market, all players in the market make forecasts of how much electricity will be needed for the next day, and then at 12 pm, they make offers for the amount of electricity they will produce (or buy) for every hour of the 24 hours of the next day. About four hours later the market is cleared by the ISO, and it releases the specific commitments for each player. For example, if player 1 submitted a bid for consuming 2 MWh for a price of $15 from 3 pm to 4 pm, player 1 has to do that, otherwise, she will be penalized financially.

Since predicting the exact energy demand a day in advance is impossible, the market needs to have a real-time component to correct prediction errors from the day-ahead market. If the day-ahead market committed to less generation than what is currently in demand, players make new bids and offers for electricity. If the day-ahead market is committed to more generation than what is currently in demand, the prices of electricity in the real-time market can plummet and in some cases can become negative (asking industries to consume electricity and being rewarded for that).

Both markets work the same way. A bid/offer submitted to the ISO (for the day-ahead or real-time market) at a specific time slot is shown in Figure 5.1. As illustrated in the figure, each player of the market submits a quantity-price pair to the ISO for each time interval. The ISO sorts the bids/offers based on the suggested prices and solves the optimization problem expressed in Equation 5.1–Equation 5.4 to maximize the social welfare of the market players and determine the optimal price of the market at each time slot while satisfying the power system physical constraints.

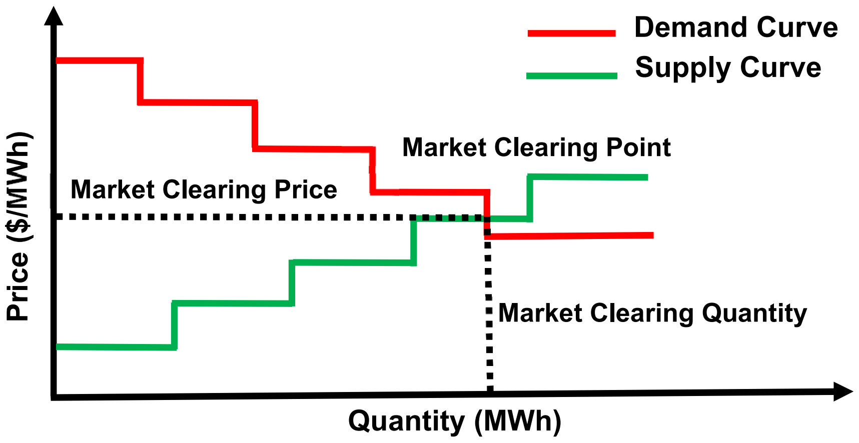


Figure 5.1: Illustration of a typical bid/offer in the market and its settlement mechanism.

$$\text{maximize} \quad welfare = \sum_{d \in \Omega_D} P_d^D \lambda_d^D - \sum_{s \in \Omega_S} P_s^S \lambda_s^S \tag{5.1}$$

subject to

$$0 \leq P_d^D \leq P_d^{D,\max}, \forall d \in \Omega_D \tag{5.2}$$

$$0 \leq P_s^S \leq P_s^{S,\max}, \forall s \in \Omega_S \tag{5.3}$$

$$system\ reliability\ constraints \tag{5.4}$$

The intuition behind Equation 5.1 is to maximize the area between the red and the green curve in Figure 5.1. P_d^D is the power demand (in MWh) by player d and λ_d^D is the price player d is willing to pay to buy that amount of power. In the figure, P_d^D is one of the steps in the x-axis of the red curve and λ_d^D is one of the steps in the y-axis of the red curve. Similarly, P_s^S is the amount of power supplier s is willing to provide at price λ_s^S. At the market-clearing price all players are happy because consumers are buying for less than (or equal) to their bid, and suppliers are receiving more (or equal) for the generation they promised. Equation 5.2 and Equation 5.3 denote that one of the bids or offers is not going to be accepted in its totality (e.g., that is why in Figure 5.1 the red line intersects the green line, meaning that one of the supply offers is cut shorter than what the supplier was offering). Finally, Equation 5.4 is beyond the scope of this chapter, but it basically deals with the physical topology of the grid and makes sure that the scheduled supply and demand do not violate any capacity constraints of the transmission lines in the power grid.

5.3 Threat Model

We assume our attacker has a high-wattage botnet, as proposed in recent work [5, 6, 84]. The difference with previous work on high-wattage botnets is that we are not using the botnet in an attempt to cause electricity blackouts, instead, we study how an attacker can profit from the botnet by manipulating the electricity market.

Market manipulation in the wholesale electricity market is not new. Perhaps the most popular case of wholesale electricity market manipulation is the case of Enron, a company that claimed revenues of over 100 billion during 2000 according to Fortune magazine, and who Fortune magazine named *America's Most Innovative Company* for six consecutive years. In the deregulated wholesale electricity market, traders–often pure middlemen who did not own power plants–began to ply their trade. One of their functions, which Wall Street calls arbitrage, was to try to buy power at a low price in one place and sell it at a higher price somewhere else. The biggest and savviest of traders was Enron [171]. Throughout the years Enron used a variety of tools to manipulate the electricity market in California, including urging operators to remove power generation plants to perform unnecessary maintenance, in order to cut the supply and share the profits of higher prices for generators [172]. Enron was finally caught due to unrelated accounting scandals [163], and it was only after the fallout of Enron that investigators found out about their energy market manipulation strategies. If Enron had not engaged in accounting fraud, their energy market manipulation tactics might not have been discovered for several years.

There are dozens of investigations for market manipulation every year. One high-profile case happened when FERC found evidence of manipulative bidding by JPMorgan in the California electricity market back in 2013 [164]. After a long fight in court, JPMorgan agreed to pay $410 million USD to settle allegations [165]. The company had rented two power plants and used manipulative bidding strategies in the market by creating artificial conditions (e.g., temporary power shortage in the grid) to sell the generated power at expensive premium rates [165]. More recently in 2017, FERC approved a $105 million settlement with the British bank Barclays for market manipulation [166].

In this chapter, we focus on attackers that want to manipulate the market. We assume two types of attackers with access to a high-wattage botnet:

Attacker Type I: The first attacker is a fraudulent trader, similar to one of the cases identified in the last two paragraphs. The goal of this trader is to use the high-wattage botnet to her advantage, manipulating the electricity market and profiting financially from the attack.

Attacker Type II: The second attacker does not participate in the market, but instead uses the high-wattage botnet to make the market as inefficient as possible, and thus cause widespread economic damage to operators of the power grid.

The overall structure of the threat model for these attackers is shown in Figure 5.2. Attackers first crawl the historical and real-time market data from available online sources to obtain the optimization parameters that are necessary for designing the attack scenarios (⓪). An Attacker Type I (fraudulent insider) then submits bids or purchase orders, and then also submits commands to the botnet (①). An Attacker Type II does not participate in the market, and simply sends commands to the botnet to cause market inefficiencies (②).

5.3.1 Basics of MaMIoT

The intuition behind the MaMIoT attack is the following: with a high-wattage IoT botnet, the attacker can predict better the real-time demand than other peers in the market, because

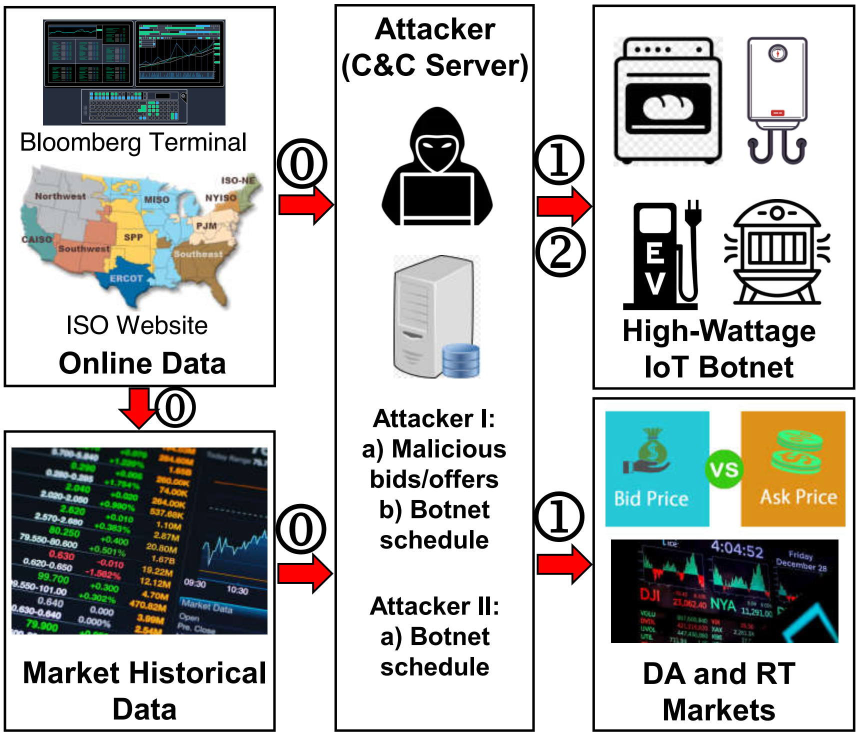


Figure 5.2: The overall view of the threat model and attack scenarios. ⓪ Crawler: Crawling the historical and real-time market data to be used for designing the attack scenario, ① Attacker Type I: Submitting the malicious bids/offers to the day-ahead and real-time markets and modifying the grid demand with the available botnet, ② Attacker Type II: Modifying the grid demand with the available botnet.

the high-wattage IoT botnet can allow the attacker to increase or decrease the electricity load slightly at will.

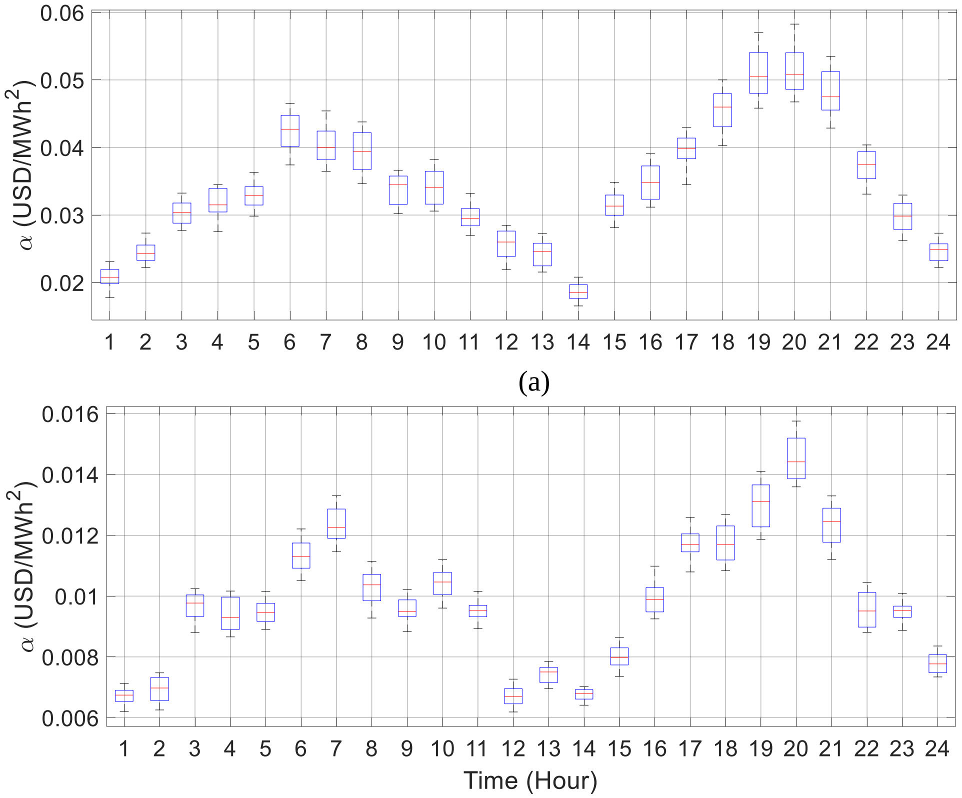
While not entirely an accurate analogy, using an example from the airplane industry can provide insights into how the electricity market can be manipulated: suppose you book an airline ticket for a flight you don't intend to board: it is a waste of time and money unless you are sure the flight will be overbooked and the airline will have to dish out rewards to passengers who agree to stay home [171]. Similarly, if you commit to producing electric power in the day-ahead market but the load does not materialize in the real-time market (e.g., by turning off several high-wattage IoT bots), you will get rewarded for not producing the power you did not have in the first place. On the other hand, an attacker can increase the load on a given day by turning on several high-wattage IoT bots. If the attacker is prepared (e.g., putting two generators in service for the day, instead of only one), it can deliver electricity in the real-time market at lower prices than other generators who did not anticipate this extra demand (and who did not turn on reserves).

More concretely, an adversary can manipulate the real-time market prices by slightly changing the total demand of the power grid through a high-wattage IoT botnet. This observation can be mathematically represented as:

$$\lambda_k^{RT} = \lambda_k^{RT0} + \alpha_k \Delta D_k^{System}, \forall k \in \Omega_K \tag{5.5}$$

where λ_k^{RT} is the manipulated real-time market price, λ_k^{RT0} is the original market price, ΔD_k^{System} is the power grid demand manipulation, and α_k is a constant number that can be obtained by analyzing market historical data. Additionally, k and Ω_K are the indexes and set of time intervals (e.g., 15 min.) in the market. According to this equation, an attacker can manipulate the real-time market price in his own favor by slightly changing the total demand of the power grid through high-wattage IoT botnets (ΔD_k^{System}). Based on our analysis, α_k changes considerably at every hour in a given market. Therefore the attacker needs to be strategic and find the *optimal* time to attack, as changing the load at different times will give different benefits.

By analyzing the historical data of two large electricity markets (New York and California) [117, 118, 173, 174] during one month period, we can estimate the value of α_k at each time interval; this is illustrated in Figure 5.3. According to this figure, the real-time market price in the New York market is more sensitive to demand manipulation compared to the California market. As we can see, price manipulation at certain hours (19-21) can be done with a fewer number of high-wattage IoT bots because of the higher price-load sensitivity factor (α_k). For example, a high wattage IoT botnet with 100,000 bots can change the system demand by 1% and this could result in +15 USD ($\sim$30% increase) in New York and +5 USD ($\sim$20% increase) in California.



(a)

(b)

Figure 5.3: The coefficient representing the price-load sensitivity in the real-time market obtained from analyzing the market historical data for one month. a) New York ISO, b) California ISO.

Launching successful market manipulation attacks requires sophisticated strategies for maximizing the objective function while maintaining the committed resources cleared in the market, and a low profile to avoid being detected by the market regulator. Before we discuss sophisticated optimization strategies, we first describe a naive baseline attack.

5.3.2 Baseline Attack

A naive attack strategy for a consumer to get lower electricity prices would be to turn off all high-wattage devices in the botnet. With lower demand, the price of electricity will fall and the consumer will pay less for electricity. The equivalent naive attack strategy for a generator is to turn on all high-wattage devices in the botnet, increasing the demand, and thus increasing electricity prices. The algorithm for the baseline attack is outlined in

Algorithm 1.

Algorithm 1 Baseline Attacker

```
function BASELINE($URL_{ISO}$)
    $History = Crawl(URL_{ISO})$    ▷ Read market historical data
    for $k = 1$ to $K$ do
        $\alpha_k = Statistics(History)$    ▷ Estimate price-load sensitivity at each time slot
        $botnet_k = Maximize(\alpha_k)$    ▷ Maximize the price at each time slot and find the relevant botnet attack
return $botnet_k$
```

Although the baseline attack may seem reasonable and effective at first glance, our analysis shows that it has two major weaknesses. First, if the adversary tries to benefit a single market player, this price manipulation must be accompanied by the consideration of the player's physical constraints; otherwise, this strategy will lead to lower attack gains because of the inevitable market penalties (making promises to produce or consume electricity, and then not being able to fulfill these promises). Figure 5.4 illustrates the profit breakdown of a typical market player in a single day with different bidding strategies. As we can see, the overall profit of the player increases in the baseline attack scenario compared to when there is not attack. However, there are some penalties in the baseline attack scenario because of the violation of the market limitations and the exclusion of the player's physical constraints (breaking the promises, as explained above). To prevent these penalties we need a more sophisticated attacker, which we introduce in the next section. In the more sophisticated attack, the adversary gains less profit in the day-ahead market; however, he obtains a large profit in the real-time market with no market penalty. The small day-ahead profit reduction can be regarded as the preparation cost for gaining the maximum profit in the real-time market with no penalties.

The second weakness of the baseline attack model is that the adversary might be detected by FERC fairly easily. Stealth is a key point for the success of MaMIoT attacks as this will allow the attacks to be repeatable (otherwise short-term gains will be small). Figure 5.5 shows the system load profile associated with different bidding strategies men-

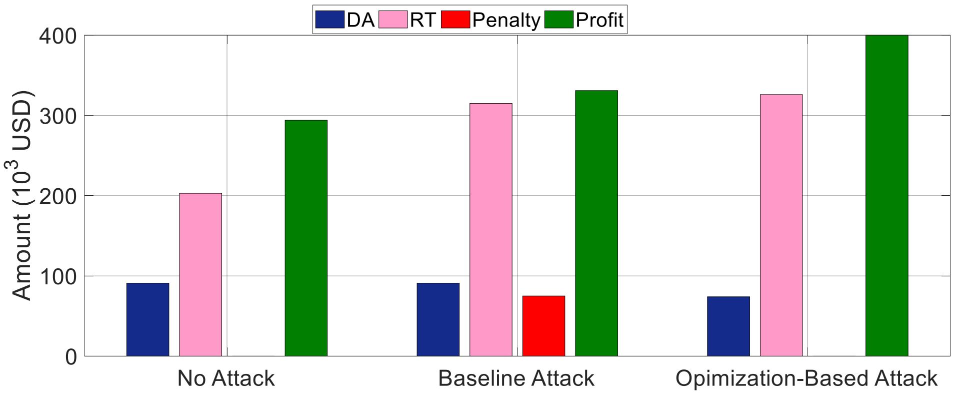


Figure 5.4: The profit breakdown of the simulated market player in a single day with different bidding strategies in the New York market. DA: day-ahead profit, RT: real-time profit, Penalty: market penalties, Profit: overall profit.

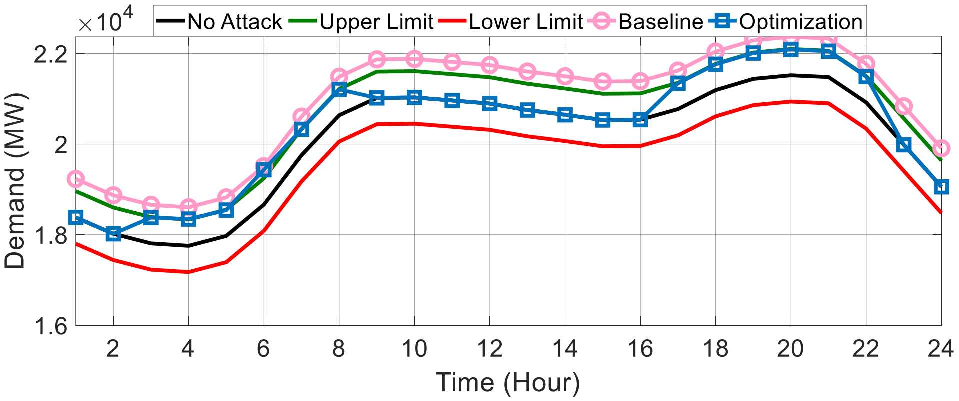


Figure 5.5: This figure shows that the optimized attack is less disruptive to the grid than the baseline attack. The optimized attack only only activates the botnet at certain times, and with fewer active bots.

tioned in Figure 5.4. As can be seen, the load profile of the system during the baseline attack exceeds the upper limit of a typical load forecasting error. Therefore the system operator can easily differentiate and detect this as an anomaly. Conversely, the load profile of the optimization-based attack remains within the lower and upper error limit band, and hence, it will be hard to differentiate these small electricity changes from the general daily errors in forecasting.

In short, while the naive attack may be better for the adversary than not launching attacks, the gains will be short-lived. There are too many variables and constraints (physical constraints of the player, market constraints, and stealth constraints) that the baseline attack does not consider. Therefore, we introduce more sophisticated adversaries who leverage mathematical optimization frameworks to maximize the attack gains.

5.3.3 Attacker Type I

There are two main decision variables for this type of attacker: i) malicious bids/offers made by the market player (attacker), and ii) system demand alteration at each time interval through the high-wattage IoT botnet (see ① in Figure 5.2).

To determine the key parameters (e.g., price-load sensitivity (α) as shown in Figure 5.3) for the optimization model, the adversary first analyzes publicly available historical market data from the market's website [117–119] or on a Bloomberg terminal [175]. Next, the attacker runs an optimization problem to determine the malicious day-ahead and real-time bids/offers in the electricity market and the required system demand change of each time slot (this will be realized through the high-wattage IoT botnet). In addition, we constrain attacks to be stealthy so that it is hard to accuse a specific market player of abuse. The algorithm for the first attacker type is outlined as follows:

Algorithm 2 Attacker Type I

```
function ATTACKI($URL_{ISO}$)
    $History = Crawl(URL_{ISO})$    ▷ Read market historical data
    for $k = 1$ to $K$ do
        $\alpha_k = Statistics(History)$    ▷ Estimate price-load sensitivity at each time slot
        $D_k^{stealthy,max} = Statistics(History)$    ▷ Estimate stealth parameter at each time slot
    $botnet_k, Bid_t^{DA}, Bid_k^{RT} = Optimization(\alpha_k, D_k^{stealthy,max}, physics)$    ▷ Maximize the player's gain subject to player's physical constraints, stealth constraints, and market constraints
return $botnet_k, Bid_t^{DA}, Bid_k^{RT}$
```

5.3.4 Attacker Type II

In this case, the attacker is a nation-state actor whose goal is to maximize the economic damage to a group of market players by manipulating real-time market prices through high-wattage IoT botnets. Because this attacker is external to the system, the only decision variable that is needed to be implemented in the market is the power demand changes at each time interval through the available high-wattage IoT botnet (see ② in Figure 5.2).

Financial markets have already seen nation-state attacks [62] as part of cold/trade wars and MaMIoT is the first cyber-based energy market manipulation that could damage the electric industry generation/demand of a targeted country. A nation-state attacker could even be a foreign investor in generation/demand companies who wants to alter the total revenue of the electricity generation/consumption corporations to affect their stock shares in his favor.

Similar to the previous attacker, the nation-state actor analyzes the historical market data to price-load sensitivity at each time slot (price-load sensitivity (α) as shown in Figure 5.3). Then, the attacker solves an optimization problem to determine the optimal attack vector to be implemented with the botnet of high-wattage IoT devices at each time interval. As mentioned earlier, we design the attack mechanism to be stealthy. The algorithm for the second attacker type is outlined as follows:

Algorithm 3 Attacker type II

```
function ATTACKII($URL_{ISO}$)
    $History = Crawl(URL_{ISO})$                    ▷ Read market historical data
    for $k = 1$ to $K$ do
        $\alpha_k = Statistics(History)$    ▷ Estimate price-load sensitivity at each time slot
        $D_k^{stealthy,max} = Statistics(History)$    ▷ Estimate stealth parameter at each time slot
    $botnet_k = Optimization(\alpha_k, D_k^{stealthy,max})$    ▷ Maximize the attack's gain subject to stealth constraints and market constraints
return $botnet_k$
```

5.3.5 Attack Feasibility

When we consider the feasibility of the MaMIoT attack there are two questions that come up, i) Will this attack work in practice? and ii) Can one acquire, compromise, and control a large botnet of high wattage IoT devices located within certain geographic boundaries

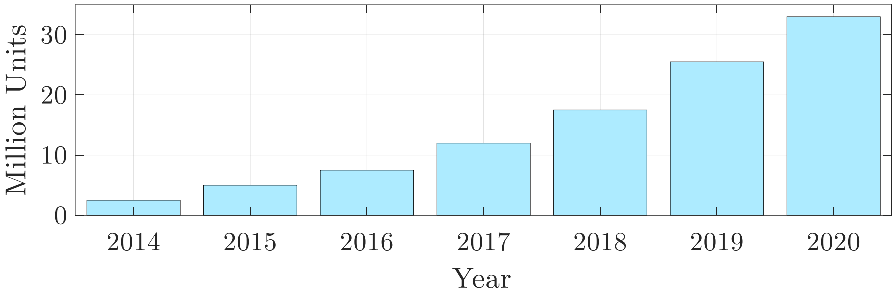


Figure 5.6: The growing trend of homes with smart thermostats in the North America region [178].

(e.g., within the state of California)?

We argue the answer to both of these questions is yes. To start, the command and control of IoT botnets is not new [176]. As IoT devices have grown in complexity and become more widely deployed, their power consumption has increased accordingly. This is emphasized in [177] where we see the average power consumption of an air purifier is 200W, making the premise of a high wattage IoT botnet fairly reasonable.

Number of Available High Wattage IoT Bots

The number of high-wattage IoT devices that an attacker can use in a MaMIoT attack is growing. The number of houses with smart thermostats in North America alone has increased at an unprecedented scale, representing a small fraction of the total high-wattage IoT devices in the automation field (see Figure 5.6) [178]. EV chargers are another big source of high-wattage devices. Concerning the matter of location, attackers can trivially determine whether a compromised device is within a certain geographical area through the device's IP address.

A MaMIoT attack does not need a significant number of compromised high-wattage IoT devices to be effective, but as the size of the botnet increases so does the economic impact of the attack (discussed at length in section 5.6). Even with a small botnet of high wattage devices, the attack can be extremely devastating as illustrated in subsection 5.6.3 and subsection 5.6.4. All things considered if we take into account that IoT botnets, such as Mirai, are capable of containing over six hundred thousand compromised devices [12], a future implementation of MaMIoT with a high wattage botnet of 100,000 bots would be a common scenario. Now, we discuss how this botnet could be obtained.

IoT Botnet Acquisition

The Mirai worm was first revealed in 2016 when it was used to DDoS KrebsOnSecurity, a computer security and cyber crime blog ran by former Washington Post Journalist Brian Krebs. Since the release of its source code in 2016, variants of Mirai have run rampant [179] and have been credited with several attacks including assaults against OVH (French cloud computing company), Dyn (DNS service provider), and the Liberian Internet infrastructure. These and other IoT malware such as, Bashlite, Reaper, Satori, and Linux.Aidra, have been able to infect IoT devices through primarily known and patchable vulnerabilities [176] resulting in a low barrier to entry for the supply and demand of botnet for hire services.

Botnet rental services level the playing field for entities that are unable to create/deploy malware for building their own army of bots. On the dark web, buyers can obtain access to DDoS services for periods ranging from days to several months [128]. Within their service period, clients can launch a limited or unlimited (for a premium) number of attacks per day with a guaranteed minimum duration ranging from minutes to hours. Table 5.1 gives a breakdown of some advertised and estimated costs for utilizing DDoS for hire and IoT botnet rental services. This table shows how the commoditization of cybercrime has made it feasible to launch attacks for less than the cost of most cyber certifications. It is worth mentioning that although the botnets presented in Table 5.1 are not necessarily built from high wattage IoT devices, the given numbers in the table can still be used for estimating the cost of building/renting a typical high wattage IoT botnet.

Based on the presented results in section 5.6, even if the cost of building/renting a high wattage IoT botnet is ten times bigger than what is mentioned in a realistic botnet rental

Table 5.1: IoT botnet rental and DDoS for hire cost breakdown.

Name	**Botnet Size**	**Rental Cost**	**Duration**	**Bandwidth**	**Type of Bots**
JenX [129]	-	$20/target	-	295Gbps	small/office routers
Mirai variant [128]	50k	$3-4000/2 weeks	1 hour	-	cameras, routers, DVRs, etc.
Bushido [130]	20k	$20-150/month	-	500Gbps	cameras, routers, DVRs, etc.
Reaper [180]	30k	-	-	-	cameras, routers, DVRs, etc.
Satori [131]	100k	-	-	-	small/office routers
Estimate for IoT Botnet Services [132]	-	$\sim$$15/week	-	300Gbps	-
Estimate for DDoS Services [133]	-	$20-45/month	1 hour	220Gbps	-

service, this cost is still negligible compared with the attack gain.

Effect of the Attack on the End User's Billing Statement

The financial effect of the proposed attacks on each end-user depends on their monthly total power consumption as well as the duration of the attack. According to the EIA, the average electricity consumption of Americans is 914 kWh per month. Tennessee has the highest electricity consumption at 1,282 kWh per residential customer, and Hawaii has the lowest at 517.75 kWh per residential customer [135]. Assuming that each of the high wattage IoT bots consumes 3 kW electricity and considering the stealth strategies explained in section 5.6 (the attack is carried out 100 days per year (8 days/month) and each bot is turned on for 3 hours on average during the daily attack), each compromised home would consume 72 kWh more electricity in each month. This means a 7.8% increase in the billing statement in the attacked residents, which will likely be unnoticeable. For example, a typical customer who pays $120 monthly for his electricity bill in the U.S., will pay $129 if he is attacked. Note that the considered numbers are associated with the most severe IoT botnet attack on the electricity market (see NY3 and CA3 in Figure 5.8, Figure 5.14, and Figure 5.15). For example, replacing 3 kW with 1 kW will lead to a trivial 2.6% increase in the monthly electricity bill.

5.4 Stealth Strategies

In order to make the MaMIoT attack repeatable and add to the motivation of the attackers, the adversary can employ several strategies, alone or in combination. Some of the practical strategies are outlined as follows:

From the End-User's Perspective

It goes without saying that the attacker should try to hide his activity from the compromised homes. To achieve this goal, one effective strategy would be the use of compromised high wattage IoT devices when the awareness of the home owner is very low. According to the typical time of use for some popular categories of high wattage home IoT devices summarized in Table 5.2, it can be surmised that there are many opportunities for botnet attacks outside of the normal time of use which would be undetected by an end user. While some HVAC devices such as AC and heaters tend to run on/off all day, others such as an EV charger may only consume power during "after work" hours when end users are home.

Table 5.2 shows the typical time of use for some popular categories of high wattage home IoT devices. From the table it can be surmised that there are many opportunities for botnet attacks outside of the normal time of use which would be undetected by an end user. While some HVAC devices such as AC and heaters tend to run on/off all day, others such as an EV charger may only consume power during "after work" hours when end users are home.

In order to conceal additional device usage for limited period of time (i.e., 1-3 hours on average), the attacker can classify the compromised IoT devices and leverage their potential based on their availability time. For example devices such as ovens are used during hours when presumably no one is in the kitchen (1-4AM) while devices such as EV chargers can be used during the night when the EV is connected to the grid (see Table 5.2). Some of these devices such the EV charger have been proven to have a great potential in these

Table 5.2: High wattage consumer IoT device availability [182]. Wattage represents maximum per device.

Smart IoT Device	Energy Consumption (W)	Peak Use Time	Avg Use Length	Time to Attack
Water Heater [183]	5000	Morning	3h/day	Early Morning
AC [184]	1000	All-day	9h/day	Anytime
Garage Opener [185]	1100	All-day	3min/day	Midday
Fridge [186]	900	All-day	24h/day	Midday
Heater [187]	1500	Evening	3h/day	Anytime
EV charger [188]	12000	Evening	8h/day	Early Morning
Oven and Stove [189]	4000	Evening	1h/day	Early Morning
Washer [190]	1200	Sporadic	2h/wk	Early Morning
Dryer [190]	1800	Sporadic	2h/wk	Early Morning
Dishwasher [191]	852	Sporadic	120min/day	Early Morning
Treadmill [192]	735	Sporadic	90min/wk	Early Morning

attacks [181].

From the Market Operator's Perspective

Additionally, the attacker needs to hide his activity from the market operator. The following items list some of the practical strategies in this category.

I) Smooth Load Profile Changes: The main way the system operator (SO) can detect the MaMIoT attack, is to analyze the daily load profile of the system. A naive attacker changes the system demand without considering any limitations, which might lead to a noticeable difference between the attacked load profile and a typical benign one. In this chapter, we formulate the model such that the attacked load profile of the system becomes very similar to a typical daily load profile, making it very challenging for the SO to detect any abnormalities in the system (see section 5.6 for numerical results).

II) The Frequency of Attack: As the frequency of the attack increases, the possibility of it being caught by SO increases as well. A smart attacker will launch the MaMIoT attack only for a certain number of days (e.g., 100) in each year. By doing this the attack days can be determined randomly, making it hard for the SO to determine which days are normal and which days the market is attacked.

III) Choosing a Suboptimal Attack Scenario: In this strategy, the attacker does not implement the optimal attack scenario on the market. Instead, he sacrifices a portion of his profit to make his attack stealthier. To achieve this, the attacker runs the proposed optimization model and chooses a suboptimal point (e.g., 80% of the optimal point).

IV) Targeting Other Players: In this strategy, the attacker occasionally maximizes the profit of the other players in the market to defer the suspicion of the SO onto them. These players can be the competitors of the attacker or the entities whose loss result in economic benefit for the attacker.

5.5 Formulation of the Attack Model

In this section, we explain the optimization models that adversaries can employ to determine the attack scenarios as explained in section 5.3.

5.5.1 Attacker Type I

As mentioned in section 5.3, this type of attacker is one of the market players whose goal is to maximize his own profit by manipulating the real-time system demand through the strategic use of high wattage IoT botnets. To show the effectiveness of the MaMIoT attack, we present one sample optimization model for a common market player: a generation company. Note that without loss of generality, the proposed optimization framework with slight changes can be leveraged to model the other types of market players.

We assume that a conventional power plant, which includes multiple steam turbines and generators, can control a botnet of high wattage IoT devices to make profit from the energy market. The following optimization problem is developed to determine the optimal offers in the day-ahead and real-time markets along with the attack vector to be sent to the bots in the botnet. The objective function of the model is defined as:

$$\begin{aligned} \text{maximize} \quad profit^{G} = \sum_{g \in \Omega_G} \sum_{t \in \Omega_T} profit_{gt}^{DA,G} \\ + \sum_{g \in \Omega_G} \sum_{k \in \Omega_K} profit_{gk}^{RT,G} - \sum_{k \in \Omega_K} Cost_{k}^{Botnet} \end{aligned} \tag{5.6}$$

where $profit^{G}$ is the total profit of the generation company. Similarly, $profit_{gt}^{DA,G}$ and $profit_{gk}^{RT,G}$ denote the profit of unit g at hourly (sub-hourly) time interval t (k) in the day-ahead and real-time markets, respectively. Also, $Cost_{k}^{Botnet}$ represent the cost of building/renting the required botnet for the desired attack. These variables can be calculated as follows:

$$\begin{aligned} profit_{gt}^{DA,G} = \lambda_{t}^{DA} P_{gt}^{DA,G} - \left(\lambda_{g}^{SU} u_{gt} + \lambda_{g}^{SD} v_{gt}\right) \\ -\lambda_{g}^{G,Constant} x_{gt}^{G}, \forall g \in \Omega_G, t \in \Omega_T \end{aligned} \tag{5.7}$$

$$\begin{aligned} profit_{gk}^{RT} = \lambda_{k}^{RT} P_{gk}^{RT,G} - \left(\lambda_{g}^{G,Fuel} P_{gk}^{RT}\right) \\ -\frac{\lambda_{t}^{DA,Dev}}{\mathcal{K}} \left(P_{gt}^{DA,Dev+,G} + P_{gt}^{DA,Dev-,G}\right), \\ \forall g \in \Omega_G, k \in \Omega_K, t \in \Omega_k, \end{aligned} \tag{5.8}$$

$$Cost_{k}^{Botnet} = \lambda_{k}^{Botnet} D_{k}^{attack}, \forall k \in \Omega_K. \tag{5.9}$$

The day-ahead profit for each unit, $profit_{gt}^{DA,G}$, includes the revenue from the day-ahead market participation ($\lambda_{t}^{DA} P_{gt}^{DA,G}$) minus the costs associated with the unit start-up, shut-down ($\lambda_{g}^{SU} u_{gt} + \lambda_{g}^{SD} v_{gt}$), and its constant operation ($\lambda_{g}^{G,Constant} x_{gt}^{G}$). The real-time profit for each unit, $profit_{gk}^{RT,G}$, includes the revenue from the real-time market participation ($\lambda_{k}^{RT} P_{gk}^{RT,G}$) minus the fuel cost of the unit ($\lambda_{g}^{G,Fuel} P_{gk}^{RT}$) along with the cost associated with the penalty for deviating from the day-ahead bid in real-time operation. According to our analysis, the real-time market price (i.e., λ_{k}^{RT}) in Equation 5.8 can be notably affected by the real-time power mismatch between the system generation and demand. This property can be effectively used by the adversary to change the profit which can be obtained from the real-time market. The attacker can change the real-time system demand through the high wattage IoT botnets and affect the real-time market price in his favor. By analyzing the historical data of the market (which is publicly available on the official websites of ISOs and Bloomberg terminal [117–119, 173–175]), we can extract the relationship between the system real-time power mismatch and the real-time market price. In this chapter, we assumed a linear model for this change as follows:

$$\lambda_k^{RT} = \lambda_k^{RT0} + \alpha_k \Delta D_k^{System}, \forall k \in \Omega_K \tag{5.10}$$

where λ_k^{RT} is the real-time market price after the attack, λ_k^{RT0} is the expected real-time market price before the attack, ΔD_k^{System} is the total change in the system demand which can be done through a high wattage IoT botnet, and α_k is a constant number which can be obtained by analyzing market historical data. According to Equation 5.10, the attacker can significantly alter the real-time market price in his favor if he has access to a large number of compromised IoT devices. However, if the attacker changes the system demand significantly, it can be easily detected by the ISO in the market as an anomaly. Therefore, in order to keep the attack stealthy and undetectable, we need to limit the system demand change to stay within the normal load forecasting error (as determined from historical market data). The mathematical representation of this limitation can be defined as:

$$-\Delta D_k^{stealthy,\max} \leq \Delta D_k^{System} = D_k^{attack} - D_k^{actual} \leq \Delta D_k^{stealthy,\max}, \forall k \in \Omega_K \tag{5.11}$$

in which $\Delta D_k^{stealthy,\max}$ is the average of the load forecasting error at time slot k which is determined by analyzing the market historical data from the ISO's public website. Another point that should be considered here is that the system demand alteration should be capped with the maximum capability of the high wattage IoT botnet, that is,

$$-\Delta D_k^{botnet,\max} \leq \Delta D_k^{System} = D_k^{attack} - D_k^{actual} \leq \Delta D_k^{botnet,\max}, \forall k \in \Omega_K \tag{5.12}$$

where $\Delta D_k^{botnet,\max}$ is the maximum capability of the IoT botnet at time slot k. This parameter represents the maximum capability of the attacker in changing the total demand of the power grid. It should be noted that additional strategies, such as limiting the number of hours for the demand alteration, can be embedded in Equation 5.11 to maintain attack stealth. The physical constraints associated with the power plant are listed as follows:

$$\begin{aligned} P_{gk}^{Act,G} = P_{gt}^{DA,G} + \left(P_{gt}^{DA,Dev+,G} - P_{gt}^{DA,Dev-,G}\right) \\ +P_{gk}^{RT,G}, \forall g \in \Omega_G, k \in \Omega_K, t \in \Omega_k \end{aligned} \tag{5.13}$$

$$x_{gt}^G P_g^{\min} \leq P_{gk}^{Act,G} \leq x_{gt}^G P_g^{\max}, \quad \forall g \in \Omega_G, k \in \Omega_K, t \in \Omega_k \tag{5.14}$$

$$-R_g^D \leq P_{gk}^{Act,G} - P_{g(k-1)}^{Act,G} \leq R_g^U, \quad \forall g \in \Omega_G, k \in \Omega_K \tag{5.15}$$

$$x_{g(t-1)}^G - x_{gt}^G + u_{gt}^G \geq 0, \forall g \in \Omega_G, t \in \Omega_T \tag{5.16}$$

$$x_{gt}^G - x_{g(t-1)}^G + v_{gt}^G \geq 0, \forall g \in \Omega_G, t \in \Omega_T \tag{5.17}$$

$$x_{gt}^G - x_{g(t-1)}^G \geq x_{g\tau}^G, \forall g \in \Omega_G, t \in \Omega_T, t \neq t_1, \tau \in \left[t+1, \min(t + T_g^{U,G} - 1, T)\right], \tag{5.18}$$

$$x^G_{g(t-1)} - x^G_{gt} \geq 1 - x^G_{g\tau}, \forall g \in \Omega_G, t \in \Omega_T, t \neq t_1, \tau \in \left[t+1, \min(t + T^{D,G}_g - 1, T)\right], \tag{5.19}$$

The group of Equation 5.13–Equation 5.19 is related to the physical constraints of every power plant including various types of units. More specifically, the real-time output power of each generating unit at each time slot can be calculated through Equation 5.13. Equation 5.14 describes the constraint in which the output power of a generator must be between its minimum and maximum amount when it is running (i.e., $x_{gt} = 1$). Also, Equation 5.15 defines the ramp limit on the increase/decrease of the output power of each generator. Generator start-up and shut-down constraints are modeled through Equation 5.16–Equation 5.17. Finally, depending on the type of the unit, it has minimum up and down time limitations which are mathematically represented via Equation 5.18–Equation 5.19.

Ultimately, most electricity markets do not allow the players to deviate too much from their submitted bids in the day-ahead market [117–119]. The mathematical model of this constraint is given as:

$$0 \leq P^{DA,Dev+,G}_{gt} \leq \kappa P^{DA,G}_{gt}, \forall g \in \Omega_G, t \in \Omega_T \tag{5.20}$$

$$0 \leq P^{DA,Dev-,G}_{gt} \leq \kappa P^{DA,G}_{gt}, \forall g \in \Omega_G, t \in \Omega_T \tag{5.21}$$

where κ (e.g., 20%) is the percentage that allows the players to deviate from their day-ahead bids subject to a specified penalty. Different markets may have various regulations which can be mathematically incorporated in the optimization model without the loss of generality. It should be noted that the proposed optimization formulation considers the integrated behavior of all market players including the malicious one. The effect of the attack on the other market players is discussed in section 5.6.

5.5.2 Attacker Type II

As pointed out in section 5.3, this type of attacker is a nation state actor whose goal is to maximize the economic damage to the market players by manipulating the system real-time demand through high wattage IoT devices. This attack can target either the generation side or the demand side depending on the ultimate goal of the attacker. The optimization model for attacking the demand side companies (i.e., retailers) is as:

$$\begin{aligned}\text{maximize } & \mathit{economic\ damage} = \\ & \sum_{k\in\Omega_K}\left(D_k^{attack}\lambda_k^{RT} - D_k^{actual}\lambda_k^{RT0}\right) - \sum_{k\in\Omega_K}\lambda_k^{Botnet}D_k^{attack}\end{aligned} \tag{5.22}$$

$subject\ to$

Equation 5.10–Equation 5.12.

According to this model, the attacker seeks to maximize the economic damage to the retailers through affecting the real-time market prices while keeping his attack stealthy. Similar to this case, the model for attacking the generation side can be defined as:

$$\begin{aligned}\text{maximize } & \mathit{economic\ damage} = \\ & \sum_{k\in\Omega_K}\left(G_k^{actual}\lambda_k^{RT0} - G_k^{attack}\lambda_k^{RT}\right) - \sum_{k\in\Omega_K}\lambda_k^{Botnet}D_k^{attack}\end{aligned} \tag{5.23}$$

$subject\ to$

Equation 5.10–Equation 5.12.

Note that in both of the aforementioned models we assumed that the attacker can attack either the generation side or the demand side in one day. We can easily modify this assumption by changing the limits of the sums in the objective functions.

5.6 Numerical Analysis and Discussion

5.6.1 Description of the Studied Test Cases

To evaluate the attack scenarios with real-world datasets, we collected market data associated with New York and California ISOs during a one-year (May 2018 – May 2019) period [117, 118, 173, 174]. The historical data is presently available on the ISOs websites and on Bloomberg terminal, and are updated every 5 minutes. Publicly available historical datasets are also typically available in the other electricity markets around the world which makes these markets vulnerable to attacks such as MaMIoT. The California ISO is one of the largest ISOs in the world, which is responsible for delivering roughly 0.300×10^9 MWh of electricity each year to its customers [193]. Similarly, the New York ISO is another large electricity market in the U.S. with 0.156×10^9 MWh of total annual energy consumption [194]. In the following subsections, we will present our analysis of the aforementioned markets. Since the direct implementation of this attack in electricity markets can have huge financial consequences (e.g., 2 million USD per day with a relatively small botnet), we have used the real-world market data to simulate the attack with reasonable and detailed models. This helped us avoid any law-related repercussions while investigating the attack consequences with real-world data.

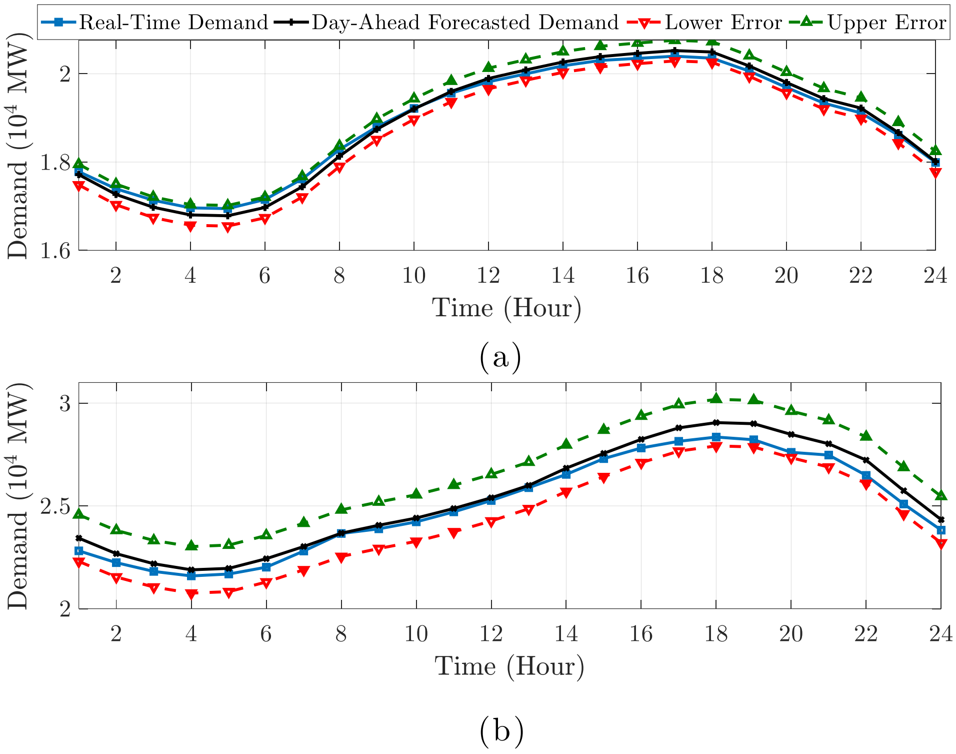
5.6.2 Determining the Input Parameters of the Optimization Models

As explained in subsection 5.5.1, a slight deviation of the system's real-time loads from their forecasted value has a linear effect on the real-time market price (see Equation 5.10). In order to launch a successful MaMIoT attack, the adversary must first obtain this relationship from the market historical data. In fact, the goal is to determine α_k for the market under investigation. Since the trends in load profiles and market prices change every month, the α_k parameter must also be updated every month. Figure 5.3 shows the value of this parameter for the California and New York markets for each time interval from the market data on June 2019. This figure was acquired through analyzing the historical data of these markets.

Another important parameter that plays a key role in keeping the attack stealthy is $\Delta D_k^{stealthy,\max}$. According to our analysis, the average prediction error of the system real-time demand at different time slots is 580 MW and 2265 MW in the New York and California ISOs. Figure 5.7 shows a typical day-ahead forecast and the real-time demand associated with each of the analyzed markets. The dashed lines in the figure indicate the upper and lower prediction errors for each market. The figure illustrates that the load forecasting error band for the California market is higher than that of the New York market. Some reasons for this are i) the California market is a bigger market and has more maximum power capacity, and ii) the share of flexible loads in the California market is larger than that of the New York market. By limiting the system demand change to the specified error range (typical prediction error), the attacker can make the attack look similar to normal real-time system demand, thereby keeping the attack stealthy and repeatable. Note that in the simulated cases, we considered three different average power consumption for each bot within the botnet (see Figure 5.8, Figure 5.14, and Figure 5.15). The subscripts 1, 2, and 3 of each bar plot in the figures represent 1 kW, 2 kW, and 3 kW for the two markets (NY and CA), respectively.

5.6.3 Market Player Attacker Results

In this section, we assume that the attacker owns a power plant and can participate in the day-ahead and real-time electricity markets. The simulated power plant consists of ten different units (generators) with the technical characteristics given in Table 5.3 [195]. In this table, the units of the given parameters in the first row from left to right are USD/MWh, USD, USD, USD, MW/hr, MW/hr, hr, hr, MW, MW, hr, nothing, and hr. Also, U_g^0 denotes time periods unit g has been on at the beginning of the planning horizon (end of hour 0). Similarly, S_g^0 represents the time periods that unit g has been shut-down at the beginning of



(a)

(b)

Figure 5.7: Typical load forecasting error band: a) New York ISO (580 MW), b) California ISO (2265 MW).

the planning horizon.

Table 5.3: Technical data of the simulated power plant units [195].

Unit	$\lambda_g^{G,Fuel}$	$\lambda_g^{G,Constant}$	λ_g^{SU}	λ_g^{SD}	R_g^U	R_g^D	$T_g^{U,G}$	$T_g^{D,G}$	$P_g^{\min}$	$P_g^{\max}$	U_g^0	$x_{g(t=0)}^G$	S_g^0
g_1	12.1	82	42.6	42.6	80	80	3	2	80	200	1	0	1
g_2	12.6	49	50.6	50.6	120	120	4	2	120	320	2	0	0
g_3	13.2	100	57.1	57.1	50	50	3	2	50	150	3	0	3
g_4	13.9	105	47.1	47.9	250	250	5	3	250	520	1	1	0
g_5	13.5	72	56.6	56.9	80	80	4	2	80	280	1	1	0
g_6	15.4	29	141.5	141.5	50	50	3	2	50	150	0	0	0
g_7	14	32	113.5	113.5	30	30	3	2	30	120	0	1	0
g_8	13.5	40	42.6	42.6	30	30	3	2	30	110	0	0	0
g_9	15	25	50.6	50.6	20	20	0	0	20	80	0	0	0
g_{10}	14.3	15	57.1	57.1	20	20	0	0	20	60	0	0	0

The maximum power generation of the power plant is 1990 MW. We simulated the participation of this power plant in the New York and California markets and assumed that the player had control over a high wattage IoT botnet. Figure 5.8 illustrates the total additional daily profit the power plant owner stands to gain versus the varying numbers of compromised high wattage IoT devices in the botnet. According to this figure, as the size of the botnet increases, the total additional profit increases in both of the studied markets. Our analysis revealed that the power plant owner can gain up to 326,000 USD daily profit (in NYISO) without the implementation of MaMIoT attack ($\Delta D_k^{botnet,\max} = 0$), but with only 200,000 compromised IoT devices (with an average power consumption of 3 kW per device), they could gain an additional 150,000 USD in profit. This is 30% more than the base case without any attacks. By implementing the MaMIoT attack for only 100 days in a year, the studied market player would be able to gain an additional 15 million USD in profit from the electricity market. Interestingly, MaMIoT does not require any specific number of compromised IoT devices to launch a successful attack. This means that the success rate for the attack is 100% with any given botnet size. However, working with a smaller-sized botnet simply results in less additional profit.

Figure 5.8 shows that with a larger number of compromised IoT devices, the attacker can gain more economic profit from the bigger electricity markets. Another interesting observation from Figure 5.8 is that the daily additional profit of the power plant owner in the New York market saturates once the botnet size exceeds 200,000 bots. The reason being the attacker can only control 600 MW of system demand with 200,000 bots (with an average power consumption of 3 kW per device). However, according to Figure 5.7, a stealth attack on the New York ISO can alter a maximum 580 MW of the system's total demand in real-time. So, although the attacker controls over 580 MW with more than 200,000 bots, he is limited to the allowable range (below 580 MW) to keep the attack stealthy. With the maximum demand alteration for botnets greater than 200,000 bots capped at 580 MW, the attack's effect will be the same in all the cases where the botnet size is greater than 200,000 bots.

Figure 5.9 shows the load profile of the system at each time interval associated with different botnet sizes. In this figure, attackers 10 k, 50 k, 100 k, 150 k, 200 k, and 250 k are associated with botnets with 10,000, 50,000, 100,000, 150,000, 200,000, and 250,000 compromised high wattage IoT devices. The figure shows the attacked load profiles are within

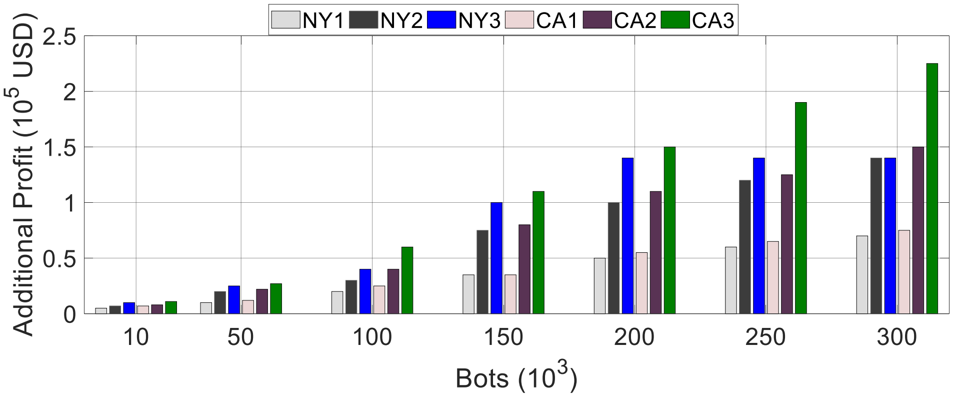
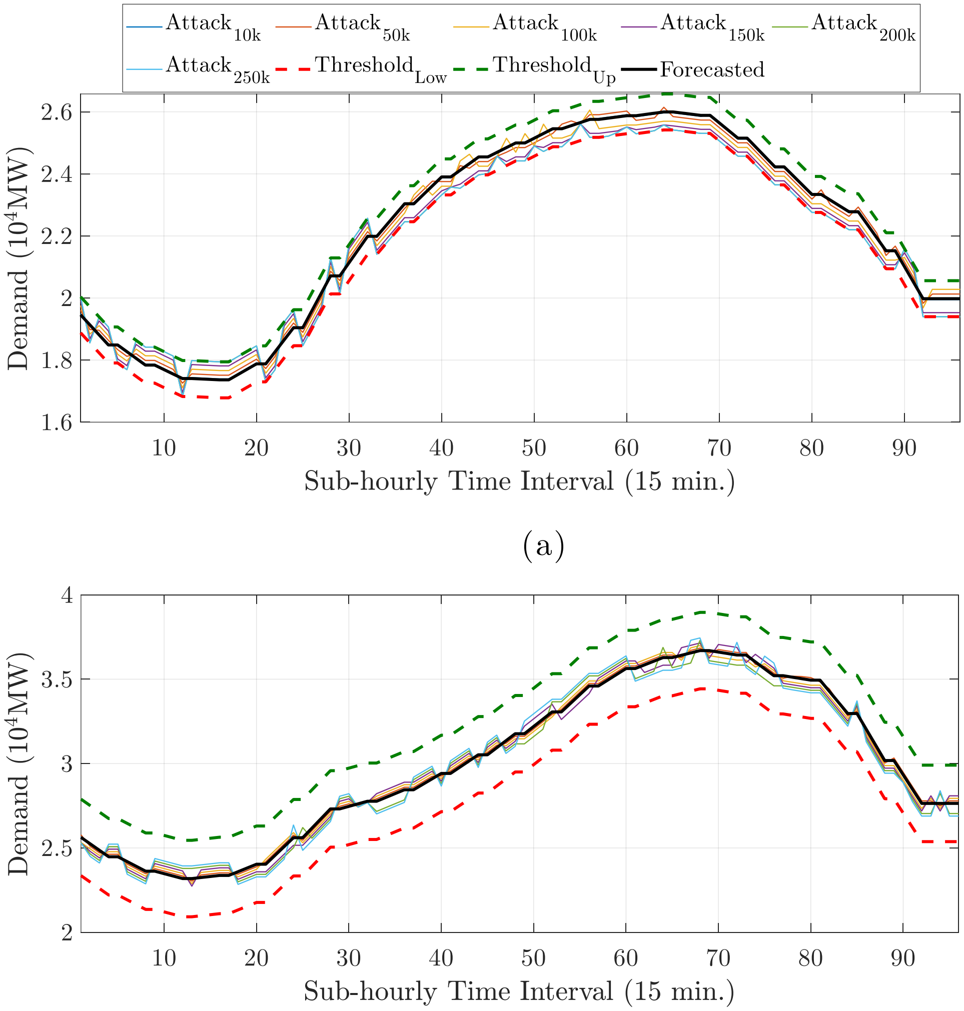


Figure 5.8: Total additional daily profit of the power plant owner versus the number of compromised high wattage IoT devices.

the specified load forecasting error range and therefore maintain stealth in the proposed attack model. The manipulated system load profile is very similar to typical real-time system demand. This makes it very hard for the market regulator or ISO to detect one player is abusing the market mechanism in his own favor. Such stealth strategies enable the adversary to repeat his attack and multiple times per month and make significant additional profits from the electricity markets.



(a)

(b)

Figure 5.9: Load profile of the power grid at each time interval associated with attacks launched by the power plant owner with different botnet sizes: a) New York ISO, b) California ISO. Notice how the attack increases and decreases the consumption of energy.

Figure 5.10 illustrates the profit breakdown of the adversary in the New York and California markets with different attack scenarios. As can be seen, the overall profit of the attacker in both New York and California markets is maximum when the adversary uses the optimization-based attack. The baseline attack excludes the key constraints in the attack scenario, and hence, causes monetary penalties from the market. The optimization-based attack on the other hand has zero penalties in both markets, which leads to the maximum profit for the malicious market player.

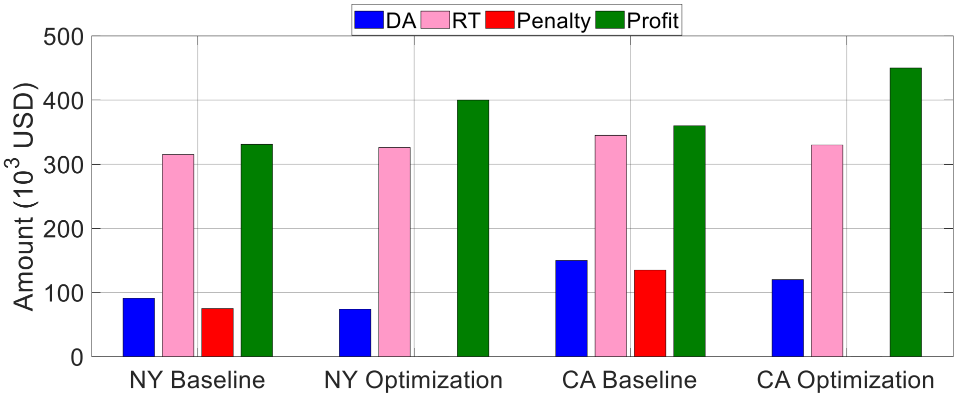


Figure 5.10: The profit breakdown of the simulated market player in a single day with different bidding strategies in the New York and California markets. DA: day-ahead profit, RT: real-time profit, Penalty: market penalties, Profit: overall profit.

To illustrate the interaction between multiple market players in the New York market, we considered 21 generation players and 20 consumer players. For the first case, let's assume one of the generation players is malicious and can control a botnet of high-wattage devices. Figure 5.11 shows the overall daily profit of the market players during the no attack and optimization-based attack scenarios. As it can be seen, the manipulations of the malicious market player increase the gain of the other generation players in the market as well. However, since the adversary knows about the manipulated real-time prices in advance, he prepares for the manipulated situation and obtains the maximum profit out of that. The consumer market players lose small profits because of this market manipulation.

In the other simulated case, we assumed that the adversary is one of the consumer players in the New York market. Accordingly, one of the 20 players on the consumer side is malicious and can control a high-wattage IoT botnet. Figure 5.12 shows the overall daily profit of the market players during the no attack and optimization-based attack scenarios. As it can be seen, the malicious market player gains the maximum profit from the attack while the other consumer players gain marginal profit from the manipulations. Conversely, the benign generation players lose small profits because of the price manipulations.

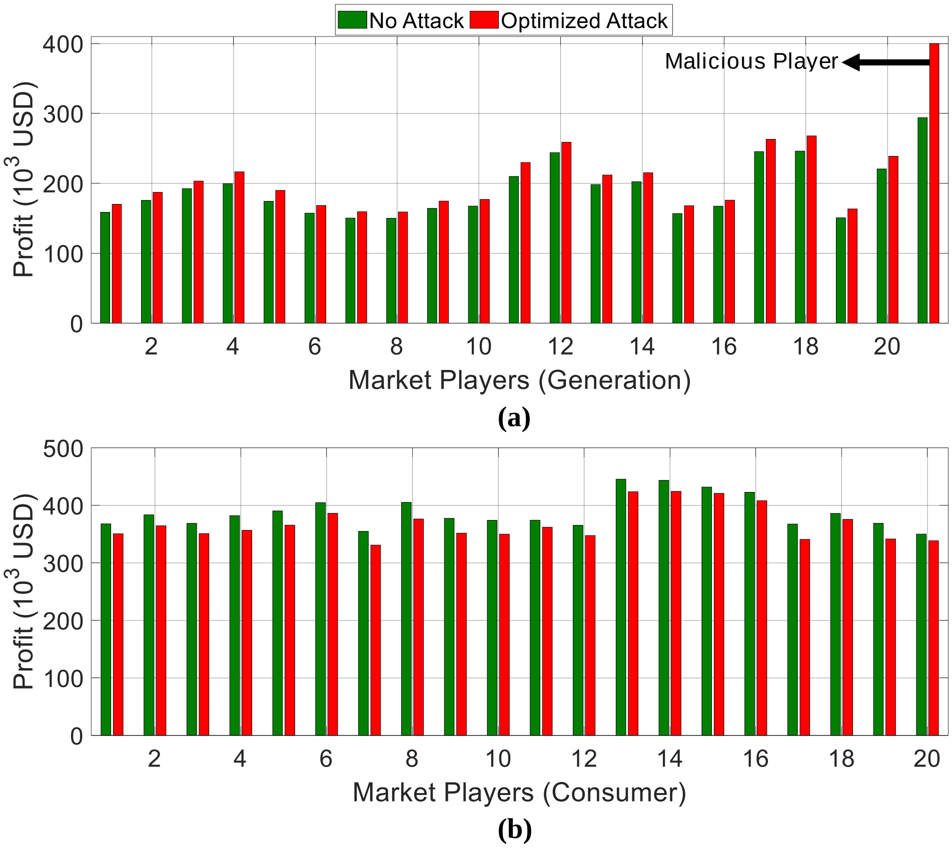
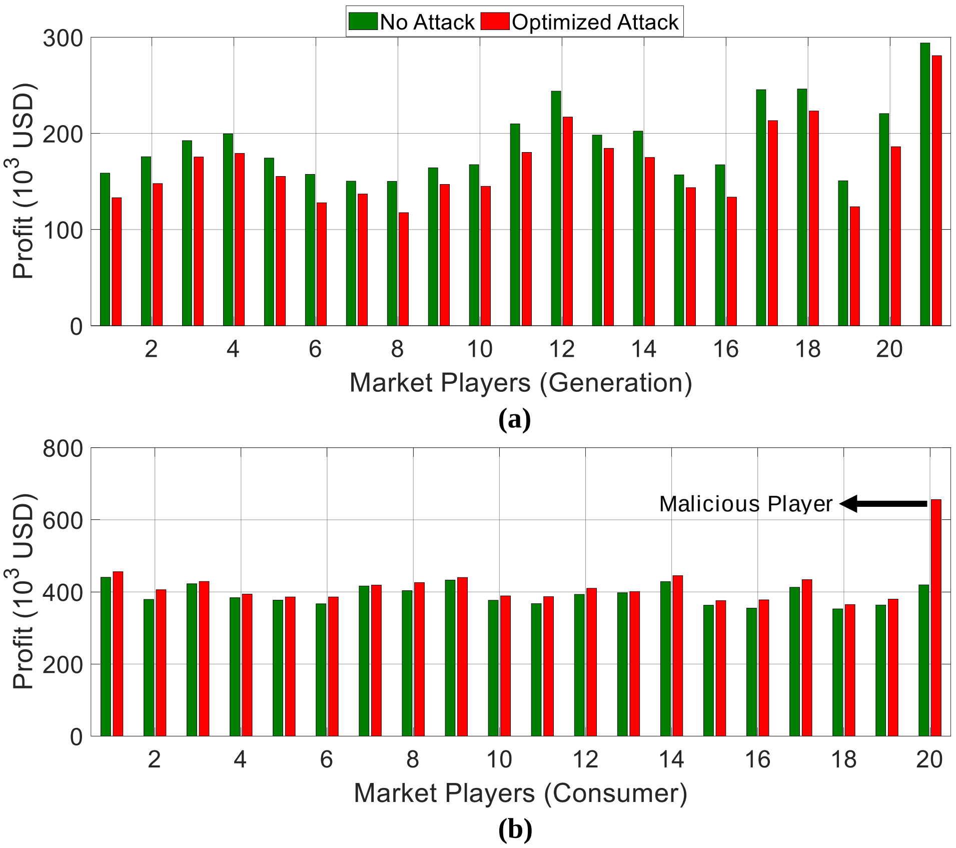


Figure 5.11: The daily profit of the market players in the New York ISO (only 21st generation player is malicious). a) Generation players, and b) Consumer players.

Finally, as it was discussed in subsection 5.5.1, the day-ahead price forecasts are used to determine the optimal attack scenario by the malicious market player. Here, we aim to analyze the effect of prediction error in this parameter on the attack's gain. Figure 5.13 shows the daily profit of the attacker in both markets versus the estimation error in the day-ahead market prices. According to this figure, the adversary's gain does not change significantly with the increase in the estimation error. This observation illustrates that we



(a)

(b)

Figure 5.12: The daily profit of the market players in the New York ISO (only 20th consumer player is malicious). a) Generation players, and b) Consumer players.

made a reasonable assumption in our formulation to consider this parameter in the optimization model.

5.6.4 Nation-State Attacker Results

As explained in subsection 5.5.2, this type of attacker is a nation-state actor who can target the generation or demand-side players in a specific electricity market. To attack the demand side, we executed the first optimization model with the objective function given in Equation 5.22. Figure 5.14 shows the total daily economic damage that the attacker can impose on the demand side players of the studied markets versus the number of compromised high wattage IoT devices. According to this figure, with only 200,000 compromised IoT devices, the attacker can impose 3.5 million USD and 5 million USD daily economic damage

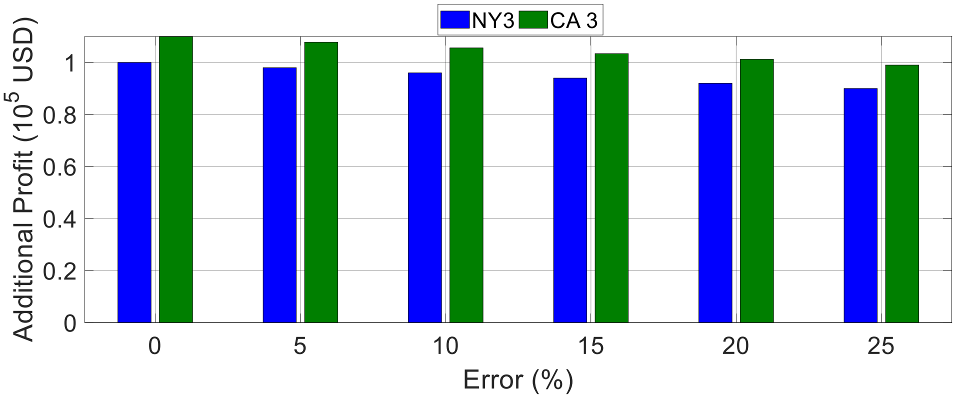


Figure 5.13: Total additional daily profit of the malicious market player versus the estimation error in the day-ahead market price. This plot shows that the effect of the prediction error in the attack is not significant.

to the California and New York markets, respectively. If we simulate the attacker performing the attack 100 days per year, the annual economic damage would be 350 million USD and 500 million USD for the California and New York markets. From the figure, we see the economic damage to the California market is higher than that of the New York market when the size of the botnet is big enough (more than 270,000 compromised devices). Note that the attacker can impose this huge economic damage on the studied markets while his attack is still stealthy.

The nation-state attacker can also target the players in the generation side of the market. To evaluate this attack on the studied markets, we executed the proposed optimization model with the objective function given in Equation 5.23. Figure 5.15 shows the total daily economic damage to the generation companies in each of the studied markets versus the number of compromised IoT devices that the attacker controls. According to this figure, with only 200,000 compromised IoT devices, the attacker can impose 2.8 million USD and 2.9 million USD economic damage to the generation companies in the California and New York ISOs, respectively. Similar to the demand side attack and with the assumption that the attacker will launch MaMIoT attack on the studied markets 100 days per year, the total annual economic damage will be 280 million USD and 290 million USD in the California and New York markets, respectively. The attacker can cause greater damage in the California market than the New York market once the botnet size exceeds 220,000 compromised devices. Even with a small number of compromised IoT bots, the attacker can still cause notable damage to the studied markets. For example, if the botnet includes 10,000 bots (with 3 kW average power consumption for each bot), the annual economic damage to the generation companies will be 1.75 million USD and 2.5 million USD in the California and New York markets, respectively. To achieve this, we assume that the attacker will launch MaMIoT attack 100 days per year. It is worth mentioning that the SO is not able to detect the attack in any of the simulated scenarios as the system load profile is very similar to typical real-time system demand.

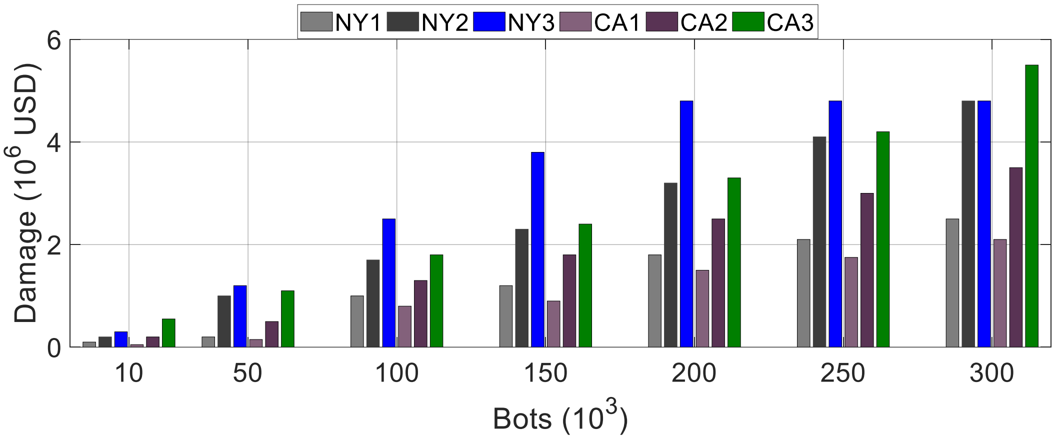


Figure 5.14: Total daily economic damage that the nation state attacker can impose on the demand side of the studied markets versus the number of compromised high wattage IoT devices.

Figure 5.16 depicts the load profile of the studied electricity markets under different levels of MaMIoT attacks on the demand side companies and further illustrates how all of the attack scenarios stay within a normal load forecasting error range. As can be seen in the figure, since the system demand change in the California ISO is much less sensible than the New York ISO, the attack detection in the California market will be a harder process.

The load profile of the California and New York ISOs under different levels of MaMIoT attacks on the generation side companies is represented in Figure 5.17. Similar to the demand side attack, the load profile of different attacks are within the normal load forecasting

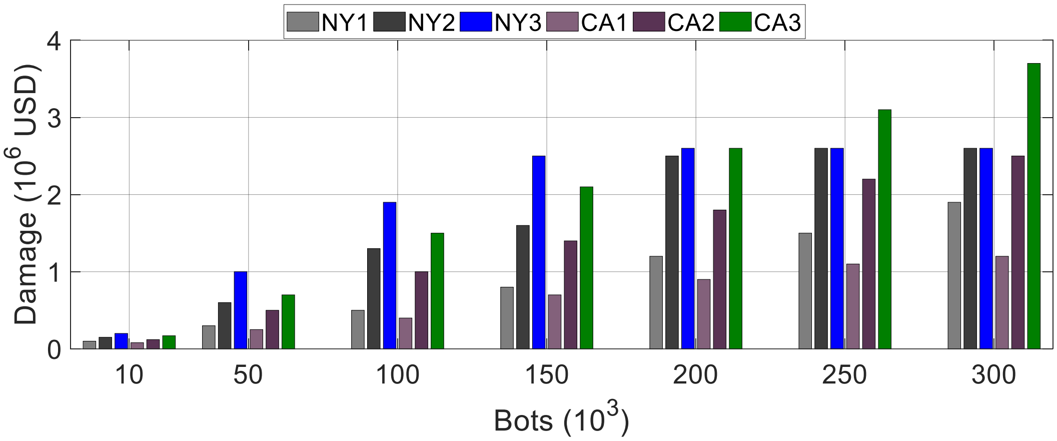
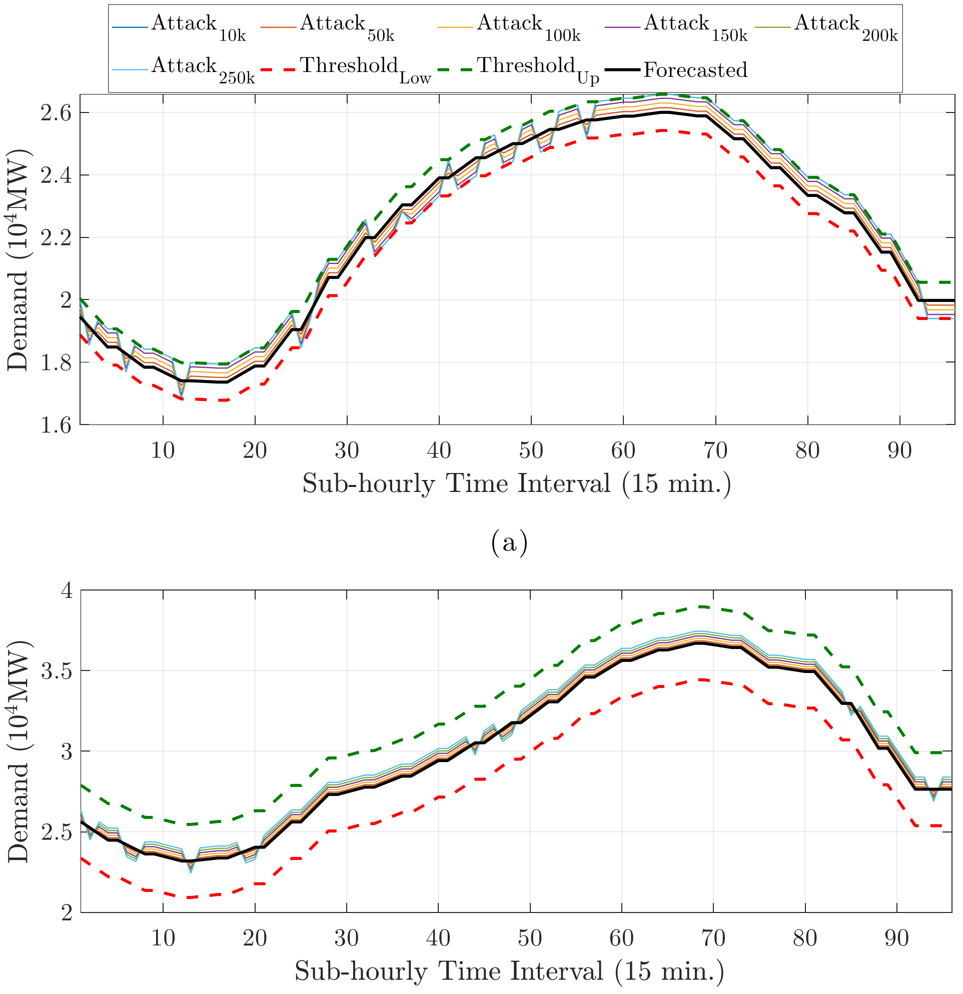


Figure 5.15: Total daily economic damage that the nation state attacker can impose on the generation side of the studied markets versus the number of compromised high wattage IoT devices.

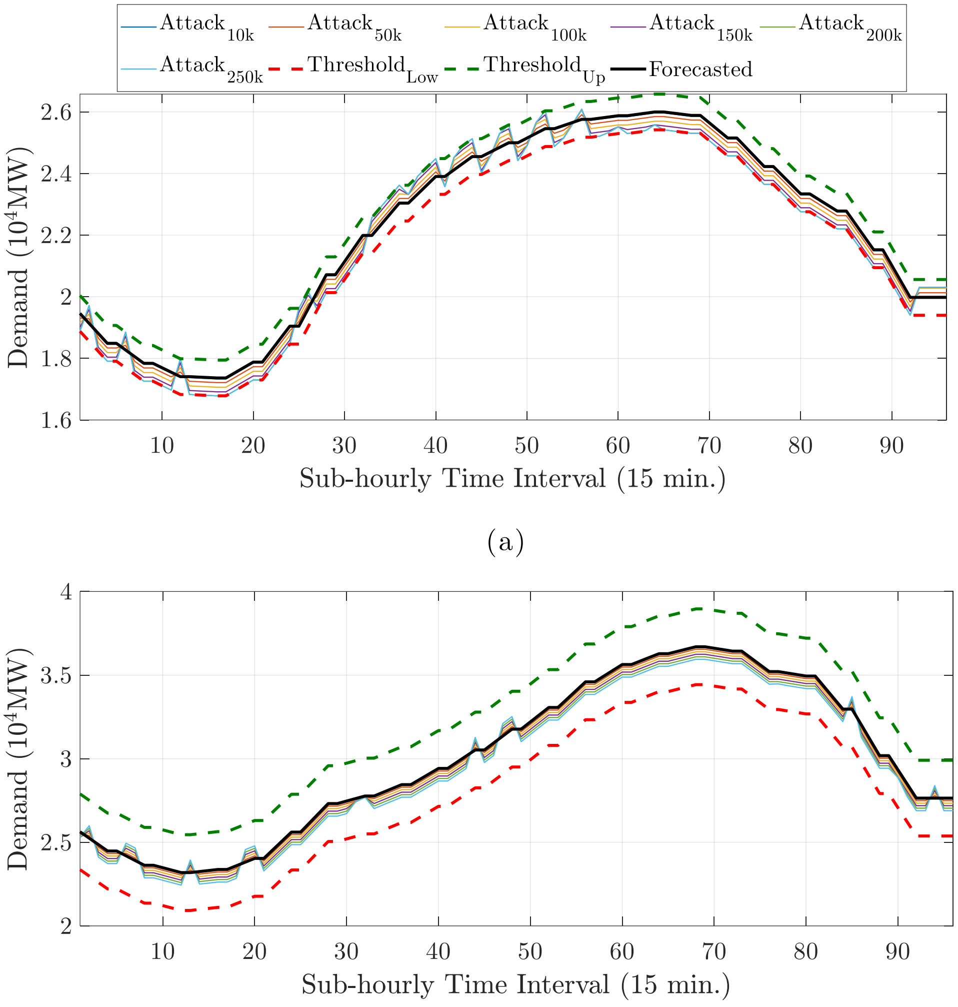
error range. As a general rule, which is true in most of the time intervals, the nation state attacker can harm the demand side companies by increasing the real-time market system demand. On the other hand, decreasing the system real-time demand will lead to economic damage to the generation side companies in the electricity markets.



(a)

(b)

Figure 5.16: Load profile of the power grid at each time interval associated with attacks on the demand side companies with different botnet sizes: a) New York ISO, b) California ISO.



(a)

(b)

Figure 5.17: Load profile of the power grid at each time interval associated with attacks on the generation side companies with different botnet sizes: a) New York ISO, b) California ISO.

Table 5.4: Computation time for solving the developed models with different solvers.

Model	Type	Computation Time of Solvers (sec.)			
		BARON	BONMIN	QOUENNE	DICOPT
subsection 5.5.1	MINLP	30.1	103.7	Infeasible	0.3
Model	**Type**	**BARON**	**CONOPT**	**QOUENNE**	**IPOPT**
subsection 5.5.2-Equation 5.22	NLP	0.2	0.1	0.5	0.1
subsection 5.5.2-Equation 5.23	NLP	0.2	0.1	0.5	0.1

NLP: nonlinear programming model

MINLP: mixed-integer nonlinear programming model

5.6.5 Computational Aspect of the Proposed Method

The computation time required to solve the developed optimization models is an important factor for launching successful attacks in real-world cases. To show the applicability of the proposed mathematical formulations and choose the best approach for solving them, we solved these models with assorted available solvers. The summary of the results is given in Table 5.4. The table shows the best solver for the attacker I models (see subsection 5.5.1) is DICOPT [196] as it has the minimum computation time compared with the other solvers. This small execution time indicates that the proposed model can be solved even with significantly larger models with more detailed modeling approaches. For the attacker II (see subsection 5.5.2), CONOPT [197] and IPOPT [198] solved the proposed models with the same execution time. This shows the practical merit of the developed formulation in real-world cases. All the computations in this chapter were performed on a lap top with Intel Core^{TM} i7-7700HQ @2.80 GHz and 32 GB RAM.

5.7 Countermeasures

While currently there is no single effective countermeasure to prevent the MaMIoT attack, a combination of the following strategies could be employed to reduce its damaging consequences.

Our detailed analysis in section 5.6 illustrates the economic consequence from attacker

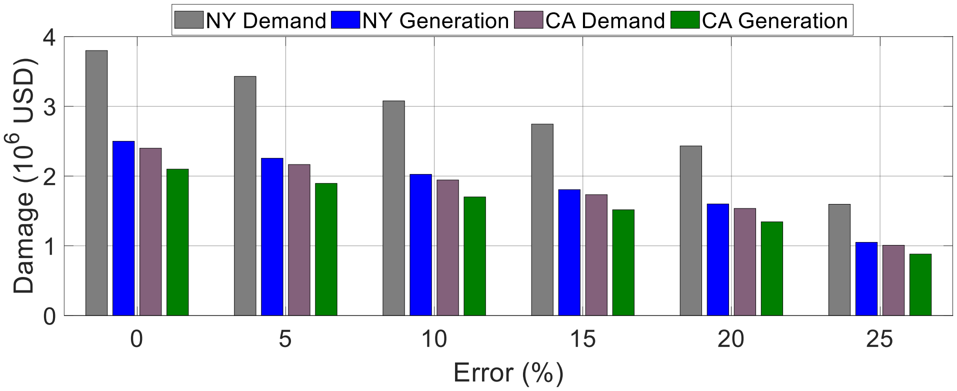


Figure 5.18: Total daily economic damage of the nation state adversary in the simulated markets versus the estimation error in the stealth parameter ($D^{stealthy,\max}$).

II is much more detrimental than attacker I. Attackers in class II are more likely to occur in real-world scenarios because of the reduced concern for negative legal repercussions, such as prosecution. Therefore reducing the effect and possibility of nation-state attackers is the first priority in determining countermeasures. Publicly available historical market data is one of the biggest contributing factors for making the MaMIoT attack possible. To eliminate the risk of nation state attackers, the ISOs should only release detailed market data to market players. This new data privacy plan would add the first barrier for nation state attackers to get access to recent historical market data for estimating price sensitivity and other crucial parameters required to launch a successful stealth attack. Without this information (α_k and $\Delta D_k^{stealthy,\max}$), the economic consequence of an undetectable attack is limited. An intelligent attacker would be forced to launch an overly conservative attack to maintain stealth, causing minimal demand changes.

Figure 5.18 and Figure 5.19 show the daily economic damage of the attacker type II on both simulated markets versus the estimation error in the stealth and price-load sensitivity parameters, respectively. As can be seen, the influence of the attack severely declines following the increase in the estimation error of the key parameters ($\sim$50% influence decline when there is 25% estimation error). These results verify the partial effectiveness of the data privacy countermeasure discussed in the previous paragraph.

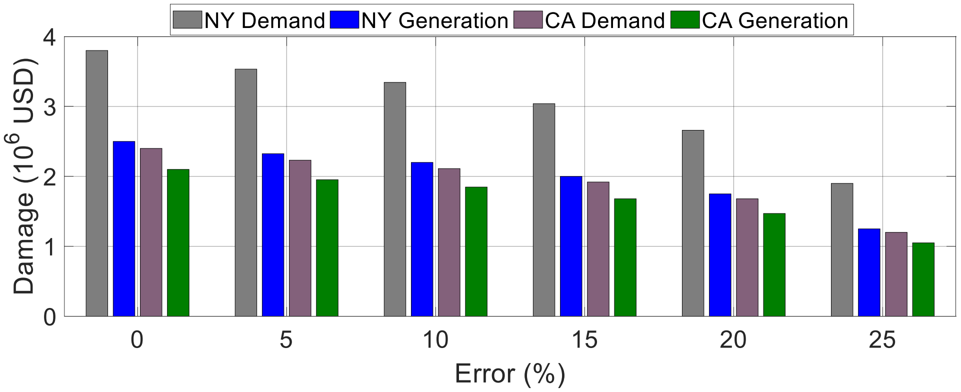


Figure 5.19: Total daily economic damage of the nation state adversary in the simulated markets versus the estimation error in the price-load sensitivity parameter (α).

While tightening access to historical market data will thwart many attackers, it may also prevent researchers and market analysts from performing analyses on these markets. To avoid this, a more practical solution would be releasing redacted or altered versions of the market data or even delaying the release of the full datasets, such that it cannot be used in real-time. This would significantly reduce the effectiveness of the MaMIoT attack by a nation-state actor. This strategy would make it very hard for the attacker to estimate the crucial parameters of the optimization models reliably. As an illustrative example, our analysis shows that releasing the down-sampled (i.e., every 2 hours instead of every 5 minutes) version of the market data with a month delay can decrease the attack economic damage up to 87%.

The most effective and practical countermeasure against MaMIoT attacks is to develop and install non-intrusive load monitoring (NILM) or non-intrusive appliance load monitoring (NIALM) algorithms on the electricity meters of homes in the power grid. NILM and NIALM can be defined as the process of analyzing voltage and current going into a house (through the electricity meters) and deducing what appliances are used at which times in the house as well as their individual energy consumption [199]. These algorithms have been traditionally developed to help the home owners and/or utility companies optimize the energy usage of the home and minimize their monthly electricity bill. It goes without

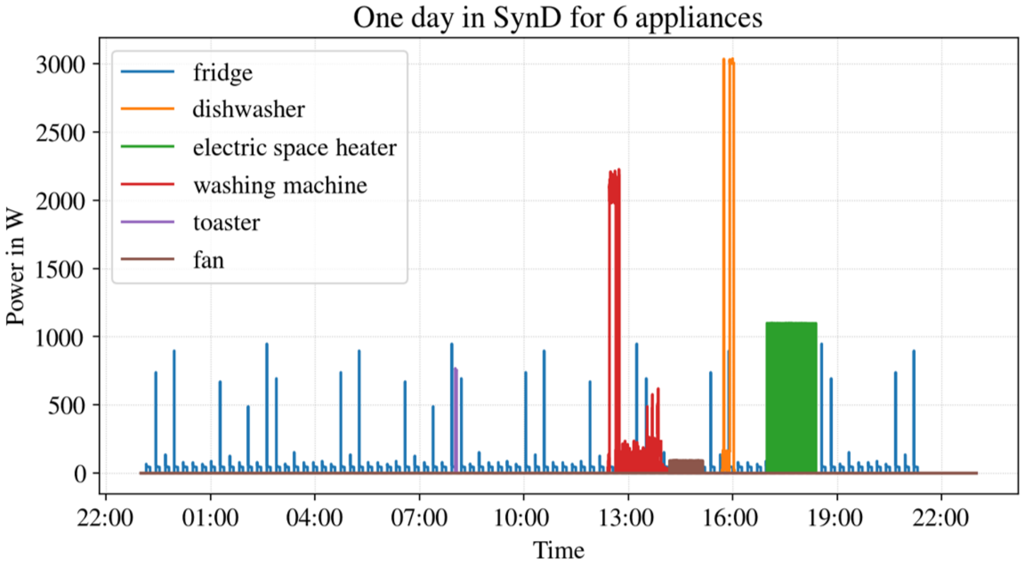


Figure 5.20: A sample data of a residential customer which can be used in the NILM attack detection [200].

saying that NILM is considered a low-cost alternative to attaching individual monitors on each appliance and the concept of high-wattage IoT database explained above. With the recent advancements in the field of machine learning, especially with the introduction of deep learning, reliable NILM algorithms can be developed to quickly detect the MaMIoT attacks and inform the suspicious activities to the home owner and utility companies. For example, the NILM can easily reveal the suspicious use of electric oven in the morning when the home owner is at work and detect it as an anomaly in the meter's data. Of course, further detailed analysis is needed to design and tune reliable and state-of-the-art NILM algorithms to be used in practice. A sample data of a residential customer which can be used in the NILM attack detection is shown in Figure 5.20 [200]. To address the privacy concerns of the customers, the developed machine learning can learn about the energy usage pattern without a specific reference to the used devices in the house. In such cases, the issued alert by the trained model will let the home owner to know there is an authorized use of the devices in the house without point to a specific device.

5.8 Conclusions

In this chapter, we introduced MaMIoT, the first energy market manipulation cyberattack in which an adversary can slightly alter the power system real-time demand through a botnet of high wattage IoT devices to help market players gain additional profit from the electricity market or cause major economic damage to a set of market players. We evaluated the performance of the developed attack models on real datasets from the two biggest electricity markets in the U.S., the California and New York markets. The simulation results revealed that with only 200,000 bots in a botnet, the attacker can cause 2.8 (2.1) million USD and 3.8 (2.2) million USD worth of economic damage to the demand (generation) side players of the California and New York markets, respectively. We also showed that the MaMIoT attack can help a typical power plant owner gain an additional 30% in profit from the energy market, all while maintaining attack stealth for increased repeatability.

We hope that this thesis raises awareness of the significance of MaMIoT attacks to the market operators, ISOs, IoT manufacturers, and system security experts to make the electricity markets more secure against cyberattacks. In the near future, this problem will be even more critical as the number of smart appliances with Internet connectivity continues to grow. In closing, we recommend the following next directions:

- Market operators should reconsider the current online data sharing mechanisms and policies. Access to historical market data can be easily leveraged for malicious purposes.

- Further research is required to develop effective countermeasures for reducing the damaging consequences of MaMIoT attacks on electricity markets. For example, the idea of online database for high wattage IoT devices should be further analyzed in details.

CHAPTER 6
CONCLUSIONS AND FUTURE WORK

In this thesis, we deeply analyzed the effect of three classes of emerging cyberattacks on smart grids and a set of possible defense mechanisms to prevent them or at least reduce their damaging consequences in the grid.

In the first part, we proposed an air-gapped physical signal-based distributed intrusion detection system (i.e., RFDIDS) to protect power substations (as the most critical part of power networks) against advanced types of cyberattacks. Although in the proposed IDS, the SCADA system and even the side channel measurements are considered untrusted entities, it still can provide high level of security to protect substations against advanced types of attacks. In fact, the RF signal is encoded with the quasi-random sequence of lightning strokes around the globe, which acts as a watermark/nonce and this is an effective feature to authenticate the signal. Once the RF signal's integrity is verified, we can estimate the substation measurement and control actions from the magnetic field measurements with high accuracy. This allows us to check the integrity of the SCADA system traffic. The simulation and real-world experimental results revealed the effectiveness of RFDIDS in authenticating the magnetic field signal and estimating the SCADA system measurements and commands with an acceptable level of resiliency and robustness.

Despite the progress made in this part, there are still a set of challenges in the proposed scheme. Our future studies will focus on the following existing issues:

- In the lightning authentication scheme, we used the location and occurrence time of lightning strokes as diagnostic tools. Future studies can include the shape and intensity of sferics in the authentication scheme with machine learning methods in order to increase the security of this approach.

- The proposed effort in this chapter analyzed the utilization of RF receivers placed inside the substation fences. We noticed that some of the circuit current attributes can be detected from the receivers located at distant locations. One possible future study is to investigate and formulate the use of remote LF antennas to monitor the substation activities.

- In this chapter, we assumed that there is one antenna for securing each of the substation circuits. Future studies can focus on finding the optimal number and location of LF receivers to reduce the implementation cost.

- Another existing challenge is the lack of secure wide-area monitoring system for the power grid. Owing to the fact that the current SCADA system is highly unreliable and vulnerable, one can study the use of proposed substation monitoring system to quickly detect and defend against system level attacks (on multiple substations at the same time).

In the second part, we introduced MaDIoT 2.0: a hierarchical two-stage attack mechanism that leverages the potential of high-wattage IoT botnets to attack the power grid and cause a widespread blackout in the entire system. The performance of the developed attack methods is evaluated using extensive simulations and the results showed the superiority of MaDIoT 2.0 over the previously studied attack mechanisms. More specifically, the success rates of the new IoT botnet attack were 91% and 67% for voltage stability Index 1 and Index 2, respectively. In addition, MaDIoT 2.0 requires a smaller number of bots involved in the attacks, since it targets the weakest nodes of the system in the current operating state. Finally, we discussed and showed the effectiveness of proposed countermeasures to mitigate or reduce the damaging consequences of the studied attacks.

We hope that this chapter raises awareness of system operators, ISOs, IoT manufacturers, and system security experts to make the electricity grid more secure against IoT botnet attacks. In the near future, this problem will be even more critical as the number of smart appliances with Internet connectivity continues to grow. In closing, we recommend the following next directions:

- System operators should reconsider the current unnecessary online data sharing mechanisms and policies. As it was shown in the chapter, access to historical and real-time system data can be easily leveraged for malicious purposes.
- Further research is required to develop additional MadIoT attacks and effective protection schemes to help the power grid withstand emerging high-wattage botnet attacks.

In the third part, we introduced MaMIoT, the first energy market manipulation cyberattack in which an adversary can slightly alter the power system real-time demand through a botnet of high wattage IoT devices to help market players gain additional profit from the electricity market or cause major economic damage to a set of market players. We evaluated the performance of the developed attack models on real datasets from the two biggest electricity markets in the U.S., the California and New York markets. The simulation results revealed that with only 200,000 bots in a botnet, the attacker can cause 2.8 (2.1) million USD and 3.8 (2.2) million USD worth of economic damage to the demand (generation) side players of the California and New York markets, respectively. We also showed that the MaMIoT attack can help a typical power plant owner gain an additional 30% in profit from the energy market, all while maintaining attack stealth for increased repeatability.

We hope that this thesis raises awareness of the significance of MaMIoT attacks to the market operators, ISOs, IoT manufacturers, and system security experts to make the electricity markets more secure against cyberattacks. In the near future, this problem will be even more critical as the number of smart appliances with Internet connectivity continues to grow. In closing, we recommend the following next directions:

- Market operators should reconsider the current online data sharing mechanisms and policies. Access to historical market data can be easily leveraged for malicious purposes.

- Further research is required to develop effective countermeasures for reducing the damaging consequences of MaMIoT attacks on electricity markets. For example, the idea of online database for high wattage IoT devices should be further analyzed in details.

REFERENCES

[1] Marshall Brain, William Harris, and Robert Lamb. “How electricity works”. In: *How Stuff Works, Inc.* (2014).

[2] Meg Jacobs. *Panic at the pump: the energy crisis and the transformation of American politics in the 1970s*. Macmillan, 2016.

[3] Mathew J Morey, Laurence D Kirsch, et al. “Retail choice in electricity: What have we learned in 20 years”. In: *Electric Markets Research Foundation* (2016).

[4] Gerald Brown et al. “Defending critical infrastructure”. In: *Interfaces* 36.6 (2006), pp. 530–544.

[5] Saleh Soltan, Prateek Mittal, and H Vincent Poor. “BlackIoT: IoT botnet of high wattage devices can disrupt the power grid”. In: *27th USENIX Security Symp.* 2018, pp. 15–32.

[6] Bing Huang, Alvaro A Cardenas, and Ross Baldick. “Not everything is dark and gloomy: Power grid protections against IoT demand attacks”. In: *28th USENIX Security Symp.* 2019, pp. 1115–1132.

[7] C Unal, K Werley, and P Giguere. “Energy interdependence modeling and simulation”. In: *Tech. Rep. LAUR-01-1879*. Los Alamos National Laboratory, 2001.

[8] Steven M Rinaldi, James P Peerenboom, and Terrence K Kelly. “Identifying, understanding, and analyzing critical infrastructure interdependencies”. In: *IEEE Control Systems* 21.6 (2001), pp. 11–25.

[9] Tonya Riley. *The Cybersecurity 202: Securing the electric grid should be priority for Biden’s first 100 days, expert says*. Dec. 2020.

[10] Jose Monteagudo. *Power Grid Cybersecurity – where are we now?* Dec. 2020.

[11] Klaus-Peter Brand, Volker Lohmann, and Wolfgang Wimmer. *Substation automation handbook*. Utility Automation Consulting Lohmann Bremgarten, Switzerland, 2003.

[12] Manos Antonakakis et al. “Understanding the Mirai botnet”. In: *26th USENIX Security Symp.* 2017, pp. 1093–1110.

[13] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. “Security analysis of emerging smart home applications”. In: *IEEE Symp. on Security and Privacy (IEEE S&P)*. 2016, pp. 636–654.

[14] Muhammad Naveed et al. “Inside Job: Understanding and Mitigating the Threat of External Device Mis-Binding on Android”. In: *Network and Distributed System Security (NDSS) Symp.* 2014, pp. 1–14.

[15] Omar Alrawi et al. “SoK: Security Evaluation of Home-Based IoT Deployments”. In: *IEEE Symp. on Security and Privacy (IEEE S&P)*. 2019, pp. 1–19.

[16] Tamara Denning, Tadayoshi Kohno, and Henry M Levy. “Computer security and the modern home”. In: *Commun. of the ACM* 56.1 (2013), pp. 94–103.

[17] Eyal Ronen et al. “IoT goes nuclear: Creating a ZigBee chain reaction”. In: *IEEE Symp. on Security and Privacy (IEEE S&P)*. 2017, pp. 195–212.

[18] Tamara Denning, Tadayoshi Kohno, and Henry M Levy. “Computer security and the modern home”. In: *Commun. of the ACM* 56.1 (2013), pp. 94–103.

[19] Pardis Emami Naeini et al. “Privacy expectations and preferences in an IoT world”. In: *Symp. on Usable Privacy and Security*. 2017, pp. 399–412.

[20] Arsalan Mosenia and Niraj K Jha. “A comprehensive study of security of Internet of Things”. In: *IEEE Trans. Emerg. Topics in Comput.* 5.4 (2017), pp. 586–602.

[21] Anna Kornfeld Simpson, Franziska Roesner, and Tadayoshi Kohno. “Securing vulnerable home IoT devices with an in-hub security manager”. In: *IEEE Int. Conf. on Pervasive Comput. and Commun. Workshops (PerCom Workshops)*. 2017, pp. 551–556.

[22] Milijana Surbatovich et al. “Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of IFTTT recipes”. In: *Proc. of the 26th Int. Conf. on World Wide Web*. 2017, pp. 1501–1510.

[23] Tianlong Yu et al. “Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet of Things”. In: *Proc. of the 14th ACM Workshop on Hot Topics in Networks*. 2015, pp. 1–7.

[24] Dennis Fisher. *Pair of Bugs Open Honeywell Home Controllers Up to Easy Hacks*. Ed. by Threat Post.

[25] Grant Hernandez et al. “Smart nest thermostat: A smart spy in your home”. In: *Black Hat USA* (2014), pp. 1–8.

[26] Sergio Pastrana, Jorge Rodriguez-Canseco, and Alejandro Calleja. “ArduWorm: A functional malware targeting Arduino devices”. In: *COSEC Computer Security Lab* (2016).

[27] Guoming Zhang et al. “Dolphinattack: Inaudible voice commands”. In: *Proc. of the ACM SIGSAC Conf. on Computer and Commun. Security (CCS)*. 2017, pp. 103–117.

[28] Eyal Ronen et al. “IoT goes nuclear: Creating a ZigBee chain reaction”. In: *IEEE Symp. on Security and Privacy (IEEE S&P)*. 2017, pp. 195–212.

[29] Yao Liu, Peng Ning, and Michael K Reiter. “False data injection attacks against state estimation in electric power grids”. In: *ACM Trans. Inform. and Syst. Security* 14.1 (2011), pp. 1–33.

[30] Gaoqi Liang et al. “The 2015 Ukraine blackout: Implications for false data injection attacks”. In: *IEEE Trans. Power Syst.* 32.4 (2017), pp. 3317–3318.

[31] Arman Sargolzaei, Kang K Yen, and Mohamed N Abdelghani. “Preventing time-delay switch attack on load frequency control in distributed power systems”. In: *IEEE Trans. Smart Grid* 7.2 (2016), pp. 1176–1185.

[32] Kim Zetter. *Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid*. July 2018. (Visited on 07/2018).

[33] Katherine R Davis et al. “A cyber-physical modeling and assessment framework for power grid infrastructures”. In: *IEEE Trans. Smart Grid* 6.5 (2015), pp. 2464–2475.

[34] Sriharsha Etigowni et al. “CPAC: securing critical infrastructure with cyber-physical access control”. In: *Proc. 32nd Annu. Conf. Comput. Security Appl.* 2016, pp. 139–152.

[35] David Formby et al. “Who’s in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems.” In: *Proc. Network & Distributed Syst. Security (NDSS) Symp.* 2016, pp. 1–15.

[36] Dayna A Byrne and Jeffrey J Holm. *Shared embedded trace macrocell*.

[37] Stephen McLaughlin and Patrick McDaniel. “SABOT: specification-based payload generation for programmable logic controllers”. In: *Proc. 2012 ACM conf. Comput. and commun. security*. 2012, pp. 439–449.

[38] Jason Reeves et al. “Intrusion detection for resource-constrained embedded control systems in the power grid”. In: *Int. J. of Critical Infrastructure Protection* 5.2 (2012), pp. 74–83.

[39] John Mulder et al. “WeaselBoard: zero-day exploit detection for programmable logic controllers”. In: *Sandia Nat. Lab. Rep. # SAND2013-8274* (2013).

[40] Yi Yang et al. “Multiattribute SCADA-specific intrusion detection system for power networks”. In: *IEEE Trans. Power Del.* 29.3 (2014), pp. 1092–1102.

[41] Yichi Zhang et al. “Distributed intrusion detection system in a multi-layer network architecture of smart grids”. In: *IEEE Trans. Smart Grid* 2.4 (2011), pp. 796–808.

[42] Hussain Almakrami. “Intrusion detection system for smart meters”. In: *IEEE Saudi Arabia Smart Grid (SASG)*. 2016, pp. 1–8.

[43] Jorge Valenzuela, Jianhui Wang, and Nancy Bissinger. “Real-time intrusion detection in power system operations”. In: *IEEE Trans. Power Syst.* 28.2 (2013), pp. 1052–1062.

[44] Mahdi Jamei et al. “Anomaly Detection Using Optimally-Placed μPMU Sensors in Distribution Grids”. In: *IEEE Trans. Power Syst.* pp.pp (2017), pp. 1–12.

[45] Shengyi Pan, Thomas Morris, and Uttam Adhikari. “Developing a hybrid intrusion detection system using data mining for power systems”. In: *IEEE Trans. Smart Grid* 6.6 (2015), pp. 3104–3113.

[46] Yang Chen, Le Xie, and PR Kumar. “Dimensionality reduction and early event detection using online synchrophasor data”. In: *IEEE Power & Energy (PES) Soc. General Meeting*. 2013, pp. 1–5.

[47] Le Xie, Yang Chen, and P Roshan Kumar. “Dimensionality reduction of synchrophasor data for early event detection: Linearized analysis”. In: *IEEE Trans. Power Syst.* 29.6 (2014), pp. 2784–2794.

[48] Jorge Valenzuela, Jianhui Wang, and Nancy Bissinger. “Real-time intrusion detection in power system operations”. In: *IEEE Trans. Power Syst.* 28.2 (2013), pp. 1052–1062.

[49] Yinyin Ge et al. “Power system real-time event detection and associated data archival reduction based on synchrophasors”. In: *IEEE Trans. Smart Grid* 6.4 (2015), pp. 2088–2097.

[50] Alicia Allen et al. *PMU data event detection: A user guide for power engineers*. Tech. rep. Nat. Renewable Energy Lab. (NREL), 2014.

[51] Milan Biswal, Sukumar M Brahma, and Huiping Cao. “Supervisory protection and automated event diagnosis using PMU data”. In: *IEEE Trans. Power Del.* 31.4 (2016), pp. 1855–1863.

[52] Mahdi Jamei et al. “Micro synchrophasor-based intrusion detection in automated distribution systems: Toward critical infrastructure security”. In: *IEEE Internet Computing* 20.5 (2016), pp. 18–27.

[53] S Brahma et al. “Real-time identification of dynamic events in power systems using PMU data, and potential applications—Models, promises, and challenges”. In: *IEEE Trans. Power Del.* 32.1 (2017), pp. 294–301.

[54] *What is Snort?* July 2018. (Visited on 07/2018).

[55] Z. Li, M. Shahidehpour, and F. Aminifar. “Cybersecurity in Distributed Power Systems”. In: *Proc. of the IEEE* 105.7 (2017), pp. 1367–1388.

[56] Christopher Wang et al. “An algorithm for finding carriers of amplitude-modulated electromagnetic emanations in computer systems”. In: *IEEE 10th European Conf. on Antennas and Propag. (EuCAP)*. 2016, pp. 1–5.

[57] Milos Prvulovic et al. “A Method for Finding Frequency-Modulated and Amplitude-Modulated Electromagnetic Emanations in Computer Systems”. In: *IEEE Trans. Electromagn. Compat.* 59.1 (2017), pp. 34–42.

[58] Christian Bayens et al. “See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Patterns Detection in Additive Manufacturing”. In: *Proc. of the 26th USENIX Security Symp.* (2017), pp. 1–18.

[59] Yi Han et al. “Watch Me, but Don’t Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations”. In: *ACM Conf. on Computer and Communications Security (CCS)*. 2017, pp. 1095–1108.

[60] Alireza Nazari et al. “Eddie: Em-based detection of deviations in program execution”. In: *ACM/IEEE 44th Annu. Int. Symp. Computer Architecture (ISCA)*. 2017, pp. 333–346.

[61] C. Cheng, S. Kim, and A. Zajic. “Comparison of path loss models for indoor 30 GHz, 140 GHz, and 300 GHz channels”. In: *11th European Conf. Antennas and Propag. (EUCAP)*. Mar. 2017, pp. 716–720.

[62] -. *DDOS Attacks against Global Markets*. Ed. by PLXsert. 2019.

[63] Office of Enforcement Federal Energy Regulatory Commission Washington, D.C. *2018 Report on Enforcement*. Ed. by FERC. 2019.

[64] Siddharth Sridhar. “Cyber risk modeling and attack-resilient control for power grid”. In: *Ph.D. dissertation, Dept. Elect. Comput. Eng., Iowa State Univ., Ames, IA, USA* (2015).

[65] Kianoosh G Boroojeni, M Hadi Amini, and Sundararaja S Iyengar. *Smart grids: security and privacy issues*. Springer, 2017.

[66] Arman Sargolzaei et al. “Security challenges of networked control systems”. In: *Sustainable interdependent networks*. Springer, 2018, pp. 77–95.

[67] Amin Gholami et al. “Toward a consensus on the definition and taxonomy of power system resilience”. In: *IEEE Access* 6 (2018), pp. 32035–32053.

[68] Junsoo Kim et al. “Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors”. In: *IEEE Trans. Autom. Control* 64.3 (2019), pp. 1162–1169.

[69] Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo. “Attack detection and identification in cyber-physical systems”. In: *IEEE Trans. Autom. Control* 58.11 (2013), pp. 2715–2729.

[70] Hamza Fawzi, Paulo Tabuada, and Suhas Diggavi. “Secure estimation and control for cyber-physical systems under adversarial attacks”. In: *IEEE Trans. Autom. control* 59.6 (2014), pp. 1454–1467.

[71] Chanhwa Lee, Hyungbo Shim, and Yongsoon Eun. “Secure and robust state estimation under sensor attacks, measurement noises, and process disturbances: Observer-based combinatorial approach”. In: *European Control Conf. (ECC)*. 2015, pp. 1872–1877.

[72] Yasser Shoukry et al. “Secure state reconstruction in differentially flat systems under sensor attacks using satisfiability modulo theory solving”. In: *54th IEEE Conf. on Decision and Control (CDC)*. 2015, pp. 3804–3809.

[73] Jeanne Meserve. *Mouse click could plunge city into darkness, experts say*. Ed. by CNN.com.

[74] Department of Homeland Security, ed. *FOIA response documents*.

[75] Mark Zeller. “Myth or reality – Does the Aurora vulnerability pose a risk to my generator?” In: *64th Ann. Conf. for Protective Relay Engineers*. 2011, pp. 130–136.

[76] Symantec, ed. *Dragonfly: Western energy sector targeted by sophisticated attack group*.

[77] John Kennedy. *https://www.siliconrepublic.com/enterprise/dragonfly-us-russia-energy-grid-hackers*. Ed. by Silicon Public.

[78] Robert M Lee, Michael J Assante, and Tim Conway. "ICS Defense Use Case: Analysis of the cyber attack on the Ukrainian power grid". In: *Electricity Information Sharing and Analysis Center, SANS ICS* (2016).

[79] Luis Garcia and Saman A Zonouz. "Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit." In: *Network and Distributed System Security (NDSS) Symp.* 2017, pp. 1–15.

[80] Amir-Hamed Mohsenian-Rad and Alberto Leon-Garcia. "Distributed internet-based load altering attacks against smart power grids". In: *IEEE Trans. Smart Grid* 2.4 (2011), pp. 667–674.

[81] Zhang Xu et al. "Power Attack: An Increasing Threat to Data Centers". In: *Network and Distributed System Security (NDSS) Symp.* 2014, pp. 1–15.

[82] Sajjad Amini, Fabio Pasqualetti, and Hamed Mohsenian-Rad. "Dynamic load altering attacks against power system stability: Attack models and protection schemes". In: *IEEE Trans. Smart Grid* 9.4 (2016), pp. 2862–2872.

[83] Yury Dvorkin and Siddharth Garg. "IoT-enabled distributed cyber-attacks on transmission and distribution grids". In: *North American Power Symp. (NAPS)*. 2017, pp. 1–6.

[84] Adrian Dabrowski, Johanna Ullrich, and Edgar R Weippl. "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well". In: *Proc. of the 33rd Ann. Computer Security Applications Conf. (ACSAC)*. 2017, pp. 303–314.

[85] Paul M Anderson. *Power system protection*. Wiley, 1998.

[86] Tohid Shekari, Farrokh Aminifar, and Majid Sanaye-Pasand. "An analytical adaptive load shedding scheme against severe combinational disturbances". In: *IEEE Trans. Power Syst.* 31.5 (2015), pp. 4135–4143.

[87] Mircea Eremia and Mohammad Shahidehpour. *Handbook of electrical power system dynamics: modeling, stability, and control*. Vol. 92. John Wiley & Sons, 2013.

[88] Allen J Wood and Bruce F Wollenberg. *Power generation, operation, and control*. John Wiley & Sons, 2012.

[89] J Duncan Glover, Mulukutla S Sarma, and Thomas Overbye. *Power System Analysis & Design*. Cengage Learning, 2012.

[90] J.T. Langill. "Defending Against the Dragonfly Cyber Security Attacks". In: *Belden, White Paper* (2014), pp. 1–33.

[91] Sophie Tatum. *US accuses Russia of cyberattacks on power grid*. March 2018. (Visited on 08/2017).

[92] *US power grid needs defense against looming cyber attacks*. March 2018. (Visited on 08/2017).

[93] Courtney Kube. *Dem, GOP senators join to ask Trump to get tough on Russia cyber threat*. July 2018. (Visited on 07/2018).

[94] Tiff B. Armstrong et al. "Transmission & Distribution Infrastructure". In: *A Harris Williams & Co. White Paper* (2010), pp. 1–14.

[95] Stan Mark Kaplan. "Electric power transmission: background and policy issues". In: *US Congressional Research Service* 14 (2009), pp. 4–5.

[96] Julia E Sullivan and Dmitriy Kamensky. "How cyber-attacks in Ukraine show the vulnerability of the US power grid". In: *The Electricity J.* 30.3 (2017), pp. 30–35.

[97] Vulnerability# ICS-VU-255987. Advisory (ICSA-17-089-02). *Schneider Electric Modicon M221, M241, and M251 Programmable Logic Controllers (PLCs) TCP Predictability Vulnerability, Insufficiently Random/Shared Session Numbers Vulnerability, and Insufficiently Protected Credentials Vulnerability*. March 2017. (Visited on 08/2017).

[98] Vulnerability# ICS-VU-794684. Advisory (ICSA-16-070-01). *Schneider Electric Telvent RTU Improper Ethernet Frame Padding Vulnerability*. March 2016. (Visited on 08/2017).

[99] Vulnerability# ICS-VU-130124. Advisory (ICSA-15-300-01). *Siemens RuggedCom Improper Ethernet Frame Padding Vulnerability*. October 2015. (Visited on 08/2017).

[100] Vulnerability# ICS-VU-435619. Advisory (ICSA-15-006-01). *Eaton's Cooper Power Series Form 6 Control and Idea/IdeaPLUS Relays with Ethernet Vulnerability*. July 2015. (Visited on 08/2017).

[101] Vulnerability# ICS-VU-532813. Advisory (ICSA-15-169-01). *Wind River VxWorks TCP Predictability Vulnerability in ICS Devices. Vendor: Wind River (vendors affected - Schneider Electric)*. June 2015. (Visited on 08/2017).

[102] Alfred A Ghirardi. *Radio Physics Course*. Radio Technical Publishing Company, 1932.

[103] Morris B Cohen, Umran S Inan, and Evans W Paschal. "Sensitive broadband ELF/VLF radio reception with the AWESOME instrument". In: *IEEE Trans. Geosci. Remote Sens.* 48.1 (2010), pp. 3–17.

[104] Morris Bernard Cohen. “ELF/VLF Phased Array Generation via Frequency-Matched Steering of a Continuous HF Ionospheric Heating Beam”. PhD thesis. Stanford University, 2009.

[105] *National Lightning Detection Network (NLDN)*. July 2018. (Visited on 07/2018).

[106] Morris B Cohen, RK Said, and US Inan. “Mitigation of 50–60 Hz power line interference in geophysical data”. In: *Radio Science* 45.6 (2010).

[107] Tilo Strutz. *Data fitting and uncertainty: A practical introduction to weighted least squares and beyond*. Vieweg and Teubner, 2010.

[108] *Choptank Electric Cooperative*. August 2018. (Visited on 08/2018).

[109] *Georgia Power*. August 2018. (Visited on 08/2018).

[110] Grazia Barchi et al. “Performance of synchrophasor estimators in transient conditions: A comparative analysis”. In: *IEEE Trans. Instrum. Meas.* 62.9 (2013), pp. 2410–2418.

[111] Grazia Barchi, David Macii, and Dario Petri. “Synchrophasor estimators accuracy: A comparative analysis”. In: *IEEE Trans. Instrum. Meas.* 62.5 (2013), pp. 963–973.

[112] Richard A Serrano and Evan Halper. “Sophisticated but low-tech power grid attack baffles authorities”. In: *Los Angeles Times* 11 (2014).

[113] Arthur R. Bergen and Vijay Vittal. *Power system analysis*. Upper Saddle River, NJ: Prentice-Hall, 2000.

[114] P.M. Anderson. *Power System Protection*. IEEE Press power engineering series. McGraw-Hill, 1999.

[115] Tohid Shekari, Farrokh Aminifar, and Majid Sanaye-Pasand. “An analytical adaptive load shedding scheme against severe combinational disturbances”. In: *IEEE Trans. Power Syst.* 31.5 (2016), pp. 4135–4143.

[116] Wikipedia, ed. *Bloomberg Terminal*.

[117] New York Independent System Operator. *Load Data*. Ed. by New York Independent System Operator.

[118] California Independent System Operator. *Reliability Requirements*. Ed. by California Independent System Operator.

[119] Pennsylvania and New Jersey Independent System Operator. *Energy Market*. Ed. by Pennsylvania and New Jersey Independent System Operator.

[120] T. Shekari et al. "An Adaptive Wide-Area Load Shedding Scheme Incorporating Power System Real-Time Limitations". In: *IEEE Syst. J.* 12.1 (Mar. 2018), pp. 759–767.

[121] Manos Antonakakis et al. "Understanding the Mirai botnet". In: *26th USENIX Security Symp.* 2017, pp. 1093–1110.

[122] Sam Edwards and Ioannis Profetis. "Hajime: Analysis of a decentralized internet worm for IoT devices". In: *Rapidity Networks* 16 (2016).

[123] Paganini Pierluigi. *LuaBot is the first Linux DDoS botnet written in Lua Language*. Ed. by Security Affairs.

[124] Goodin Dan. *BrickerBot, the permanent denial-of-service botnet, is back with a vengeance*. Ed. by Arts Technica.

[125] Lily Hey Newman. *The Web-Shaking Mirai Botnet Is Splintering—But Also Evolving*. Ed. by Wired. 2016.

[126] Hao Jiang, Yaoqing Liu, and Jeanna N Matthews. "IP geolocation estimation using neural networks with stable landmarks". In: *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE. 2016, pp. 170–175.

[127] *IP Geolocation Accuracy: How Reliable Is the Technology?*

[128] Catalin Cimpanu. *You Can Now Rent a Mirai Botnet of 400,000 Bots*. 2016.

[129] Dan Goodin. *New IoT botnet offers DDoSes of once-unimaginable sizes for $20*. 2018.

[130] Rommel Joven and Evgeny Ananin. *DDoS-for-Hire Service Powered by Bushido Botnet*. 2018.

[131] Dan Goodin. *100,000-strong botnet built on router 0-day could strike at any time*. December 2017.

[132] Security Boulevard. *Here's how anyone with $20 can hire an IoT botnet to blast out a week-long DDoS attack*. 2018.

[133] imperva. *Booters, Stressers and DDoSers*. 2019.

[134] Electricity Consumers Resource Council (ELCON). *The Economic Impacts of the August 2003 Blackout*.

[135] US Energy Information Administration. *2018 Average Monthly Bill- Residential*. Ed. by US Energy Information Administration. 2020.

[136] Tohid Shekari et al. “RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid.” In: *Network and Distributed System Security (NDSS) Symp.* 2019, pp. 1–15.

[137] Gerhard Ziegler. *Numerical distance protection: principles and applications*. John Wiley & Sons, 2011.

[138] Fenghai Sui et al. “A method to assess GIC impact on zero sequence overcurrent protection of transmission lines”. In: *IEEE Power & Energy Society General Meet.* 2013, pp. 1–5.

[139] M Begovic et al. “Summary of” System protection and voltage stability””. In: *IEEE Trans. Power Del.* 10.2 (1995), pp. 631–638.

[140] Zhiming Song et al. “Review on over-frequency generator tripping for frequency stability control”. In: *IEEE PES Asia-Pacific Power and Energy Engineering Conf. (APPEEC)*. 2016, pp. 2240–2243.

[141] Armando Guzman et al. “A current-based solution for transformer differential protection. I. Problem statement”. In: *IEEE Trans. Power Del.* 16.4 (2001), pp. 485–491.

[142] Sanjay Dambhare, SA Soman, and MC Chandorkar. “Adaptive current differential protection schemes for transmission-line protection”. In: *IEEE Trans. Power Del.* 24.4 (2009), pp. 1832–1841.

[143] Demetrios A Tziouvaras and Daqing Hou. “Out-of-step protection fundamentals and advancements”. In: *57th Ann. Conf. for Protective Relay Engineers*. 2004, pp. 282–307.

[144] John Berdy. “Loss of excitation protection for modern synchronous generators”. In: *IEEE Trans. Power Apparatus and Syst.* 94.5 (1975), pp. 1457–1463.

[145] John Wilson. *Phishing Attacks: Why Energy Companies and Utilities Are Getting Zapped*. Ed. by Agari.

[146] Anastasis Keliris et al. “Open source intelligence for energy sector cyberattacks”. In: *Critical Infrastructure Security and Resilience*. Springer, 2019, pp. 261–281.

[147] Google, ed. *Google Maps*. 2020.

[148] C Arderne et al. "Predictive mapping of the global power system using open data". In: *Scientific data* 7.1 (2020), pp. 1–12.

[149] Heetae Kim et al. "In-depth data on the network structure and hourly activity of the Central Chilean power grid". In: *Scientific data* 5.1 (2018), pp. 1–10.

[150] Wided Medjroubi et al. "Open data in power grid modelling: new approaches towards transparent grid models". In: *Energy Reports* 3 (2017), pp. 14–21.

[151] Junjie Tang et al. "Adaptive load shedding based on combined frequency and voltage stability assessment using synchrophasor measurements". In: *IEEE Trans. Power Syst.* 28.2 (2013), pp. 2035–2047.

[152] Baofu Gao, GK Morison, and Prabhashankar Kundur. "Voltage stability evaluation using modal analysis". In: *IEEE trans. Power Syst.* 7.4 (1992), pp. 1529–1542.

[153] Prabha Kundur, Neal J Balu, and Mark G Lauby. *Power system stability and control*. Vol. 7. McGraw-hill New York, 1994.

[154] , ed. *DIgSILENT PowerFactory*. 2020.

[155] University of Illinois at Urbana-Champaign, ed. *IEEE 39-Bus System*. 2020.

[156] Fitiwi Desta Zahlay and KS Rama Rao. "Neuro-Prony and Taguchi's methodology-based adaptive autoreclosure scheme for electric transmission systems". In: *IEEE Trans. Power Del.* 27.2 (2012), pp. 575–582.

[157] Moein Abedini, Majid Sanaye-Pasand, and Sadegh Azizi. "Adaptive load shedding scheme to preserve the power system stability following large disturbances". In: *IET Gen., Transm. & Dist.* 8.12 (2014), pp. 2124–2133.

[158] Yan Sun and Thomas J Overbye. "Visualizations for power system contingency analysis data". In: *IEEE Trans. Power Syst.* 19.4 (2004), pp. 1859–1866.

[159] Mohammad Shahidehpour, Hatim Yamin, and Zuyi Li. *Market operations in electric power systems: forecasting, scheduling, and risk management*. John Wiley & Sons, 2003.

[160] US Energy Information Administration. *Wholesale electricity prices were generally lower in 2019, except in Texas*. Ed. by US Energy Information Administration. 2019.

[161] US Energy Information Administration. *U.S. energy facts explained*. Ed. by US Energy Information Administration. 2019.

[162] Carter Yagemann et al. “On the Feasibility of Automating Stock Market Manipulation”. In: *Annual Computer Security Applications Conference*. 2020, pp. 277–290.

[163] Bethany McLean and Peter Elkind. *The smartest guys in the room: The amazing rise and scandalous fall of Enron*. Penguin, 2013.

[164] Maureen Farrell. *JPMorgan settles electricity manipulation case for $410 million*. July 2013. (Visited on 07/2020).

[165] Scott DiSavino. *JPMorgan to pay $410 million to settle power market case*. July 2013. (Visited on 07/2020).

[166] Troutman Pepper. *FERC Approves $105 Million Settlement with Barclays for Market Manipulation*. November 2017. (Visited on 07/2020).

[167] Paul J Burke and Ashani Abayasekara. “The price elasticity of electricity demand in the United States: A three-dimensional analysis”. In: *The Energy Journal* 39.2 (2018).

[168] Kankar Bhattacharya, Math HJ Bollen, and Jaap E Daalder. *Operation of restructured power systems*. Springer Science & Business Media, 2012.

[169] Daniel Sadi Kirschen and Goran Strbac. *Fundamentals of power system economics*. Vol. 1. Wiley Online Library, 2004.

[170] Stylianos I Vagropoulos and Anastasios G Bakirtzis. “Optimal bidding strategy for electric vehicle aggregators in electricity markets”. In: *IEEE Trans. Power Syst.* 28.4 (2013), pp. 4031–4041.

[171] T Mulligan. “How Enron Manipulated State’s Power Market”. In: *Los Angeles Times* (2002).

[172] Timothy Egan. “Tapes show Enron arranged plant shutdown”. In: *New York Times* (2005).

[173] New York Independent System Operator. *Energy Market & Operation Data*. Ed. by New York Independent System Operator. 2019.

[174] California Independent System Operator. *Energy Market & Operation Data*. Ed. by California Independent System Operator. 2019.

[175] -. *Bloomberg Terminal*. Ed. by Bloomberg Terminal. 2019.

[176] Radware. *A Quick History of IoT Botnets*. 2018.

[177] General Electric, ed. *GE Wi-Fi connect appliances*.

[178] Statistica. *Number of homes with smart thermostats in North America from 2014 to 2020 (in millions)*. Ed. by Statistica.

[179] KrebsonSecurity. *Did the Mirai Botnet Really Take Liberia Offline?*

[180] Dan Goodin. *Assessing the threat the Reaper botnet poses to the Internet—what we know now*. 2017.

[181] Christian Vasquez. *'Major vulnerability': EV hacks could threaten power grid*. June 2020. (Visited on 07/2018).

[182] Energy Efficiency and Renewable Energy Clearinghouse. *Energy Use of Some Typical Home Appliances*. 2020.

[183] Jessica Lietz. *How Much Does the Hot Water Heater Affect an Electric Bill?* 2018.

[184] HVAC Talk. *How many hours should the AC run during the hottest days of the year?* 2019.

[185] Martin Holladay. *Garage Door Openers Are Always On*. 2013.

[186] Payless Power. *How Many Watts Does a Refrigerator Use*. 2019.

[187] We Energies. *Appliance savings with Time-of-Use*. 2020.

[188] Union of Concerned Scientists. *Electric Vehicle Charging Types, Time, Cost and Savings*. 2018.

[189] Craig Lloyds. *How Much Electricity Do All Your Appliances Use?* 2018.

[190] Laundry Butler for You. *How Much Laundry Does the Average Person Do?* 2019.

[191] Whirlpool. *How long do dishwashers run?* 2020.

[192] Buyexerciser. *Treadmill workout tips: How long should I run on the treadmill?* 2020.

[193] California Independent System Operator. *California Independent System Operator*. Ed. by California Independent System Operator. 2019.

[194] New York Independent System Operator. *Annual Report*. Ed. by New York Independent System Operator.

[195] Alireza Soroudi. *Power system optimization modeling in GAMS*. Springer.

[196] Ignacio E Grossmann et al. "GAMS/DICOPT: A discrete continuous optimization package". In: *GAMS Corporation Inc* 37 (2002), p. 55.

[197] Arne Stolbjerg Drud. "CONOPT—a large-scale GRG code". In: *ORSA J. Computing* 6.2 (1994), pp. 207–216.

[198] Andreas Wächter and Lorenz T Biegler. "On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming". In: *Mathematical Programming* 106.1 (2006), pp. 25–57.

[199] EJ Aladesanmi and KA Folly. "Overview of non-intrusive load monitoring and identification techniques". In: *IFAC-PapersOnLine* 48.30 (2015), pp. 415–420.

[200] Christoph Klemenjak et al. "A synthetic energy dataset for non-intrusive load monitoring in households". In: *Scientific Data* 7.1 (2020), pp. 1–17.