

Tackling the Electric Vehicle-Related Threats to Power Grid Stability

Mohammad Ali Sayed

**A Thesis
In the Concordia Institute
for
Information Systems Engineering**

**Presented in Partial Fulfillment of the Requirements
For the Degree of
Doctor of Philosophy (Information and Systems Engineering) at
Concordia University
Montreal, Quebec, Canada**

March 2024

© Mohammad Ali Sayed, 2024

**CONCORDIA UNIVERSITY SCHOOL
OF GRADUATE STUDIES**

This is to certify that the thesis prepared

By: *Mohammad Ali Sayed*

Entitled: Resilience in the EV Era: Tackling the Electric Vehicle-Related Threats to Power Grid Stability

and submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY (*Information and Systems Engineering*)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____	Chair
Dr Samuel Li	
_____	External Examiner
Dr. Hany Farag	
_____	Arms-Length Examiner
Dr. Chunyan Lai	
_____	Internal Examiner
Dr. Jun Yan	
_____	Internal Examiner
Dr. Walter Lucia	
_____	Thesis Supervisor
Dr. Chadi Assi	
_____	Co-supervisor
Dr. Mourad Debbabi	
_____	Co-supervisor
Dr. Ribal Atallah	

Approved by

Dr. Jun Yan, Graduate Program Director

March 28, 2024

Dr. Mourad Debbabi, Dean, Gina Cody School of Engineering and Computer Science

Abstract

Tackling the Electric Vehicle-Related Threats to Power Grid Stability

Mohammad Ali Sayed, Ph.D.

Concordia University, 2024

Due to the growing threat of climate change, the world's governments have been encouraging the adoption of Electric Vehicles (EVs). Thus, EV numbers have been growing exponentially and gaining a significant market share. As a result, EV Charging Stations (EVCs) are being rapidly deployed to satisfy the rising charging demand. These EVCs are connected to a complex and interconnected system of cyber and physical components. However, without proper security in place, the EV charging load can become a weapon yielded by adversaries to destabilize the power grid. To this end, this thesis examines the security of the EV ecosystem and the impact of EV-based attacks against the grid. The thesis starts by examining the different components and technologies of the EV ecosystem before examining their vulnerabilities. We then demonstrate the greater impact that EV-based attacks can have on the grid as compared to traditional high-wattage smart loads attributed to their bi-directional power flow capabilities and their non-linear nature. We then propose a novel dynamic Load altering (LA) attack strategy that takes advantage of feedback control theory to induce large frequency instabilities on the grid. To address the serious consequences of such attacks, two distinct detection methods are devised. The first is a two-tiered detector tailored specifically to be deployed on the EV ecosystem's Central Management System (CMS) and EVCs to detect attacks emanating from the EV ecosystem. The second method is a detection scheme from the perspective of the utility aimed at detecting all kinds of LA attacks against the grid. This detector utilizes the grid's mathematical model to preprocess the collected data and feed it to a Feature Fusion Neural Network (FFNN) that achieves 99.9 % detection accuracy while remaining robust against data poisoning. Finally, we show case the potential strength EVs can introduce into the grid once secured, by developing a robust LA attack mitigation

scheme. This mitigation scheme utilizes the EV loads/injections to mitigate the impact of the three types of LA attacks. Additionally, we mathematically model the possible real-life uncertainties that hinder the operation of this mitigation scheme to achieve a robust performance.

Acknowledgments

I would like to express my deepest gratitude to my supervisors, Dr. Chadi Assi, Dr. Mourad Debbabi, and Dr. Ribal Atallah, for their invaluable guidance throughout this research. Their insights and encouragement were crucial in shaping this thesis.

I am also immensely grateful to my thesis committee members, Dr. Jun Yan, Dr. Walter Lucia, and Dr. Chunyan Lai, whose constructive feedback and expertise have greatly contributed to my research.

My sincere thanks to Dr. Khaled Saredidine, my college, and more importantly my dear friend. Working alongside him for the past few years has been both a pleasure and a learning experience. Looking forward to further discussions of research ideas we used to come up with over a cup of tea.

I am also greatly indebted to my family, especially Nizar, Elham, Houssien, Issa, Iman, and Jimmy, for their unwavering support and encouragement. Their love and belief in me have been my constant source of strength.

I would also like to thank my wife, Layal, for her companionship and moral support during this journey and for being my pillar of strength in challenging times.

Lastly, I would like to acknowledge the moral support of my friends Charbel, Nathalie, Ronald, Talal, Hassana, Lolwa, and Mahamoud.

Table of Contents

Table of Figures	x
Table of Tables	xiii
1 Introduction.....	1
1.1 Problem Statement and Contributions.....	4
1.2 Thesis Organization.....	5
2 Background.....	7
2.1 EV Numbers and Technology	7
2.2 Non-Attack EV Charging Impact on the Grid	10
2.3 EV Attacks Against Users.....	11
2.4 Related Work: LA Attack Types and Models	11
2.5 Related Work: Attack Detection	14
2.6 Related Work: EV Support of Grid Operation.....	16
2.7 Related Work: Grid Reconnaissance Techniques	17
3 Examining the Electric Vehicle Ecosystem: Security and EV Charging Load Nature	19
3.1 EV Ecosystem Exploits.....	19
3.2 EV Vulnerabilities.....	21
3.3 EV Charging Station Vulnerabilities.....	21
3.4 EV to EVCS Communication Vulnerabilities.....	22
3.4.1 IEC Vulnerabilities [103] [104].....	22
3.4.2 ISO 15118 Vulnerabilities	22
3.5 OCPP Protocol Vulnerabilities [43] [103] [106].....	24
3.6 EVCS Firmware / IoT Vulnerabilities	26
3.7 EV Charging Mobile App Vulnerabilities [56].....	27
3.8 EV Operator's OCPP Backend Vulnerabilities.....	28
3.9 EV Ecosystem Malware Landscape	29
3.10 Distinct Nature of EV Load and Straightforward Attack Strategy	30
3.10.1 EV Charging Properties	30
3.10.2 Straightforward EV Attack Vector.....	31

3.11	EV Botnet Command and Control	33
3.12	EV Attack Feasibility	35
3.13	Case Study: EV Attacks Against the Power Grid	37
3.13.1	Simulation Setup	37
3.13.2	EV Load Manipulation Attack Scenarios.....	39
3.13.3	EV-Specific Attack Scenarios	40
3.13.4	Other Attack Implications	43
3.13.5	Comparison to non-EV Attacks	44
3.14	Hardening the EV Ecosystem Security	48
3.15	Chapter Concluding Remarks	51
4	Novel EV-Based Dynamic Attack Strategy.....	52
4.1	System Modeling and Attack Methodology.....	53
4.1.1	Linearized Power System Model	54
4.1.2	Feedback Control as an Attack Model.....	55
4.1.3	Attack Region Constraints	56
4.1.4	Attacker Reconnaissance Including Parameter Uncertainty	56
4.1.5	Robust Attack Formulation.....	61
4.1.6	Observer Design.....	63
4.2	Case Studies and Simulations	64
4.2.1	Attack Feasibility	65
4.2.2	Reduced Power Grid State-Space Model.....	66
4.2.3	EVCS Botnet Command and Control	67
4.2.4	Case Studies: Attacks Against NE 39-Bus System.....	67
4.2.5	Discussion of Attack Results in the Context of Existing Literature	76
4.3	Chapter Concluding Remarks	78
5	Two-Tier EV-Based Attack Detection.....	79
5.1	Detector Design.....	80
5.1.1	CMS Detector Algorithm.....	81

5.1.2	EVCS Detector Algorithm.....	82
5.2	Dataset Curation.....	83
5.2.1	CMS Detector Dataset Curation and Collection.....	83
5.2.2	EVCS Detector Dataset.....	84
5.3	Evaluation of Detector Performance	85
5.3.1	Detection Algorithms Performance Evaluation	88
5.3.2	Comparison to State-of-the-Art	89
5.4	Chapter Concluding Remarks	90
6	LA Attack Detection and Localization Using a Physics-Assisted Feature Fusion Neural Network.....	91
6.1	Grid Modeling and Detection Methodology	92
6.1.1	Power System Representation.....	92
6.1.2	State Estimation and Load Variation Estimation.....	94
6.1.3	Design of Detector	95
6.1.4	Dataset Curation and Collection	98
6.1.5	A Family of Detectors for Systematic Comparison.....	99
6.2	Case Studies and Performance Results	101
6.2.1	Tuning of Detection Algorithm Parameters.....	102
6.2.2	Deployed Detector Performance	103
6.2.3	Comparison with State of the Art	105
6.2.4	Robust Performance Facing Data Poisoning Attacks	106
6.3	Chapter Concluding Remarks	110
7	An EV Robust Mitigation Scheme Against Load Altering Attacks	112
7.1	System Modeling and Mitigation Methodology	114
7.1.1	Power System Representation and Defender Model	114
7.1.2	Observer Design.....	116
7.1.3	Choice of Controller for EV-Based Mitigation Scheme.....	117

7.1.4	H-2 and H- ∞ Controller Design.....	117
7.1.5	Robust Controller Under Uncertain EV Feedback Load	120
7.1.6	Mixed Robust H-2/ ∞ Controller	122
7.1.7	EV User Impact and Privacy Concerns	123
7.2	Case Studies and Simulations	124
7.2.1	Reduced Power Grid State-Space Model.....	127
7.2.2	Case Study 1: Attacks in Absence of Mitigation without PSS	127
7.2.3	Case Study 2: Attacks in Absence of Mitigation with PSS	129
7.2.4	Case Study 3: H-2 and H- ∞ Control EV-Based Mitigation.....	130
7.2.5	Case Study 4: Robust Mixed H-2/ ∞ EV-Based Mitigation	133
7.2.6	Case Study 5: Smaller LA Attacks	135
7.2.7	Impact on EV Range	136
7.2.8	Mitigation Scheme Feasibility	136
7.2.9	Mitigation Scheme Reaction to Non-Attack Scenarios	137
7.3	Stability and Performance Evaluation.....	140
7.3.1	Uncertainty and Controller Stability	140
7.3.2	Smaller Defender Load	142
7.3.3	Effect of Communication Delay	143
7.3.4	Impact of Clustering	144
7.3.5	Impact of Grid Operating Point	144
7.4	Chapter Concluding Remarks	145
8	Thesis Conclusion and Future Research Directions	147
	References.....	151

Table of Figures

Figure 2-1: EV ecosystem as depicted in [37]	9
Figure 3-1: Signals emitted by communication of charging cable [53].....	23
Figure 3-2: (a) Typical PV curve and (b) typical QV curve based on PowerWorld Manual on PV and QV Curves.....	32
Figure 3-3: Simplified model of EV ecosystem and possible attacker entry points.....	33
Figure 3-4: WSCC 9-Bus System	38
Figure 3-5: Glover 7-Bus System	38
Figure 3-6: Frequency drop on 9-Bus System due to increased demand 2000 EVs.....	39
Figure 3-7: Frequency rise on 9-Bus System due to power injection.....	41
Figure 3-8: Voltage limit violation at (a) bus 4 (●), (b) 5 (▲), (c) 7 (◆), and (d) 9 (■) due to power injection.....	41
Figure 3-9: Transient frequency response to the switching attack	42
Figure 3-10: Transient voltage response at load (a) bus 5 (●), (b) bus 6 (◆), and (c) bus 8 (■) due to the switching attack	42
Figure 3-11: Modified 7-Bus System	44
Figure 3-12: 7-Bus System: transient frequency response after the 48 MW attack	45
Figure 3-13: 7-Bus System: Transient frequency response in area 1 after a 4400 EV attack	45
Figure 3-14: 7-Bus System: Transient voltage response at bus 1 after a 4400 EV attack	46
Figure 3-15: 7-Bus System: Generator 1 active power output after a 4400 EV attack	46
Figure 3-16: 7-Bus System: Generator 1 reactive power output after a 4400 EV attack	46
Figure 3-17: 7-Bus System: Transient frequency response of area 1 after a 3300 EV attack.	47
Figure 3-18: 7-Bus System: Generator 1 active power output after a 3300 EV attack	47
Figure 4-1: State-space attacker model and interaction with the power grid	55
Figure 4-2: Sample of pole placement using D-stabilization methods.	56
Figure 4-3: New England 39-bus grid	65
Figure 4-4: Hankel Singular Value weights.....	66
Figure 4-5: Output frequency of generators 2 and 9 in Scenario 1 with no PSS.....	69
Figure 4-6: Output frequency of generators 1 and 4 in Scenario 2.....	69

Figure 4-7: Bus 18, 37, and 39 voltages in Scenario 2.	70
Figure 4-8: Output frequency of generators 1 and 6 in Scenario 3.....	70
Figure 4-9: Aggregate EV attack load – first 5 seconds of Scenario 3.....	71
Figure. 4-10: Aggregate EV attack load on buses 4 and 18 – first 5 seconds of Scenario 3	71
Figure. 4-11: Bus 3, 24, and 29 voltages in Scenario 3.	71
Figure 4-12: Output frequency of generator 6 in Scenario 4.	71
Figure 4-13: Bus 14 and 16 voltage.in Scenario 5.....	72
Figure 4-14: Output frequency of generators 2 and 10 in Scenario 5.....	72
Figure 4-15: Output frequency of generators 2 and 10 in Scenario 6.....	73
Figure 4-16: Maximum frequency deviation under parameter uncertainty	75
Figure 6-1: Detection mechanism based on load variation recovery and feature fusion NN	93
Figure 6-2: Histogram of error in load variation reconstruction probability	94
Figure 6-3: New England 39-bus grid	101
Figure 6-4: Kundur 2-area power grid.....	101
Figure 6-5: Results of random label flipping and targeted label flipping attack	107
Figure 6-6: Results of perturbation attacks.....	109
Figure 6-7: Data poisoning attack impact on the F1-score of the different models	110
Figure 6-8: Data poisoning attack impact on FN rate of the different models	110
Figure 7-1: Defender’s state-space model and interaction with the attacked grid.....	115
Figure 7-2: New England 39-bus grid	125
Figure 7-3: EVCS Public and Private charging load for 24 hours.....	126
Figure 7-4: Generator frequency response under attack 1 with no PSS	128
Figure 7-5: Generator frequency response under attack 2 with no PSS	128
Figure 7-6: Generator frequency response under attack 3 with no PSS	128
Figure 7-7: Generator frequency response under attack 2 with PSS	129
Figure 7-8: Attack 1 load on each of the buses.....	129
Figure 7-9: Generator frequency response under attack 3 with PSS	130
Figure 7-10: Attack 3 load on bus 4.....	130
Figure 7-11: Attack 3 aggregate load.....	130
Figure 7-12: Generator frequency - attack 2 with H-2 controller.....	131
Figure 7-13: Generator frequency - attack 3 with H-2 controller.....	131

Figure 7-14: Generator frequency - attack 2 with $H-\infty$ controller	132
Figure 7-15: Generator frequency - attack 3 with $H-\infty$ controller	132
Figure 7-16: Generator frequency - attack 2 with mixed $H-2/\infty$ controller	133
Figure 7-17: Generator frequency - attack 3 with mixed $H-2/\infty$ controller	133
Figure 7-18: Generator frequency - attack 4 with mixed $H-2/\infty$ controller	135
Figure 7-19: Grid frequency after line tripping line 4-5	137
Figure 7-20: Grid frequency after Generator 1 tripping	137
Figure 7-21: Grid frequency under normal random consumer behavior	138
Figure 7-22: Frequency deviation probability during normal behavior	138
Figure 7-23: Grid frequency under attack 3 in the presence of a 0.03 Hz threshold	139
Figure 7-24: Generator frequency with normal and robust controllers	140
Figure 7-25: Maximum frequency deviation vs defender resources level	142
Figure 7-26: Generator frequency with controller feedback communication delay	143
Figure 7-27: Generator frequency with controller EV load clustering	144

Table of Tables

Table 3-1: Maximum Potential Public EVCS Load in MW vs EV Levels and Charging Rate ...	36
Table 4-1: Maximum Total EV Load In MW vs EV Levels and Charging Rates.....	65
Table 4-2: Vulnerabilities and EVCS botnet control.....	67
Table 4-3: Max Frequency Deviation vs Different Attack 2 EV Load Magnitudes.....	73
Table 4-4: Impact of EV Load Uncertainty	74
Table 4-5: Attack Scenarios Summary	75
Table 5-1: Optimal Hyperparameters of the Different DL Algorithms Considered for the CMS Detector.....	86
Table 5-2: Parameters of the Different DL/ML Algorithms Considered for the EVCS Detector	87
Table 5-3: Confusion Matrices of the CMS-Based Algorithms	87
Table 5-4: Confusion Matrices of the EVCS-Based Algorithms.....	87
Table 5-5: Performance Metrics of the CMS-Based Algorithms	88
Table 5-6: Performance Metrics of the EVCS-Based Algorithms.....	88
Table 6-1: Hyperparameters of the Supervised DL Algorithms	102
Table 6-2: Hyperparameters of the AE	103
Table 6-3: Hyperparameters of the FFNNs	103
Table 6-4: Confusion Matrices of the ML/DL Algorithms	104
Table 6-5: Performance Metrics of the ML/DL Algorithms	105
Table 6-6: Results of the Trojan Attacks	108
Table 7-1: Possibilities for Reducing System Order	127
Table 7-2: Max Frequency Deviation Vs Different Attack 2 and 3 Magnitudes.....	134
Table 7-3: Controller Stability Margin	141
Table 7-4: Max Frequency Deviation vs Communication/Synchronization Delay	144

Chapter One

Introduction

Humanity's increasing reliance on electricity has transformed the course of society's development over the past couple of centuries [1]. The power grid has become the backbone of modern society, and its security is directly linked to the security and economic stability of any nation. To this end, smart technologies have been introduced to support reliable grid operation [2] [3]. This has transformed the traditional grid into a smart grid that relies on sensors and remote-controlled actuators to perform tasks that were traditionally manual or localized [3]. This move towards a smart grid improves the grid's efficiency, reduces Greenhouse Gas (GHG) emissions, allows easier integration of renewable energy, distributed generation [2], and quicker restoration after faults. These technologies, however, pose a security risk, linking the security of the smart grid to the security of these newly incorporated technologies [4]. This has made the smart grid prone to attacks, initiated through its cyber layer, which can have devastating impacts on its stability.

Cybersecurity has become a major concern in recent years. A recent cyber-attack in the United States (US) is the ransomware attack against the Colonial Pipeline that disrupted gas supplies and caused a global hike in prices [5]. Another major recent cyber threat is the SolarWinds hack [6] that affected around 18,000 clients who downloaded the compromised Orion software update. The infected users include high-security entities such as the US Department of Energy, the US Department of Homeland Security, the Center for Disease Control, and multiple Fortune 500 companies. Other clients that use the infected software include NATO, the European parliament, and various governments worldwide. Other examples of cyber-attacks include the Saudi Aramco hack in 2012 when 35,000 computers were compromised threatening 10% of the world's oil supply [7]. The US OPM hack in 2014 also saw the personal information of 21.5 million users stolen [8].

In the field of smart grids, two of the first cyber-attacks directly come to mind, i.e., Stuxnet [9] and the BlackEnergy attack [10]. The 2010 Stuxnet malware attack, against Iran's nuclear

facilities, represents the first major example of state-level attacks against the smart grid. A worm introduced into a Windows machine propagated to its destinations (Siemens PLC-S7) while maintaining minimum chances of detectability. Eventually, the malware stealthily manipulated the centrifugal pressures destroying 10% of Iran's centrifuges in a major setback to their nuclear program [9]. The Ukraine BlackEnergy Malware-attack in 2015 represents the first confirmed successful cyber-attack against a power grid that left 230,000 consumers without electricity.

However, since then new types and families of more sophisticated attacks have been observed against the world's power grids. The ShadowPad malware is an example of a successful attack against industrial control systems that has also been used against the power grid [11]. The Aurora Generator Test is another example that demonstrated how malware comprised of 30 lines of code can destroy the rotors of the generators in a power grid if allowed to propagate into the utility's systems [12]. In the past two years alone, the Indian power grid has been exposed to 4 verified attacks as reported in [11], [13], [14], and [15].

Recent studies have also considered the disruption of power grid operation by compromised high-wattage IoT (Internet of Things). The work presented by Soltan et al. [16] demonstrated how a botnet of compromised high-wattage devices, such as smart water heaters, could be used to launch large-scale attacks against the grid. The Mirai Botnet [17] is a clear example of the weaknesses inherent to IoT devices where the attackers compromised over 600,000 devices and used them to launch DDoS attacks.

These examples, however, should not outweigh the advantages that are introduced into the traditional power grid through the shift towards the smart grid. This shift would allow for reduced power losses, reliable real-time monitoring and protection, easier and quicker restoration after disturbances, and the increased integration of renewable energy resources and smart/green technologies [2].

One such system is the Electric Vehicle (EV) ecosystem. Given that transportation is a huge contributor to GHG emissions [18], there is a global push toward the adoption of EVs to combat climate change [19] which has led to rapid growth in EV numbers. As the world is witnessing a great push toward combating climate change, the world's governments have been encouraging the adoption of EVs to reduce the emissions of the transportation sector. The advancement of the underlying technologies and larger production volumes has also decreased EV prices improving

public opinion on EVs. One major factor is the massive reduction in battery cost which contributes roughly 25% of the EV price. As such, we are witnessing exponential growth in EV numbers on the road. By the end of 2019, there were 7.2 million EVs on the road [20]. The exponential growth is demonstrated by the record EV sales reaching 3.2 million EVs in 2020 [21] and 6.6 million in 2021 [21]. The trend has continued with 10.5 million EV sales in 2022 and an anticipated 13.6 million EV sales in 2023 [22].

The International Energy Agency (IEA) has set a target of 30 million EVs will be on the road in 2030 [19], thus reducing the demand for oil products by 2.5mb/d (or 127 million tons a year) and displacing the total emissions by 189.1 Mt CO₂. However, this target was already surpassed by mid-2023. Most notably, EVs constituted 79% of new car sales in the Norwegian market in 2020 [23] [24] rising to 90.6% in 2023 [25]. Furthermore, EV sales are expected to reach 100% in 2025 [26].

The Canadian EV market has also grown to gain a 10.5% share of all new vehicle registrations [27]. The Canadian Government has also dedicated 900 million CAD to establish a network of additional 50,000 EVCSs on top of the currently existing networks and to supplement the current provincial deployment strategies. In line with the global and Canadian vision of achieving 100% zero-emission vehicle sales, Quebec has set a target of 1 million EVs by 2030 [28] and will ban new gasoline car sales in 2035 [29].

Multiple non-governmental initiatives such as the Zero Emission Transportation Association (ZETA) have also been undertaken to support the proliferation of EVs. Two chief members of ZETA, pushing towards increased EV proliferation, are Uber and Tesla. Indeed, Uber's CEO expects that Uber's service will become fully based on EVs by 2030 in the US and Canada [30] [31]. Given the global push towards EVs, this proposal examines the EV ecosystem and the threat it introduces to the power grid.

Bearing all the above in mind, and the undeniable importance EVs will play in humanity's future, we conduct this comprehensive study of the EV ecosystem. In this study, we examine the ecosystem's security, the impact of attacks initiated through this ecosystem against the power grid, attack detection methodologies, and finally the possibility of using EVs to support the power grid and mitigate attacks against its stability.

1.1 Problem Statement and Contributions

To support the rapid growth in EV numbers and improve the quality of charging service, communication networks and IoT-enabled smart charging have been widely adopted in the EV ecosystem. Additionally, operators have been hastily deploying EV Charging Stations (EVCSs) to meet the increasing charging demand. This has contributed to the EV ecosystem’s lack of proper security measures. The EV ecosystem has inherited the vulnerabilities of its underlying IoT and communication systems. In March and April of 2022, two separate attacks occurred against EVCSs in Russia [32] and the United Kingdom [33] respectively. The attackers in both cases changed the display on the screens of the chargers and caused a Denial of Service (DoS) hindering their usage. An attacker who gained full control over these chargers could have easily manipulated the charging load. In addition to that, in 2021, a teenager hacked into multiple Tesla vehicles and locked their owners out [34]. Additionally, in February 2023, a security researcher was able to gain full control of several EVCSs owned and operated by Electrify America by exploiting third-party software on these EVCSs without being detected [35]. Coupled with the fact that attackers can manipulate not only the charging schedule but the charging load itself as demonstrated by a study by the US Department of Transportation [36], EV attacks can have detrimental impacts if used to attack the grid. To this end, we present an overview of the EV ecosystem’s security posture and summarize the vulnerabilities that allow adversaries to hack into the EV ecosystem and launch attacks against the power grid. We also examine the special nature of the EV load profile that makes it ideal for attacks aimed at disrupting power grid operation. By highlighting these vulnerabilities and suggesting readily available security patches, we assist the industry in securing the EV ecosystem.

Additionally, we create a novel Dynamic Load Altering (LA) attack strategy through the EV charging load and demonstrate its devastating impacts on the power grid. In this thesis, we intend to address the gaps in previous works that attempted to create LA attacks. Through our work, we have identified that the vast majority of studies on LA attacks either consider attackers with full knowledge of the grid thus oversimplifying the attack design, or consider very simplistic attacks with limited impacts. To this end, we suggest an attack methodology that accounts for the uncertainties of the power grid topology and incorporates it into the attack design to compensate for modeling errors. Finally, unlike other EV-based attack studies, we do not consider the EVs as

a generic load but rather take their special nature into account which amplifies the attack impacts significantly.

Moreover, most of the studies related to LA attacks and EV attacks consider attack detection out of their scope. As a result, we intend to address this gap by developing multiple LA attack detection schemes tailored to both the cyber and physical layers of the EV ecosystem and the power grid. To address the immediate danger of attacks through EV charging, we suggest a two-tiered detection mechanism specifically tailored to the EV ecosystem's components. Additionally, we develop a novel and extremely powerful detection mechanism to be deployed by the utility for the detection of LA attacks whether initiated through EV charging or any other high-wattage load.

Finally, we explore the positive aspects of introducing the EV loads into the power grid and examine using these EVs to support the grid's operation. To this end, we devise a novel LA attack mitigation scheme that takes advantage of the EVs' unique properties that are ideal for such a purpose. EVs can support the power grid by acting as distributed battery storage as well as distributed generators owing to the Vehicle-to-Grid (V2G) power flow capability in new EVCSs. The specific nature of the EVs that makes them ideal for such scenarios is explored and a robust mitigation scheme against LA attacks is created.

1.2 Thesis Organization

Based on the above-identified gaps, we examine the following research directions within this thesis. The thesis is organized as follows:

- Chapter 2 provides a detailed background on the cyber and physical components of the EV ecosystem as well as a brief on the current state of EV technology. Additionally, we perform a literature review and examine the current studies available in the fields of LA attacks, attack detection, and EV-based mitigation.
- In Chapter 3 we examine the security posture of the different components of the EV ecosystem and identify the possible entry points for attackers that allow them to take control of the EV charging process and use it to compromise the stability of the power grid. Beyond that, we

examine the special non-linear nature of the EV charging load that makes it ideal for attacks against power grid stability. We then demonstrate the impact of EV-based attacks vs attacks based on traditional high-wattage devices.

- In Chapter 4, we present a novel dynamic LA attack strategy against the grid's frequency and voltage stability initiated through the EV ecosystem. To this end, we develop an attacker methodology that allows the attacker to account for the uncertainties introduced by the changes in grid condition as well as the errors in estimating grid parameters and the EV load connection to EVCSs. We mathematically model this uncertainty and incorporate it into our attack design.
- Chapter 5 then presents a bi-level detection mechanism aimed at detecting EV-based attacks and LA attacks in general. This mechanism is tailored to detect attacks through the EV ecosystem by creating a two-tiered detector deployed on the EV ecosystem's Cloud Management System (CMS) and the individual EVCSs.
- Chapter 6 presents a novel LA attack detection mechanism created from the perspective of the utility. The detection mechanism utilizes the mathematical model of the underlying physical system, i.e., the grid, to pre-process the collected frequency measurements and uses them as an input to a Neural Network (NN) for attack detection and localization.
- Finally, in Chapter 7 we demonstrate our robust wide-area controller that utilizes the EVs as its control inputs to mitigate the impact of unknown persistent LA attacks even when they are sustained for long durations. We design our robust feedback controller to account for uncertainties introduced by real-life deployment obstacles. We mathematically model this uncertainty and incorporate it into our controller synthesis.
- Chapter 8 concludes this thesis and recaps the main contributions as well as highlighting the current work's gaps and suggesting future research directions that form a logical continuation for the current work.

Chapter Two

Background

In this section, we take a brief look at the EV ecosystem and technology. We then discuss existing LA attack models and present related studies in the field of EVs, attack detection, and power grid protection.

2.1 EV Numbers and Technology

The EV charging ecosystem is a complex cyber-physical system composed of interconnected hardware and software elements as well as communication protocols making it an IoT paradigm at the heart of the smart grid. These elements are discussed below and in Figure 2-1.

- EV: The central element of this ecosystem is the EV itself. These vehicles have large lithium-ion batteries on board, that require charging at dedicated EVCSs. Once an EV is connected to the EVCS, it will communicate over the charging line. EVs as well as all modern vehicles contain 100s of processing units known as electronic control units (ECUs) that control all the vehicle's critical functions. These ECUs are connected through a Controller Area Network (CAN) bus. The CAN bus is a peer-to-peer network, where the ECUs and peripherals interact with one another directly. The CAN bus also has an onboard diagnostic (OBD) port [37] that is accessed by mechanics via smartphones. EVs also have USB ports, SD card readers, Bluetooth, smartphone interfaces, and internet connectivity for external communication.
- EVCSs: are the connection point between the power grid and the EVs. The EVCS itself is an IoT device running management firmware that controls the power converters and manages the

communication with the EV and the EV management system. EVCSs are classified into 3 levels based on their charging rate [38] [39] [40].

- Level 1 chargers are the slowest chargers providing a rate of 1.4 kW and can be plugged into a 110 V wall outlet and rely on the on-board chargers inside the EV. These chargers are only found in residences in North America but are currently being phased out in favor of the faster Level 2 chargers.
- Level 2 chargers require extra hardware to be installed and provide a charging rate up to 40 kW at a voltage level of 208-240 V. Currently the highest level 2 rate is 19 kW, but these chargers are not commercially available yet. Commercially available Level 2 chargers provide a charging rate of 11 kW. Level 2 chargers can be either AC or DC.
- Finally, DC Level 3 fast chargers deliver a charging rate of 40 to 360 kW.

Nonetheless, DC chargers are becoming more common owing to their bidirectional inverter/converter circuits [37] that allow higher charging rates and support the V2G functionality allowing the injection of the energy stored in the EV battery back into the grid [37]. The EVCS's power factor corrector can be adjusted to achieve any desired power factor (pf).

EVCSs also have touchscreens and card readers used for local control of charging sessions, choice of connector type and charging rate, making payments, and so on. EVCSs can also be connected to smartphones and have USB, serial, and Ethernet ports.

Communication between the servers and the EVCSs is not standardized but the Open Charge Point Protocol (OCPP) is the de facto standard. Public EVCSs are connected to CMS [37] [41] [42] via OCPP to communicate, monitor, and control all functionalities of the EVCSs in real-time. These EVCSs are connected to the internet through onboard 5G routers and synchronized together using the Network Time Protocol (NTP) [43] [44]. NTP ensures the synchronization of the EVCSs' clocks with a guaranteed accuracy of 10ms over the public Internet [45] and 1ms over a local area network [45]. Users interact with public EVCSs through this server through smartphone apps. This control includes payment, scheduling, starting and stopping charging sessions, and every other EVCS operational aspect.

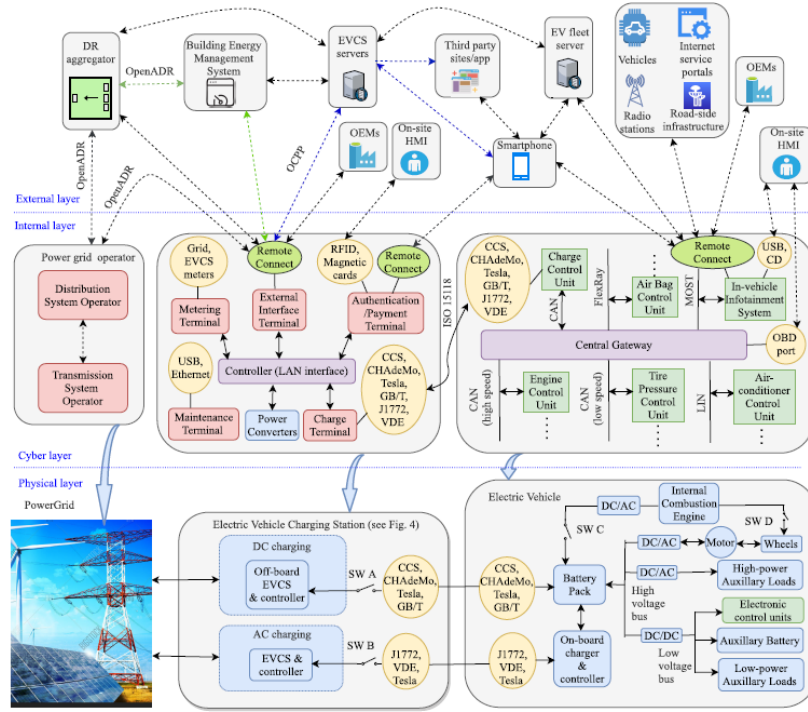


Figure 2-1: EV ecosystem as depicted in [37]

- **EV Cloud Management System (CMS):** This software is hosted on a cloud server and manages all operations of the public EVCS. Through this system, users are directed to available EVCS, charging sessions are scheduled and managed and EVCS utilization data is logged. The EV CMS can send specific control signals to the EVCS related to the duration of the charging session, charging rate, beginning and termination commands, etc.
- **User applications:** These are either web applications or smartphone applications through which users can talk to the EVCS through the management system over the internet (in case of public EVCS) or directly to the charger over a LAN (in case of private EVCS). These services allow users to reserve and control charging sessions, pay for public charging, control charging rates, start/terminate charging sessions, and monitor the status of the EV.
- **EV Protocols:** As mentioned earlier in this section, bilateral communication occurs between the components of the EV ecosystem. Thus, communication between user apps, EVs, EVCS, and the EV management system needs to be secure to ensure safe and reliable operation. The adopted protocols vary between different equipment manufacturers, countries, and EVCS operators [36] [46]. This lack of standardization exposes the system to multiple weaknesses presented by the US Department of Transport [36] and discussed below.

- **Power Grid:** The power grid is the backbone of most modern activities including EV charging. EVCSs are connected to the power grid and draw the needed electricity from it and as such have a great impact on the security and stability of this grid.

This new EV ecosystem can add a significant load to the power grid and its specific nature might sometimes become problematic. Below we present a brief discussion of the EV charging load impact on the power grid.

2.2 Non-Attack EV Charging Impact on the Grid

As EV numbers increase further, irregular charging behavior becomes more problematic and can negatively impact the power system operation. The work performed on [47] demonstrated how uncontrolled EV charging especially during peak load time can cause a loss of load up to 6.89%. In fact, it is estimated that a 10% EV penetration in Portugal can cause a significant voltage drop at peak times [48]. The work in [49] performed a comparison between two optimization objectives, to reduce the peak load by shifting the EV charging to night times and by utilizing the Vehicle to Grid reverse power flow to reduce day peaks respectively. Their work demonstrated that reducing peak load and minimizing operation costs cannot be achieved simultaneously. The authors concluded that it is important to properly manage the EV charging schedule to improve system load without significantly increasing the operation cost.

Another aspect of EV impact on power system cost was studied in [50] that focused on power system infrastructure investment cost as well as system losses. This study performed simulations on a residential area and a mixed residential/industrial area. Multiple EV penetration levels were considered between 35% and 62% of the total car numbers. The simulations were performed for the peak and off-peak demand scenarios in each area and the results show increased investment costs and system losses at all levels of EV penetration. The incremental investment was found to be larger in the grid that was operating close to its operating limits. The authors also simulated the impact of the EV load on system losses that rose by up to 40% under a 62% EV penetration level.

2.3 EV Attacks Against Users

Several works in the literature have discussed attacks against or through the EV ecosystem against the users and the power grid. Attackers that gain control of the EV battery management system through compromised web services or malware downloaded to the EV's systems can cause severe damage to the EV itself. In fact, [51] and [52] discuss how attackers can cause damage to the EV batteries by manipulating the charging current and bypassing the safety measures in place. Another study in [53] examined an eavesdropping attack against the communication between the EV and the EVCS over the charging cable bundle. This attack allows the attacker to capture the EV ID and maladdress giving the attacker the ability to charge their EV and bill it to other customers. The second concern is the simplest possible attack, which is user tracking. From the EV ID appearing at different charging locations, the user can be tracked, and his/her actions can be inferred creating a huge violation of privacy. However, attacks against the users are considered out of the scope of this work.

2.4 Related Work: LA Attack Types and Models

Unlike False Data Injection (FDI) attacks, which tamper with the grid's measurement [54], LA attacks manipulate actual power consumption to harm the grid [16], thus bypassing the grid's bad data detection mechanisms.

LA attacks can be broadly classified into 3 subfamilies which are static attacks [16], [55], [56], switching attacks [57], [58], [59], and dynamic attacks [60] [61] and [62]. These LA attacks are stealthier and stronger than attacks targeting the grid's cyber layer alone as demonstrated below.

The authors of [16] and [55] demonstrated how static attacks based on a single spike in load, can be initiated by manipulating high-wattage home IoT devices to cause line tripping and load shedding while remaining unobservable to the utility. On the contrary, switching and dynamic attacks can induce frequency instability in the grid using small portions of the connected load even in the presence of a grid's protection mechanisms. The work in [57] relied on the manipulation of

distribution feeders to initiate switching attacks while mimicking natural phenomena on the grid which makes them hard to detect while simultaneously forcing generator tripping.

Soltan et al. [16] proposed a family of large-scale static attacks, sudden spikes in load, against the grid using a botnet of compromised high-wattage IoT devices. These attacks are based on a single abrupt spike or drop in load to cause problems such as line tripping and tie-line overloading leading to cascading line failure. Static attacks can also cause limited frequency disturbances. Static attacks only require knowledge of high-level geographical information on the IoT devices' distribution. The authors found that compromising a small fraction of the available water heaters or air conditioners in a grid is sufficient to disrupt its operation. However, the authors of [55] demonstrated how the impact of static attacks has been exaggerated in the literature and how their impact on transient stability is amplified by neglecting some of the grid's existing protection mechanisms. As a result, they proposed a multi-step static attack based on the grid's transient conditions. This variation requires the attacker to have the ability to monitor the grid's transient behavior to launch the attack steps accordingly. Another multistep static attack has been proposed in [56] launched through the EV charging ecosystem. Furthermore, the work performed in [63] presents a much more impactful set of static attacks that are crafted to have a larger impact when the attackers know the grid's topology and target the weakest buses to cause larger frequency and voltage deviations as well as line tripping. Finally, the authors of [64] proposed a distributed static attack and emphasized the infeasibility of protecting all the grid's smart loads due to the extremely prohibitive costs that render the task practically impossible.

The second family of LA attacks is known as switching attacks that can be launched by adversaries to excite certain unstable modes that pre-exist in a given grid due to its specific dynamics e.g., inter-area oscillation [57] [58]. The attackers do not require any topology information for the success of such attacks. However, during the reconnaissance phase, the attackers introduce a probing signal into the grid using the compromised loads. This signal allows the attacker to record the grid's response to a signal containing a variety of frequency components. The attackers then calculate the impulse response of the grid to the introduced probing signal and estimate its eigenvalues. These eigenvalues allow the attacker to identify the frequency of the unstable mode, if any. The attacker then switches the compromised loads on/off at this specific frequency to induce instability. The inter-area oscillation mode was targeted in [57] by switching the distribution

feeders, and in [58] using the EV charging loads. The authors of [57] discussed how switching attacks can be initiated by switching distribution feeders but overlooked the cyber vulnerabilities that need to be used and the ease at which the utility can detect an attacker who has gained full control of an entire substation. Alternatively, the authors of [58] launched their switching attacks from the EV loads but neglected to account for the special nature of the EV load and treated it as any generic high-wattage device. Other modes can also be excited using switching attacks, such as the sub-synchronous resonance mode in [65]. The authors of [59], however, stressed the need to design the switching attacks while keeping in mind the variation of the unstable modes depending on the grid's condition. The success of these attacks hinges on the chosen probing signal, the accuracy of the frequency estimation, and most importantly whether an unstable mode exists in the targeted grid. The work in [66], however, demonstrated that sustained switching attacks can deteriorate grid performance in the absence of such unstable modes but fall short of causing blackouts.

The third form of LA attacks is the dynamic attack described in [60] [61] and [62]. During the reconnaissance phase, the attacker gathers information about the power grid's topology and parameters to build a state-space model of the system [61]. This state-space is then used to craft the attack as a feedback controller that manipulates the magnitude and oscillation frequency of the compromised load to shift the grid's eigenvalues to unstable operation regions. The dynamic attack load is tailored to the instantaneous changes in the grid's response. A simplified form of dynamic attacks was proposed in [67] to take advantage of the low inertia conditions during the COVID-19 pandemic. This attack can be considered a midpoint between static attacks and dynamic attacks. The authors created an attack vector that maximizes attack impact by tailoring it to the grid's weak point during low inertia times. The authors of [61] and [62] suggested a dynamic attack strategy based on modeling the feedback controller as a simple proportionality gain controller. The drawback of this type of controller is that the attack load will constantly keep on increasing as the frequency instability increases since the attack load is proportional to the absolute value of the frequency deviation. Additionally, the authors did not provide any robust methodology on how the accurate power grid parameters are recovered by the attacker. Based on the formulation in [61] and [62], another dynamic attack was suggested in [68] based on estimated grid parameters by using generic machine parameters described in public sources. This work, however, has severe limitations in that it assumes that the generic parameters will capture the behavior of the real

system. The discussed attack was only tested against the approximated grid representation and not against the actual grid. Additionally, their work relied on the DC power flow model that completely ignores the reactive power flow and other grid dynamics. Additionally, the authors mentioned that their attacks will exploit the EV load, yet they did not account for the uncertainty in EV user behavior, nor did they consider the reactive power of the EV load which are the two main elements distinguishing the EV load from traditional IoT loads.

2.5 Related Work: Attack Detection

Most of the attack studies mentioned above focus on attacker strategy and consider attack detection out of their scope. However, several studies focused on the detection of LA attacks or intrusion detection into EV and other IoT systems.

The detection mechanism developed in [58] to detect LA attacks initiated through the EV charging ecosystem based on the arrival of charging requests. The detector is based on a fully connected Neural Network (NN) deployed on the EV charging CMS. This detector, however, misclassified 30% of all attacks even after observing 20 seconds of attack data. This is considered a considerably low detection rate and a very slow detection time. Moreover, the deployment of such a detector on the EV CMS makes it vulnerable to the same vulnerabilities of this ecosystem.

The authors of [69] proposed a Long-Short-Term-Memory (LSTM) algorithm based on network packets to detect DoS attacks against EV chargers. This work, however, was not specific to EV network traffic and is generalizable to all high-wattage IoT devices. Although the LSTM model achieved comparable results to our work, with an F1-score of 99%, they did not mention the time required for detection. Additionally, this detector is not optimized to detect LA attacks but rather DoS attacks which do not have a direct impact on the grid. Additionally, their detector is optimized to detect these DoS attacks by monitoring the volume of incoming data packets which is in the order of hundreds per second. As a result, this mechanism fails to detect LA attacks since they require only a few requests per second. In our attack scenarios, the attacker is sending a maximum of 1.2 requests per second to the targeted devices.

A Deep Learning (DL) detection mechanism against IoT malware was created in [70] based on paranoia activity by studying 3,000 malware families. Similarly, another DL mechanism was devised in [71] to detect malware in the EV ecosystem. The authors, however, trained their detector using 561 samples, which is a small unrepresentative set for NN training. More importantly, LA attacks do not necessarily require the presence of malware and can be initiated through a multitude of methods. Another work aimed at detecting spoofing attacks in the EV ecosystem was discussed in [72]. Yet this detector does not help in the detection of LA attacks.

Another DL mechanism was devised in [71] to detect malware in the EV ecosystem based on paranoia activity. The authors trained their detector using 561 samples, which is a small unrepresentative set for NN training. Another work aimed at detecting spoofing attacks in the EV ecosystem was discussed in [72]. Yet this detection mechanism does not help in the detection of LA attacks.

The work in [73], [74], and [75], all created detection mechanisms based on control systems-inspired techniques at the power grid level. However, these works did not consider the possibility of stealthy attacks and only considered straightforward attacks with significantly large magnitudes. Furthermore, none of these works considered the naturally occurring load fluctuations in a power grid. Their results even demonstrate how all load variations are zero until an attack occurs making their detection approaches rather simplistic. Finally, a major drawback is that these works did not report any accuracy-related metrics for their detection results leaving any comparison with these works impossible.

Finally, the authors of [76] created the most relevant attack detection and localization mechanism. The authors follow similar reasoning and rely on the generator frequencies as the most reliable measurements at the utility's disposal. These frequencies are used to train a series of Machine Learning (ML) and DL algorithms and were able to achieve a 93% accuracy. However, a 7% attack misclassification rate is high since it leaves the grid prone to a lot of attacks. Moreover, the authors did not assume any normal load fluctuations making attack classification straightforward.

This discussion demonstrates the lack of proper countermeasures for dynamic attacks on the level of the power grid as well as the EV ecosystem. Additionally, the current EV-based attack detection mechanisms in the literature are not optimized for the detection of LA attacks in general and dynamic attacks specifically.

2.6 Related Work: EV Support of Grid Operation

Multiple studies have considered using EV charging to support the power grid in its steady-state operation. The work in [77] for example discusses the scheduling of EV charging at non-unity power factor to inject or draw reactive power into the grid. The reactive power flow is then included in the optimization of the EV charging schedule [77]. This strategy reduced the overall cost of EV integration into the distribution grid and improved voltage steady-state stability [77]. A similar study was performed in [78] in which the bidirectional EV charging is optimized to perform peak shaving for the grid during peak demand times. EVs were also considered in [79] as a virtual distributed storage system to mitigate the intermittency of wind generation. The EV charging is optimized to store excess wind generation and then inject it back into the grid at times when wind generation is lower than expected. Another EV usage to support the power grid was suggested in [80] where the authors suggested a local control scheme for 3-phase EV chargers coupled with photovoltaic inverters to balance 3-phase distribution grids. The EVCSs would draw the power from the lightly loaded phases while the inverters inject power into the highly loaded phases. The authors were able to improve 3 phase balance and reduce the power losses by 28%. Other studies have considered EV-based frequency regulation mechanisms against disturbances caused by renewable energy intermittency [81] [82] [83]. As a result, the control mechanisms in [81] [82] are designed to handle frequency deviations below 0.07 Hz. Furthermore, the work performed in [83] is designed to deal with frequency fluctuations below 0.06 Hz with the occasional sudden spike or drop in renewable energy output power. As such this study is optimized to deal with a single sudden spike or drop in generation and not persistent LA attacks. On the other hand, in our work, we will utilize the EVs to support the small-signal stability of the transmission grid against persistent LA attacks by treating these attacks as persisting disturbances to be attenuated through the action of our EV-based mitigation scheme.

The work in [61] also proposed a mitigation scheme against LA attacks. However, the developed methodology was based on optimizing the number of buses and loads that need to be protected to significantly diminish the attack impact. However, no practical protection mechanism was suggested, and the authors relied solely on the assumption that a protected load can no longer be compromised. This assumption is rather simplistic, especially since securing IoT devices and loads

sometimes requires a total recall of the product which is extremely prohibitive. A far more realistic countermeasure against cyber-attacks meant to induce frequency oscillations was suggested in [84]. They studied the impact of cyber-attacks on the performance of WAMS systems and developed a protection mechanism against such attacks. While promising, their work is limited to attacks that induce oscillations in the range of 0.05 Hz. The suggested mechanism cannot support the grid in the case of dynamic attacks that induce oscillations in the range of a few Hertz.

2.7 Related Work: Grid Reconnaissance Techniques

Attackers with knowledge of the power grid can craft smarter attacks that target the power grid with smaller numbers of compromised EVs and still disrupt the power grid operation. Attackers can gain access to knowledge from the power utility by exploiting multiple techniques. These techniques include (i) insider information [85], (ii) compromising the data centers of the utility [85], (iii) injecting malware into the utility's systems [85], (iv) eavesdropping on the control center communication [85], (v) weakness in network and communication devices [86], third-party services [86], and intrusion through the supply chain [86]. Also, there is a lack of widespread employment of cybersecurity personnel as well as the lack of cyber hygiene for utility employees. Attackers can also introduce malware into the utility's control system through insiders (knowing or unknowing) The Stuxnet attack shows how malware can be introduced into the system by an insider [9]. Malware can also be delivered by compromised software updates like the SolarWinds hack [6] that infected users such as the U.S. Department of Energy and Department of Homeland Security. Multiple studies have considered the estimation of power grid topology by monitoring the measurements of the power grid [87], [88], [89], [90], [91], [92], [93], [94], [95]. Some grid topology estimation methods are summarized as:

- Monitoring voltage and loads at terminal buses and extrapolating the topology based on their observed relation [87] [88].
- MILP programming and monitoring the response to load perturbation [89].
- Perturbing inverter injections and monitoring system reaction [90].

- Monitoring grid response to load perturbation and optimizing the estimated parameters to fit the response [91] [92] [93].
- Machine Learning (ML) approximation of parameters and line impedances based on PMU measurements [91] [94] [95].
- Using public data published by equipment manufacturers to obtain system parameters [68].
- Identifying the frequencies of the grid modes through analysis of line measurements following an induced fault [57] or after injecting a chirp signal [58].
- Using the public data of the high-voltage transmission grid, power plants, and renewable energy generation published online by utilities such as the U.S. Energy Information Administration [96] and the European Network of Transmission System Operators for Electricity [97]. Further granularity can be obtained by using the public data published by distribution system operators or regional utilities such as the New York Independent System Operator dashboard [98] that publishes historical and real-time load, generation, and load flows.

Chapter Three

Examining the Electric Vehicle Ecosystem: Security and EV Charging Load Nature

The contributions included in this chapter can be summarized as:

- We present an overview of the different vulnerabilities in the EV charging ecosystem as well as demonstrate multiple attack scenarios against the power grid by utilizing these vulnerabilities.
- We discuss the non-linear nature of the EV load and demonstrate how these attacks can be more harmful than traditional residential and IoT loads. We then present an attack formulation method that takes advantage of the grid conditions to maximize the attack impact through the least number of compromised EVs.
- Finally, we suggest mitigation measures to address the vulnerabilities discussed in this chapter as well as 2 detection mechanisms tailored to detect EV attacks against the power grid.

3.1 EV Ecosystem Exploits

Being IoT devices that adopt multiple communication platforms and web applications, the EV infrastructure inherits the vulnerabilities of the adopted technologies [99]. The pressure to achieve rapid expansion has also been considered a great hindrance to the secure deployment of the EV infrastructure. Operators and manufacturers often forgo security measures to achieve faster and cheaper deployment of their equipment. Due to the connection of the EV infrastructure to the power grid, the secure operation of EV charging is considered pivotal for the security of the smart

grid. To this end, we present the following insight into the security issues surrounding the EV ecosystem. The US Department of Transport mentions the following four vulnerabilities [36]:

- EV/Charging Infrastructure Lacks Cybersecurity Best Practices: The EV industry lacks secure software design and development methodologies.
- EV/Charging Infrastructure Lacks a Trust Model: There is no agreement on a secure communication standard for communication between EVs and the EVSCs.
- EV/Charging Infrastructure Lack Cybersecurity Testing: There are inadequate integrity protections and there are limited cybersecurity monitoring tools to detect malicious activity.
- Commercial Charging Infrastructure Lack Physical Security: Most EVCS are exposed and can be physically accessed and tampered with. Different EVCSs have different physical features.

Given the mentioned vulnerabilities, this section discusses possible EV ecosystem exploits and provides an examination of these vulnerabilities that can ultimately be used to infiltrate into the EV ecosystem and used as an attack vector against the power grid [66]. The National Institute of Standards Technology [100] classifies attacks against the EV ecosystem as:

- Physical: EVCSs lack physical security and malicious actors can damage the EVCS, steal electricity, or even install malware through the available USB ports. EVCS can even be blocked at public locations by parking Internal Combustion Engine vehicles in front of them (known as ICEing) to cause a denial of service.
- Local: This exploit is based on gaining logical access to the EVCS through firmware vulnerabilities. The firmware updates of some vendors such as Schneider Electric are available online and can be disassembled, and reverse engineered by attackers to find their weaknesses and possible entry points into the system [36] [101]. Kaspersky Labs was able to reverse engineer the firmware of ChargePoint home chargers [102].
- Limited Remote: Attackers can take advantage of Local Area Networks at homes or public charging locations to access the EVCS. These networks usually employ weak credentials and outdated encryption techniques. The communication between the EV and the EVCS takes place through a set of protocols over the charging line adding vulnerabilities to the system.
- Remote: As mentioned above, EV users communicate with the EV management system online. Whether this communication takes place through a webpage or a mobile application, it creates

a plethora of entry points for malicious actors. Furthermore, the EVCSs communicate with the EV management system through protocols such as the OCPP.

3.2 EV Vulnerabilities

As cyber-physical systems, each of the EV's components has its specific vulnerabilities. Communication over the CAN bus takes place in a peer-to-peer manner which allows malware to be injected by an attacker that compromises just a single ECU. Attackers can also eavesdrop, replay, and spoof CAN messages. Moreover, to ensure fast communication the CAN bus lacks any sophisticated encryption and authentication. Thus, all communication takes place in plain text to ensure swift data transfer over a limited bandwidth channel. An entry point for an attacker into the CAN bus is the OBD port. The OBD port is accessible physically or remotely through smartphone apps and EV monitoring devices throughout the production cycle and lifetime of the EV via wireless or cellular networks. The compromise of the CAN bus can be used to tamper with the EV's charging process. USB ports, SD card readers, and touch screens are used for software updates and interaction with the EV. Attackers can inject malware through these channels to compromise the ECUs. Smartphone connection to the EV leaves it vulnerable to eavesdropping, reverse-engineering the encryption raising security concerns related to their usage. Original Equipment Manufacturers (OEMs) wireless updates are vulnerable to Man-in-the-Middle attacks where attackers can eavesdrop, deny, or send malicious update packages to the EVs. Also, EVs can be accessed through mobile or web-based apps for monitoring and control purposes. Smartphones are also connected to the dashboard via Bluetooth or USB ports.

3.3 EV Charging Station Vulnerabilities

Just like EVs, EVCs have internal vulnerabilities and communication channel vulnerabilities. Internal communication takes place using LAN and RS232 under legacy Linux kernels with weak

passwords, hash functions, and unnecessary root privileges. Software updates are usually unsigned and can be easily extracted and tampered with. USB ports and touch screens leave EVCSs vulnerable to physical tampering by attackers. USBs allow attackers to copy and modify EVCS configuration or upload malware to an EVCS. Phone and web apps, especially those developed by third parties, contain bugs and vulnerabilities that can be used to compromise the EV charging process. OEM wireless malicious update packages to the EVs.

3.4 EV to EVCS Communication Vulnerabilities

The IEC and ISO protocols define the communication between the EV and the EVCS over the charging line bundle. However, this communication has the vulnerabilities explained herein.

3.4.1 IEC Vulnerabilities [103] [104]

IEC protocols are well established in the control of substations but have also been included in the EV ecosystem. These protocols define multiple aspects of EV charging, but we only mention two of them herein. IEC 61850-90-8 fulfills smart charging requirements and has considered other standardization efforts from the beginning. However, basic functionality for EV charging like user authentication was considered outside the scope of this protocol and was delegated to other protocols like OCPP or other IEC protocols. IEC 61851-1 defines a safety-related signaling mechanism between EVs and EVCS based on Pulse-Width Modulation (PWM). The PWM signal is transferred over the control pilot pin of the charging cable as demonstrated in [53].

3.4.2 ISO 15118 Vulnerabilities

The ISO/IEC 15118 defines an international complementary standard to IEC 61851-1 and provides bidirectional digital communication [104]. However, ISO 15118 is not demand response compliant and does not devote a space for privacy except by stating that private information shall only be transferred, when necessary, to the intended addressees [105]. External studies have highlighted

the potential privacy concerns related to the usage of this protocol [105] and the work done in [53] even performed a real-world attack campaign. The authors of [104] [53] and [105] highlighted some weaknesses in the protocol or the improper use of the available security measures. These security measures, however, are optional and have been mostly ignored by manufacturers and operators to reduce cost and overhead leaving the communication vulnerable to attacks.

- Signal-Level Attenuation Characterization (SLAC) is a protocol that can operate in a secure mode, with mutual authentication and encrypted communication. Despite the availability of secure SLAC, it is only used if implemented by both entities. Furthermore, ISO 15118 operates mostly in plaintext mode, delegating message security to TLS (Transport Layer Security).
- TLS encryption is supported by this protocol but is dropped when the charging session is authorized by an external source such as RFID (Radio-frequency identification) cards, mobile app networks, or manually by an operator.
- Public key infrastructure can also be implemented with ISO 15118.

The authors of Baker et al. [53] developed an EM eavesdropping tool to exploit the vulnerabilities of the ISO15118 communication that takes place over the charging cable. Their work demonstrated the vulnerability of power line communication (PLC) and proved the widespread nature of the problem highlighting the privacy issues and user tracing that is possible through such a tool.

The implementation of PLC or the CAN protocol over the control pin makes this communication susceptible to eavesdropping. The nature of PLC itself makes it ideal for wireless observation. The single-ended signal is radiated making the wire behave like an antenna. Although The signal itself does not leak over the powerline, its gradient can be observed. Observing this gradient is equivalent to observing the change in voltage levels as seen in Figure 3-1.

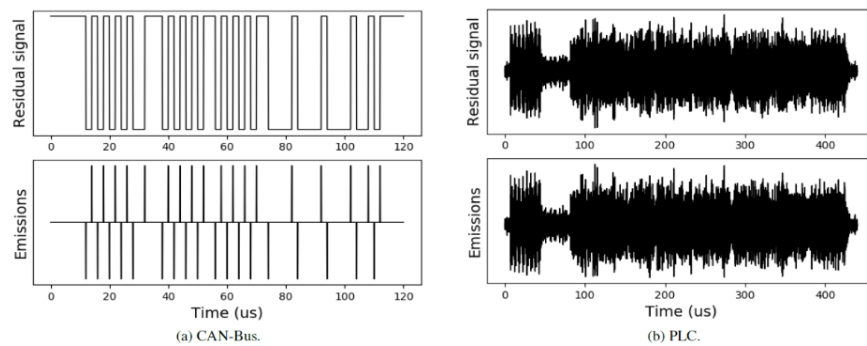


Figure 3-1: Signals emitted by communication of charging cable [53]

The recovery of the gradient allows an attacker to reconstruct the original signal. The eavesdropping attack becomes as simple as having the receiver near the line to capture the radiated signal. This receiver bears many similarities to a WiFi receiver, in concept, albeit the different protocol dictates different demodulation specifications.

The weak or absent security and encryption of this communication make it even easier for the attackers to eavesdrop. Although TLS and public key infrastructure are also available with ISO 15118. So far, these practices are optional and have been omitted by operators and manufacturers to reduce price and overhead. This omission has left a gap in the security of this protocol. Furthermore, when a charging session is authorized by RFIDs, mobile apps, or manually by an operator, no TLS is required for communication.

Using the developed tool, the authors launched an eavesdropping campaign using 3 different EVs at 54 different locations across the United Kingdom. The eavesdropping sessions were performed at service stations, highway rest stops, superstores, and hotels. During all sessions, a leaked signal was recovered fully or partially. In 76% of the cases, the MAC address and EV ID were successfully recovered, and error-free. To the surprise of the authors, no TLS tunnel was created during any of these sessions. This highlights that even though some basic security methods are available, they are mostly ignored by operators.

3.5 OCPP Protocol Vulnerabilities [43] [103] [106]

OCPP coordinates communication and power flow between EVCS, EV management system, EVs, and the grid and allows full remote control of the EVCS in real-time. OCPP is leading the efforts towards standardization and has become a de facto open-source protocol and is currently the most widespread charging protocol. The protocol is mainly concerned with reservations and the management of charging processes. OCPP supports online monitoring and change in charging configuration, as well as starting and ending charging sessions and online billing. OCPP supports smart charging by controlling session scheduling, charging rate, and duration of charging.

OCPP communication uses simple HTTP to manage EV charging and adopts diverse communication infrastructures. Although OCPP 2.0 and 2.0.1 were released in 2018 and 2020 respectively, OCPP versions 1.5 and 1.6 remain the dominant versions deployed. OCPP 1.6 includes some functional improvements over 1.5 such as smart charging OCPP 1.6 adopts diverse communication infrastructures such as SOAP/extensible markup language or javascript object notation over WebSockets.

OCPP has an optional TLS layer for secure communication but has been mostly ignored by manufacturers and operators to reduce overhead and price. OCPP 1.5 had an optional hash function that can be used for extra security. However, instead of making it mandatory in newer versions, OCPP 1.6 eliminated this option. Attackers that can intercept the plaintext messages, might be able to disrupt the energy supply, steal electricity, or even inject fake OCPP messages to manipulate the ecosystem operation. Even in the presence of TLS OCPP is still vulnerable to impersonation attacks when an attacker manages to place itself between the EV and CMS.

The main security concern for OCPP is ensuring that a charging session is authorized by a billing system. This along with communication using plain text and the absence of wide adoption of encryption allows attackers to hijack the communication and gain control of EV charging. Some issues related to the lack of encryption can be summarized as:

- Disclosure of private information to unauthorized parties.
- Distortion of the real messages by false data injection.
- Disruption of the proper communication chain by deleting messages.

Due to the basic security measures, a malicious actor can launch a Man-in-the-Middle attack. This attacker can now direct all messages toward itself to cause a sinkhole or flood the system with replayed messages to cause a wormhole a man in the middle, can also disrupt charging rates. Injecting more current into the charging EV can severely damage the battery as well as cause sudden surges in demand (if multiple EVs are targeted). Also, when multiple charging stations/connected EVs are targeted and forced to discharge into the grid, a surge in generation will occur causing over frequency on the grid. Attackers that are unable to break the encryption, can capture messages such as those that start and terminate charging sessions and use them in replay attacks to disrupt the EV charging. OCPP 1.5 and 1.6 also offer a functionality known as

Local Authorization List, which allows an EVCS to serve customers if it is disconnected from the Management System. An attacker, however, can use this functionality to force the CMS into accepting charging requests after connection restoration without authentication.

3.6 EVCS Firmware / IoT Vulnerabilities

As mentioned above, EVCSs host firmware that controls their operation and interacts with multiple online services available for management and user interaction. As IoT devices, EVCSs exhibit the same types of vulnerabilities present in other IoT devices. In addition, web pages and phone apps used in this environment also exhibit the same vulnerabilities as other web/phone apps. These vulnerabilities are discussed in the OWASP Top 10 Application Security Risks [107] and can be discovered through the framework presented in [108]. Other vulnerabilities include malicious update packages sent to replace the authentic updates by the manufacturers like the Solar Winds Hack [6] that would allow the attacker to embed code in the deployed system and virtually control all aspects of the charging process. The most critical vulnerabilities that were proven to be present in the EV ecosystem in [36] [101] [102] and by the dedicated work in [109] are summarized below:

- SQL Injection: allows the attacker to gain access to user information and manipulate the EVCS firmware.
- XML/External Entity Injection: allows the attacker to inject HTTP requests into the system and in some cases gain remote access to the EVCS.
- Server-Side Request Forgery (SSRF): allows the attacker to redirect traffic towards internal/external endpoints causing a denial of service and reading files and logs of the EVCS.
- Cross-Site Scripting (XSS): allows the attacker to inject malicious code into the EVCS allowing them to hijack user accounts or even administrator accounts in some cases.
- Comma-Separated Values (CSV) injection: allows attackers to embed XSS payloads that get triggered and stored on the EVCS leading to hijacking administrator session tokens. Using this vulnerability, attackers can manipulate EVCS functionality.

- Cross-Site Request Forgery (CSRF): allows the attacker to induce target users to perform unintentional actions that lead to setting modification and manipulation of EVCS functionality. This weakness can allow attackers to gain control of the EVCS.
- Hard-coded credentials: are utilized by developers to ease the coding process, but they allow attackers to recover the hardcoded login credentials in the source code of the EVCS or the associated application and gain unauthorized access to the EVCS.
- Missing Authentication: allows the attacker to gain unauthorized access to user accounts without being properly verified by the EV management system.

3.7 EV Charging Mobile App Vulnerabilities [56]

The mobile application is another component that has been introduced into the EV ecosystem to facilitate user interactions as well as offer the user remote control and monitoring of their charging EVs. These mobile apps, however, may suffer from vulnerabilities that can be exploited by attackers to compromise the charging process. Extensive static, dynamic, and network traffic analysis was performed in [56] to investigate the security of a wide host of mobile apps. These mobile applications were found to suffer from vulnerabilities that allow unverified ownership of the mobile app user and the EV as well as improper authorization for critical functions such as starting and stopping charging sessions. This boils down to a severe vulnerability that allows any individual with a valid email address to create a valid account through the mobile app and control the charging of someone else's EV. This of course requires that an EV should be connected to an EVCS, yet not currently charging. These conditions were verified to actually occur in several cases when users connect their EVs and wait before starting the charging session or when users leave their EVs plugged into EVCSs after the charging session ends. The only authentication required to start these charging sessions takes place by examining the validity of the credit card that is linked to the mobile app account. Thus a state-backed adversary or an attacker with enough resources will be able to create a botnet of valid and legitimate mobile app accounts and use them to compromise a large botnet of EVs/EVCSs and launch LA attacks against the power grid. Another weakness in the current setup of the system is the inability of the EV ecosystem to link

the identity of the EV currently connected to an EVCS to the identity of the person initiating the charging session through the mobile app.

Furthermore, the work in [56] uncovered the absence of any rate limiting to the number of requests a single mobile app can send to a single or multiple EVCSs. The implications of this vulnerability are twofold. First, attackers can use this as a method to initiate DoS attacks against the charging infrastructure. When a start charging request is sent to an EVCS in the absence of a connected EV, the EVCS continuously keeps attempting for several seconds (up to 1 minute) to (i) check the presence of an EV and (ii) start a charging session. During this time the EVCS will appear busy, and no new mobile app can be used to control it. The second and more dangerous implication is the attacker's ability to utilize this vulnerability to initiate a scanning campaign against the network of EVCSs to learn user habits, i.e., connection and disconnection times, charging and idle times while connected, and finally to map the entire usage pattern of the entire EVCS network.

3.8 EV Operator's OCPP Backend Vulnerabilities

An operator's backend hosts the CMS and the OCPP server. However, these backends suffer from their own set of vulnerabilities that are not necessarily stemming from the OCPP protocol itself. When combined with the vulnerabilities in the OCPP protocol, the backend vulnerabilities allow the attacker to compromise an operator's visibility over the charging network and launch covert attacks that range from firmware theft, data collection, data poisoning, DoS against both EVCSs and the CMS itself, and attacks against the power grid through compromised charging sessions. The work in [110] demonstrated the presence of 6 zero-day vulnerabilities in these backends allowing the attackers to launch the previously mentioned attacks. These vulnerabilities can be categorized as:

- **Improper and weak authentication:** Where a phantom EVCS (a virtual Python-based EVCS) assumes the ID number of an actual EVCS and uses it to connect to the backend. The backend in this case failed to properly authenticate the identity of the connected EVCS. It is worth

mentioning that EVCS IDs are readily available online either publicly or easily attainable through device search engines (Zoomeye).

- **Improper Restriction of Communication Channel to Intended End Points:** Where the backend allows the phantom EVCS to connect to it even when the legitimate EVCS is already connected. In this case, the phantom EVCS hijacks the communication to substitute the actual EVCS and gains the same level of access to the backend.
- **Improper Control of Interaction Frequency:** Where the backend does not limit the number of EVCSs that can connect to it having the same ID.
- **Session Fixation:** Although the backend will only communicate with the last EVCS that is connected to it using a given ID, it does not invalidate the connection to the legitimate EVCS which consumes its resources and can be used for DoS attacks. Another implication of this vulnerability is the inability of the legitimate EVCS to receive communication from the OCPP backend even though the sessions are maintained.
- **Improper Restriction of Excessive Authentication Attempts:** Where the backend does not have a limitation on the number of connections and failed connection attempts with an unregistered EVCS ID. This can be used by attackers to brute force the legitimate list of EVCS IDs.
- **Reliance on a Single Factor in a Security Decision:** Which is the easily attainable EVCS ID.

3.9 EV Ecosystem Malware Landscape

Being IoT devices, EVCSs are actively being targeted by malware. The work in [111] launched an investigation into the presence of malware in the public EVCS network and was able to verify the presence of 455 EVCS infected by malware that were conducting scans on the darknet in 2023. The study discussed the presence of 4 different probing rates indicating 4 different malware families. Most interestingly, 55% of the identified malware samples exhibited the features of the Mirai family. Given that the number of global public chargers was around 2.7 million, the ratio of infections is in the same neighborhood as other IoT device infections and the proportion of Mirai infections is also in line with the ratio of other IoT device infections by Mirai. While no malware

was dedicated to EVCSs and generic IoT, malware families were discovered, the study demonstrates the feasibility of infecting EVCSs with malware as easily as any other IoT system.

One extremely dangerous repercussion of this discovery is the future feasibility of EVCS-specific malware families that can take over these chargers completely giving attackers unrestricted access to large botnets of compromised EVCSs.

3.10 Distinct Nature of EV Load and Straightforward Attack Strategy

This section examines the EV charging load properties that distinguish it from traditional IoT and residential loads making it more impactful if used to attack the power grid. This section also proposes a smart yet straightforward attack vector that is used to determine the weak buses in the power grid that the attacker needs to target to maximize the attack impact.

3.10.1 EV Charging Properties

Unlike conventional residential loads, EVs are battery storage loads that present a new concern to the power grid. Charging this battery is a non-linear process that would reduce the quality of the delivered power [112] [113]. The EV charging load would increase the reactive power demand and reduce the pf, introduce harmonics, cause voltage distortion and fluctuation, and can also cause three-phase imbalance [112] [113] [114].

EV charging is a non-linear load based on rectifier circuits and power converters [113]. Non-linear loads draw non-sinusoidal current from a sinusoidal voltage [114] causing voltage and current waveforms to have different shapes. Some mainstream EVCS utilize uncontrollable rectifier circuits having high harmonic distortion. Other EVCS that support V2G technology, utilize controllable power converters [115]. These non-linear loads contribute to a poor power quality on the grid [116]. New solid-state devices are feasible using MOSFETs and IGBTs as well as

incorporating active and passive filters into the chargers [116]. Yet these devices are costly, bulky and incur losses that reduce the overall efficiency. Regardless of the specific circuit of the EVCS, adding a large amount of non-linear load would increase the reactive power demand of the system [117]. As the work in [115] demonstrated, nonlinear loads can have a pf as low as $\text{pf}=0.15$ lagging. The authors also discussed that although power factor correctors can improve the pf, a perfect $\text{pf}=1$ is not possible due to the harmonic distortion of these non-linear loads. The authors of [112] also demonstrated that an AC-DC converter (rectifier) can have a pf as low as $\text{pf}=0.4$.

Uncompensated battery chargers have a pf slightly above or below 0.6 [117]. To make things worse, an attacker who gains control of an EVCS with controllable power converters can manipulate it to draw more reactive power from the grid [114]. As a middle ground, we consider the EV attack loads will have a $\text{pf}=0.6$ lagging [118].

Transmitting large amounts of reactive power from generators to the loads causes large transmission losses in the power lines, reduces voltage levels, and might cause severe problems in terms of grid stability. Synchronous generators (not being operated as condensers) are limited in terms of the total reactive power they can produce at a given point of active power generation [119].

On the other hand, traditional residential loads and home IoT loads have a high pf being mostly resistive. This is especially true for larger loads such as electric water heaters and space heaters that have a power factor very close to $\text{pf}=1$. Other large loads such as air conditioners and refrigerators have a power factor of $0.8 < \text{pf} < 0.9$. Although recent loads such as laptop chargers, LED lights, and smart TVs are power electronic-based and have a nonlinear load, their size and overall contribution to the total residential load remains acceptable where the average residential load is usually considered to be higher than $\text{pf}=0.8$. Due to this distinct nature and size of the EV loads, their impact will be much larger than that of the residential and IoT loads.

3.10.2 Straightforward EV Attack Vector

Attackers with knowledge of the power grid can determine its weakest buses and craft attacks with smaller numbers of compromised EVs and still disrupt the power grid operation. Attackers can gain access to power grid topology information by utilizing one of the strategies presented in

Chapter 2 Section 2.7. The attacker can utilize the following strategy to determine the grid's weakest buses.

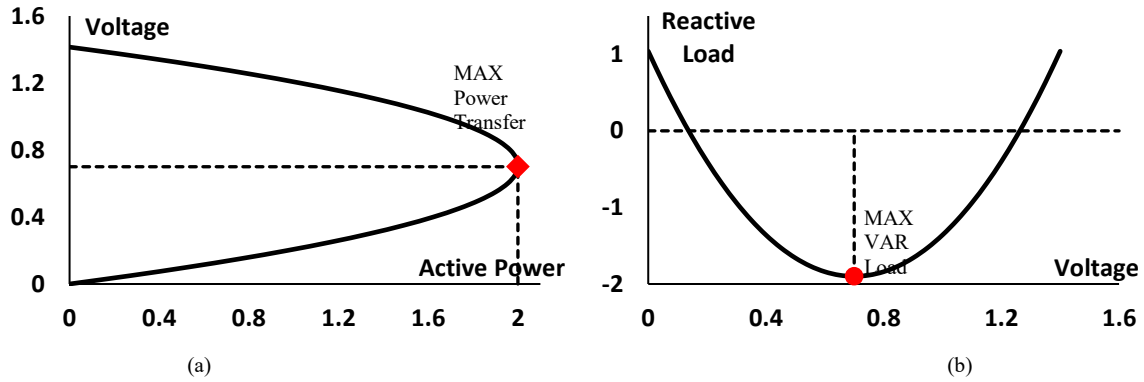


Figure 3-2: (a) Typical PV curve and (b) typical QV curve based on PowerWorld Manual on PV and QV Curves

3.10.2.1 PV and QV Curves

PV curves monitor the voltage at target buses due to load and generation increases in the system. The curve is generated by selecting a set of loads and increasing them incrementally. Specific generators are selected to supply the extra load. At each iteration, the power flow equations are solved, and the voltage value is recorded. A curve like Figure 3-2 (a) is generated where the knee point, marked with a diamond, represents the maximum extra load that can be added before voltage collapse occurs. QV curves monitor the voltage at a bus due to increased reactive power demand in the system. The curve is generated for a certain bus by adding a fictitious generator at that bus and varying the VAR output. A curve like Figure 3-2 (b) is generated where the valley point, marked with a dot, is the maximum reactive power that can be drawn before voltage collapse.

3.10.2.2 Attack Strategy

The attacker can perform grid reconnaissance and generate the PV and QV curves for the system buses to determine the active and reactive load needed to cause the collapse. However, the attacker can use these methods to locate the weakest buses that are more likely to cause larger disturbances once attacked. By attacking these buses, the attacker can disrupt the system while simultaneously minimizing the needed number of compromised EVs to reduce the attack cost and difficulty.

The V2G capability of the EVs can also be incorporated by considering it as part of the generator vector in the PV curve. These stability methods can be performed for the system base case as well as in the presence of contingencies. Attackers that can simultaneously launch physical attacks,

such as disconnecting lines, can use this option to determine their attack impact beforehand. These PV and QV curves can also be plotted to take into consideration the presence of VAR compensators and tap-changing transformers. By utilizing these features, the attacker can craft an attack to circumvent these protection methods.

3.11 EV Botnet Command and Control

The EV ecosystem can pose a threat to power grids since EV charging/discharging can add significant load/generation into the grid. Moreover, the complex and interconnected EV ecosystem, in Figure 3-3, can be used by adversaries to launch their attacks. This figure also indicates the possible entry points for attackers into the system. These entry points allow attackers to manipulate EV charging loads. We reiterate herein the specific vulnerabilities that can allow an attacker to hijack the EV charging process and target the power grid stability.

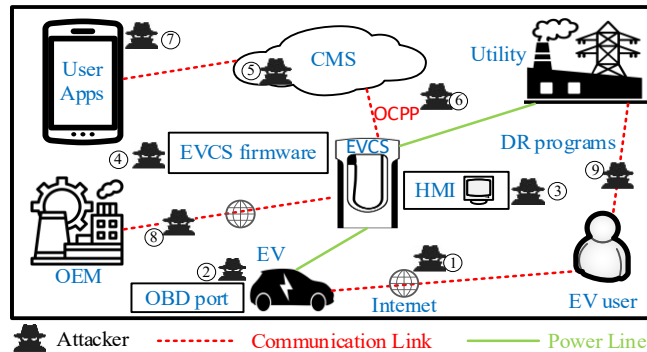


Figure 3-3: Simplified model of EV ecosystem and possible attacker entry points

An EV's internal systems have internet connectivity, which can be used by attackers to compromise the EV and its charging process [37] (attack①). The On-Board Diagnostics (OBD) port can be accessed physically or wirelessly and grant an attacker access to the EV's Controller Area Network (CAN) bus (attack②). The CAN bus is connected to all the EV's internal systems and does not utilize any encryption, giving the attacker control over all the EV's systems including the charging process [37]. EVCSs have a Human Machine Interface (HMI) for users to initiate charging sessions manually. This HMI includes physically accessible USB ports that can be used

by attackers to inject malware into the EVCS and consequently all connected EVs [37] (attack③). EVCSs also host firmware that acts as their local management software to control all their functions. This firmware transforms an EVCS into an IoT device, which is exposed to the same attack types as traditional IoT systems. SQL injection, XML injection, and Cross-Site Scripting are among the firmware vulnerabilities that allow attackers to manipulate EV charging [66]. In addition, these systems run on legacy Linux kernels and simple hardware with weak authentication which allows attackers to obtain admin access and tamper with EVCS operation [66]. Attackers can also infect EVCSs with malware that is controlled by a botnet grand master [111]. This grand master can synchronously and autonomously control the functionality of the EVCS based on the attacker's pre-determined strategy (attack④).

The EV CMS is the software that remotely manages public EVCS charging and other functionalities. This cloud-hosted software is prone to get hacked if not properly secured (attack⑤). To achieve bidirectional communication between the different components of the EV ecosystem, specific protocols have been used, among which the OCPP is the most common. OCPP is used for communication between EVCSs and the CMS. This protocol uses simple HTTP to manage the charging sessions [66]. Also, the optional Transport Layer Security (TLS) encryption scheme has mostly been ignored by operators [66] to reduce overhead. This leaves the OCPP vulnerable to Man-in-the-Middle attacks allowing attackers to gain total control over the operation of the EVCSs including starting and stopping charging sessions (attack⑥). Furthermore, phone applications are used to allow remote user control over EVCS operation. These applications, especially ones developed by third parties, contain bugs and design flaws that allow attackers to control and manipulate the operation of EVCSs with connected EVs [56] (attack⑦). Also, if the phone is compromised that would give the attacker access to these applications. Original Equipment Manufacturers (OEMs) of the EVCSs also maintain internet communication with their EVCSs to roll out updates. This communication link can be used by the attackers to gain direct access to the EVCSs, similar to the Russia EV attack [32] (attack⑧). The majority of EVCSs utilize OCPP 1.6 meaning their firmware update process takes place over plain HTTP which can be exploited by attackers to install their own malicious firmware with minimal effort. In addition, even the OCPP 2.0.1 secure update procedure can be contaminated with malicious software, similar to the SolarWinds attack. This malicious update can be used to tamper with EVCS operations. Finally, utility demand response programs rely on interactions between the utility and

EV owners to schedule EV charging [120]. Such programs are vulnerable to some types of attacks if automated (attack©).

3.12 EV Attack Feasibility

Being an integral part of the power grid, the security of the EV ecosystem seriously impacts the secure grid operation. By exploiting the EV ecosystem’s vulnerabilities, attackers can manipulate EV charging to disrupt the grid [121]. The following section discusses how attackers can locate EVCSs, the attack feasibility, and the vulnerabilities needed to control the EV’s charging load.

3.12.1.1 EV Locations

Attackers can locate EVCSs using publicly available maps provided by the EVCS operators or by third parties. Chargepoint for example offers maps that contain the locations of EVCS offered by them and other manufacturers [122]. Other maps are offered on websites such as Plug Share [123], Chargemap [124], and the Alternative Fuels Data Center (AFDC) [125]. The work in [56] also mentions tens of such applications that provide live data on the EVCS network status as well as other statistics on historical usage. Using this data, attackers can know the location, power rating, and historical utilization profiles of EVCSs to plan the attack. Additionally, the EV charging mobile apps can be exploited as discussed in Section 3.7 to conduct reconnaissance of the EVCS network and its utilization.

3.12.1.2 EV Load Size

To demonstrate the number of EVs and the EV load in comparison to the total system load we present the following discussion. We acknowledge that the current number of EVs might not be sufficient to cause the intended damage, but the following discussion demonstrates its future possibility. To demonstrate this, we choose the New South Wales (NSW) grid on a day in December 2021 [126]. The average load is 6968 MW [126] and the total registered vehicles are 5,892,206 [127]. As per the IEA [128] EVCS operators, utilities, and governments have maintained a ratio of 1 public EVCS for every 10 EVs on the road to guarantee the quality of

service. Furthermore, according to the IEA [128], based on the mixture of different EVCS rates, the average charging rate is 24 kW per EVCS. Table 3-1 demonstrates the total public EVCS load in MW at different EV penetration levels and charging rates under the assumption of 1 public EVCS per 10 EVs.

Table 3-1: Maximum Potential Public EVCS Load in MW vs EV Levels and Charging Rate

EV Penetration Level	Level 2 EVCS		Level 3 EVCS		Global Average Rate
	11 kW	19 kW	40 kW	360 kW	24 kW
10%	649	1,120	2,357	21,212	1,415
20%	1,297	2,240	4,714	42,424	2,829
30%	1,945	3,359	7,071	63,636	4,243
40%	2,593	4,479	9,428	84,848	5,657
50%	3,241	5,598	11,785	106,060	7,071
60%	3,889	6,718	14,142	127,272	8,485
70%	4,537	7,837	16,499	148,484	9,899
80%	5,186	8,957	18,856	169,696	11,314
90%	5,834	10,076	21,212	190,908	12,728
100%	6,482	11,196	23,569	212,120	14,142

Table 3-1 shows how even with the rate of 1 public EVCS for every 10 EVs, the EV load can still surpass the total grid load. To gain further insight, we will also consider the EVCS occupancy which would result in smaller EV loads on the grid. For the sake of demonstration, if we consider a 50% EV penetration level, this will mean the presence of 294,610 public EVCSs in the NSW grid. With an average occupancy rate of 31% [129], we can estimate the number of connected EVs to the grid on average to be 91,329. From the presented statistics, we can estimate that at a 50% EV penetration level, there will be 2,192 MW of EV load connected to the grid on average at public EVCSs (a third of the grid's load). This is equivalent to 31% of the total grid load on average. Given that the attacks herein only require an attacker to compromise a total EV load equivalent to 3% to 13% of the grid's load, this attacker will require a third of the connected EVs to perform the attack.

Furthermore, there are roughly 9 private EVCSs for every 10 EVs [128]. This means that at 50% penetration, there will be over 2.6 million private EVCSs. Given the user tendency to connect EVs to home EVCSs even if no significant charging is needed, there will be large numbers of EVs connected at residences. Once combined, the numbers of total EVs connected to the grid through both public and private EVCS can give an attacker much larger loads than needed to successfully

launch the proposed dynamic EV attack. Another aspect to consider is using the EVCSs located in residences is their impact on the distribution grid. The work in [130] demonstrated residential EV attacks against the transmission system that have no impact on the distribution grid's stability but whose aggregate impact causes the transmission lines to be overloaded and tripped.

3.13 Case Study: EV Attacks Against the Power Grid

Power grid stability depends on the balance between the demand load and generation supply. EVs can be used to perform the same types of attacks as residential loads to disturb this balance and new attacks not previously possible through other loads. However, the special nature of EV loads presents a surface for attacks that were previously not possible. Attacks through the EV charging load can cause larger disturbances while utilizing smaller loads. In addition to that, due to the nature of power grids, the frequency can sharply increase or decrease in response to sudden drops or spikes in loads. Voltage also needs to be maintained within acceptable limits, usually 5% of the nominal value, and is tightly connected to the reactive power flow. Due to the nature of generators and power systems, reactive power is more difficult to generate and push onto the grid than active power [117]. Due to the nonlinearity of battery charging, an EV load's high reactive power demand would have a larger impact on the voltage.

When voltage and frequency violations exceed a given limit, utilities take corrective action to restore the normal levels to avoid damage to the grid. Persistent violations can cause the operator to start load shedding and eventually force the grid to go into a blackout. In the following section, we discuss the possibility of EV attacks and then present general EV attack scenarios and others specific to EVs. We also compare the impact of the EV load to the impact of traditional residential loads when used to attack the grid. We then perform simulations to demonstrate the attack results.

3.13.1 Simulation Setup

To demonstrate the impact of the attacks, we perform simulations on the WSCC 9-bus system shown in Figure 3-4 and the Glover 7-bus test case taken from the Glover et al textbook [131]

38

- Machine Model: GENSAL
- Generator Exciter Model: IEEE T1
- Turbine Speed Governor: IEEE G2
- Power System Stabilizer based on IEEE Std 421.2
- EV V2G injection: Negative fixed MW/MVAR load to represent a controlled power injection.

3.13.2 EV Load Manipulation Attack Scenarios

EVs can be used to launch the same types of attacks as any residential load such as manipulating the power demand to cause line trips and cascading failure. This is demonstrated by attacking the 7-bus system. Through the controlled EVCS mass synchronized charging can be initiated to increase the demand at bus 3 by 50 MW of EV load (82 MVA). This would cause the line connecting bus 1 to bus 3 to overload and trip. After this initial trip, the line connecting bus 2 to bus 3 would be overloaded and would trip. Subsequently, the lines L3-4, L2-4, and L2-5 would be overloaded leading to multiple failures followed by a blackout.

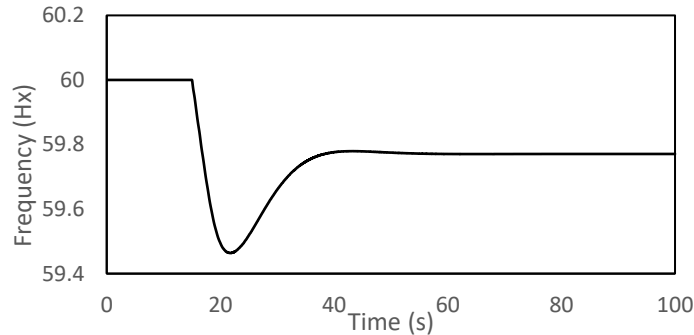


Figure 3-6: Frequency drop on 9-Bus System due to increased demand 2000 EVs

Another attack that takes advantage of load manipulation is creating a surge in demand to cause a frequency drop on the power grid. Such an attack is simulated against the 9-bus system by adding 7.2 MW of load representing 650 EVs charging at 11k W level 2 EVCSs at each of the 3 load buses. The attack was launched at $t=15$ seconds and the frequency response is presented in Figure 3-6. Due to the increased power load, the generators would slow down resulting in a frequency drop in the power grid. When the frequency drops below the preset threshold, the generators are disconnected from the grid eventually leading to further reduction in frequency and possibly a blackout. This attack can be made worse by initiating it during peak times when the grid has fewer

reserves to supply the extra demand. Also, when the renewable energy resource (RES) share is high, the attack can have a larger impact due to lower grid inertia.

3.13.3 EV-Specific Attack Scenarios

The nature of EVs allows for new types of attacks not available through traditional residential loads. These attacks are made possible through the V2G power flow feature that allows EVs to inject the energy stored in their batteries into the grid. This feature, however, can be maliciously exploited by attackers to create injections that can disrupt the grid operation. In fact, attackers can inject power at a pf controlled by them to maximize the attack impact causing disruptions larger than attacks that reduce the load. The power injection is even more impactful than adding a generator because the injection does not participate in generation control and voltage control. This attack would also greatly impact the grid's pf, giving this injection a larger impact on the voltage and frequency. Two attacks that utilize this feature are presented below.

3.13.3.1 Controlled V2G Attack

To demonstrate this attack, we added a negative load of -50 MW and -10 MVAR at bus 5. A negative load would resemble a power injection by a botnet of compromised EVs forced to discharge at the same time. As discussed earlier, this sudden injection would disrupt the balance between the total load and total generation causing frequency and voltage violations. The attack was performed by initiating the power injection at $t=15$ seconds which caused a frequency rise and voltage violations at multiple buses. Due to the imbalance between the extra generation and the load, the system frequency rises to 61.6, and the generators' rotational speed increases causing the frequency behavior represented in Figure 3-7.

Similarly, Figure 3-8 represents the voltages at buses 4, 5, 7, and 9 that increase due to the added generation. The voltage at all buses experienced an increase above 1.05 pu during the transient response, but these graphs represent the voltage at the buses that remained greater than 1.05 after the system went back to steady-state. The same experiment was performed by replacing the power injection with a generator to compare the impact of a controlled injection to a regular generator. This alternative attack resulted in smaller violations and required 51 MW to reach the edge of the frequency limit of 61.5 Hz (but not cross it) and caused no voltage limit violations. This

demonstrates that a smaller controlled V2G power injection has a higher impact than a power imbalance caused by excess generation from a rotating generator. The V2G injection attack causes instantaneous generator tripping while the 51 MW imbalance remains shy of achieving the same.

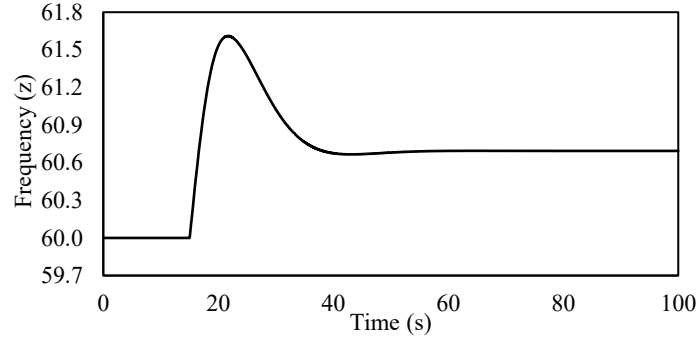


Figure 3-7: Frequency rise on 9-Bus System due to power injection

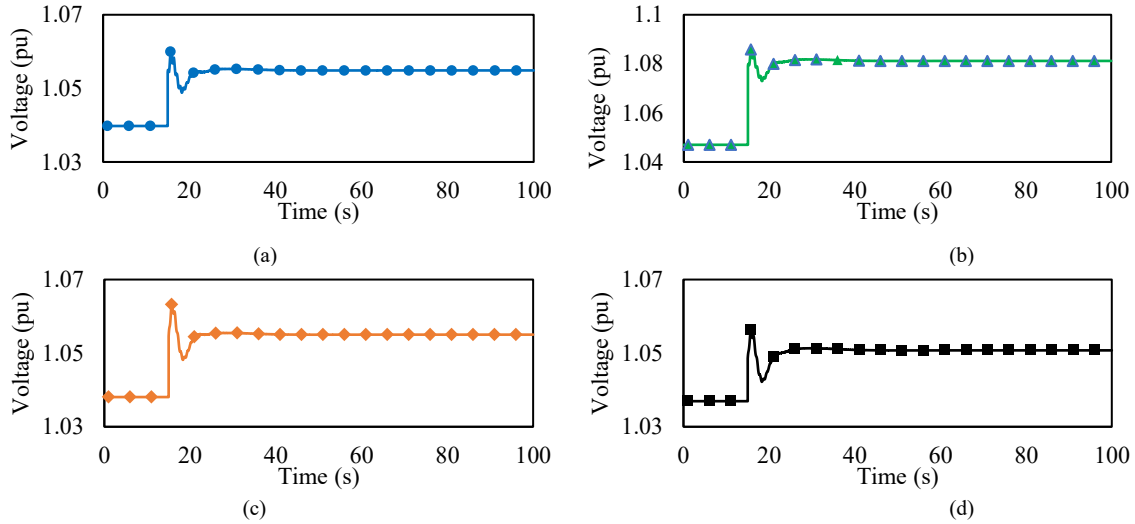


Figure 3-8: Voltage limit violation at (a) bus 4 (●), (b) 5 (▲), (c) 7 (◆), and (d) 9 (■) due to power injection

3.13.3.2 Switching Attacks

The second type of attack is a switching attack, which is performed by alternating between increased power injection and increased power demand. This attack is initiated by increasing the power demand to cause a frequency drop as in the attack in Section 3.13.2. The second step of this attack happens when the system starts its recovery. The attacker would switch off the EVCSs initiated in the first step and initiate a power injection to cause a frequency increase that is amplified by the operator's effort to increase the speed in response to the extra load. The attacker would then alternate between these steps for the desired duration.

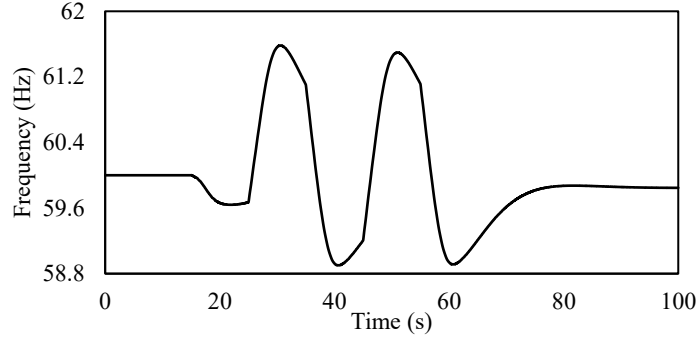


Figure 3-9: Transient frequency response to the switching attack

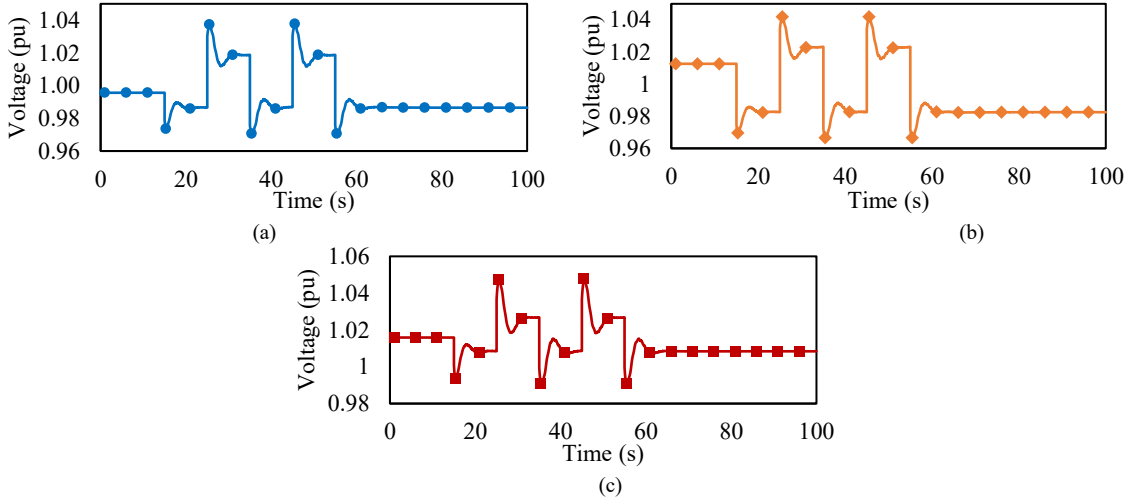


Figure 3-10: Transient voltage response at load (a) bus 5 (●), (b) bus 6 (◆), and (c) bus 8 (■) due to the switching attack

We simulate this attack against the 9-bus system by adding a 21 MW (highly inductive) load at bus 6 representing 1900 EVs charging at 11 kW and a negative 60 MW load (power injection) at bus 5 representing 5400 discharging EVs. The attack is initiated by closing the load at bus 6 at $t=15$ seconds then opening it and closing the V2G injection at bus 5 at $t=25$ seconds. This process is repeated at $t=35$ seconds, 45 seconds, and 55 seconds. This attack causes the frequency to fluctuate as depicted in Figure 3-9 as well as frequency limit violations while simultaneously causing the voltage fluctuations at the load buses shown in Figure 3-10. A similar effect is achieved by adding 21 MW (highly inductive) load at each of buses 5 and 6 and a 21 MW V2G injection at the same buses and alternating between them. The importance of a switching attack is that it does not require huge loads or injections to cause the behavior depicted in Figure 3-9 and Figure 3-10. Even when the compromised EV numbers are much less than in the example above, a sustained switching attack can cause frequency and voltage oscillations hindering the system's return to normal operation. A sustained load oscillation would damage the turbines due to the constant

acceleration and deceleration. Other equipment such as transformers might require more frequent maintenance intervals if the attacks are sustained for long durations. The performance of the appliances connected by the consumers might be impacted as well but this is beyond our scope.

Another variation of the attack that amplifies its impact is when the V2G injection at bus 6 is accompanied by a demand drop at bus 5. The normal demand at bus 5 is 125 MW. When this demand is decreased by 20% simultaneously with the power injection, the frequency response goes over 62.5 Hz. This would trigger multiple protection mechanisms further exasperating the problem depending on the grid protection mechanisms and the regulations (varies by geographic location). This frequency deviation would trip all the generators instantaneously and cause a blackout.

3.13.4 Other Attack Implications

Even when the controlled botnet of compromised EVs is not large enough to cause frequency and voltage violations, the attacker can still launch attacks that disrupt power grid operation. By increasing the demand even by moderate amounts, an attacker can shift the system away from the optimal dispatch point and cause extra costs to be incurred on the grid. EV charging is usually scheduled during low-demand periods to benefit from the low electricity cost. However, when an attacker forces the compromised EVs and EVCSs to charge during peak times, the increased load on an already taxed grid would cause increased transmission losses, voltage imbalance, and the use of peak load generators. The latter are generators available to the utility to supply loads when the baseload generation units cannot serve the entire demand. Peak generation units are generally more expensive to operate but are used due to their flexibility and ease of ramping up the generation and short startup time. Also, the increased cycling of these units between on and off would require shorter maintenance intervals and increased maintenance costs.

Sudden spikes in demand or generation also cause oscillations in the generator output. The increased variation in generator output can also have an impact on the lifetime and maintenance frequency of the generators. The increased load, especially the reactive nonlinear EV load, would add Time Distortion Harmonics into the system. EV attacks can also theoretically be used to hide transmission line outages like FDI attacks [134]. By manipulating the load at both ends of a disconnected line the attacker can hide the line outage from state.

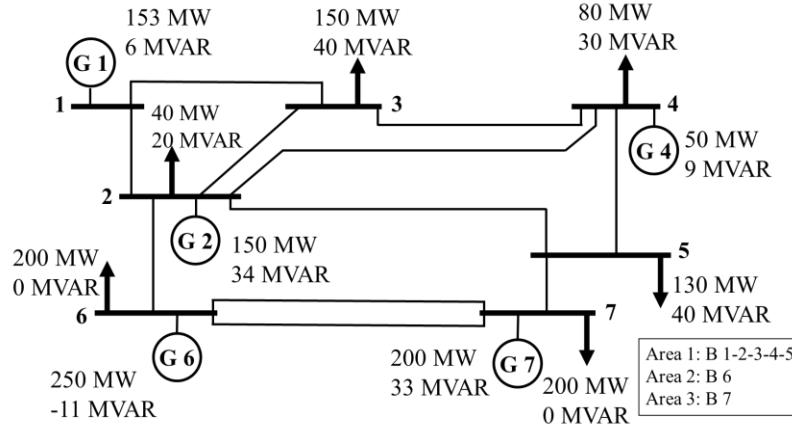


Figure 3-11: Modified 7-Bus System

3.13.5 Comparison to non-EV Attacks

In this sub-section, we aim to demonstrate how attacks launched through EV loads can be more impactful than those launched through traditional residential loads. For this purpose, we will simulate our results on a modified version of the 7-bus system presented in Figure 3-11 also taken from Glover et al [131]. The total load on this system is 800 MW and the transmission line limits have been increased. The Optimal Power Flow has been solved on PowerWorld and the extra load to be supplied will be divided among the generators based on the cost of the extra generation.

3.13.5.1 Residential/Home IoT Load Attack

We will first perform an attack using traditional residential loads having $\text{pf}=0.8$ as described in Section 3.13.2. This attack was simulated by adding a load of 48 MW (60 MVA) divided equally on each of buses 2, 3, 4, and 5 (12 MW each). The sudden load increase at $t=15$ seconds causes a frequency drop as demonstrated in Figure 3-12. Although the frequency dropped to 59 Hz, the system was able to maintain transient stability as all the areas, and generators remained in synchronism and the values returned to a steady value. As for the steady-state stability, the system did not exhibit any voltage violations and all parameters remained within acceptable limits. After the system stabilizes, the system operator could ramp up generation beyond the automatic control to go back to the nominal frequency. This is to demonstrate that although the frequency dropped to 59 Hz which might initiate load shedding, the system was not completely destabilized as the case is for the attacks in the following subsections.

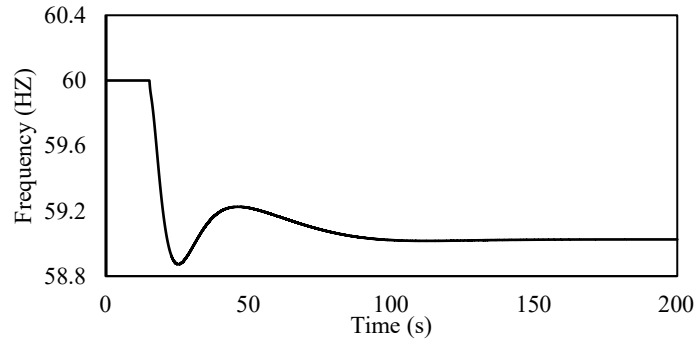


Figure 3-12: 7-Bus System: transient frequency response after the 48 MW attack

3.13.5.2 EV Load Attack – Similar MW load (4400 EVs)

The first EV attack is launched against the same locations as the attack in Section 3.13.5.1 (bus 2, 3, 4, and 5). This attack was performed with an EV load having the same active power demand of 48 MW. At the $\text{pf}=0.6$ assumed for this type of load, the apparent power is equal to 80 MVA instead of the 60 MVA of the previous attack. This attack represents a synchronized mass charging of 4400 EVs charging at a rate of 11 kW. The EVs are split equally among the 4 buses leading to 4 equal loads of 12 MW (20 MVA).

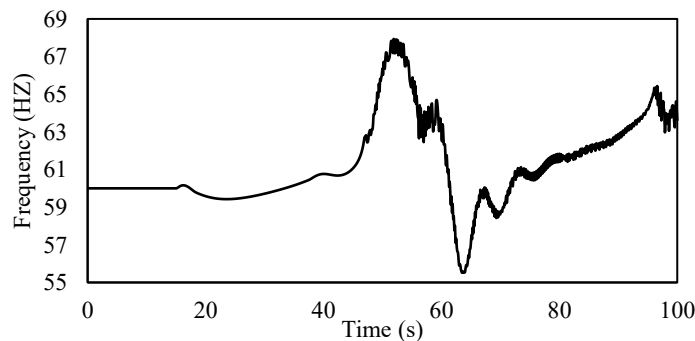


Figure 3-13: 7-Bus System: Transient frequency response in area 1 after a 4400 EV attack

The impact of this attack is represented by the graphs in Figure 3-13 to Figure 3-16. After the load was connected at $t=15$ seconds. As depicted in Figure 3-13 the frequency of the top area drops after the initial attack and never recovers after that. After the initial drop in frequency caused by the extra load, the generation starts being ramped up to initiate the system recovery but at around $t=50$ seconds the 3 areas start oscillating at different frequencies and the generators go out of synchronization. The erratic frequency behavior and voltage fluctuation at bus 1 depicted in Figure 3-13 and Figure 3-14 respectively violate the safe operation standards and would result in tripping of the different protection relays causing large portions of the load to be dropped and generators

to trip causing a blackout. Another result of this attack would be the damage to the transformers connecting the generators to the grid as well as the transformers and other equipment connected within the grid.

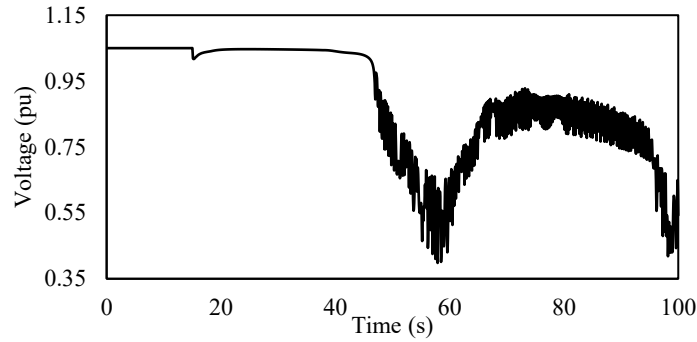


Figure 3-14: 7-Bus System: Transient voltage response at bus 1 after a 4400 EV attack

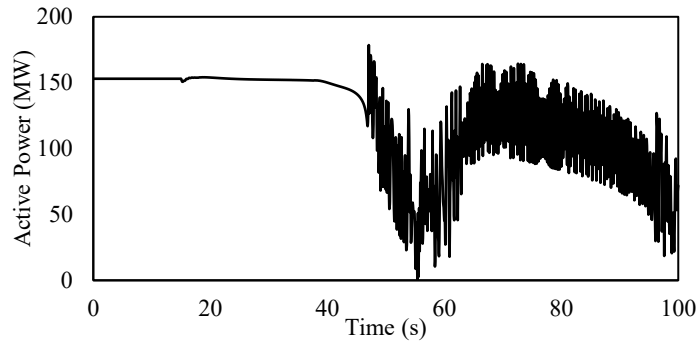


Figure 3-15: 7-Bus System: Generator 1 active power output after a 4400 EV attack

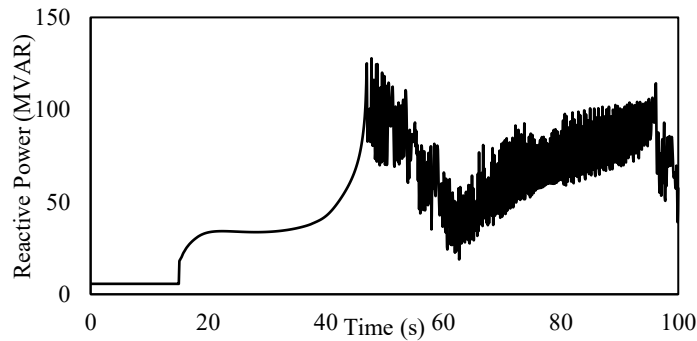


Figure 3-16: 7-Bus System: Generator 1 reactive power output after a 4400 EV attack

Another dangerous impact of this attack is the generators' behavior in response to this sudden increase in the high VAR load. Figure 3-15 and Figure 3-16 represent the rapid fluctuation in active and reactive power output respectively. Similar to the frequency behavior, the response starts at $t=15$ seconds after the attack, and at around $t=50$ seconds the fluctuations become erratic causing the complete destabilization of the grid and the generator protection relays to trip leading to a

blackout. The most dangerous impact, however, is that the requirement to keep up with the oscillatory power requirements would result in the turbine/prime movers of the generator experiencing rapid acceleration and deceleration. This phenomenon would result in high vibration levels of the rotors leading to irreparable damage worth millions of dollars. The only way to avoid such damage is by having very sensitive protection relays that disconnect the generators before any damage occurs which would result in a blackout and the loss of millions of dollars by the affected consumers. The 3 Areas exhibit a similar frequency behavior to Figure 3-13, all the busses exhibit wild fluctuations similar to Figure 3-14. Finally, all the generators get out of synchronization and exhibit behavior similar to Figure 3-15 and Figure 3-16.

3.13.5.3 EV Load Attack – Similar MVA Load (3300 EVs)

This second iteration of the EV attack is achieved by launching a surge in EV charging load having the same MVA load (60 MVA) as the residential load attack of Section 3.13.5.1. This demonstrates that the devastating impact achieved in Section 3.13.5.2 is not just due to the larger MVA load.

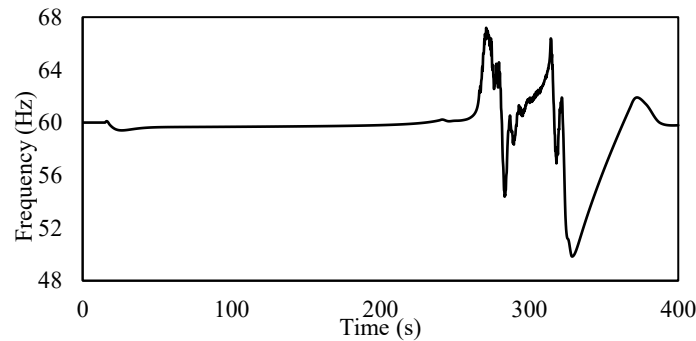


Figure 3-17: 7-Bus System: Transient frequency response of area 1 after a 3300 EV attack.

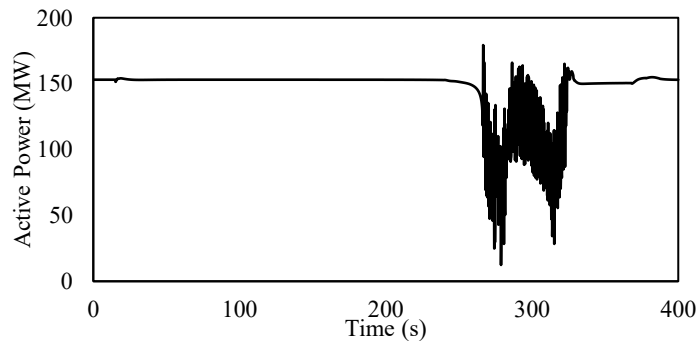


Figure 3-18: 7-Bus System: Generator 1 active power output after a 3300 EV attack

This attack is achieved by an EV charging load of 9 MW (15 MVA) at each of the 4 buses 2, 3, 4, and 5. This is equivalent to 3300 EVs or a 36 MW (60 MVA) load. As in the case of 4400 EVs, the different generators exhibit an erratic variation in output power as well as erratic voltage and frequency oscillations. The frequency in Area 1 and generator 1 output power are presented in Figure 3-17 and Figure 3-18 respectively. This demonstrates that even though the total apparent power of the attack is the same, the high reactive component can still destabilize the grid. The analysis of the impacts of this attack is the same in terms of causing grid instability, damage to the generators, electric equipment and consumer appliances, and financial losses.

3.13.5.4 EV Load Attack – Smaller Load (2750 EVs)

The final iteration of this attack is performed with a smaller attack in terms of EV numbers, real power load, and reactive power load. The location of the compromised load used for this attack is determined by locating the most sensitive buses using the method described in Section 3.10.2 above. This attack is mounted through 1100 EVs or 12 MW (20 MVA) are added to bus 2, while 825 EVs or 9 MW (15 MVA) are added to each of bus 3 and bus 5. The grid frequency, voltage, and generator output exhibit similar behavior to the 2 previous EV attacks. As with the previous cases, the generators and the 3 areas go out of synchronization, the erratic behavior results in the disconnection of the generator leading to an unstable system and the system goes into a blackout. This serves to demonstrate that the high reactive power demand of the non-linear EV charging amplifies the impact of the attack against the power grid. A 30 MW (50 MVA) EV load destabilized and damaged the grid as opposed to a 48 MW (60 MVA) residential load that only caused a frequency drop with no other violations and a return to stability after generation is ramped up.

3.14 Hardening the EV Ecosystem Security

The previous sections highlighted the vulnerabilities in the EV ecosystem and the attacks that can be launched against the power grid through this ecosystem. Given that these vulnerabilities are present in other IoT systems, we present practical mitigation schemes for the vulnerabilities based

on industry best practices [107]. These mitigations are achieved by addressing the individual vulnerabilities in the EV ecosystem.

- Protocol vulnerabilities: to prevent the multiple vulnerabilities raised by the different protocols, a standardized set of protocols must be enforced on the EV ecosystem instead of allowing different vendors and manufacturers to use their own set of protocols. Furthermore, the optional (and sometimes nonexistent) authentication and encryption schemes must be enforced, and no data should be allowed to be transmitted in plain text.
- SQL Injection: to mitigate SQL injection attackers must be denied the chance of abusing string concatenation issues to overcome the user/admin authentication process. Parametrized queries can be used to distinguish code from data thus preventing the attacker from gaining access to these accounts and denying the attacker from gaining control of the EVCS.
- XML/External Entity Injection: to mitigate XML vulnerabilities, external entities must be disabled whenever possible.
- Server-Side Request Forgery (SSRF): the IP addresses used should be validated and only pre-approved (pre-mapped) clients should be allowed to access the system.
- Cross-Site Scripting (XSS): to mitigate XSS, HTTP parameters must be filtered, and user inputs must be encoded to prevent them from being manipulated by attackers.
- Comma-Separated Values (CSV) injection: to mitigate CSV injection, the system should parse the received data and reject the data that contains special characters used to trigger or execute codes.
- Cross-Site Request Forgery (CSRF): to mitigate CSRF add random values to the communication process with each HTTP request to ensure the attacker cannot craft fake messages and cause system modification.
- Hard-Coded Credentials: to mitigate the issues raised by this vulnerability, the hardcoded credentials should be replaced by hash values of the credentials instead of the actual message in plain text.

- **Missing Authentication:** to mitigate this vulnerability, authentication should be enforced on all functionalities, especially the critical functions that can be used to manipulate the charging session parameters.
- **Vulnerable Phone Apps:** To mitigate the vulnerabilities in the phone applications, the system (mobile app/ EVCS) should verify that the ID of the EV connected to the EVCS matches the EV ID entered in the mobile app by the user or even restrict each application to a single EV ID that is verified when the account is created. Additionally, creating and using these apps should include methods to verify the user is a human rather than a bot by implementing a CAPTCHA system and eliminating the possibility of automating the account creation and attack process.
- **Vulnerable OCPP backend:** To address the vulnerabilities of the OCPP backend the first step is to ensure strict device authentication. One such method to achieve this is to utilize mutually authenticated TLS certificates. Additionally, the backend should have strict conditions on rate limiting the interactions in the communication channel, and authentication attempts. Additionally, the Backend should be designed to accept only a single connection from an EVCS with a given ID. Finally, the EVCS IDs should be generated randomly with sufficient length to make brute forcing them unfeasible. Additionally, the EVCS IDs that are used for authentication, should not be publicly available online through maps of the EVCS network that operators currently use.
- **Malware defense best practices:** The EVCS malware landscape can be to a large extent mitigated or reduced by adopting industry best practices. Firstly, firmware updates should be managed over the air by the manufacturer and not left to the operator to do manually to ensure that security updates occur in a timely fashion. Additionally, strong password policies should be implemented in place of the currently employed weak passwords (some EVCSs do not provide the operator with the option to change the default password creating a huge security risk and increasing the chances of infection by malware). All services that are not necessary for the operation of the EVCS must be restricted to avoid exposing the EVCS to malware infection through these exposed services. IP traffic should be filtered and restricted as an EVCS should only communicate with a very small number of trusted IPs and should not be left open to the entire range of possible IPs.

Other best practices include the development of secure-by-design products instead of redesigning systems after vulnerabilities are found. Vendors and manufacturers must also assess the security of their products continuously and patch vulnerabilities. Users must also be made aware of the dangers of using weak credentials to prevent attacks like the Mirai Botnet [17].

3.15Chapter Concluding Remarks

In this chapter, we gave an overview of the current EV penetration levels as well as their underlying infrastructure and technology. We also demonstrated the presence of vulnerabilities in the different elements of the EV ecosystem that can be used by attackers to gain control over the EVCS. This control can be used to launch attacks against the power grid by inducing mass charging and discharging. We then discussed attack scenarios through the EV ecosystem to disrupt the grid operation and demonstrated the larger impacts they can have on the grid. Given the non-linear nature of the EV charging load and their power injection capabilities (V2G), we compared attack simulations utilizing residential loads and EV loads and found that the EV loads can be more damaging to the operation of the grid.

The nature of the EV ecosystem also makes it an ideal target for cyber-attacks to create a botnet of high wattage / high VAR load to attack the grid. We also presented a straightforward attack strategy by utilizing stability metrics to craft smarter attacks using a smaller number of EVs while maximizing the impact. Finally, we presented patches for the vulnerabilities using industry best practices.

Chapter Four

Novel EV-Based Dynamic Attack Strategy

In this chapter, we intend to address the gaps in the attack studies above. Unlike static attacks that have a limited impact that is realistically restricted to line tripping and limited frequency or voltage deviations, our dynamic EV load attack causes severe frequency violations leading to generator tripping within a few seconds of attack initiation. Additionally, unlike switching attacks whose success depends on the pre-existence of unstable modes in a grid, our dynamic attack forces new instabilities onto the grid. Finally, unlike other works that discussed dynamic attacks, namely, [61] and [62], our work does not consider that the attacker has all the topology and dynamic behavior information of the power grid. Rather we suggest a reconnaissance methodology that allows the attacker to build the state-space representation and mathematically model the uncertainties into the attack design to compensate for modeling errors and uncertainties. Finally, unlike [61] and [62], our case studies are performed on the actual power grid model rather than the linearized state-space to capture the behavior of the actual grid rather than the attacker-built mathematical representation.

Based on the above discussions, in this chapter, we create a dynamic EV LA attack that manipulates the magnitude and the trajectory of the compromised EV loads to create grid instability. This dynamic attack is crafted as a feedback controller based on the grid's state-space model and an EV attack load trajectory calculated using Linear Matrix Inequalities (LMIs). Synthesizing the controller as an optimization problem using LMIs allows us to fine-tune the attack design and integrate multiple objectives into a single problem. Similar to the utility's lack of real-time observability of individual consumer loads [16], the utility has no way to monitor the public EVCSs in real-time. It should be noted that utilities have no observability or control over the EV ecosystem since the public charging infrastructure is owned and operated by private companies such as Tesla [135], ChargePoint [136], Electrify America [137], and Electrify Canada [138]. Also, by targeting only EVs that are connected to the grid at the instance of attack, attackers can achieve

their malicious intent while leaving the EV owners oblivious to their actions. Additionally, by using the Vehicle to Grid (V2G) functionality of the EVs [139], attackers can also inject power into the grid amplifying the impact of their attack. These facts coupled with the large aggregate EV power demand, make them ideal for LA attacks against the grid. We also formulate our attack trajectory such that the EV load change doesn't raise too much attention. The contributions included in this chapter are:

- We develop a family of robust EV dynamic LA attack strategies against the grid's frequency and voltage stability initiated through the EV ecosystem by exploiting its vulnerabilities that allow the attacker to control EVCS charging. The EV attack load trajectory is calculated using LMI control techniques and attacker-defined instability regions to maximize the impact on the grid while remaining hidden from the utility.
- We develop an attacker reconnaissance strategy that allows the attacker to account for the uncertainties introduced by the changes in grid condition as well as the errors in estimating grid parameters and the EV load connection to EVCSs. We mathematically model this uncertainty and incorporate it into our controller design.
- We demonstrate the EV dynamic attacks and evaluate their impacts through extensive time-domain simulations. We also examine the feasibility of our attack scenarios by examining the EV statistics, vulnerabilities, and technologies that make these attacks possible. Additionally, we demonstrate the robust performance of our suggested attack strategy against the discussed uncertainties.

4.1 System Modeling and Attack Methodology

In the following section, we discuss the state-space representation of the grid based on its topology and dynamic behavior. This representation is necessary for designing dynamic attack vectors through EVs to destabilize the grid. The system inputs are considered the compromised EV loads through any combination of the vulnerabilities discussed above.

4.1.1 Linearized Power System Model

The power system's dynamic behavior, which is the focus of this chapter, is mostly dependent on the generators and their control systems. For the modeling of the generators and control systems, we use the models that are widely accepted in similar studies [133], i.e., (i) round rotor synchronous machine with order 6, (ii) generator exciter Model IEEE T1, (iii) single mass IEEE G2 steam turbine prime mover, and (iv) Power System Stabilizer (PSS) based on IEEE Std 421.2. Then, the power flow equations expand this model to represent the entire grid. The grid dynamic behavior is governed by the transfer functions $\dot{x} = f(\bar{x}, \bar{u})$ and $y = g(\bar{x}, \bar{u})$ that define the relation between the system states, the inputs, and the outputs. Based on those transfer functions, the grid is linearized into a state-space model with the active and reactive power of the aggregate EV-attacker loads being the inputs and the generator frequencies being the outputs. This representation is expressed as (4.1) where x , y , and u represent the vector of system states, outputs, and inputs, respectively. Additionally, ΔP_{EV_n} , ΔQ_{EV_n} , and f_{Gen_m} represent the change in active and reactive power of the aggregate EV attack load at bus n and the frequency of generator m respectively.

$$\dot{x} = Ax + Bu \quad (4.1a)$$

$$y = Cx + Du \quad (4.1b)$$

$$\text{such that } y = (f_{Gen_1} \ f_{Gen_2} \ \cdots \ f_{Gen_m}) \quad (4.1c)$$

$$\text{and } u = \Delta P_{EV} = (\Delta P_{EV_1} \ \Delta Q_{EV_1} \ \cdots \ \Delta P_{EV_n} \ \Delta Q_{EV_n}) \quad (4.1d)$$

where A , B , C , and D are the state-space matrices that represent the power grid and its dynamic behavior. While matrix A represents the dynamics of the system based on its different components, control mechanisms, and their impact on one another, matrix B represents the relationship between the impact of the inputs, u , on the grid's behavior. Additionally, matrix C represents the relationships between the system states to the system's outputs, i.e., its generator frequencies. The authors of [140], [141], and [142] discuss how the power grid can be linearized to maintain all its behavioral properties while the work presented in [91] and [143] discusses how power grids are linearized for the sake of designing their control techniques. Finally, the details of modeling the power grid as a state-space are presented in [144] and [60]. To this end, we do not dive further into the details of linearizing a power grid into its state-space model and focus mostly on the attack design in the sections below.

4.1.2 Feedback Control as an Attack Model

Figure 4-1 represents the attacker model and its interaction with the grid. The state-space representation in the dashed box is constructed by the attacker, based on the power grid parameters and (4.1). This state-space representation is then used to calculate (i) the EV gain matrix K and capture the behavior of the input $u = \Delta P_{EV}$ to replicate it on the set of compromised EVs in the grid, and (ii) the observer gain matrix L that enables the attacker to accurately recover the grid states, by observing the grid frequency, to incorporate them in the attack model. Our EV attack load will be crafted based on full-state feedback control law, i.e., $u = Kx$, where K is the gain controller designed to determine the required input trajectory u for a system. Since the attackers do not have access to all system states (x), they need to obtain an estimate of these states ($\hat{x}$) through an observer. As such, the EV load, ΔP_{EV} , used by the adversary in the attacker block of Figure 4-1, is based on $\Delta P_{EV} = u = K\hat{x}$. Designing the EV attack load input based on a feedback controller changes the A matrix to its closed-loop form, i.e., $A_{cl} = A + BK$. Since the eigenvalues of A_{cl} define the stability of the system, selecting K that shifts the eigenvalues of A_{cl} to the right half-plane of the s -domain will destabilize the grid and fulfill the attack objectives.

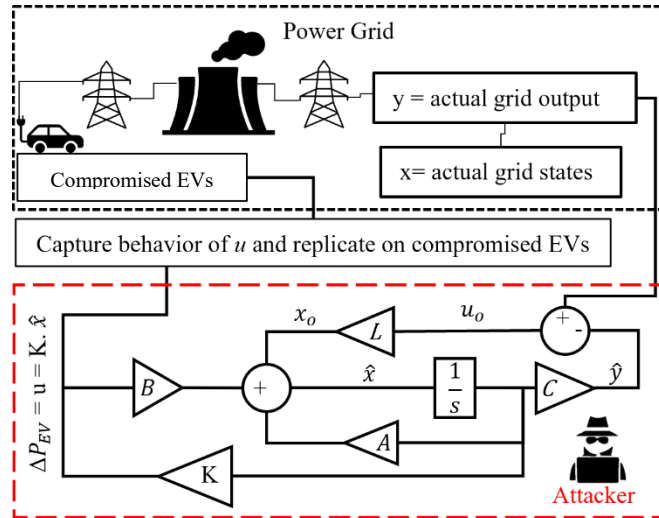


Figure 4-1: State-space attacker model and interaction with the power grid

4.1.3 Attack Region Constraints

In our dynamic EV attack, the intent is to relocate the system's eigenvalues to a predefined region of instability while minimizing the required EV load. The selected region of instability is based on grid standards followed by different utilities, such as New England ISO [145]. These standards specify ζ and ωn , which are the damping ratio and natural oscillation frequency of the grid eigenvalues. The eigenvalues can be written in terms of ζ and ωn as:

$$\lambda = a \pm jb \quad (4.2a)$$

$$a = -\zeta \omega n \quad (4.2b)$$

$$b = \omega n \sqrt{1 - \zeta^2} \quad (4.2c)$$

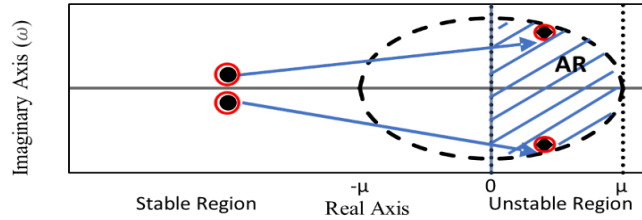


Figure 4-2: Sample of pole placement using D-stabilization methods.

For the attack to successfully destabilize the grid, it should move the eigenvalues of the system to the Attack Region (AR) demonstrated in Figure 4-2. Without loss of generality, a tight region around the imaginary axis is chosen as AR to obtain eigenvalues that do not have a large positive a . Since the system output growth is proportional to e^a , an eigenvalue with a large positive a (having a negative ζ) (i) would dictate very rapid growth of ΔP_{EV} , which increases the attack difficulty since the attacker might not control enough EVs to launch such an attack, and (ii) it would cause the system to become unstable rapidly, raising alarms for the utility. Moreover, AR must be selected such that b (that is mostly influenced by ωn for a predefined ζ) remains within a tight range to avoid rapid oscillation, to avoid alarming the operator. Also, such a tight region makes the attack possible since it will not require very rapid EV oscillation.

4.1.4 Attacker Reconnaissance Including Parameter Uncertainty

Contrary to the power grid reconnaissance models presented above, we consider a realistic adversary that does not have all the accurate information regarding the power grid parameters and

its state-space representation. To this end, we propose a specifically tailored stealthy reconnaissance technique that accounts for the power grid uncertainties. It is important to note that any deviation from the accurate model would reduce the efficiency and the maximum impact of the attack. As a result, our reconnaissance technique would produce a family of polytopic systems representing the power grid state-space models as well as the modeling uncertainties. This representation is essential for a robust attack formulation that is immune to these uncertainties as well as changes in the grid loading conditions. Our proposed technique starts with a small probing signal followed by the Eigenvalue Realization Algorithm (ERA) [146] and finally estimates the uncertainties and inaccuracies in the obtained model and creates a family of polytopic systems that will be used in our robust attack formulation. Additionally, we will only assume that an attacker has compromised EVs on a subset of the total load buses, and consequently will calculate the grid's state- space while considering that only the compromised loads are the inputs.

4.1.4.1 Estimation of State-Space Matrices

The probing signal chosen in this work is an exponential chirp signal described by (4.3) where f_s and f_e represent the start and end frequency of the range the AR is capped at. T is the duration of the probing signal.

$$s_{probe} = \sin \left(\frac{2\pi f_s \left(\left(\frac{f_e}{f_s} \right)^{1/T} - 1 \right)}{\ln \left(\left(\frac{f_e}{f_s} \right)^{1/T} \right)} \right) \quad (4.3)$$

The magnitude of this probing signal is capped at 2% of the load on the compromised buses to avoid raising any alarms at the operator's side. Since we are interested in the low-frequency behavior of the grid, our f_s and f_e are chosen to be 0.1 Hz and 2 Hz. After this signal is applied to the grid using the EV loads, the generator frequencies are captured and the Fourier Transform of the probing signal at each bus is calculated as well as the frequency response at each generator in response to that signal. After that, the attacker would calculate the impulse response of each generator to each load and rearrange the obtained input-output data into a time series representing snapshots of the grid's response over time. This time series is then used to calculate the system's Hankel matrices as detailed in [146], [147], and [148]. Following this step, Singular Value Decomposition (SVD) is performed on the Hankel matrix to factorize this matrix into three

matrices U , Σ , and V that will be used to estimate matrices A and C . Matrices B and D are then calculated using the least squares method. The detailed mathematical formulations of the ERA are omitted from this chapter and can be found in [146], [147] and [148].

4.1.4.2 Representation of System Uncertainties

Unlike previous work that assumes the model obtained from reconnaissance is 100% accurate, our attack model includes modeling the system uncertainties. At this stage, the system is not probed another time. However, after estimating the state-space matrices, the attacker will simulate the obtained system with the same probing signal, s_{probe} in Section 4.1.4.1 as an input to generate the predicted output data (y_{sim}) as demonstrated in (4.4).

$$\dot{x}_{sim} = Ax_{sim} + Bs_{probe} \quad (4.4a)$$

$$y_{sim} = Cx_{sim} + Ds_{probe} \quad (4.4b)$$

The simulated output, y_{sim} , is then sampled at the same rate as the actual output, y , was collected from the power grid to achieve a stacked matrix having m rows and N columns where N is the total number of samples. The residual matrix, R having m rows and N columns, is obtained in (4.5) by subtracting the actual output y and the simulated output y_{sim} . After calculating the residuals, the attacker will follow the steps outlined in (4.6) to (4.9) to calculate the covariance matrix A_a .

$$R = [y_{sim1} \ y_{sim2} \ \dots \ y_{simN}] - [y_1 \ y_2 \ \dots \ y_N] \quad (4.5)$$

$$C_{xy} = X_{sim}R^T \quad (4.6)$$

$$\text{where } X_{sim} = [x_{sim1} \ x_{sim2} \ \dots \ x_{simN}] \quad (4.7)$$

where X_{sim} is a k -by- N state trajectory matrix where each column represents a sample of the k simulated system states, x_{sim} , and C_{xy} represents the cross-covariance between the simulated states and the residual matrix R .

$$C_{yy} = \frac{1}{N}(RR^T) \quad (4.8)$$

$$A_a = C_{xy} C_{yy}^{-1} \quad (4.9)$$

where C_{yy} represents the covariance of the residuals quantifying the relationship between these residuals at different points in time. The term RR^T is scaled by $(1/N)$ to make the calculated covariance independent of the number of data points. A_a represent the variance matrix of the estimated matrix A .

Next, the attacker performs the Cholesky decomposition on A_a to factorize it into a lower triangular matrix Z such that $A_a = ZZ^T$. This matrix Z and the original matrix A are then used to generate a set of random samples from a multivariate Gaussian distribution with a mean of A and a variance of Z forming the family of systems presented in (4.10):

$$A(\delta) = A + \delta_1 A_1 + \delta_2 A_2 + \dots + \delta_j A_j \quad (4.10)$$

where each matrix A_j represents a deviation from the original matrix A with a given probability δ_j , where $\sum_j \delta_j = 1$. It is important to mention that the larger the number of systems, j , the more confident the attacker would be in the system's ability to capture all possible uncertainties.

4.1.4.3 Representation of Polytopic System

In case the attacker's strategy involves reconnaissance in advance of the attack not immediately before it, the above suggested reconnaissance strategy needs to be amended as follows. The first step would be the attacker specifying the time, T_a , at which the attack is intended to start on the target day. The attacker would then perform the steps described in Section 4.1.4.1 and Section 4.1.4.2 on several days before the attack is intended to be launched using the same probing signal, s_{probe} in (4.3). On each day, the attacker would perform the reconnaissance multiple times during the hour preceding and following T_a . This is performed to capture the variation in the behavior of the load during that specific time of day over several days. This step guarantees the attacker that the constructed system below will be able to accommodate for the different loading conditions of the grid around the specified attack time T_a . Although the load generally follows a repetitive pattern from one day to the other, the exact loading conditions are not identical. Using the system developed in (4.11) and (4.12) the attacker will be able to account for the changes in dynamic system behavior by representing the grid as a polytopic family of systems that accounts for uncertainties in system representation. Each instance of the performed reconnaissance shall be indexed by variable i while each instance of uncertainty within each reconnaissance window is indexed by j in (4.11). Each matrix A_{ij} represents a deviation from the original matrix A with a given probability $\rho_i \delta_{ij}$, where $\sum \rho_i = 1$. Equation (4.11) is simplified in (4.12) by combining the probabilities $\rho_i \delta_{ij}$ into a single variable ∂_{ij}

$$A(\delta, \alpha) = A + \rho_1(\delta_{11}A_{11} + \dots + \delta_{1j}A_{1j}) + \rho_2(\delta_{21}A_{21} + \dots + \delta_{2j}A_{2j}) \dots \rho_i(\delta_{i1}A_{i1} + \dots + \delta_{ij}A_{ij}) \quad (4.11)$$

$$A(\partial) = A + \Delta A \quad (4.12)$$

$$\text{where } \Delta A = \partial_{11}A_{11} + \partial_{12}A_{12} + \partial_{1j}A_{1j} + \dots + \partial_{i1}A_{i1} + \dots + \partial_{ij}A_{ij} \quad (4.13)$$

$$\text{and } \sum_i \sum_j \partial_{ij} = 1 \quad (4.14)$$

4.1.4.4 Uncertain EV Load

In this subsection, we also address another form of uncertainty introduced by the EV attack load itself. Unlike other works that assume that the attacker is fully aware of the status of the entire attack surface, we consider the realistic scenario that the attacker can never be 100% sure about the connection of the EVs to their EVCSs beforehand. As a result, we intend to model the uncertainty in the EV load arising from the user behavior that is unknown to the attacker. This uncertainty is modeled as an uncertain vector $\emptyset$ that determines how much EV load is subtracted from the output of the controller K in the feedback attack loop. This changes the value of the EV load to $\Delta P_{EV-\emptyset} = u_{\emptyset} = \Delta P_{EV} - \emptyset \Delta P_{EV} = K\hat{x} - \emptyset K\hat{x}$, where $\emptyset$ is a diagonal matrix having each entry corresponding to an independent random variable representing the uncertainty in EV load at each of the attacked buses. As a result, the state-space representation in (1a) becomes (4.15).

$$\dot{x} = Ax + B(K\hat{x} - \emptyset K\hat{x}) \quad (4.15)$$

By rewriting $\Delta P_{EV-\emptyset}$ as a function of the original input u , (4.15) becomes (4.16a) which is restructured through (4.16b) to become the state-space representation in (4.16c) which models the uncertainty in the feedback signal as uncertainty in matrix B .

$$\dot{x} = Ax + (Bu - B\emptyset u) \quad (4.16a)$$

$$\dot{x} = Ax + \{B(I - \emptyset)\}u \quad (4.16b)$$

$$\dot{x} = Ax + (B + \Delta B)u \quad (4.16c)$$

where $\Delta B = -B\emptyset$. It is worth noting that the attacker can perform reconnaissance to gather historical data using the charging applications or webpages of the EVCS operators discussed above [135]- [138] or using third-party services such as Chargemap [124] that provide real-time status of the charging infrastructure occupancy of different vendors. This reconnaissance will give the attacker an estimate of the charging profile during the day but cannot guarantee that all the EVCSs

will have connected EVs as anticipated by the attacker. The attacker, however, can aggregate the data of EV connectivity on each bus, fit its distribution into a Gaussian distribution function, and determine the mean μ and Standard deviation σ . As a result, ΔB , is used to estimate the uncertainty in the EV attack load itself. By generating a series of independent random variables for each entry on the diagonal of Φ as a Gaussian variable with the mean and standard deviation determined above, the attacker can generate the series of matrices depicted in (4.17) representing the uncertainty in the EV load and then simplifying the representation as (4.18).

$$\Delta B = \gamma_1 B \Phi_1 + \gamma_2 B \Phi_2 + \dots + \gamma_f B \Phi_f \quad (4.17)$$

$$\Delta B = \gamma_1 B_1 + \gamma_2 B_2 + \dots + \gamma_f B_f \quad (4.18)$$

where γ_f represents a probability assigned to each permutation and $\sum_f \gamma_f = 1$. It is worth noting that the larger the number of permutations, f , the more possibilities the attacker's model will account for.

4.1.5 Robust Attack Formulation

In this subsection, the robust EV attack strategy is developed, and its mathematical formulation is obtained based on LMIs [149]. LMIs are convex optimization problems with matrix inequality constraints. In our study, we utilize LMIs to calculate the value of the gain K used by the adversary to force the eigenvalues of the A_{cl} into the AR. Unlike the work in [68] and [60], which assume the estimated grid model is accurate, we will modify two D-Stabilization techniques [149] to account for the parameter uncertainties and the variation of grid dynamic behavior with time. The modified LMIs of both techniques are then combined to achieve a confined result in a narrow region adhering to our constraints on the real and imaginary parts (a and b) of the eigenvalues, i.e., the shape of AR. Figure 4-2 is a demonstrative figure with generic poles used to clarify the methods we explain herein.

- 1) $H(a, \beta)$ *Stabilization* is a pole placement technique used to design feedback controllers such that the eigenvalues of A_{cl} belong to $\{a \pm jb \mid -\beta < a < -\alpha\}$ as demonstrated between the vertical dotted lines in Figure 4-2. There can only be a solution to this equation if there exists a symmetric positive definite matrix P satisfying (4.19):

$$\begin{cases} (A + BK)P + P(A + BK)^T + 2\alpha P < 0 \\ -(A + BK)P - P(A + BK)^T - 2\beta P < 0 \end{cases} \quad (4.19)$$

Equation (4.19) is linearized and rewritten as (4.20) by assuming $K = WP^{-1}$ and solving for W and P .

$$\begin{cases} AP + PA^T + BW + W^T B^T + 2\alpha P < 0 \\ -AP - PA^T - BW - W^T B^T - 2\beta P < 0 \end{cases} \quad (4.20)$$

We now modify (4.20) by adding the representation of the polytopic system including the system uncertainties in (4.12) and (4.18) to form (4.21). Given our AR that dictates the eigenvalues have a real part, α , larger the zero, we will assign the variable $\beta = 0$.

$$\begin{cases} (A + \Delta A)P + P(A + \Delta A)^T + (B + \Delta B)W + W^T(B + \Delta B)^T + 2\alpha P < 0 \\ -(A + \Delta A)P - P(A + \Delta A)^T - (B + \Delta B)W - W^T(B + \Delta B)^T < 0 \end{cases} \quad (4.21)$$

The gain K achieved through $H(0, \alpha)$, keeps the real part of the closed-loop eigenvalues between 0 and $-\alpha$. This LMI is used to guarantee that the eigenvalue will have an α that is positive to cause instability but small enough to avoid the rapid growth of the EV input.

2) *D(q, r) Stabilization* is a pole placement technique used to design feedback controllers with the eigenvalues of A_{cl} satisfying $\{a \pm jb \mid (x + q)^2 + y^2 < r\}$ as highlighted within the dashed circle of Figure 4-2. There can only be a solution to this equation if there exists a symmetric matrix P satisfying the matrix inequality (4.22).

$$\begin{bmatrix} -rP & qP + (A + BK)P \\ qP + P(A + BK)^T & -rP \end{bmatrix} < 0 \quad (4.22)$$

Equation (4.22) is linearized and rewritten as (4.23) by assuming $K = WP^{-1}$ and solving for W and P .

$$\begin{bmatrix} -rP & qP + AP + BW \\ qP + PA^T + W^T B^T & -rP \end{bmatrix} < 0 \quad (4.23)$$

We now modify (4.23) by adding the representation of the polytopic system including the system uncertainties in (4.12) and (4.18) to form (4.24). Given our AR that dictates the eigenvalues fall within a tight region around the imaginary axis, we will assign the variable $q = 0$.

$$\begin{bmatrix} -rP & (A + \Delta A)P + (B + \Delta B)W \\ P(A + \Delta A)^T + W^T(B + \Delta B)^T & -rP \end{bmatrix} < 0 \quad (4.24)$$

The gain K achieved through $D(0, r)$, keeps the eigenvalues of the closed-loop system centered at 0 with radius r . This LMI is used to guarantee that the eigenvalue will have parameters b and ωn that are bound within a tight region around the real axis to avoid the need for a rapidly oscillating EV input.

For the attacker to successfully craft the AR as discussed above, the attacker now combines both methods to form the robust pole placement problem in (4.25). Such linear matrix optimization problems can be readily solved in MATLAB or similar software that can handle LMI-based systems.

$$\begin{cases} P > MI & (4.25a) \\ (A + \sum_i \sum_j \partial_{ij} A_{ij})P + P(A + \sum_i \sum_j \partial_{ij} A_{ij})^T + (B + \sum_f \gamma_f B_f)W + W^T(B + \sum_f \gamma_f B_f)^T + 2\vartheta P < 0 & (4.25b) \\ -(A + \sum_i \sum_j \partial_{ij} A_{ij})P - P(A + \sum_i \sum_j \partial_{ij} A_{ij})^T - (B + \sum_f \gamma_f B_f)W - W^T(B + \sum_f \gamma_f B_f)^T < 0 & (4.25c) \\ \begin{bmatrix} -\vartheta P & (A + \sum_i \sum_j \partial_{ij} A_{ij})P + (B + \sum_f \gamma_f B_f)W \\ P(A + \sum_i \sum_j \partial_{ij} A_{ij})^T + W^T(B + \sum_f \gamma_f B_f)^T & -\vartheta P \end{bmatrix} < 0 & (4.25d) \end{cases}$$

$$K = W P^{-1} \quad (4.26)$$

Constraint (4.25a) can be incorporated into the controller design where M is a positive integer. This new constraint guarantees a smaller value of the gain K and consequently, a smaller input signal, $u = \Delta P_{EV}$. Using this method, the attacker crafts the attack that forces the grid's eigenvalues to the AR governed by the rules $H(0, -\vartheta)$ and $D(0, \vartheta)$.

4.1.6 Observer Design

Since our EV attack strategy is based on full-state feedback control law, the attacker also needs to choose an appropriate design for the observer to accurately estimate the states of the system. With the introduction of the gain K and the observer L , the state-space (4.1) becomes (4.27).

$$\dot{\hat{x}} = A\hat{x} + BK\hat{x} + L(y - \hat{y}) \quad (4.27)$$

Given that the design of the observer is equal to finding an appropriate gain matrix L , this matrix should be designed to ensure that the matrix $(A - LC)$ has stable poles. Therefore, to accurately estimate the system states, we choose the Linear Quadratic Controller (LQR) technique [150].

LQR is a control technique that achieves the desired performance while optimizing the balance between the energy of states, and control signals. This balance is controlled by their respective weights Q and R , where Q is a square symmetric positive semi-definite matrix and R is a square symmetric definite matrix. The observer gain L is designed as an optimization problem that minimizes the cost function J in (4.28):

$$J = \int_0^{\infty} x_o^T Q x_o + u_o^T R u_o dt \quad (4.28)$$

where $x_o = (y - \hat{y})$ and u_o is the input being fed back into the state-space and given that $Q = Q^T \geq 0$ and $R = R^T > 0$.

Without going into detailed calculations, this problem can be solved by finding the value of S that satisfies the Algebraic Riccati Equation (4.29)

$$0 = SA_o + A_o^T S - SB_o R^{-1} B_o^T S + Q \quad (4.29)$$

where $A_o = A^T$, $B_o = C^T$ and $S = S^T \geq 0$.

Equation (4.29) is quadratic in S and has no trivial solution, but it has a single positive definite solution in S that makes the observer stable. Thus, the observer gain L is determined as

$$L = -R^{-1} B_o^T S. \quad (4.30)$$

4.2 Case Studies and Simulations

In this section, we utilize the New England (NE) 39-bus grid in Figure 4-3 [151] to demonstrate the proposed EV attack methodology and its impact in the presence of the PSS and all the grid protection mechanisms. Using the methodology presented in Section 4.1.4.1, the attackers would introduce the chirp signal into the power grid and estimate its state-space representation based on the achieved response using the ERA. Following that, the attackers will use the methodology presented in Sections 4.1.4.2 – 4.1.4.4, to model the uncertainty in their state-space model. The NE 39-bus grid has 39 buses, 10 generators, and 19 loads with a total of 6,097 MW. Based on the presented methodology, the EV attack load is calculated as $\Delta P_{EV} = u = K\hat{x}$ then captured from

the state-space model and replicated on the EVs in the actual grid. Our attack simulations were performed on MATLAB-Simulink 2020a Specialized Power Systems Toolbox using a variable step size of 1×10^{-12} to 1×10^{-9} .

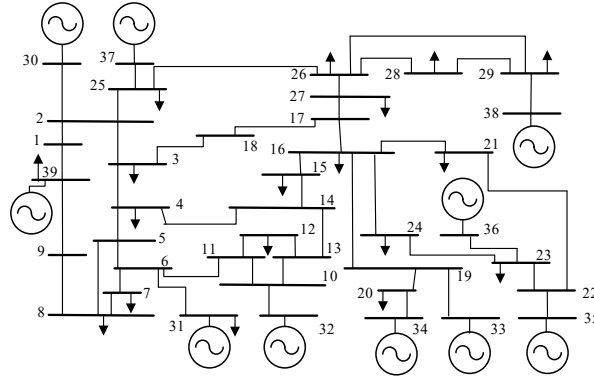


Figure 4-3: New England 39-bus grid

4.2.1 Attack Feasibility

Similar to the discussion in Section 3.12.1.2 we will utilize the New South Wales (NSW) grid [126] to demonstrate the feasibility of the attacks. The average load is 6968 MW [126] and the total registered vehicles are 5,892,206 [127]. Scaled down to fit the NE grid, the number of vehicles is 5,155,681. Table 4-1 demonstrates the total EV load in MW at different EV penetration levels and charging rates at the 10 EVs per EVCS ratio.

Table 4-1: Maximum Total EV Load In MW vs EV Levels and Charging Rates

EV Penetration Level	Level 2 EVCS		Level 3 EVCS		Global Average
	11 kW	19 kW	40 kW	360 kW	24 kW
25%	1,418	2,449	5,156	46,401	3,093
50%	2,836	4,898	10,311	92,802	6,187
75%	4,253	7,347	15,460	139,203	9,280
100%	5,671	9,796	20,623	185,605	12,374

This demonstrates that the total EV load surpasses the total grid demand. At a 50% EV penetration level, there will be 2,577,841 EVs and 257,784 public EVCSs in our NE grid based on the 10 to 1 ratio. With an average occupancy rate of 33% [129] for fast EVCSs (higher for Level 2), we can estimate the number of connected EVs to the grid on average to be 85,000. Furthermore, according

to the IEA [128], based on the mixture of different EVCS rates, the average charging rate per EVCS is 24 kW. From the presented statistics, we can estimate that at a 50% EV penetration level, there will be 2,041 MW of EV load connected to the grid on average at public EVCSs (2.55 times our largest attack load).

The work in [130] demonstrated how EV attacks against the transmission system can be carried out with no impact on the distribution system stability. Attackers will distribute their attacks such that the impact per distribution grid remains minimal while the aggregate impact causes serious issues on the transmission level. We stress that given the ability of these distribution grids to handle the total load of the EVCS charging, our attack will not cause any line tripping or transformer overloading but rather stealthily and quickly force the frequency of the grid's generators to destabilize.

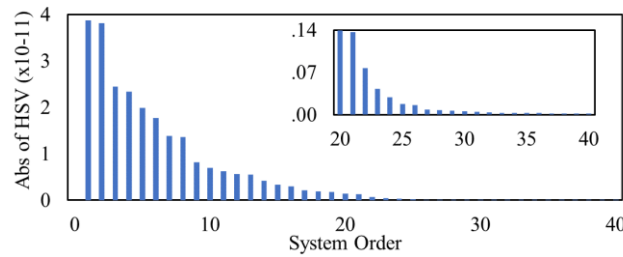


Figure 4-4: Hankel Singular Value weights

4.2.2 Reduced Power Grid State-Space Model

Due to the complexity of the power grid, the size of the state-space matrices is relatively large. Designing controllers and working with such high-order systems is prohibitive. To preserve the correct system behavior while reducing its order, we use Hankel model reduction [152]. Figure 4-4 represents the energy contained within the Hankel Singular Values (HSVs) of the first 40 states. Figure 4-4 shows the sharp decrease in the energy of the HSVs as the order of the system states increases. When the attacker reduces the state-space order, it is important to perform the steps presented in Section 4.1.4.2 on the reduced model to capture the uncertainties in the model itself as well as the uncertainties introduced by the reduced model. One important factor to consider is that the proposed methodology estimates an accurate state-space model of the power grid, only

in the frequency range of the probing signal of Section 4.1.4.1. However, all the simulations and case studies are performed on the actual grid including all its control mechanisms, not the linearized model or the reduced model.

Table 4-2: Vulnerabilities and EVCS botnet control

EV Vulnerability	Target	Attack Scalability	Attack Synchronization	Ability To Manipulate EV Charging	Ability To Control EVCS Charging Rate	Attack Difficulty
1	EV Internet Connectivity	Moderate	Difficult	Possible	Unlikely	Difficult
2	EV Onboard Systems	Moderate	Difficult	Possible	Unlikely	Extremely Difficult
3	EVCS HMI	Difficult	Difficult	Possible	Very Likely	Difficult
4	EVCS Firmware	Easy	Guaranteed	Yes	Guaranteed	Feasible
5	CMS	Easy	Guaranteed	Yes	Guaranteed	Feasible
6	OCPP	Easy	Guaranteed	Yes	Guaranteed	Feasible
7	Charging Mobile App	Easy	Easy	Yes	Very Likely	Feasible
8	OEM Communication	Easy	Easy	Yes	Very Likely	Feasible
9	DR Programs	Difficult	Very Difficult	Yes	Not Possible	Feasible

4.2.3 EVCS Botnet Command and Control

Through the vulnerabilities mentioned in Chapter 3, attackers can gain control of the EVCSs and create a botnet of EV loads readily available for the dynamic EV attack against the grid. Table 4-2 summarizes these vulnerabilities and evaluates their usage by the attacker to launch the suggested attacks. Based on this evaluation, the most suitable vulnerabilities for such an attack are vulnerabilities 4, 5, 6, 7, and 8.

4.2.4 Case Studies: Attacks Against NE 39-Bus System

In this case study, we demonstrate five different attack scenarios against the NE 39-bus grid. Due to its 10 generators and their relatively high inertia, this is a relatively resilient grid that would serve to demonstrate the effectiveness of our method. In this case study, we demonstrate the

importance of properly selecting the attack EV locations and their impact on the attack's success. We also demonstrate the importance of utilizing the robust system model and including the reactive power (and EV load power factor) as input to our state-space. It is worth noting that in the first four attack scenarios, we target 4 load buses each of which satisfies $-200 \text{ MW} \leq \Delta P_{EV} \leq 200 \text{ MW}$. In the sixth attack, the load is capped at a total of 415 MW split proportionally on the attack buses. The total of the first 5 EV attack loads is equal to 33,333 EVs charging at the 24 kW average rate. This load of 800 MW is equal to 13.1% of the grid load. Attack scenario 6, however, requires a total of 17,290 EVs which is equivalent to 6.8% of the grid's load. However, at no point in time are all EV attack loads operating in the same dis/charging mode. In Scenarios 1, 2, 3, 4, and 6, the attacker's state-space outputs are the generator frequencies. In Scenario 5, the outputs of the attacker's state-space are the load bus voltages. A summary of the attacks and their impacts is presented below with an AR in the first 3 scenarios based on rules $H(0,-0.5)$ and $D(0,0.5)$.

- Scenario 1: EV attack against generator frequency stability launched from buses 3, 4, 24, and 39 with an attack load input, $\Delta P_{EV} = u$, based on EV active power alone. In this scenario alone, we assume the absence of a PSS in the grid to establish a baseline result in the absence of power grid defense mechanisms.
- Scenario 2: EV attack against generator frequency stability launched from buses 3, 4, 18, and 39 with an attack load input, $\Delta P_{EV} = u$, based on EV active power alone. In this scenario and all the following scenarios, the power grid is assumed to have a PSS which is the grid's strongest defense mechanism against such load oscillations.
- Scenario 3: EV attack against generator frequency stability launched from buses 3, 4, 24, and 29 with an attack load input, $\Delta P_{EV} = u$, based on EV active power alone.
- Scenario 4: EV attack against generator frequency stability launched from buses 3, 4, 24, and 29 with an attack load input, $\Delta P_{EV} = u$, based on EV active and reactive power.
- Scenario 5: EV attack against load bus voltage stability launched from buses 3, 4, 24, and 29 with an attack load input, $\Delta P_{EV} = u$, based on EV active and reactive power. with an AR based on rules $H(-1,0)$ and $D(0,1)$.
- Scenario 6: EV attack against generator frequency stability launched from buses 3, 4, 24, and 29 with an attack load input, $\Delta P_{EV}=u$, based on EV active power alone with an AR that is based on rules $H(-1,0)$ and $D(0,1)$ and a load capped at 415 MW.

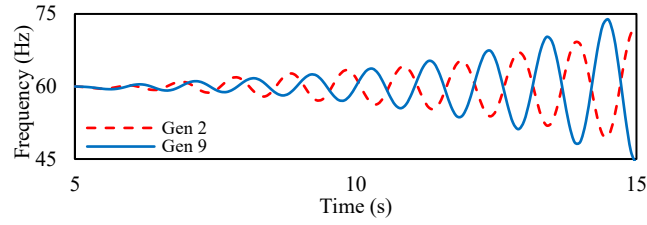


Figure 4-5: Output frequency of generators 2 and 9 in Scenario 1 with no PSS

4.2.4.1 Attack Scenario 1

This attack results in catastrophic frequency oscillations as depicted in Figure 4-5. The frequencies of all generators experience wild oscillations and continue to grow unrestricted by any defense mechanisms until they reach 74 Hz in a matter of 9 seconds. Additionally, the generators surpass the 1.5 Hz (2.5%) deviation limit in 2.5 seconds tripping all generators within 2.5 seconds of attack initiation. In contrast, the remaining attacks all take place in the presence of the PSS.

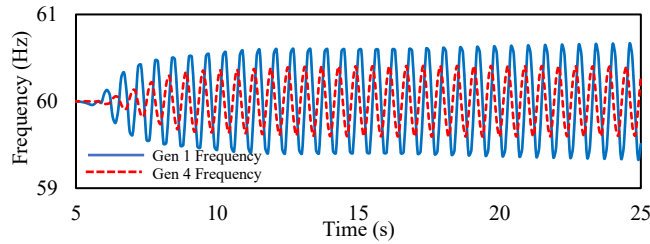


Figure 4-6: Output frequency of generators 1 and 4 in Scenario 2

4.2.4.2 Attack Scenario 2

The attack caused the continuous oscillation of the generator frequency with a frequency deviation magnitude of 0.6 Hz as demonstrated in Figure 4-6. This demonstrates how the grid went into a region of diminished behavior (frequency deviation 1%) and continuous oscillation. If this impact is maintained for 9 minutes the generators will trip, however, this attack does not cause an instantaneous generator trip. The amplitude of the frequency oscillation rose rapidly and then plateaued within the range of ± 0.6 Hz. The voltage in this scenario experienced oscillations well within the 5% safe operation margin. The voltages on the buses that came closest to the 5% limit are depicted in Figure 4-7.

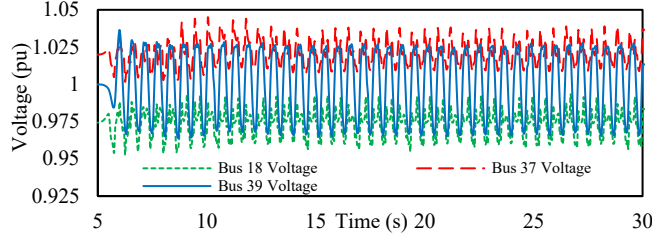


Figure 4-7: Bus 18, 37, and 39 voltages in Scenario 2.

4.2.4.3 Attack Scenario 3

The frequency responses of generators 1 and 6 are presented in Figure 4-8. The frequency deviation, which is larger than 1.5 Hz (2.5%), prompts the utility to trip the generators. In this scenario, the grid experiences larger oscillations than in Scenario 1. Moreover, the frequency follows a slight downward trajectory where it is no longer centered around 60 Hz but is slowly decreasing with time.

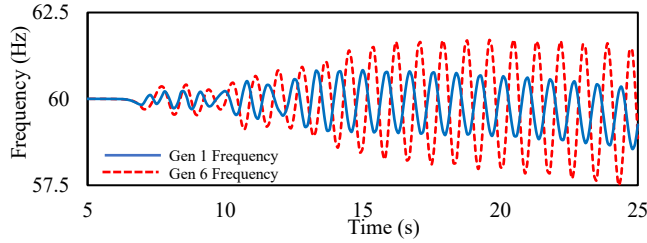


Figure 4-8: Output frequency of generators 1 and 6 in Scenario 3.

Figure 4-9 demonstrates the aggregate EV attack load, at the four attack buses, which lead to this behavior. This figure shows that while, theoretically, the EV attack load can reach 800 MW, it never does since the dynamic attack trajectory of these EV loads is never the same. The maximum aggregate load is 400 MW, which is 6.6% of the total grid load. Based on the obtained EV attack gain K , the oscillation of the attack loads at bus 4 and 18 will follow the trajectory shown in Figure. 4-10. Figure. 4-10 illustrates how the magnitude and trajectory of the dynamic attack are not predetermined but rather vary continuously. The voltages in this attack experienced wild oscillations and their magnitude deviation reached 0.04 pu which is within the safe operation margin. This voltage behavior is depicted in Figure. 4-11.

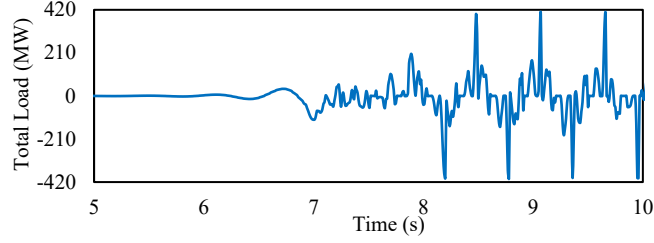


Figure 4-9: Aggregate EV attack load – first 5 seconds of Scenario 3.

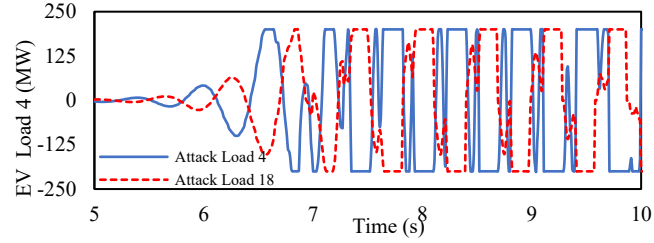


Figure. 4-10: Aggregate EV attack load on buses 4 and 18 – first 5 seconds of Scenario 3

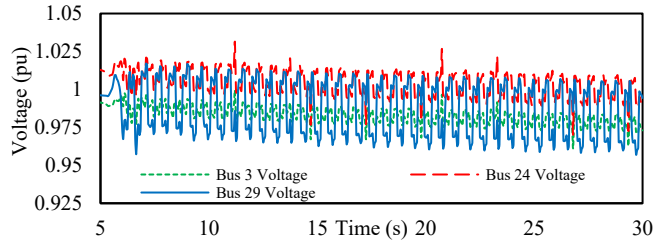


Figure. 4-11: Bus 3, 24, and 29 voltages in Scenario 3.

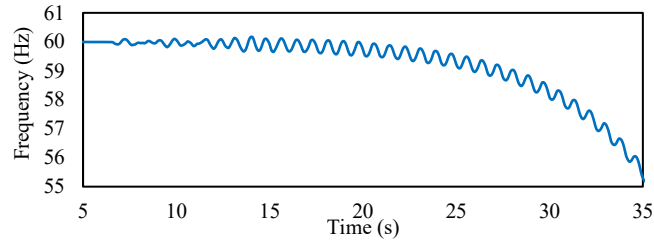


Figure 4-12: Output frequency of generator 6 in Scenario 4.

4.2.4.4 Attack Scenario 4

This scenario is achieved by utilizing the ability of DC chargers to control the power factor and the active/reactive power consumed/injected into the grid from the EV's battery [66] [36]. It is worth noting that all Level 3 fast/superchargers are DC, while Level 2 chargers can be AC or DC. Figure 4-12 demonstrates the severe drop in frequency, not just the oscillatory behavior, caused

by this attack scenario. Such a response would prompt the utility to trip generator 6 as well as other generators with similar behavior and possibly cause damage to the grid and consumers. The voltage in this scenario remained within the safe operation range until $t=27$ seconds. By then, however, the frequency started dropping sharply and the generators would trip forcing the grid into a blackout.

4.2.4.5 Attack Scenario 5

The voltage responses on buses 4 and 16 are presented in Figure 4-13. All bus voltages of the grid experience similar oscillations and 8 buses experience a voltage deviation beyond 0.05 pu which would trip the voltage relays. This attack impact is local to these buses and requires a faster oscillating EV load in comparison with the first three attack scenarios. This can be attributed to the fact that the voltage is mostly impacted by the generator's exciter which is an electrical system capable of a faster reaction than the turbine governors controlling the frequency.

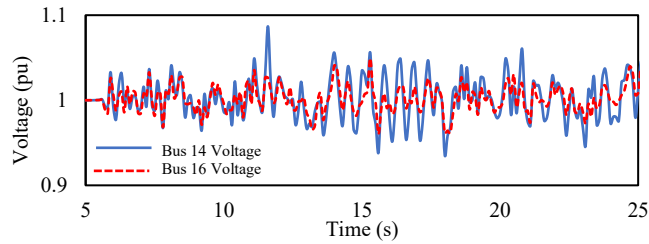


Figure 4-13: Bus 14 and 16 voltage.in Scenario 5.

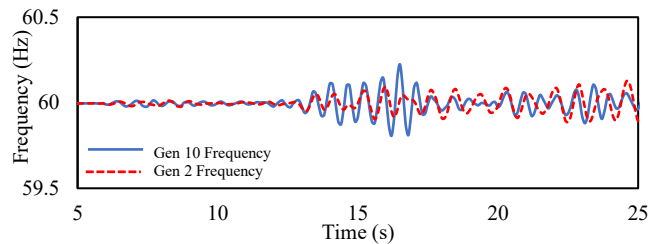


Figure 4-14: Output frequency of generators 2 and 10 in Scenario 5.

The frequency oscillations associated with this attack are depicted in Figure 4-14. No major frequency issues occurred since the EV attack trajectory was calculated to target only the voltage stability. From these results, we can say that the attacks against frequency stability are more impactful and are stealthier due to the slower attack load oscillations they require.

4.2.4.6 Smaller Attack Loads

In this case study, further experiments were conducted to demonstrate the impact of the attackers' ability to compromise different numbers of EVs. To this end, we re-examine the impact of Attack Scenario 2 under different EV attack magnitude caps between 100 MW and 800 MW (original Attack 2). Table 4-3 demonstrates the impacts of such attacks in terms of maximum frequency deviation and the time required for the attack to be sustained to force the generators to trip.

Table 4-3: Max Frequency Deviation vs Different Attack 2 EV Load Magnitudes

Attack Magnitude	Max Frequency Limit	Time until 1.5 Hz Deviation	Time Until Generator Tripping
800 MW	1.69 Hz	9.5 s	9.5 s
700 MW	1.51 Hz	14.1 s	14.1 s
600 MW	1.29 Hz	NA	34 s
500 MW	1.11 Hz	NA	34.1 s
400 MW	0.97 Hz	NA	9 min
300 MW	0.81 Hz	NA	9 min
200 MW	0.49 Hz	NA	NA
100 MW	0.29 Hz	NA	NA

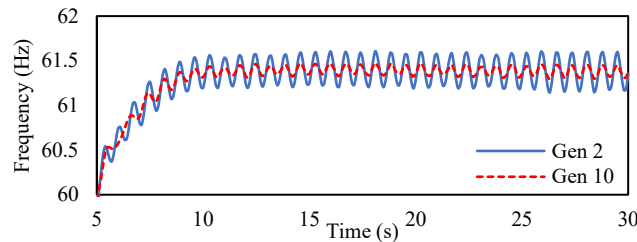


Figure 4-15: Output frequency of generators 2 and 10 in Scenario 6.

4.2.4.7 Attack Scenario 6: Faster and Less Constrained Attack

We now examine a new dynamic attack (Attack Scenario 6) based on the conditions outlined at the beginning of Section 4.4 while shifting the eigenvalues of the system further right (unstable region) than Attack 3 according to conditions $H(0,-1)$ and $D(0,1)$. Additionally, we remove constraint (4.25a) that limits the rate at which ΔP_{EV} grows resulting in faster oscillation of the attack load. While this attack was limited to a magnitude of 415 MW, it was able to achieve a 1.5

Hz frequency deviation within 4.6 s after the start of the attack as demonstrated in Figure 4-15. This serves to show that when the attacker chooses to risk using a faster-oscillating attack load, the resulting attack impact can be amplified.

4.2.4.8 Impact of Modeling Uncertainties

In this subsection, we examine the performance of our suggested attack strategy in the face of the different uncertainties that were modeled into the attack gain K . To establish a baseline, all the simulations are performed using a normal attack strategy that considers zero uncertainty, and the robust attack strategy designed in Section 4.1.5. We will first examine the impact of misestimating the size of the connected EV load under the attacker's control. To this end, we now simulate Attack 2 after subtracting $\emptyset$ in increments of 5% from each attack feedback signal. Table 4-4 represents the impact of EV load misestimation between 0% and 25%. Additionally, we consider an attacker with and without the ability to compromise further numbers of EV charging sessions.

Table 4-4: Impact of EV Load Uncertainty

$\emptyset$	Impact under normal attack	Impact under robust attack (without extra load)	Impact under robust attack (with extra load)
0	1.72 Hz	1.69 Hz	1.69 Hz
5%	1.6 Hz	1.61 Hz	1.69 Hz
10%	1.49 Hz	1.51 Hz	1.68 Hz
15%	1.38 Hz	1.4 Hz	1.67 Hz
20%	1.24 Hz	1.29 Hz	1.67 Hz
25%	1.13 Hz	1.2 Hz	1.65 Hz

More importantly, we examine the attack strategy's robustness in the face of uncertain grid parameters and small changes in dynamic behavior due to the difference in actual system dynamics and loading conditions between the model built during the reconnaissance phase and the actual time of the attack, T_a . To demonstrate the success of our robust attack strategy we examined the behavior of the attack under different grid uncertainty conditions varying between 0% and 25%. To demonstrate the result of this analysis, Figure 4-16 demonstrates the maximum frequency deviation that would occur in the case of a normal controller and our robust controller.

Figure 4-16 demonstrates how the impact of the attack decreases significantly the less accurate the attacker model is. However, when the robust attack is formulated to account for such uncertainties,

their impact on the frequency deviation (i.e., the attacker's objective) is reduced. The impact of the normal attack scenario experienced a decrease in terms of maximum frequency deviation from 1.72 Hz to 1.15 Hz, meaning the attack would no longer cause instantaneous generator tripping. On the other hand, the robust attack scenario proved to be more resilient to parameter uncertainty by maintaining an impact (maximum frequency deviation) above 1.495 Hz (in the case of 20% uncertainty). This demonstrates how although the robust controller is affected by uncertainty, it would remain more successful in achieving the attacker's objectives and would still cause generator tripping.

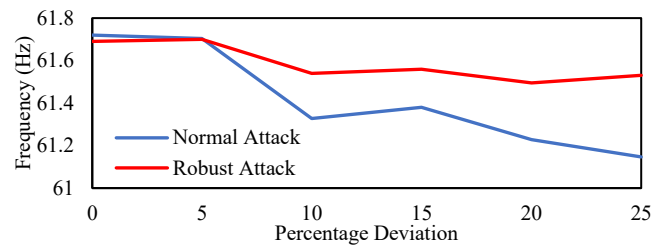


Figure 4-16: Maximum frequency deviation under parameter uncertainty

Table 4-5: Attack Scenarios Summary

Attack Scenario	Target	AR	Attacked Buses	Maximum Impact	Impact Severity	Attack Stealth	EV Oscillation	Load	Attack Difficulty
1	Frequency	H(0.5,0) and D(0,0.5)	3, 4, 24, 39	14 Hz Deviation	Devastating	Stealthy	Slow		Feasible (in the absence of PSS)
2	Frequency	H(0.5,0) and D(0,0.5)	3, 4, 18, 39	0.6 Hz Deviation	Moderate	Stealthy	Slow		Feasible
3	Frequency	H(0.5,0) and D(0,0.5)	3, 4, 24, 29	2.3 Hz	Extremely High	Most Stealthy	Very Slow		Feasible
4	Frequency	H(0.5,0) and D(0,0.5)	3, 4, 24, 29	5 Hz & Sharp Frequency Drop	Catastrophic	Stealthy	Slow		Moderate
5	Voltage	H(1,0) and D(0,1)	3, 4, 24, 29	0.1 Pu Voltage Deviation	High	Least Stealthy	Very Fast		Extremely Difficult
6	Frequency	H(1,0) and D(0,1)	3, 4, 24, 29	1.5 Hz Deviation	Extremely High	Stealthy	Fast		Moderate

4.2.4.9 Attack Impact Evaluation

The results of the attacks against the NE 39 bus grid are summarized in Table 4-5 for ease of reference. These results demonstrate the difference between the different variations of the attacks and the impact of using different ARs as well as the impact of targeting different buses. One important finding to highlight is that although the presence of the PSS reduces the original impact of the attacks, it cannot eliminate it. Additionally, in Scenarios 3, 4, and 6 the generator frequencies surpass 61.5 Hz leading to generator tripping even in the presence of the grid's strongest defense against such oscillations which is the PSS.

4.2.5 Discussion of Attack Results in the Context of Existing Literature

After the attack results were extensively discussed in the sections above, this section aims to compare the attack impact, feasibility, and limitations in the context of the existing studies in the literature.

4.2.5.1 Comparison to Static Attacks

as mentioned earlier in the context of [16] [55] [63] [64], static attacks have limited impacts that are restricted to given geographical locations due to their simplicity. Even the work in [55] demonstrated how static attacks have limited impacts. On the other hand, our EV-dynamic attacks can cause generator tripping and force the entire grid into a blackout within a few seconds of attack initiation. Additionally, the minor frequency disturbances caused by static attacks can be almost entirely eliminated through the action of the PSS. Yet even in the presence of a PSS, we demonstrated the success of dynamic attacks in causing the frequency to oscillate wildly and cause generator tripping.

4.2.5.2 Comparison to Switching Attacks

While switching attacks can eventually lead to generator tripping by causing large frequency deviations, they inherently have several limitations that make them less effective than dynamic attacks. First and foremost, the works in [57], [58], and [59] discussed earlier rely on the pre-existence of an unstable mode to be successful. In the absence of such an unstable mode that might naturally occur in a targeted power grid, the attacks will have severely limited impacts.

Additionally, depending on the frequency of the existing unstable mode, the required attack load oscillations might become difficult to achieve. The work in [65] for instance requires a switching attack with a load on/off frequency of exactly 26.81 switches per second to excite the sub-synchronous resonance unstable mode that exists in the target grid. Realistically, it is extremely difficult to achieve this fast-switching behavior while maintaining the proper synchronism required for attack success. On the contrary, our suggested dynamic attack can be crafted to have very slow oscillations to facilitate the EV load manipulation and remain as stealthy as possible. Additionally, all switching attacks suffer from one very significant limitation, i.e., their predictability. Given that the utility can easily identify the existing unstable modes using well-established system identification techniques [148], the power grid can be fortified against switching attacks or even natural phenomena that induce these instabilities [148]. On the other hand, dynamic attacks introduce a level of sophistication and unpredictability since they introduce new instabilities into the power grid that did not exist before. Theoretically, a dynamic attack can have a very large number of possible input (load bus)-output (target generator) configurations. Each of the combinations results in a different system representation with different possible attack scenarios. Additionally, since the attackers are not bound by any pre-existing unstable modes, the AR discussed in Section 4.1.3 can be any one of hundreds of possibilities. As a result, it would become rather prohibitive (almost impossible) to anticipate all the attack load oscillation frequencies, the attack load trajectories, induced instabilities, and system reactions to the specific attacks. This would eliminate the predictability of switching attacks which allow the utility to prepare for such attacks beforehand.

4.2.5.3 Comparison to Other Dynamic Attacks

As mentioned earlier, dynamic attacks require the attacker to have a state-space representation of the power grid. Our method involves probing the grid with a chirp signal followed by an ERA and then mathematically modeling the uncertainties in the grid model. Additionally, our modeling method accounts for the uncertainties that are introduced by the changes in grid dynamics that occur over a few hours and from one day to the next. On the contrary, all the models in [61] and [62] [68] assume that a single constant state-space captures all the variations in system dynamics throughout the time of day and over several days which is unrealistic. Further still, the work in [68] assumes that a state-space of a power grid can be modeled using generic parameters of the

generators typically used in a given power grid which is an oversimplification of the problem at hand. Furthermore, all of these discussed studies do not test their attack models on the actual grid and assume it is sufficient to examine the behavior of the estimated state-space model they developed. Finally, to the best of our knowledge, none of the existing dynamic attacks mathematically model the attack load uncertainty into their design to make the attack method robust against such uncertainties.

4.3 Chapter Concluding Remarks

In this chapter, we demonstrated how EVs can be modeled to mimic feedback loop controllers to destabilize a power system. The attack formulation is conducted from the perspective of the attacker who has performed an advanced reconnaissance method and successfully modeled the system as a state-space representation that accounts for the modeling uncertainties. The attacker then uses that model to design a robust attack strategy based on LMIs to cause unstable grid operations. Instability was achieved through compromised EVs equal to 6.6%-13.3% of the total grid load even in the presence of up to 25% uncertainty in the estimated grid parameters.

Chapter Five

Two-Tier EV-Based Attack Detection

Considering the harmful consequences arising from attacks leveraging EVs, we propose a two-tier DL LA detection mechanism. The first tier of the detector would monitor the entire collective of EVCS by being deployed on the CMS. This detector would search for anomalous mass charging/discharging and flag this behavior as an attack. The second tier of the detector would be a lightweight DL algorithm embedded in the EVCS itself (e.g., in the firmware or local management system). This algorithm would monitor the behavior of the individual EVCS and raise an alarm to the CMS if any local anomalous behavior is detected. The CMS would aggregate all the individual alarms it receives from the EVCSs and incorporate that into its decision-making process. This two-layer architecture assists in reducing the possibility of attacks going unnoticed by building redundancy into the system, examining the data at different points in the system, and eliminating any single point of failure for our detector. This two-layered approach also serves to reduce the stealth of the attacks. While the attacker might be able to manipulate the entire botnet of compromised EVs to craft an attack that remains stealthy to the CMS, the EVCS itself will need to be turned on and off by the attacker following a certain malicious pattern. Additionally, if the attacker successfully compromises an extremely large number of EVCSs and successfully distributes the attack load among them to fool the EVCS detector, the collective load monitored by the CMS detection algorithm will look anomalous thus exposing the attack. Finally, the DL algorithm deployed on the EVCS can be tuned to be extremely sensitive to attacks even at the expense of a few False Negatives (FNs). Even if the alarm raised by an individual EVCS is false, the overall architecture is immune to such kinds of false alarms. This is due to the CMS detector's decision-making based on all alarms received from all EVCSs thus diluting the impact of a single false alarm.

Additionally, due to the similarities of switching attacks and dynamic attacks at the level of EVCSs and CMS in terms of the anomalous behavior of charging requests/sessions, we tailor our detector

to recognize both dynamic attacks as well as switching attacks. To create a detector that can recognize attacks it has not seen before, we train it on a wide variety of attacks in terms of attack frequency, period, duty cycle, and attack magnitude. To demonstrate their effectiveness, the testing datasets on which the performance of our two models is evaluated contain attacks that were not part of the training dataset on which the algorithms were trained. The contributions contained in this chapter are summarized as:

- We develop a novel two-tier attack detection mechanism based on Neural Networks (NNs). The proposed detection mechanism is tailored against dynamic attacks as well as switching attacks to achieve a comprehensive detector specific to the EV ecosystem.
- We optimize a centralized CMS-based detector to identify attacks through the overall trend of charging behavior across the entire EVCS network and achieve a 99.9% detection accuracy.
- We develop a lightweight detector to be deployed on the EVCSs themselves for detecting attack and anomalous behavior from the perspective of a single EVCS as the last line of defense in the EV ecosystem. This detector is optimized and achieves an attack detection accuracy of 99.8%.

5.1 Detector Design

ML and DL have been used in recent years to solve problems that are not readily solved by traditional algorithms. ML and DL algorithms extract 100s of patterns and features from the input data that cannot be easily identified by traditional algorithms [153]. This is also performed without adding the same delays and computational overheads that would be required if such a task was attempted by using mathematical models. This is why the cybersecurity industry is witnessing a great adoption of ML and DL in the field of attack detection [154]. These learning algorithms offer the advantage of automating the retraining process of the classification algorithm [155] to keep up with the changing attack trends. ML and DL have also witnessed an increasing adoption in the area of power grids [156] for several complex real-time applications. More importantly, DL techniques have been used for fault detection in power grids [157] highlighting its importance in

critical power grid functions. The increasing importance of incorporating ML and DL into the area of dynamic power grid security has been highlighted in [158]. The authors emphasized that these algorithms are promising when moving from the traditional grids to the smart grid that incorporates external factors outside the utility's control [158]. The authors also stress the importance of future consideration of learning algorithms for instantaneous real-time power grid security applications [158]. In this regard, DL is also preferred over ML when large amounts of data need to be analyzed, by utilizing NNs [159].

5.1.1 CMS Detector Algorithm

Given that the CMS-based detector will be analyzing complex data representing all the EVCSs in the charging network, we choose the Convolution Neural Networks (CNN) for detecting the attacks from a global perspective. CNNs are DL algorithms that convolve the inputs to extract spatial features out of the input data. This is performed using filters which are matrix multiplication operations. These filters are then combined into kernels which allows the CNN algorithm to extract the spatial and temporal relationships between the different points of the input data [160]. This convolution also makes CNNs lighter than similarly sized fully connected NNs making them ideal for processing large amounts of data [159] while reducing the problem of overfitting caused by large and complex NNs. CNN is also preferred for detection due to the huge influx of data caused by the arrival of data from hundreds of thousands of EVCSs or mobile/web apps. Another advantage of using CNN is its ability to overcome the difficulty of determining whether a certain pattern in the arrival of charging requests is benign or malicious when the attack is well crafted. Some attacks utilize a small number of EVCSs and slow oscillations making them stealthy and resemble normal charging behavior. Also, in general, the attacks will resemble small perturbations in the overall charging pattern of the entire network making it extremely important to utilize a strong/complex algorithm capable of differentiating this behavior from benign perturbations resulting from normal user habits.

We also utilize the Relu activation function due to its ability to learn and incorporate non-linear relations and trends into our CNN [161]. This is especially beneficial for detecting dynamic attacks which are more complex than switching attacks since Relu allows the detection algorithm to learn the aggregate attack load complex behavior for more accurate detection. After the convolutional

layer extracts the features from the input, we utilize a Dropout layer [162] to nullify the contribution of some neurons. This is performed to prevent overfitting on the training data. Without dropout layers, the first batch of training data will disproportionately influence the learning ability and structure of the CNN. This process is repeated over several convolutional layers. We also take advantage of L2-Regularization [24] which penalizes large model weights and makes the model less sensitive to specific data points in favor of a more general structure. L2-Regularization also reduces overfitting and produces a smoother model performance. Finally, the features are fed into a single fully connected layer to perform the classification of the input as an attack or benign charging pattern. This CNN then takes advantage of Back-Propagation [163] to adjust the values of its kernels, filters, and neuron weights over several learning epochs by retraining itself based on the value of the losses and inaccuracies experienced in the previous learning epoch. Additionally, we utilize batch normalization to stabilize the input distribution to each convolutional layer during the training phase [160]. This normalization allows our CNN to converge on an optimal structure using fewer training epochs. We chose to utilize the “binary cross entropy” loss function which is preferred for binary classification problems especially when combined with the “sigmoid” output activation function. To this end, our detection mechanism was designed to take an input equal to 5 seconds of charging request history split into 0.1-second mini-slots. The specifics of the dataset are discussed below in Section 5.2.1.

5.1.2 EVCS Detector Algorithm

Given the limited memory and computational power onboard EVCSs, it is ideal to select a lightweight model to be deployed as the EVCS detector. Although some EVCSs can spare the required memory and computational power for moderately complex models, we intend to create a model that can be deployed even on the simplest and most lightweight EVCS. To this end a few models are possible, namely: (i) Single-Layer Perceptron (SLP), (ii) Multi-Layer Perceptron (MLP) with a single hidden layer, and (iii) Decision Trees. Ultimately, we select the MLP with a single hidden layer and eliminate the other models due to the following considerations. An SLP has one critical weakness due to its inability to learn non-linear relations in the data. While Decision Trees are considered good models for classification tasks, their memory requirements can grow exponentially if their size is allowed to grow unrestricted in terms of depth and number

of leaves per node. However, for the sake of an unbiased comparison, in our evaluation section, we compare Decision Trees with and without any size constraints. For the same reasons presented above, we utilize the Relu activation function, batch normalization, backpropagation, “binary cross entropy” loss function, and so on for our developed MLP.

5.2 Dataset Curation

A crucial aspect of the proposed detection mechanism is training the algorithms on comprehensive and realistic datasets. To this end, we created a data-driven model for the arrival and charging times of the EVs during normal behavior. To achieve a realistic EV charging behavior, we independently simulate a Poisson arrival process of EVs to each EVCS [164]. The charging time of these EVs is assumed to follow a truncated Gaussian distribution [164]. The parameters of these models are specified in seconds. These parameters are tuned based on a real dataset containing five years of records for 7,500 EVCSs in Quebec, Canada. This dataset was obtained from Hydro-Quebec as part of a research collaboration. However, the data required to train the CMS-based detector is different from the data required for the EVCS-based detector. Consequently, we discuss these distinct datasets below.

5.2.1 CMS Detector Dataset Curation and Collection

As mentioned earlier, the CMS-based detection algorithm needs to consider a holistic view of the entire charging network. As a result, we extract the average inter-arrival times and the average charging session durations from the Hydro-Quebec dataset and generate a similar model to the one discussed in Section 4.1. However, unlike in Section 4.1, a more granular model is created that records the aggregate number of active sessions in the entire network down to a 0.1-second granularity. Simulations are then performed for 250,000 EVCSs for 25 days independently. To create the training dataset, we randomly extract the data for 200 5-second windows from each of these 25 simulations for a total of 5,000 benign samples. Additionally, we generate 5,000 attack samples split equally between switching attacks and dynamic attacks. We vary the magnitudes,

periods, and duty cycles of the switching attacks and we construct the behavior of the dynamic attacks based on different variations of the AR proposed above as well as different values for the simple proportionality feedback controller proposed in [61] and [62]. These attacks are generated on top of an additional 5,000 normal samples to guarantee realism and capture the performance of the charging network when a portion of it is compromised and used for attacks while the majority of EVCSs are operating normally. Additionally, we extract the data for 1,000 benign samples and generate an additional 1,000 new and unique attack samples to form a dataset on which the performance of the detector is evaluated.

Furthermore, this data is pre-processed to extract useful information that can be used to train the detectors. This preprocessing is based on subtracting the average charging load calculated over the previous 1 minute to extract the variations in the total number of charging EVCSs. Beyond that, these variations are normalized by the mentioned average to achieve comparable data across the different times of day and avoid skewing the results in favor of the periods that have the largest number of active EVCSs (i.e., the afternoons). These two preprocessing steps would guarantee that the entire dataset represents the percentage variations in the number of charging requests. We created the following datasets based on the above discussion:

- CMS Detector Training Dataset comprised of 10,000 benign and attack samples split equally.
- CMS Detector Evaluation Dataset comprised of 2,000 benign and attack samples split equally on which the detector has not been trained.

5.2.2 EVCS Detector Dataset

As opposed to the previously generated datasets, the EVCS-based detector's datasets need to be from the perspective of a single EVCS. To this end, we examined the behavior of the average EVCSs in the Hydro-Quebec dataset as well as the behavior of the outliers. These outliers include the most highly loaded and the most lightly loaded EVCSs in Quebec. Additionally, we examined the EVCSs that demonstrated fast-arriving charging requests. This last category presents a unique case since some EVCSs occasionally experience multiple charging requests per minute. Upon investigation, we discovered that such behavior originates mainly from user error where sessions are started then stopped then started then stopped successively. However, this rapid on/off behavior

resembles a very slow-oscillating attack behavior which is why our model needs to learn how to distinguish between this abnormal benign behavior and the stealthy attacks.

As a result, we created a simulation profile for the arrival of benign requests at a single EVCS and generated 20,000 independent arrival and departure profiles. We made sure that each of these collected samples had at least one charging session that was running or that started during the recorded interval. 10,000 of these samples were reserved for the benign samples and 10,000 were used to augment the attack samples. The attacks, from an individual EVCS's perspective, are an on/off behavior regardless of the overall attack type (switching or dynamic). To this end, we generated 10,000 attacks with periods between 0.8 and 3 seconds and duty cycles varying between 25% and 75%. Since the attackers can split their attack among several EVCSs and reduce the switching behavior on each EVCS, the EVCS detector needs to monitor a relatively larger timeframe. Thus, we decided to use 30 seconds of data as the input sample to the detection algorithm for the benign as well as the attack samples. To generate the attack samples, we used the 10,000 samples of benign data that we reserved and replaced the last 2 to 6 seconds of these samples with the attack behavior. This guarantees that the model will learn to detect the fastest attacks in as little as 2 seconds and the slowest attacks in as little as 6 seconds. Finally, to ensure that the model remains light we only split the 30 seconds of input data into 0.5-second mini-slots where the events that occur on the EVCS are discretely allocated to these mini-slots. The generated data was then used to create the following two datasets:

- EVCS Detector Training Dataset comprised of 16,000 benign and attack samples split equally.
- EVCS Detector Evaluation Dataset comprised of 4,000 benign and attack samples split equally containing some attack scenarios that the model was never trained on.

5.3 Evaluation of Detector Performance

While classic ML algorithms have standard structures, NNs are configurable, and their properties are determined by their developer. The structure, activation functions, layers, number of neurons, and number of learning epochs are called hyperparameters. Another tunable parameter is the

testing and validation split of the data. At each learning epoch, the data is split into batches that are fed into the NN to optimize its weights. When the training of an epoch is done, it is tested against the validation subset to test its accuracy and modify the weights in the following epoch. To obtain the best combination of hyperparameters for each model, we utilize a random search algorithm. We utilize different random combinations of hyperparameters and select the combinations that offer the best results. The second step would be to finetune the best combination and test variations of these parameters in the immediate 10% vicinity of the parameters obtained in the first round. Random Search is widely adopted for hyperparameter tuning since it achieves similar performance to the extensive Grid-Search algorithm but requires much less computational complexity and time [165].

The performance of the CNN algorithm deployed on the CMS is also compared to an LSTM algorithm, an MLP, and a Decision Tree. The optimal hyperparameters of the DL models are presented in Table 5-1. The performance of the MLP algorithm deployed on the EVCS is also compared to an SLP algorithm, a Decision Tree with no restriction on size, and a Decision Tree limited to a maximum depth of 10 and a maximum number of 1024 leaves per node. The parameters of these models are presented in Table 5-2.

Table 5-1: Optimal Hyperparameters of the Different DL Algorithms Considered for the CMS Detector

Hyperparameter	Value		
Algorithm	CNN	MLP 1	LSTM
Hidden Layer Activation Function	Relu	Relu	Relu
Output Layer Activation Function	sigmoid	sigmoid	sigmoid
Neurons per Hidden Layer	[50]	[120, 40]	[100, 50]
Filters Size/ Kernel Size	4 / 3	-	-
Drop Rate	0.3	0.2	0.3
Learning Rate	0.1	0.1	0.01
Validation Split	0.2	0.2	0.1
Batch Size	128	64	256
Optimizer	SGD	SGD	Adam
Epochs	12	10	24

Table 5-2: Parameters of the Different DL/ML Algorithms Considered for the EVCS Detector

Hyperparameter	Value			
Algorithm	MLP 2	SLP	Decision Tree 1 (Restricted Size)	Decision Tree 2 (Unrestricted Size)
Hidden Layer Activation Function	Relu	-	-	-
Output Layer Activation Function	sigmoid	sigmoid	-	-
Neurons per Hidden Layer	[100]	-	-	-
Drop Rate	0.3	-	-	-
Learning Rate	0.1	0.1	-	-
Validation Split	0.2	0.2	-	-
Batch Size	256	120	-	-
Optimizer	SGD	SGD	-	-
Epochs	12	32	-	-
Max Depth	-	-	12	unrestricted
Max Leaves per Node	-	-	1024	unrestricted
Approximate Memory Requirements	24 kB	1 kB	50 kB	>> 50 kB

Table 5-3: Confusion Matrices of the CMS-Based Algorithms

Algorithm	Predicted Label \ True Label	Normal	Attack
CNN	Normal	1000	0
	Attack	1	999
MLP 1	Normal	1000	0
	Attack	6	994
LSTM	Normal	962	38
	Attack	17	983
Decision Tree 3	Normal	1000	0
	Attack	4	996

Table 5-4: Confusion Matrices of the EVCS-Based Algorithms

Algorithm	Predicted Label \ True Label	Normal	Attack
MLP 2	Normal	1993	7
	Attack	0	2000
Decision Tree 1	Normal	1970	30
	Attack	20	1980
Decision Tree 2	Normal	1978	22
	Attack	19	1981

5.3.1 Detection Algorithms Performance Evaluation

For a systematic evaluation of the different algorithms, we follow well-established metrics to assess the performance of the detection mechanisms suggested above. First, we present the results through the confusion matrices for all models except the SLP as it demonstrated extremely poor performance with an accuracy below 75% and misclassification of all the slow oscillating attacks. Table 5-3 and Table 5-4 demonstrate the confusion matrices of the CMS detectors and the EVCS detectors.

Additionally, we summarize the values of the metrics that are used to evaluate the performance of these algorithms in Table 5-5 and Table 5-6. These metrics are:

- Accuracy: which is the percentage of correctly classified samples.
- Recall: which is the percentage of attack samples that were correctly classified as attacks.
- Precision: which is the percentage of true attacks out of the total samples the algorithm classified as attacks.
- F1-score: which is the harmonic mean of precision and recall which is the preferred metric when evaluating classification algorithms.

Table 5-5: Performance Metrics of the CMS-Based Algorithms

Algorithm	F1 Score	Accuracy	Precision	Recall
CNN	99.95	99.95	100	99.90
Decision Tree 3	99.80	99.80	100	99.60
MLP 1	99.70	99.70	100	99.40
LSTM	97.28	97.25	96.28	98.30

Table 5-6: Performance Metrics of the EVCS-Based Algorithms

Algorithm	F1 Score	Accuracy	Precision	Recall
MLP 2	99.83	99.83	99.65	100
Decision Tree 1	98.75	98.75	98.51	99.00
Decision Tree 2	98.98	98.98	98.90	99.05

Based on the results presented in Table 5-2 through Table 5-6, our ultimate recommendation would be to adopt the CNN as the detection algorithm to be deployed on the CMS and the lightweight

single hidden layer MLP to be deployed on the EVCSs. Additionally, it is important to highlight that the MLP was tuned to be extremely sensitive to attacks. We developed another MLP having different parameters that suffered from 6 undetected attacks and zero misclassified benign samples. However, due to the sensitivity of the power grid, we opted for the version that is more sensitive to attacks and achieved zero misclassified attacks at the expense of 7 benign samples being seen as attacks raising false alarms to the CMS.

Finally, when combining the two detectors in a single system, the CMS can set a certain threshold for the number of alarms it needs to receive from the different EVCSs before considering the system under attack even when its detector is indicating otherwise. In the case of a single undetected attack using the CMS-based CNN detector, the CMS would have received hundreds or thousands of alarms from the different EVCS-based MLP detectors. Our recommendation is to set the threshold at 250 alarms representing an approximate 6.1 MW of attack load or 0.1% of the total grid load. Different thresholds can be selected after discussions between the utility and operator based on the specific size of the grid, the number of EVCSs an operator has, or any other factor that the utility and operator deem impactful. Alternatively, the operator can set the threshold as a percentage of the average number of EVCSs that are expected to be operating at a given time of day based on historical data.

5.3.2 Comparison to State-of-the-Art

Our proposed detection mechanisms outperform the other detectors discussed in the literature even when each of the two tiers is evaluated independently. Our proposed mechanisms offer a significant improvement over the mechanism in [58] that suffers from 30% false negative rates (misclassified attacks). Additionally, our CMS-based detector specifically was able to outperform the CMS-based detector developed in [58] after reading a maximum of 5 seconds of attack data while the detector in [58] requires a minimum of 20 seconds.

The LSTM model developed in [69] achieved comparable results to our work, with a recall and F1 score of 99% but they did not mention the time window after which detection was achieved. Their work also depends on detecting DoS attacks against the EVCSs which do not have a direct impact on the grid. Additionally, their detector is optimized to detect these DoS attacks by

monitoring the volume of incoming data packets to the EVCS which is in the order of hundreds per second for the case of DoS attacks. This mechanism would fail in our case since the attackers only need to send a maximum of 1.2 requests per second to the targeted EVCS. On top of that, their LSTM is a rather bulky NN that requires significantly more space than our lightweight single hidden layer MLP.

Moreover, the work in [71] proposed a DL model to detect attacks against the EVCSs in the form of malware. While promising, this detector does not offer an alternative to our proposed mechanism. Static and dynamic attacks do not require malware to be installed on the EVCS to succeed. Thus, the detectors of [71] cannot be used as a baseline to assess the performance of our detectors.

5.4 Chapter Concluding Remarks

In this chapter, we develop a two-tier attack detection mechanism tailored specifically to the EV ecosystem. The CMS-based detector was able to detect EV-based LA attacks from the perspective of the entire EVCS network as a collective with an accuracy of 99.95%. Additionally, the lightweight EVCS-based detector was optimized to identify attack and anomalous behavior from the perspective of a single charger. The sensitivity of this lightweight detector was biased towards attacks and as a result, was able to achieve a detection accuracy of 99.83% while suffering from zero misclassified attacks.

Chapter Six

LA Attack Detection and Localization Using a Physics-Assisted Feature Fusion Neural Network

Faced with the danger of LA attacks and the difficulty of detecting them using existing mechanisms, we propose a novel LA attack detection and localization mechanism capable of catching these attacks before they achieve the desired instability. This is increasingly vital given the relative ease with which attackers can manipulate high-wattage IoT devices as discussed in studies performed in partnership with multiple utilities [166] and cyber security companies [167]. Our novel detector is powered by a Feature Fusion Neural Network (FFNN) that is assisted by data pre-processing using the mathematical equations governing the dynamic behavior of the underlying physical system. This detector relies on a minimalist set of secure inputs which is the generator frequencies. These frequency measurements are reliable and are considered the most immune measurements against cyber-attacks [76]. These measurements are pre-processed using the mathematical/ physical model of the grid to estimate the load variation patterns on the individual load buses. This unique pre-processing of the input data and the subsequent FFNN enable our mechanism to accurately detect LA attacks and localize the exact bus/es from which the attack was initiated. Additionally, the parallel pre-processing performed by the FFNN allowing it to extract different feature types from the input data, makes it more immune to data poisoning attacks that aim to reduce its effectiveness and hinder its learning process. The contributions of this chapter are:

- Developing novel Physics-Assisted FFNN for the detection and localization of the three known types of LA attacks, i.e., static, switching, and dynamic attacks.

- Developing a method for data pre-processing using the mathematical equations of the underlying physical system making the FFNN transferable to other power grids without the need for retraining.
- Designing a robust FFNN that is resistant to three common types of data poisoning attacks and capable of maintaining high detection accuracy even after the training data has been significantly poisoned.

6.1 Grid Modeling and Detection Methodology

In this section, we discuss our detection mechanism starting with the mathematical model used to pre-process the generator frequency followed by the FFNN design. The first step towards achieving our detection goals would be the representation of the power grid in state-space form. Equally important is the utility's ability to recover the grid's states by using state-observers. After establishing the grid representation and the observer design, we introduce our load pattern recovery block required to successfully estimate the load fluctuation patterns. These patterns are then used as the input to the FFNN to classify the data and detect attacks.

6.1.1 Power System Representation

In this sub-section, we present the power grid state-space model from the utility's perspective. Figure 6-1 represents the architecture of our detection and localization mechanism including the mathematical/physical model and the FFNN. The attacker in block ① uses the attack models discussed above to launch their LA attacks. The state-space representation in block ② is constructed by the utility. The utility has perfect knowledge of the power grid's parameters and can represent its behavior with extremely high accuracy. The grid is linearized into a state-space model with the active and reactive power of the aggregate bus loads as the inputs and the generator frequencies as outputs. This representation is expressed in (6.1) where x , y , and u , represent the vectors of system states, outputs, and inputs, respectively. Additionally, ΔP_n , ΔQ_n , and f_{Gen_m}

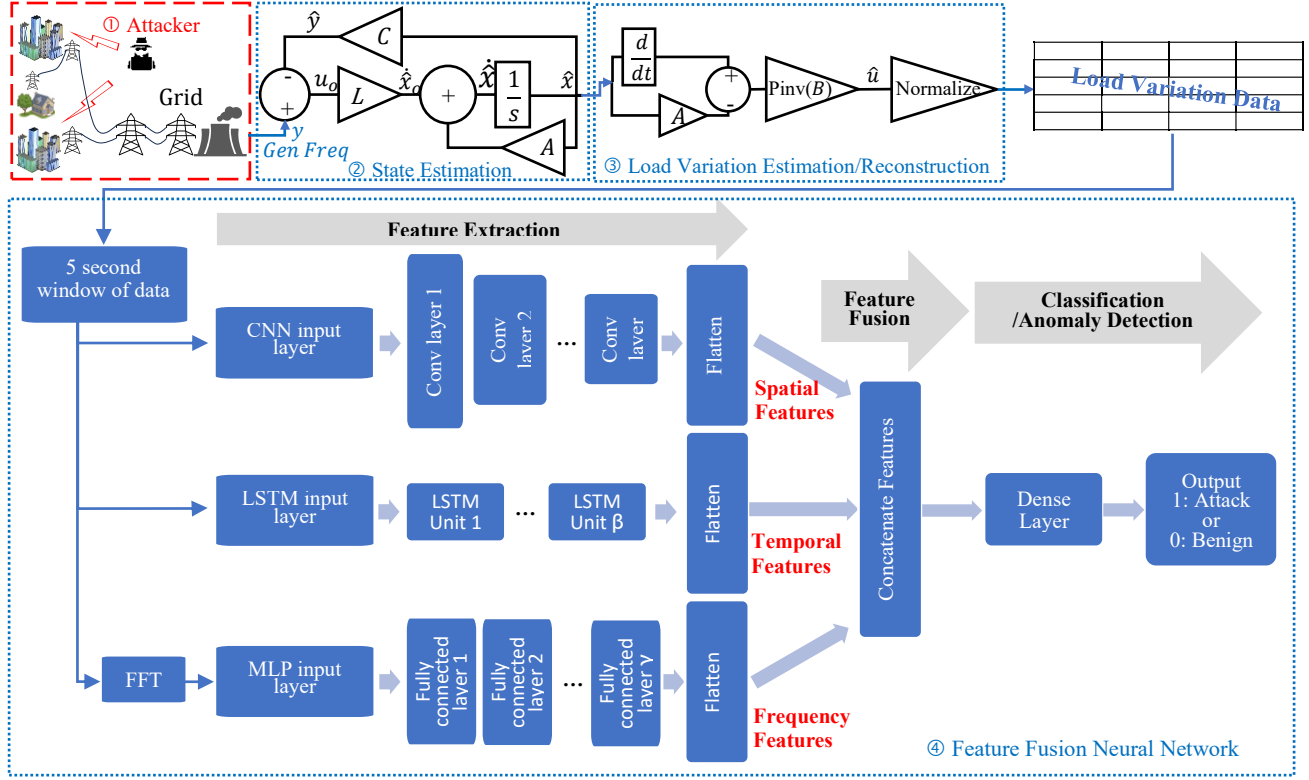


Figure 6-1: Detection mechanism based on load variation recovery and feature fusion NN

represent the change in active and reactive power of the aggregate load at bus n and the frequency of generator m respectively.

$$\dot{x} = Ax + Bu \quad (6.1a)$$

$$y = Cx + Du \quad (6.1b)$$

$$\text{such that } y = (f_{Gen_1} \ f_{Gen_2} \ \cdots \ f_{Gen_m}) \quad (6.1c)$$

$$\text{and } u = \Delta PQ_n = (\Delta P_1 \ \Delta Q_{E1} \ \cdots \ \Delta P_n \ \Delta Q_n) \quad (6.1d)$$

Block ② is constructed, based on the grid parameters and (4.1), then used to calculate the observer gain matrix L needed by the utility to approximate the grid states, $\hat{x}$, by multiplying the difference in its actual and calculated outputs ($y - \hat{y}$), by the observer gain L then feeding the observer output back into the state-space model. Finally, the model in block ③ represents the load variation estimation model used by the utility to approximate the unknown load variation patterns on the different buses. These patterns are then normalized by the nominal bus load to eliminate any bias towards large loads and fed into the FFNN in block ④ used for attack detection.

6.1.2 State Estimation and Load Variation Estimation

Since our physics-assisted detection mechanism relies on accurate recovery of the system states, the utility needs to choose an appropriate design for the observer gain matrix, L [150]. With the introduction of the observer L , (6.1) becomes (6.2).

$$\dot{\hat{x}} = A\hat{x} + L(y - \hat{y}) \quad (6.2)$$

To achieve reliable performance, we chose the Linear Quadratic Controller (LQR) technique [150] similar to the design in Section 4.1.6. The difference in this design is that the utility is unaware of the value of the input and uses this observer in conjunction with block ③ to estimate this unknown input. The output of the observer, L , is fed into the grid's state-space to estimate the states, $\hat{x}$. Using $\hat{x}$, we estimate the load variation patterns using block ③ in Figure 6-1. This block represents a mathematical approximation of the inverse of the state-space equation in (6.1) to become (6.3).

$$\hat{u} = B^{-1}(\dot{\hat{x}} - A\hat{x}) \quad (6.3)$$

The numerical derivative of $\hat{x}$ and the multiplication of matrix A and $\hat{x}$ are subtracted and the result is multiplied by the pseudo-inverse of matrix B . Since the number of inputs is always less than that of states, B always satisfies $B_{l \times m}$ such that $l \leq n$, making it right invertible.

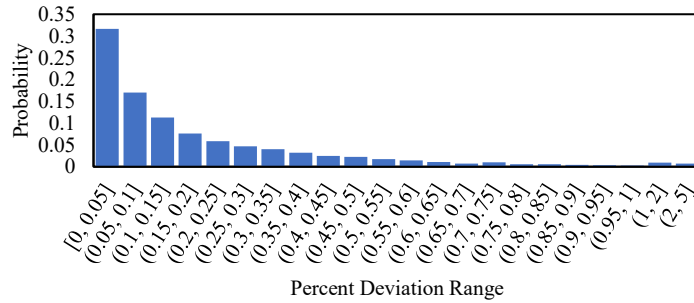


Figure 6-2: Histogram of error in load variation reconstruction probability

Figure 6-2 demonstrates the probability of the percentage error in load recovery using block ③. The average absolute error was 0.21% which means our model accurately recovers the actual load variations on the buses. The estimated load pattern at each bus is then normalized by the nominal bus load to make all recovered load patterns comparable and avoid biasing the NN.

6.1.3 Design of Detector

After the load fluctuations, $\hat{u}$, on the individual buses have been estimated, they are fed into our classification algorithm. Due to the difficulty of differentiating stealthy attacks from benign load fluctuations, we chose to utilize a DL algorithm for our classifier. ML and DL have been used in recent years to solve problems that are not easily solved by traditional algorithms. ML and DL algorithms extract hundreds of patterns and features from the input data that cannot be easily identified by traditional algorithms [153]. This is also performed without adding delays and computation overheads introduced by mathematical models. This is why the cybersecurity industry is witnessing a great adoption of ML/DL in the field of attack detection [154]. These algorithms also offer the advantage of automating the retraining process on new data [155] to keep up with the changing attack trends.

Subsequently, ML/ DL have witnessed increased adoption in power grids [155] due to their ability to perform previously computationally expensive calculations such as real-time classification and disaggregation of energy consumption of building loads [156]. More importantly, DL has been used for fault detection highlighting its importance in critical power grid functions [157]. The authors of [168] concluded that learning algorithms are extremely promising when moving from the traditional grid to the smart grid that incorporates more external factors outside the utility's control. The authors also stress the importance of future consideration of ML/DL for instantaneous real-time grid security applications [168].

DL is also preferred over ML when large amounts of data need to be analyzed, by utilizing NNs. Additionally, some attacks have low magnitudes and slow oscillations and/or have impacts resembling natural phenomena making them stealthy and hard to distinguish from the normal random load fluctuations. Also, attackers can distribute their attack over several buses to reduce its repetitiveness and make it even harder to detect. Given the criticality of our task and the danger of allowing even the smallest number of attacks to remain unrecognized, we chose to rely on FFNNs for our classification algorithm. FFNNs offer great advantages in determining whether a certain load variation pattern is benign or malicious when the attack is stealthy and well-crafted.

Due to their unique structure described below, FFNNs have enhanced feature representation of the input data. This stems from the parallel extraction of multiple types of features from the same data

to achieve a comprehensive representation of the data and capture the different features that might indicate different types of attacks. These diverse features allow the FFNN to learn a broader range of attack patterns leading to a higher accuracy and improved generalization from the training data to real-world scenarios (data patterns never seen before). This translates to a lower number of False Positives (FPs) and False Negatives (FNs) in the results. The parallel nature of the FFNN gives us the flexibility to independently tune the different branches to make the overall algorithm more sensitive to attacks (fewer FNs) or benign data (fewer FPs) to achieve the desired performance depending on the utility's priorities and end goal. A FFNN also has the ability to simultaneously handle heterogeneous data formats in its different parallel branches to provide a more holistic view/understanding of the load variation data and its underlying nature. By simultaneously examining multiple feature types, the model becomes more immune to noise and variability in the data. This makes the FFNN less likely to make wrong decisions based on outlier data and anomalies present in a single feature. More importantly, when combined with the regularization techniques discussed below, the model becomes robust against poisoned data in the training process by learning the general trend in each feature type making it extremely hard for an adversary to effectively poison the training data to mislead the model and deteriorate its performance.

In contrast to traditional NNs which are based on a single sequential string of layers, FFNNs are made up of several parallel branches. Each of these branches acts independently of the others and can have a different structure and network type. Each of these branches can then be fed with a different input to learn the features of the data from different unique representations of this data. In our work, we chose to utilize 3 parallel branches as depicted in Figure 6-1. The first branch consists of convolutional or CNN layers. This branch is responsible for the extraction of spatial features from the input data. The second parallel branch is made up of LSTM blocks meant to extract the temporal features embedded in the input data. And finally, the third branch is meant to process a different representation of the input data. We design the third branch to process and extract frequency domain features from the data. This is achieved by applying the Fast Fourier Transform (FFT) to the data to calculate its frequency response. FFT is preferred over the traditional Fourier Transform (FT) algorithm due to its significantly lighter computational complexity that is optimized for processing large amounts of digitized (discrete) data. This is why FFT is preferred for real-time data processing where minimizing the amount of added delay is critical to the proper performance of the overall process. Additionally, utilizing the FFT over the

traditional FT makes the overall process more resource-efficient since it requires significantly lower CPU resources. The frequency domain features calculated using FFT are then used as the input of a Multilayer Perceptron (MLP) as the third parallel branch in our FFNN. MLP is the basic form of NN that extracts abstract features from its input data. This is ideal to avoid the introduction of any significant changes to the type of features extracted from the frequency domain data. The kind of features extracted by an MLP is entirely data-driven meaning that the patterns in the data completely control the features learned by the MLP.

After each of the three parallel branches extracts their respective features from the input data, they are flattened into a 1-dimensional array each and fused (concatenated) before being fed into a fully connected dense layer for classification into attack or benign data samples. For optimal performance of the FFNN, we iteratively train it on the Training Dataset until the classification error loss function plateaus indicating that the FFNN has converged to the best model weights and any additional training epochs would not improve model accuracy indicating no further learning is occurring. To this end, we chose to take advantage of the “Binary Cross Entropy” loss function. “Binary Cross Entropy” is ideal for gradient optimization needed for more optimal weight optimization over the different training iterations of the FFNN. Additionally, this loss function allows for a stable convergence of the FFNN during training.

We also utilize the Relu activation function for the hidden layers in the three parallel branches due to its ability to learn and incorporate the non-linear relations and trends of the data into the FFNN structure [162]. This is especially helpful when dealing with power grids that are governed by non-linear relationships. After each layer in the 3 parallel branches, we utilize a Dropout layer [162] to nullify the contribution of some neurons. This is performed to prevent overfitting on the training data and avoid disproportionately influencing the FFNN’s learning based on the first training batch. This model then takes advantage of Back-Propagation [163] to adjust the values of its weights over several learning epochs by retraining itself based on the value of the losses and inaccuracies experienced in the previous epochs. Another important aspect is our usage of L2-Regularization [169] which penalizes large weights. This makes the model less sensitive to noise in the data and less sensitive to specific data points in favor of a more general structure resulting in a smoother more robust model.

The described FFNN is trained on the Training Dataset as described below and then tested against the Testing Dataset. The FFNN parameters are tuned, and training is repeated until the testing results are optimal. These datasets are described in more detail below. Based on the above, our FFNN was designed to take an input of 5 seconds of estimated load variation patterns. The 5-second windows are divided into 0.1-second mini-slots fed into the FFNN as 50 inputs. The load variation estimation block also allows us to localize the buses from which the attacks are launched.

6.1.4 Dataset Curation and Collection

This subsection discusses the generation of the datasets required to train and test the detector through simulations on standard IEEE benchmarks due to the lack of any real dataset that provides the required granularity. These benchmarks have constant loads representing the average load on the buses that utilities can estimate based on historical data. However, during short windows of time, such as 5 seconds, the load behavior of real consumers is random and centered around the average but cannot be predicted. These random load perturbations need to be incorporated into our grid to emulate its real behavior including normal frequency fluctuations. Thus, we will simulate these random normal load perturbations by adding random load blocks to all the load buses. These random load fluctuations are simulated as random Gaussian perturbations and random Uniform perturbations [170]. The standard deviation and range of the Gaussian and Uniform distributions are varied in every simulation run. It is established that NNs can learn the pseudorandom number generator patterns (pattern effect) [171]. To overcome the pattern effect, we use the Mersenne Twister algorithm with a period of $2^{19937} - 1$ making our random numbers appear truly random and impossible to learn by any NN [171]. Further randomness is guaranteed by shuffling the random generator's seed before each simulation. Finally, to emulate the behavior of real measurement devices that will be used to collect the generator frequency in real-life deployment, we add a White Gaussian Noise with a Signal-to-Noise ratio of 10 dB [170] to the frequency measurements.

The above-discussed simulation environment is used to create the independent datasets below:

- A dataset comprised of 25,000 benign samples and 25,000 attack samples is created to train the FFNN and optimize its performance. This data is split into 80% to be used for training the

FFNN called the Training Dataset, and 20% for testing and optimizing the FFNN's structure and performance called Testing Dataset.

- A Deployment Evaluation Dataset comprised of 2,500 benign and 2,500 attack samples generated on a different grid. This dataset is used to evaluate the performance of our detection mechanism in conditions resembling real-world scenarios where the detector has to perform its job against data that it has never encountered before. This is achieved by generating attacks that follow the general assumptions of the training data attacks but with parameters that the detector has never encountered before. Additionally, owing to our unique mathematical/physical data pre-process method, our NNs are transferable to other grids without the need for retraining. The utility/defender is only required to use the correct mathematical model of the new grid.

The attack features, random number type, standard deviation, and random number range were changed in every simulation run. The samples in the Training and Testing datasets were generated from approximately 250 independent simulations. The samples in the Deployment Evaluation Dataset were generated from approximately 620 independent simulations. These datasets incorporate the three known types of LA attacks, i.e., static attacks, switching attacks, and dynamic attacks. To this end, 20% of the attacks were static while the switching and dynamic attacks represent 40% each. The magnitude of these attacks varied between 7% and 30% of the nominal bus load and their period and duty cycle were changed between one simulation and the other. The dynamic attacks were constructed using the methodology presented in [60], [61], and [62]. We highlight that half of the switching and dynamic attacks in the Deployment Evaluation Dataset are stealthy attacks that are undistinguishable from the benign samples in the absence of a proper detection mechanism.

6.1.5 A Family of Detectors for Systematic Comparison

In addition to the FFNN that is at the core of our detection mechanism, we develop 9 other ML and DL algorithms as well as a FFNN with just the first two parallel branches. This is meant to evaluate the performance of our FFNN-based detector against algorithms that are commonly used for the classification of data having similar properties as our data. To this end, we develop 4 ML algorithms namely:

- Support Vector Machine (SVM): works by identifying the optimal hyperplane that separates the different classes to maximize the margin between these classes.
- Decision tree: classifies the data by running it through a flowchart-like structure and making binary decisions at each node until it finally assigns a class label to the data.
- Random Forest: aggregates multiple Decision Trees, trained independently on random subsets of the dataset, and performs classification by majority voting among the trees.
- K-Nearest Neighbors (KNN): classifies new data based on a distance function calculated relative to the 'K' nearest neighboring training data points.

The supervised DL algorithms are the MLP, LSTM, and CNN. We also develop a bi-directional LSTM (Bi-LSTM) that extends the traditional LSTM by processing the data in the forward and backward direction enhancing the algorithm's understanding of the underlying temporal features in the data. Additionally, we developed 2 unique implementations of the traditional LSTM. The input data for these two models is reshaped differently so that LSTM1 considers the 50 mini-slots as 50 features for 1 datapoint while LSTM2 considers them 50 sequential datapoints.

Additionally, we examine the possible detection results if an unsupervised model such as an Autoencoder (AE) is used. AEs are extremely powerful models that do not require training on malicious data but rather only on a benign dataset. The AE works by creating a compressed (encoded) version of the input data followed by expanding (decoding) it to reconstruct the input data at the output layer [172]. This AE is tuned to minimize the reconstruction error. When classifying benign data, the AE would exhibit low reconstruction error, while reconstructing malicious attack data would result in high values of this error. As a result, we chose the Mean Squared Error (MSE) as our reconstruction error loss function [172]. As the MSE drops, it indicates the convergence of the reconstructed output and the input data signifying the presence of benign data [172]. This is why the AE would be followed by a classification layer based on an MSE threshold selected during the optimization of the AE.

6.2 Case Studies and Performance Results

This section discusses the tuning and performance of our FFNN and the obtained result in comparison with other ML and DL algorithms. The New England (NE) 39-bus grid in Figure 6-3 is used to create the “Training” and Testing Datasets for our FFNN. The NE 39-bus grid has 39 buses, 10 generators, and 19 loads with a total demand of 6,097 MW. Additionally, we utilized the Kundur 2-area grid in Figure 6-4 to generate the Deployment Evaluation Dataset. This is to test our detector’s performance on data it has never been trained on before, mimicking real-life deployment. This also demonstrates the transferability of the FFNN to a different grid without retraining. The Kundur grid has 11 buses, 4 generators, and 2 loads with a total demand of 2,736 MW. All simulations were performed using MATLAB-Simulink 2020 Specialized Power Systems Toolbox with a step size of 10^{-12} to 10^{-9} .

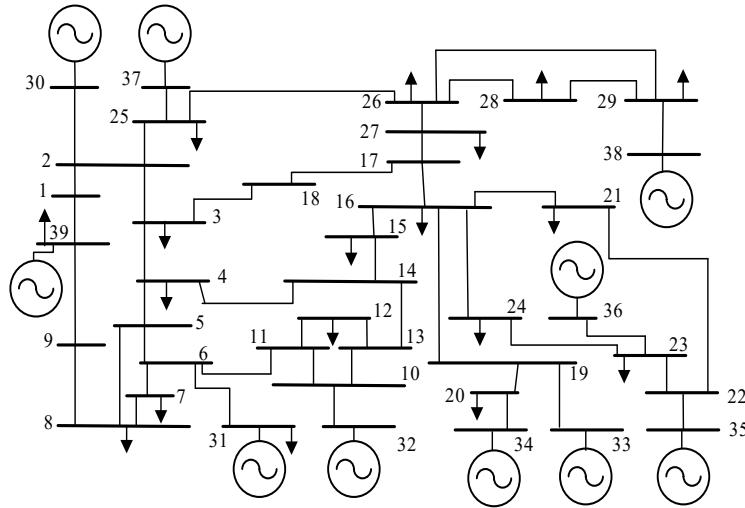


Figure 6-3: New England 39-bus grid

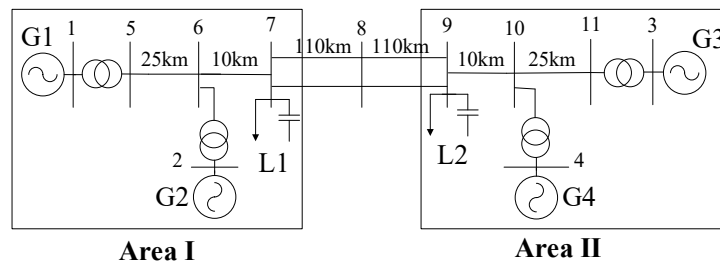


Figure 6-4: Kundur 2-area power grid

Since the grid's dynamic behavior mostly depends on its generators and their control systems, we use the models that are widely accepted in similar studies [133], i.e., (i) round rotor synchronous machine of order 6, (ii) IEEE T1 exciter, (iii) single mass IEEE G2 steam turbine prime mover, and (iv) IEEE Std 421.2 Power System Stabilizer (PSS).

6.2.1 Tuning of Detection Algorithm Parameters

Unlike classical ML algorithms, NNs have configurable properties tuned by their developer. The FFNN and the other 5 NNs are optimized by tuning their hyperparameters as discussed below. The FFNN and the 4 supervised DL algorithms were trained on the Training Dataset while the AE was trained on the benign portion of the same dataset. All these 6 algorithms were optimized on the Testing Dataset to achieve their optimal performance. Beyond that, the FFNN and the other models are all tested against the Deployment Evaluation Dataset to mimic real-life deployment.

For each model, we applied a Refined Random Search algorithm to tune the hyperparameters. Random Search is widely adopted for hyperparameter tuning since it achieves similar performance to the Grid-Search algorithm but requires less computational time [165]. During the first round of tuning, we utilize random combinations for these hyperparameters. After determining the structure with the highest F1-score, we initiate a second round of refined tuning based on random combinations of hyperparameters in the neighborhood of the optimal values of the first round.

Table 6-1: Hyperparameters of the Supervised DL Algorithms

Hyperparameter	Value				
Algorithm	CNN	MLP	LSTM1	LSTM2	Bi-LSTM
Output Activation Function	sigmoid	sigmoid	sigmoid	sigmoid	sigmoid
Hidden Layer Activation Function	Relu	Relu	Relu	Relu	Relu
Hidden Layers	1	2	2	3	3
Neurons of Layer 1	50	100	100	50	50
Neurons of Layer 2	-	100	35	100	100
Neurons of Layer 3	-	-	-	50	100
Filters	4	-	-	-	-
Kernel Size	3	-	-	-	-
Drop Rate	0.1	0.1	0.1	0.2	0.4
Learning Rate	0.1	0.1	0.01	0.001	0.001
Validation Split	0.2	0.1	0.1	0.2	0.2
Batch Size	128	64	32	64	256
Optimizer	SGD	SGD	Adam	Adam	Adam
Epochs	10	20	30	12	16

We present the optimal hyperparameters of the supervised DL algorithms and the AE in Table 6-1 and Table 6-2 respectively. Finally, Table 6-3 presents the hyperparameters of the optimized FFNN having the same structure as the 3-branched network depicted in Figure 6-1.

Table 6-2: Hyperparameters of the AE

Hidden Activation	Hidden Layers	Drop Rate	Learning Rate	Batch Size	Epochs	Optimizer	Threshold
Relu	[50 25 50]	0.1	0.01	128	64	Adam	6.7

Table 6-3: Hyperparameters of the FFNNs

Hyperparameter	LSTM Branch	CNN Branch	FFT - MLP Branch
Parallel Branch Hidden Layer Structure	[16 32 16]	-	[50 100 10]
Parallel Branch Filters	-	16	-
Parallel Branch Kernel Size	-	8	-
Parallel Branch Drop Rate	0.3	0.3	0.3
Hidden Layers Activation		Relu	
FFNN Output Activation		Sigmoid	
FFNN Learning Rate		0.001	
FFNN Optimizer		Adam	
FFNN Validation Split		0.2	
FFNN Batch Size		256	
FFNN Epochs		32	

6.2.2 Deployed Detector Performance

The performance of the different algorithms is evaluated based on well-established metrics. First, we present the results through the confusion matrices of all 11 models in Table 6-4. Additionally, we examine the performance of a 12th model that we call 2-FFNN, i.e., the FFNN after removing its FFT/MLP branch. It is noteworthy that tuning the 2-FFNN yields a hidden layer structure of [32 64 32] for the LSTM branch while the CNN branch remains unchanged. While Table 6-4. presents the numerical results of the different algorithms, a more systematic method is required to objectively compare their results. To this end, Table 6-5 summarizes the values of the four metrics on which we base our evaluation. The first metric is accuracy or the percentage of correctly

classified samples. Recall or the percentage of attack samples that were correctly classified (complement of the FN rate) is also considered. We also examine precision, which is the percentage of actual attacks out of the total samples classified as attacks. Finally, the F1-score is the harmonic mean of precision and recall which is preferred when evaluating classification algorithms.

Table 6-4: Confusion Matrices of the ML/DL Algorithms

Algorithm	Predicted Label		Normal	Attack
	True Label			
FFNN	Normal	2495	5	
	Attack	0	2500	
2-FFNN	Normal	2492	7	
	Attack	1	2499	
CNN	Normal	2482	18	
	Attack	2	2498	
LSTM1	Normal	2500	0	
	Attack	263	2237	
LSTM2	Normal	2453	47	
	Attack	139	2361	
Bi-LSTM	Normal	2500	0	
	Attack	47	2453	
MLP	Normal	2494	1	
	Attack	169	2331	
AE	Normal	2500	0	
	Attack	21	2479	
SVM	Normal	2499	1	
	Attack	23	2477	
KNN	Normal	2500	0	
	Attack	347	2153	
Decision Tree	Normal	2421	79	
	Attack	173	2327	
Random Forest	Normal	2500	0	
	Attack	68	2432	

The results in Table 6-4 and Table 6-5 demonstrate the performance of the different algorithms and show that while all have high accuracy owing to the unique mathematical/ physics-based pre-processing, the proposed FFNN proved to have superior performance over all other models. It is worth noting that, on average, the NNs performed better than the ML algorithms. More importantly, the 3 branched FFNN was the only algorithm to detect all the attacks successfully without having a single FN. While some other algorithms such as the AE did not encounter any FPs, their inability to detect over 20 attack scenarios is troublesome given the devastating impacts that could arise due to these attacks. It is also noteworthy, that among the algorithms that experienced no FPs, the AE is the single algorithm that demonstrated acceptable attack detection

results highlighting its unique nature and strength. The 2-FFNN also demonstrated great results in comparison to the other algorithm underscoring the power embedded in our design due to the parallel examination of unique feature types in the input data. Additionally, we re-tuned the parameters of the FFNN to make it more sensitive to benign data achieving a zero FP rate. However, the price of that result was the misclassification of a single attack scenario. From our perspective, the FFNN presented in Table 6-4 remains the optimal choice for a utility to defend its grid against LA attacks. This analysis is in line with the results in Table 6-5 which demonstrates how the FFNN has the highest F1-Score and accuracy at 99.9% and the highest Recall at 100%.

Table 6-5: Performance Metrics of the ML/DL Algorithms

Algorithm	F1-Score	Accuracy	Recall	Precision
FFNN	99.90	99.90	100	99.80
2-FFNN	99.84	99.84	99.96	99.72
CNN	99.60	99.60	99.92	99.28
AE	99.58	99.58	99.16	100
SVM	99.52	99.52	99.08	99.96
Bi-LSTM	99.05	99.06	98.12	100
Random				
Forest	98.62	98.64	97.28	100
MLP	96.38	96.50	93.24	99.74
LSTM2	96.21	96.28	94.44	98.05
Decision tree	94.86	94.96	93.08	96.72
LSTM1	94.45	94.74	89.48	100
KNN	92.54	93.06	86.12	100

6.2.3 Comparison with State of the Art

Our proposed Physics-Assisted FFNN detection mechanism offers tremendous advantages over the other detectors proposed in the literature. Our proposed mechanism offers significant detection rate improvements when compared to the work performed in [58] that suffers from a 30% attack misclassification rate. Additionally, our detector was able to detect all the attacks in less than 5 seconds after attack initiation as compared to the detector in [58] which requires a minimum of 20 seconds. Additionally, our FFNN is superior to the detector developed in [76] and suffers from a 7% FN. Furthermore, our detector's FP rate is significantly lower than that in [58] and [76]. Two additional algorithms were developed in [173] and [174]. While promising, these two methods are solely meant to detect a single form of dynamic attack, i.e. the attack in [62].

6.2.4 Robust Performance Facing Data Poisoning Attacks

One major drawback of data-driven detection mechanisms is their reliance on the collected data for a reliable training and classification process. These datasets are prone to be maliciously contaminated by adversaries through data poisoning campaigns when the utility is collecting data for detector training. To this end, we examine three types of data poisoning attacks.

The first of these attacks is the label flipping attack [175] [176]. This attack occurs when a malicious actor intentionally alters the labels of a portion of the dataset to hide certain attacks from being detected. This attacker requires access to the training data which can take place at the data collection stage where some attacks are given a benign label. Another method to achieve this attack is through access to the entire dataset and flipping a portion of the attack data labels to make them appear benign to the detector during the training phase.

The second type of data poisoning attack is the trojan attack [177] [178]. These attacks are based on the idea of embedding a trigger signal in the training data so that the model learns to associate this trigger with a certain label. In our specific scenario, the attacker would embed this trojan in a portion of the benign data used for training. The attacker would then embed this same trojan into the actual attacks in an attempt to force the detector to classify them as benign data due to the presence of the features of the trigger signal associated with the poisoned benign data.

The third type of data poisoning we examine is the perturbation attack [179] [180]. To realize this attack, a malicious actor would have to induce small perturbations in the training data that are sufficient to induce altered features to be extracted during the training phase. This is achieved by introducing very small perturbations resembling the attack data, into the benign data samples during data collection. This perturbation is small enough not to cause any grid stability issues but would force the detector to learn some of the attack features as part of the benign data samples during training. To this end, we perform the following case studies examining these 3 types of data poisoning attacks.

6.2.4.1 Data Flipping Attacks

To test our detector's performance, against this type of attack we retrain our detector on the original dataset but with the labels of certain attack samples flipped. Additionally, we chose to flip these

labels following two possible attacker strategies. The first strategy is an attacker that randomly flips the labels of a certain percentage of attack samples. This resembles an attacker who has the sole intention of confusing the detector without any advanced tactic in mind. The second strategy is that of a more sophisticated attacker that properly selects to flip the samples that can cause the most confusion for the detector and cause a wider range of attacks to be misclassified. This strategy is achieved by flipping the label of the stealthiest attacks i.e., the slowest oscillating attacks and those having the lowest magnitudes such that they are comparable to the benign data.

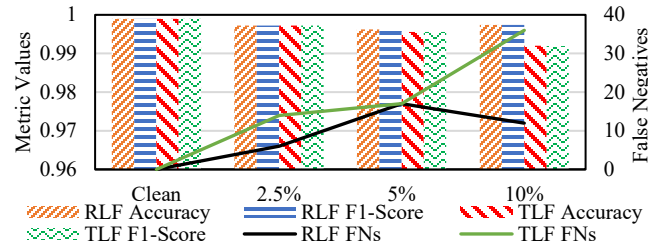


Figure 6-5: Results of random label flipping and targeted label flipping attack

We now generate 4 datasets for each of the two attacker strategies above, each containing a different percentage of flipped labels varying between 0% and 10%. The results of the two attacks on the detector performance are presented in Fig. 4. As evident from Fig. 4, a Random Label Flipping (RLF) attack does not guarantee any significant impact on the detector performance. In all cases even when considering an attacker that has successfully compromised an extremely high number of data samples of 10% the number of misclassified attacks remained below 17 and the detector maintained an accuracy and F1-score above 99.6%. In the case of a well-crafted and Targeted Label Flipping (TLF) attack, the attacker is more successful in deceiving the detector. However, our physics-assisted FFNN-based detection mechanism is designed to be robust against such types of attacks. Figure 6-5 demonstrates that although more successful than the RLF, a TLF attack compromising as much as 10% of the attack sample labels within the training data is only capable of lowering our detector's accuracy and F1-score to 99.2% and causing the detector to suffer from 36 FNs. This performance is still superior to 7 of the 10 other algorithms in Table 6-5 even when they were trained on clean data.

6.2.4.2 Trojan Attacks:

While trojan attacks are a powerful form of data poisoning attack, it is considerably more difficult to mount in the context of LA attacks against power grids. Such attacks require the attacker to actually manipulate the grid’s loads and inject the trigger signal while the utility is collecting data. To this end, the attacker needs to know when the utility is collecting its data. During this time the attacker would manipulate the grid’s actual loads to initiate oscillations that are too small to cause any stability issues. These oscillations would follow a predetermined waveform representing the trigger signal so that the utility would associate it with the collected benign data.

As a result, it is extremely unlikely that an attacker would be able to compromise a very significant number of samples. However, for the sake of a fair comparison, our trojan attacks also range between 0 and 10%. However, during the actual attacks, the attacker would always introduce this trigger signal. This is why all the attack samples in the Deployment Evaluation Dataset contain this signal. The results of this experiment are presented in Table 6-6 and demonstrate the immunity of our Physics-Assisted FFNN to such attacks up to a level of 10% sample poisoning. The results demonstrate that this type of attack is more impactful than TLF causing a 2.5% drop in accuracy and F1-score at 10% compared to the 0.7% drop caused by label flipping. This can be attributed to the fact that the trojan attack manipulates the features that an NN extracts from the data making them more impactful on the learning process. The label flipping attacks are less successful since our FFNN learns complex patterns and general trends eliminating the impact of “outlier” data on the trainable parameter weights.

Table 6-6: Results of the Trojan Attacks

Poisoning Level	F1-Score	Accuracy	FNs	FPs
Clean Data	99.90	99.90	0	5
2.5% poisoning	99.82	99.82	9	0
5% poisoning	98.67	98.66	20	47
10% poisoning	97.58	97.56	44	78

Yet our detector has proven its robustness against such attacks by maintaining an accuracy and an F1-score above 97.5% even when as much as 10% of the training data is poisoned with trojans. This is to say that even in the face of a powerful attacker that can compromise the grid, unhindered 10% of the time, while the utility collects its dataset, the detector’s performance only drops by 2

percentage points and maintains a performance that is superior to other works in the literature and the other algorithms tested in this study.

6.2.4.3 Perturbation Attacks:

The attacker would mount this attack by oscillating the grid's loads in a manner resembling switching and dynamic attacks but with low magnitudes that are too small to induce any instabilities in the grid. The utility would then collect these measurements as part of their benign data samples. To this end, we use this methodology to poison the Training Dataset benign samples up to 10%. However, like the trojan attacks, initiating these attacks is significantly challenging from an attacker's perspective. Through this attack, the adversary aims to force the NN to learn some of the actual attack features as part of the benign data. This is intended to reduce the detector's ability to successfully identify attacks during the deployment stage. The results of this experiment are presented in Figure 6-6 which demonstrates that this attack is stronger than label flipping, yet its impact on the detector performance is lower than trojan attacks. Additionally, our detector proved its immunity to such attacks that failed to cause the accuracy and F1-score to drop below 98.5%.

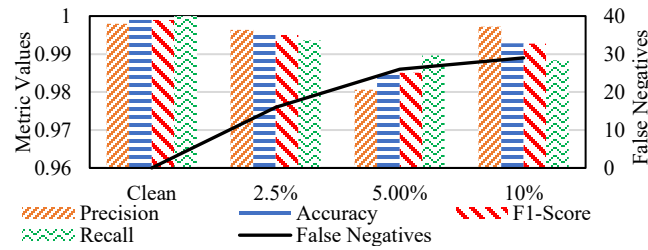


Figure 6-6: Results of perturbation attacks

6.2.4.4 Analysis of Data Poisoning Attacks' Results:

The FFNN's effective immunity against data poisoning is partially attributed to its ability to extract various unique feature types from the input data making it less vulnerable against attacks that target a single feature type. The usage of L2-Regularization also enhances the FFNN's robustness by minimizing its reliance on dominant features promoting a more balanced and general learning trend that accounts for all extracted features. Given that the trojan and perturbation attacks aim to create dominant features, this method enhances the FFNN's inherent robustness against these specific attacks.

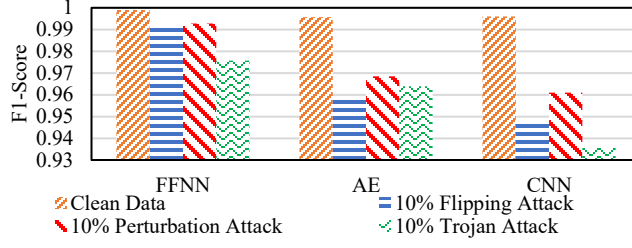


Figure 6-7: Data poisoning attack impact on the F1-score of the different models

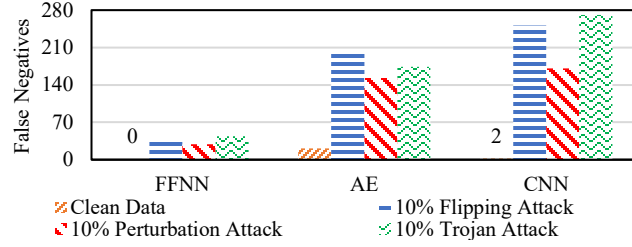


Figure 6-8: Data poisoning attack impact on FN rate of the different models

Figure 6-7 and Figure 6-8 demonstrate the results of the trojan, perturbation, and TLF attacks, at 10% poisoning, against the CNN and AE (2nd and 3rd best-performing algorithms). Figure 6-7 demonstrates a substantial deterioration in the performance of the CNN and AE compared to the FFNN when subjected to poisoning attacks. More critically, Figure 6-8 highlights the drastic increase in the number of FNs of the AE and CNN demonstrating how hundreds of attacks become undetectable. Relative to the FFNN, these attacks cause on average 6-7 times more FNs on the CNN and AE, demonstrating our FFNN is 7 times more resilient against these attacks.

6.3 Chapter Concluding Remarks

In this chapter, we presented a novel Physics-Assisted FFNN for LA attack detection and localization. The study was performed from the perspective of the utility that has an accurate state-space model of the grid. This model is used to pre-process the generator frequency measurements and estimate the load variation patterns before feeding them to the FFNN for attack classification. The proposed FFNN is transferable to different grids without any need for retraining as long as the correct mathematical model of the new grid is used for data pre-processing. This detection mechanism was able to achieve an accuracy of 99.9% when tested against data generated on a

different grid containing attacks with parameters it had never encountered before. Finally, we demonstrated our detector's robustness against three types of data poisoning attacks where the accuracy held firmly above 97.6% even when 10% of the training data was poisoned.

Chapter Seven

An EV Robust Mitigation Scheme Against Load Altering Attacks

The smart grid, however, became an interconnected system of physical and cyber components leaving it open to attacks initiated through the cyberinfrastructure that can have detrimental impacts on its stability and security [4]. Yet LA attacks against the grid demand side, rather than state estimation, can only be seen through their impact [16] bypassing the BDD.

Faced with the presented reality of the grid's vulnerability to LA attacks, we intend to create an LA attack mitigation scheme that takes advantage of the EVs' unique properties that are ideal for such a purpose. EVs can support the power grid by acting as distributed battery storage as well as distributed generators owing to the V2G power flow capability in new EV Charging Stations (EVCSs). These EV loads are also spread throughout the power grid such that their distribution covers all load buses. This widespread distribution makes EVs optimal for usage in a wide area controller. This distribution also means that the EVs are collocated with the other system loads that will be used by adversaries for LA attacks. This collocation gives EVs an edge since the disturbances can be efficiently eliminated at their source bus with minimal propagation to the rest of the grid. Finally, EVs have another advantage over generators when used to mitigate fast switching attacks, which is the speed at which EVs can change their load. Turbine generators are rotating machines, and their reaction times are determined by their size, type, weight, and control mechanisms and are usually in the order of several seconds [181] [182]. On the other hand, EVCSs are based on bidirectional power converters [37] that can change their charging rate and toggle between on, off, and V2G instantly [182] in the order of 1ms. This fast reaction time is needed to react to LA attacks especially those initiated from converter-based IoT loads. Furthermore, the current EV infrastructure for public EVCSs provides us with the communication and control mechanisms needed for our mitigation scheme. Public EVCSs are connected to the CMS [37] [41]

[42]. This CMS utilizes the Open Charge Point Protocol (OCPP) to communicate, monitor, and control all functionalities of the EVCSs in real-time. By utilizing this underlying infrastructure, our control mechanism removes the need for the addition of any new control software or hardware. Previous studies that have considered using EV loads to support the power grid fall short of achieving the mitigation capabilities suggested in this study. Most of these studies, some of which are discussed in Chapter 2, focus on using EVs to support the power grid during its steady-state operation. Other studies use EVs passively for load balancing [183].

Based on the above discussion, in this chapter, we create a robust wide-area controller based on mixed H_2/∞ controller synthesis that utilizes the EVs as its control inputs to mitigate the impact of persistent static, switching, and dynamic attacks even when they are sustained for long durations. We follow a detailed methodology to evaluate the performance of the controller and examine its performance in comparison to H_2 and H_∞ controllers. The performance of this family of controllers makes them an ideal starting point for our mitigation scheme. The Linear Matrix Inequalities (LMIs) of the controllers are modified to fit our system and incorporate the uncertainties of the EV connection to the grid resulting in the formulation of a family of robust controllers. The robust controller formulation is meant to overcome the deployment obstacles that can cause uncertainties in the control signal sent from the utility to the participating EVs. To the best of our knowledge, this is the first work to consider using EV charging loads in a scheme meant to mitigate the 3 known types of LA attacks. The contributions contained in this chapter are summarized as:

- We are the first to propose a robust mixed sensitivity wide-area controller that utilizes EV active and reactive charging load to stabilize the power grid during the 3 known types of LA attacks. Our control mechanism successfully eliminates the impact of persisting attacks without the need for a detection mechanism. Our mixed controller eliminates over 99.6% of the attack impact and returns the frequency to its normal operating range instantaneously.
- We design our robust feedback controller to account for uncertainties introduced by real-life deployment obstacles. We mathematically model this uncertainty and incorporate it into our controller synthesis. We are the first to study the stability of wide-area controllers under these uncertainties in the context of smart grid cyber-physical security.
- We demonstrate the effectiveness of our proposed EV-based mitigation mechanism through extensive time-domain simulations. These simulations show how the devastating impact of the

3 known types of LA attacks is eliminated completely and instantaneously while having a negligible impact on the range of the participating EVs as well as negligible cost.

7.1 System Modeling and Mitigation Methodology

In the following section, we discuss the defender model and the synthesis of our proposed EV-based controller to be used as our mitigation scheme against LA attacks targeting power grids. In this section, we explain the utility's state-space model of the grid. We then present our observer design that is needed to recover and incorporate the power grid's states into the state-space model. We then move on to discuss our EV-based mitigation controller selection and walk through the synthesis of the controller to fit our scenario and achieve the desired results. Finally, we address the looming issue of the impact on EV users under such a scheme.

7.1.1 Power System Representation and Defender Model

As a utility, the defender is assumed to have all knowledge of the grid's parameters and is thus able to represent its behavior with extremely high accuracy. In our study herein, the power system's dynamic behavior is considered mostly dependent on the generators and their control systems. For the modeling of the generators and control systems, we use models which are widely accepted in similar studies [133], i.e., (i) round rotor synchronous machine with order 6, (ii) generator exciter Model IEEE T1, (iii) single mass IEEE G2 steam turbine prime mover, and (iv) Power System Stabilizer (PSS) based on IEEE Std 421.2. We assume that the defender has perfect knowledge of these parameters as well as the line and load parameters to represent the grid. Finally, the grid is linearized into a state-space model with the active and reactive power of the aggregate EV-defender loads as the inputs and the generator frequencies being the outputs. Additionally, the unknown LA attack is represented by a disturbance to the grid. This representation is expressed in (7.1) where x , y , u , and ω represent the vectors of system states, outputs, inputs, and disturbances, respectively. Additionally, ΔP_{EV_n} , ΔQ_{EV_n} , and f_{Gen_m} represent the change in active and reactive power of the aggregate EV load at bus n and the frequency of generator m respectively. A , B , C ,

and D are the state-space matrices that represent the power grid and its dynamic behavior. B_d and D_d represent the impact of the LA attacks on the grid's states and outputs respectively.

$$\dot{x} = Ax + Bu + B_d\omega \quad (7.1a)$$

$$y = Cx + Du + D_d\omega \quad (7.1b)$$

$$\text{such that } y = (f_{Gen_1} \ f_{Gen_2} \ \cdots \ f_{Gen_m}) \quad (7.1c)$$

and

$$u = \Delta PQ_{EV} = (\Delta P_{EV_1} \ \Delta Q_{EV_1} \ \cdots \ \Delta P_{EV_n} \ \Delta Q_{EV_n}) \quad (7.1d)$$

The authors of [140], [141], and [142] discuss how the power grid can be linearized to maintain all its behavioral properties while the work presented in [91] and [143] discusses how power grids are linearized for the sake of designing their control techniques. Finally, the details of modeling the power grid as a state-space are presented in [144] and [60].

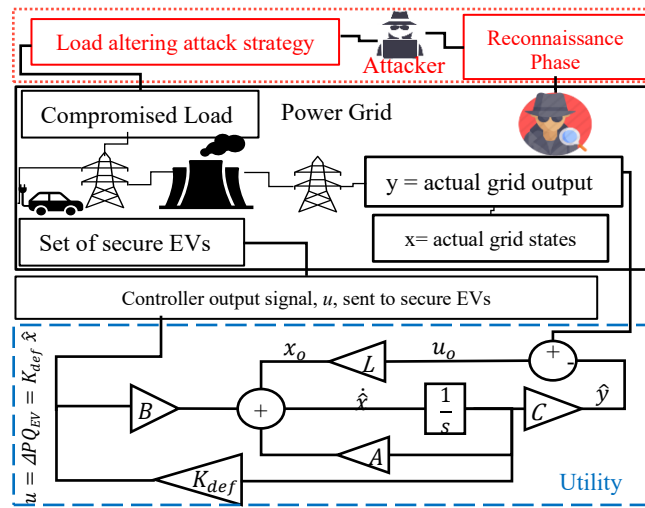


Figure 7-1: Defender's state-space model and interaction with the attacked grid

Figure 7-1 represents our system model including the LA attack against the grid and the defender's mitigation scheme we are proposing. The attacker in the dotted box above the grid relies on the LA attack models discussed above. The state-space representation in the dashed box, below the grid, is constructed by the utility as part of the EV-based controller scheme we are proposing. This state-space representation is then used to calculate the EV gain matrix K_{def} used to determine the required EV active and reactive power and capture the behavior of the input $u = \Delta PQ_{EV}$ for the system to eliminate the impact of the attack/disturbance. The relation between the disturbance and the generator frequency can be expressed as $y = T\omega$, where T is a transfer function written in

terms of the state-space matrices. The behavior of $u = \Delta PQ_{EV}$, is then captured and replicated on the set of secure EVs located throughout the grid. The mitigation controller is designed as a full-state feedback controller, i.e., $u = K_{def}x$, where K_{def} is the gain matrix that is optimized to eliminate the disturbances caused by the attack. The state-space matrices are also used to calculate the observer gain matrix L needed by the utility to recover the grid states, x . Since not all the states are measurable, the utility obtains an estimate, $\hat{x}$, by multiplying the grid's outputs, y , by the observer gain L . As such, the power of the aggregate EV load, ΔPQ_{EV} , is determined based on $\Delta PQ_{EV} = u = K_{def}\hat{x}$. Designing the EV-based controller based on feedback control law changes the A matrix to its closed-loop form, i.e., $A_{cl} = A + BK_{def}$. Since the eigenvalues of A_{cl} define the stability of the power grid, it is of paramount importance that the methodology used to calculate K_{def} guarantee the mitigation scheme's performance under different types of attacks when faced with the different uncertainties and obstacles of a real-life deployment. The mentioned sources of uncertainty in the EV load are discussed in the controller design section and studied in Section 7.3.

7.1.2 Observer Design

Since our EV-based LA attack mitigation strategy relies on full-state feedback control, the utility also needs to choose an appropriate design for the observer gain matrix L . This observer facilitates the accurate recovery and estimation of the grid states $\hat{x}$ needed to calculate the feedback control input $\Delta PQ_{EV} = u = K_{def}\hat{x}$. With the introduction of the gain K_{def} and the observer L , the state-space (7.1) becomes (7.2).

$$\dot{\hat{x}} = A_{cl}\hat{x} + L(y - \hat{y}) + B_d\omega \quad (7.2a)$$

$$y = C_{cl}x + D_d\omega \quad (7.2b)$$

where $C_{cl} = C + DK_{def}$ is the closed-loop form of matrix C that relates the system outputs to its states. B_{cl} and D_{cl} are B_d and D_d respectively. Given that an accurate observer is based on gain matrix L , it must be designed to ensure that $(A_{cl} - LC_{cl})$ has stable poles [150]. Therefore, we employ a Linear Quadratic Controller (LQR) [150] as our observer for accurate state recovery. LQR is a control technique that optimizes the balance between the energy of states, and control signals to achieve the desired output accurately.

7.1.3 Choice of Controller for EV-Based Mitigation Scheme

Unlike the studies in [77] - [80] that support the grid's steady-state operation using EVs, we utilize EVs to create a mitigation scheme to attenuate the impact of LA attacks. Additionally, unlike traditional approaches that create controllers to mitigate specific disturbances, we use EVs to mitigate the three known types of LA attacks by optimizing the controller to accomplish multiple objectives. Also, by formulating our mitigation scheme as a feedback controller, we eliminate the need for attack detection tools since the controller reacts to the changes in the grid's states. These states are recovered by the utility by using the observer suggested above. We suggest a family of H-2, H- ∞ , and mixed H-2/ ∞ control techniques to synthesize our problem as a convex optimization with LMI constraints [149] to achieve a guaranteed attenuation level of the attack impacts.

H- ∞ controllers minimize the maximum singular value of a function while H-2 controllers minimize the energy of the output signal over the entire frequency range. This would result in the H-2 controller performing better than H- ∞ over most frequencies but failing at specific frequencies. H- ∞ controllers have been adopted in mechanical systems such as missile or satellite trajectory control [184] and suspension systems [185]. However, we intend to adopt the usage of such controllers into the domain of power grid protection against LA attacks. Although, H-2 controllers have received less attention in the literature than H- ∞ , their ability to outperform H- ∞ at most frequencies merits their usage in our study. Given the complexity of our problem and the need to address multiple objectives simultaneously, we ultimately choose the mixed H-2/ ∞ controller to enable our EV-based mitigation scheme to handle the different types of LA attacks.

7.1.4 H-2 and H- ∞ Controller Design

In this subsection, the EV-based mitigation controller scheme is developed, and its mathematical formulation is obtained based on the LMIs of the desired control law [149]. Writing our controller equations as LMIs gives us the flexibility to (i) finetune their design, (ii) implement complex control schemes, and (iii) combine multiple objectives into a single optimization problem. In our study, the unknown LA attack is treated as a persisting disturbance, w , whose impact we aim to attenuate. The relationship between the disturbance and the system states and outputs is governed by (7.2) presented above. Our mitigation scheme aims to simultaneously minimize the impact of

the attack and the EV load involved in the feedback controller signal. To this end, we design our control methods below and modify the design to achieve all our desired objectives in the subsections that follow.

- 1) H-2 controllers [149] aim to minimize the L^2 norm of a system across the entire frequency range. This means that the cost function of the H-2 controller is the Euclidean distance of the outputs from the origin. This allows the H-2 controller to rapidly react and eliminate the disturbances in a system by using rapidly increasing input signals. The transfer function T_2 , representing the influence of the disturbance ω on the grid output, i.e., generator frequency y , is presented in (7.3):

$$T_2 = \frac{y}{\omega} = (C + DK_{def})(sI - (A + BK_{def}))^{-1}B_d \quad (7.3)$$

The cost function of the H-2 controller becomes $\|T_2\|_{L^2} < \gamma$. This function is rearranged in terms of its LMIs (7.4)-(7.5).

$$(AX + BK_{def}X)^T + AX + BK_{def}X + B_d B_d^T < 0 \quad (7.4)$$

$$\text{trace} \{ (C + DK)X(CX + DK_{def}X)^T \} < \text{trace}(Z) < \gamma^2 \quad (7.5)$$

Based on Schur's formulation for partitioned matrices [149], inequality (7.5) is rewritten as (7.6) and (7.7).

$$\begin{bmatrix} -Z & CX + DK_{def}X \\ (CX + DK_{def}X)^T & -X \end{bmatrix} < 0 \quad (7.6)$$

$$\text{trace}(Z) < \gamma^2 \quad (7.7)$$

Considering that the gain $K_{def} = K_{H-2} = WX^{-1}$, (7.4) and (7.6) now become (7.10) and (7.11), and the optimization problem to reduce the disturbance impact can be written as (7.8)-(7.11).

$$\text{Minimize } \gamma^2 \quad (7.8)$$

$$\text{s.t.} \quad \text{trace}(Z) < \gamma^2 \quad (7.9)$$

$$\begin{bmatrix} -Z & CX + DW \\ (CX + DW)^T & -X \end{bmatrix} < 0 \quad (7.10)$$

$$(AX + BW)^T + AX + BW + B_d B_d^T < 0 \quad (7.11)$$

This LMI optimization problem can only have a solution if there exists a matrix W and two symmetric matrices Z and X satisfying the matrix inequalities in (7.9)-(7.11).

- 2) H_∞ controllers [149] aim to minimize the maximum singular value of a function. This means that the H_∞ controller aims to minimize the largest perturbation in a system. The cost function of this controller is formulated to minimize the output and input energy meaning it eliminates the disturbances while simultaneously trying to minimize the required control inputs. This cost function can be expressed as the infinity norm, $\|T_\infty\|_\infty < \rho$, where T_∞ is the transfer function dictating the influence of the disturbance ω on the grid output y .

$$T_\infty = \frac{y}{\omega} = (C + DK_{def})(sI - (A + BK_{def}))^{-1}B_d + D_d \quad (7.12)$$

Based on Schur's formulation for partitioned matrices [149], the cost function $\|T_\infty\|_\infty < \rho$ is rewritten as an LMI and $K_{def} = K_{H-\infty} = WX^{-1}$ is replaced in the derived LMI. Then similar steps to (7.6)-(7.11) are taken to arrive at the inequality in (7.15) and the H_∞ optimization problem becomes (7.13)-(7.15).

$$\text{Minimize } \rho \quad (7.13)$$

$$\text{s.t.} \quad X > 0 \quad (7.14)$$

$$\begin{bmatrix} (AX + BW)^T + AX + BW & B_d & (CX + DW)^T \\ B_d^T & -\rho I & D_d^T \\ CX + DW & D_d & -\rho I \end{bmatrix} < 0 \quad (7.15)$$

The H_∞ LMI optimization problem can only have a solution if there exists a matrix W and a symmetric positive definite matrix X satisfying the matrix inequality problem in (7.14)-(7.15).

Each of these two control techniques is better suited to a specific class of LA attacks as we will demonstrate in Section 7.2 which is why we will also develop a mixed controller later in this section. After calculating K_{def} , the utility will have to check the attenuation levels dictated by γ

and ρ respectively. These variables should be maintained below 1 to achieve feasible and satisfactory attenuation levels. This, however, only guarantees the performance of the controller in the frequency domain. To improve the controller performance in the time domain, i.e., reduce settling time, we add the pole placement constraint (7.16).

$$AX + XA^T + BW + W^T B^T + 2\Lambda_1 X < 0 \quad (7.16)$$

where X is a positive semi-definite matrix. This LMI constraint is based on a D-stabilization pole placement technique [60] that shifts the eigenvalues of the system into a region where the real part of the eigenvalues is less than $-\Lambda_1$. To guarantee performance and fast settling time, we choose $l < \Lambda_1 < 0$ to ensure stable poles. l should also be chosen small enough to avoid an aggressive controller behavior that is not desirable.

7.1.5 Robust Controller Under Uncertain EV Feedback Load

In this subsection, we address the issue of uncertainty of the EV load. This uncertainty can arise from different sources. The first is the user behavior that can be accurately estimated but never guaranteed by the utility. The second source of uncertainty arises from the possibility of attackers targeting the EV ecosystem. Attackers might be able to compromise part of the connected EVs while giving the utility the impression they are secure. This would mean that the control signal would reach less secure EVs than the utility intended. The third source of uncertainty can be introduced in the system by the clustering method we suggest below as a privacy-preserving measure. Clustering is the only case where uncertainty can be positive. These three types of uncertainties are modeled as an uncertain matrix $\emptyset$ in the feedback loop after the output of the controller K_{def} which changes the value of the EV load to $\Delta PQ_{EV-\emptyset} = u_{\emptyset} = \emptyset K_{def} \hat{x} = \emptyset u$. As a result, the state-space representation in (7.1) becomes (7.16).

$$\dot{x} = Ax + B\emptyset K_{def} \hat{x} + B_d \omega \quad (7.16)$$

By rewriting $\Delta PQ_{EV-\emptyset}$ as a function of the original input u , (7.16) becomes (7.17) which is restructured through (7.18) to become the state-space representation in (7.19) which models the uncertainty in the feedback signal as uncertainty in matrix B .

$$\dot{x} = Ax + B\phi u + B_d\omega \quad (7.17)$$

$$\dot{x} = Ax + \{B + B(\phi - I)\}u + B_d\omega \quad (7.18)$$

$$\dot{x} = Ax + (B + \Delta B)u + B_d\omega \quad (7.19)$$

It is worth noting that since the utility is responsible for this mitigation scheme, it is considered that the system parameters are accurate, thus the uncertainty in matrix A is zero. The matrix uncertainties are written as (7.20) and (7.21).

$$\Delta A = HFE_1 \quad (7.20)$$

$$\Delta B = HFE_2 \quad (7.21)$$

Where H, E_1 , and E_2 are known quantities while F is an uncertain matrix. Since ΔA is zero, then E_1 is zero and excluded from further calculations. H is usually chosen to be an identity matrix. The uncertain matrix F can be written in the form of (7.22) if it satisfies condition (7.23).

$$F = \delta_1 F_1 + \delta_2 F_2 + \dots + \delta_k F_k \quad (7.22)$$

$$FF^T \leq I \quad (7.23)$$

Writing F in the form of (7.22) means that ΔB can be rewritten as (7.24) and consequently as (7.25) which represents a family of uncertain matrices.

$$\Delta B = H(\delta_1 F_1 + \delta_2 F_2 + \dots + \delta_k F_k)E_2 \quad (7.24)$$

$$\Delta B = \delta_1 B_1 + \delta_2 B_2 + \dots + \delta_k B_k \quad (7.25)$$

The H-2 controller constraint (7.11) is now rewritten as (7.26) and simplified as (7.26) to account for the uncertainty in B.

$$\{AX + (B + \Delta B)W\}^T + AX + (B + \Delta B)W + B_d B_d^T < 0 \quad (7.26)$$

$$(AX + BW)^T + AX + BW + B_d B_d^T + \beta < 0 \quad (7.27)$$

$$\text{where } \beta = \Delta BW + (\Delta BW)^T \quad (7.28)$$

Based on (7.21)-(7.25), β is rewritten as (7.29) and (7.30).

$$\beta = HFE_2W + (HFE_2W)^T \quad (7.29)$$

$$\beta = HFE_2W + W^TE_2^TF^TH^T \quad (7.30)$$

Using the variable elimination Lemma in [149] that states that any variable in the form of (7.30) under the condition stated in (7.23) can be rewritten as (7.31) β becomes:

$$\beta = \alpha HH^T + \alpha^{-1}(E_2W)^T(E_2W) \quad (7.31)$$

if there exists a scalar $\alpha > 0$. After substituting the value of β derived in (7.31) back into (7.27), we apply Schur's complement lemma [186], to rearrange the inequality containing α^{-1} into the equivalent inequality in (7.32) which would replace constraint (7.11) in the original H-2 formulation making it a robust H-2 controller capable of handling uncertainty in the feedback loop.

$$\begin{bmatrix} \Lambda_1 + \alpha HH^T & (E_2W)^T \\ E_2W & -\alpha I \end{bmatrix} < 0 \quad (7.32)$$

$$\text{where } \Lambda_1 = (AX + BW)^T + AX + BW + B_d B_d^T. \quad (7.33)$$

Without going into the details, similar steps to (7.21)-(7.31) are followed and the inequality in (7.15) is rewritten as (7.34)

$$\begin{bmatrix} \Lambda_2 + \alpha HH^T & B_d & (CX + DW)^T & (E_2W)^T \\ B_d^T & -\rho I & D_d^T & 0 \\ CX + DW & D_d & -\rho I & 0 \\ E_2W & 0 & 0 & -\alpha I \end{bmatrix} < 0 \quad (7.34)$$

$$\text{where } \Lambda_2 = (AX + BW)^T + AX + BW \quad (7.35)$$

This formulation represents a robust H- ∞ controller capable of handling uncertain parameters represented by ΔB corresponding to our feedback loop EV load uncertainty.

7.1.6 Mixed Robust H-2/ ∞ Controller

After presenting the robust controller formulation above, we discuss herein the robust mixed H-2/ ∞ controller. Our mitigation strategy ultimately aims at eliminating the impact of the three types of LA attacks hence the importance of its success in the different attack ranges and the maximum possible attenuation level across these ranges. To this end, we develop a mixed controller that

combines the LMI constraints of both H-2 and H- ∞ robust controllers and arrive at the formulation in (7.36)-(7.43). The optimization objective function (7.36) is a weighted mix of objectives (7.8) and (7.13).

$$\text{Minimize } a_1\gamma^2 + a_2\rho \quad (7.36)$$

$$\text{s.t. } AX + XA^T + BW + W^T B^T + 2\Lambda_1 X < 0 \quad (7.37)$$

$$\left\{ \begin{array}{l} X > MI \\ \text{trace}(Z) < \gamma^2 \end{array} \right. \quad (7.38)$$

$$\left[\begin{array}{cc} -Z & CX + DW \\ (CX + DW)^T & -X \end{array} \right] < 0 \quad (7.39)$$

$$\left[\begin{array}{cc} \xi + B_d B_d^T + \alpha H H^T & (E_2 W)^T \\ E_2 W & -\alpha I \end{array} \right] < 0 \quad (7.41)$$

$$\left[\begin{array}{cccc} \xi + \alpha H H^T & B_d & (CX + DW)^T & (E_2 W)^T \\ B_d^T & -\rho I & D_d^T & 0 \\ CX + DW & D_d & -\rho I & 0 \\ E_2 W & 0 & 0 & -\alpha I \end{array} \right] < 0 \quad (7.42)$$

$$\text{where } \xi = (AX + BW)^T + AX + BW \quad (7.43)$$

Constraint (7.14) is replaced by $X > MI$ when incorporated into the mixed controller where M is a positive integer. This new constraint guarantees a smaller value of the gain K_{def} consequently, a smaller input signal, $u = \Delta P Q_{EV}$, to be sent to the EV-based defender scheme. This mixed sensitivity LMI optimization problem can only have a solution if there exists a matrix W , two symmetric matrices Z and X , and a scalar α satisfying (7.36)-(7.43) and a gain matrix $K_{def} = K_{mix} = WX^{-1}$.

7.1.7 EV User Impact and Privacy Concerns

The main concern related to the suggested scheme is the impact on the EV users' charging experience since such a scheme would require some of the connected EVs to charge and/or discharge. However, the average charging time for 100 miles of range is 20 hours per 1 kW charging rate [187]. This means that 11 kW EVCSs would deliver a charge equal to 0.9 miles/min, which varies between different EVs. The impact on EV range is thus minimal and discussed in Section 7.2.7.

Such a scheme should only involve EVs whose owners gave their consent to participate. This can be achieved through an incentive program implemented by the utility to motivate EV users to contribute to the mitigation scheme. Hydro-Quebec, a Canadian Utility, implements a similar program, the *Hilo* project [188], which allows them to control home loads to reduce the demand during peak times with plans to extend it to EVs.

Regarding private EVCSs at residences, the issue of user privacy comes to light. The trivial solution would be to implement this scheme on public EVCSs only. However, given the abundance of home EVCSs, we suggest an EVCS clustering by the utility based on geographical location. Utilities can broadcast a signal to the entire cluster without having granular knowledge of individual home EVCSs. For example, let's consider areas A and B with 500 and 350 EVCSs respectively. Also, let's assume that the estimated EV connection to the EVCSs in area A and area B is 20% and 30% respectively. If the utility wants to cluster the EVCSs such that 10 EVs are connected per cluster, this requires area A to have 10 clusters of 50 EVCSs, and area B to have 10 clusters of 35 EVCSs. This, however, introduces uncertainty in the actual EV load used as a feedback control signal in the mitigation scheme since the number of connected EVs per cluster cannot be guaranteed. The impact of this clustering method is examined in Section 7.3 as part of our EV-based mitigation scheme's stability study.

7.2 Case Studies and Simulations

In this section, we demonstrate our EV mitigation scheme against static, switching, and dynamic attacks on the New England (NE) 39-bus grid in Figure 7-2. [151]. We first demonstrate the impact of the attacks in the absence of our scheme to highlight their devastating impact. The NE grid has 39 buses, 10 generators, and 19 loads with a total of 6,097 MW. The simulations were performed on MATLAB-Simulink 2021a Specialized Power Systems Toolbox using a variable step size of 1×10^{-12} to 1×10^{-9} .

While we acknowledge that the current number of EVs is not enough to exploit the full potential of the suggested mitigation scheme, the following example demonstrates its feasibility

with increased EV adoption levels. To demonstrate this, we choose a similarly sized grid which is the New South Wales (NSW) grid on a day in December 2021 [126]. The average load is 6968 MW [126] and the total registered vehicles are 5,892,206 [127]. Scaled down to fit our test grid, the total number of vehicles is 5,155,681.

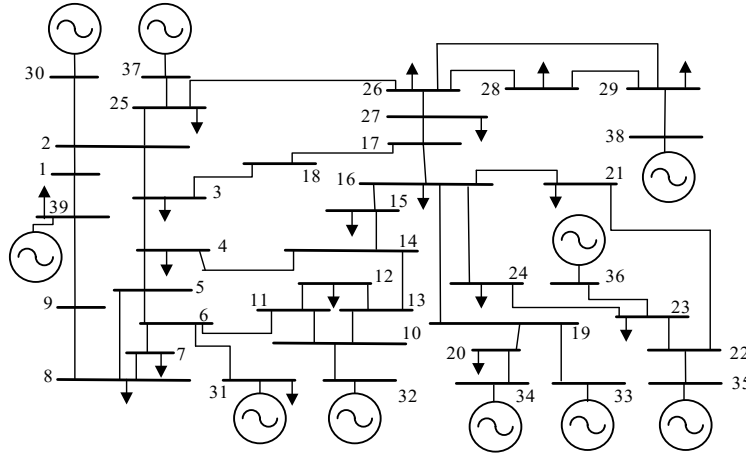


Figure 7-2: New England 39-bus grid

At future EV penetration levels, the EV load will become huge, especially with the increasing EVCS charging rates. Thus, only a small fraction of the EVs in our grid needs to be connected for our proposed EV-based LA attack mitigation scheme to achieve the results presented below. However, the EV load is variable depending on the time of day. Thus, a more detailed examination of the EV load is required. As per the International Energy Agency (IEA) [128] EVCS operators, utilities, and governments have maintained a ratio of 1 public EVCS for every 9.9 EVs on the road to guarantee the quality of service. Thus, at a future 50% EV penetration level, there will be 260,387 public EVCSs in our NE grid. With an average public EVCS occupancy of 33% [129], we can estimate the average number of connected EVs to the grid to be 86,000. Furthermore, according to the IEA [128], based on the mixture of different EVCS rates, the average charging rate per EVCS is 24 kW. From these statistics, we can estimate that at a future 50% EV penetration level, there will be 2,064 MW of EV load connected to the grid on average at public EVCS.

To examine the specific EV load during the different times of the day, we create a data-driven model for the arrival and charging times of the EVs. To achieve a realistic EV charging behavior, we independently simulate a Poisson arrival process of EVs to each EVCS [164]. The charging time of these EVs is assumed to follow a truncated Gaussian distribution [164]. The parameters of these models are specified for 1-h windows for 24 hours. These parameters are tuned based on a

real dataset containing five years of records for 7,500 EVCSs in Quebec, Canada. This dataset was obtained from Hydro-Quebec as part of a research collaboration.

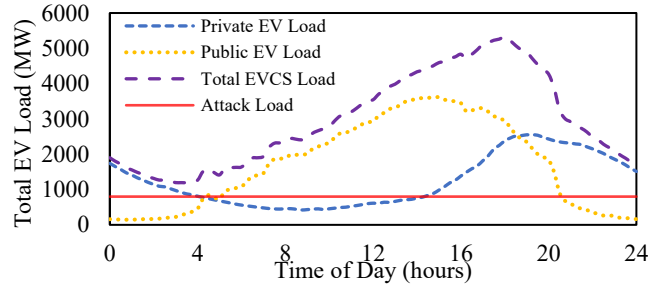


Figure 7-3: EVCS Public and Private charging load for 24 hours

Additionally, we extract the EVCS utilization information from the dataset. The average utilization rate of EVCSs in Quebec is 31% with the peak charging demand occurring in the afternoon. By examining this dataset, we were able to extract the average hourly arrival rates and charging times to simulate them as a Poisson process and a truncated Gaussian distribution respectively. From the presented statistics and data-driven EV fleet model, we generate the public EVCS load profile presented in Figure 7-3. Additionally, we acquired an approximation of the private EVCS load profile, for the presented number of EVs, by using the EV Infrastructure Projection Tool provided by the Alternative Fuels Data Center (AFDC) [189] and added the acquired data to Figure 7-3. Figure 7-3 demonstrates the change in the EV load for an entire 24-h period. Figure 7-3 demonstrates the presence of a minimum of 1196 MW of EV load connected to the grid at 3:30 am.

Furthermore, there are roughly 9 private EVCSs for every 10 EVs [128]. This means that at 50% penetration, there will be over 2.3 million private EVCSs. Given user tendency in the presence of an incentive scheme like *Hilo*, to connect EVs to home EVCSs even if no significant charging is needed, there will be large numbers of EVs connected at residences at the disposal of the utility that do not factor into the normal charging load presented in Figure 7-3. Once we factor in the EVs that will be connected due to the incentives, the utility will have a much larger EV charging load at its disposal to participate in the presented mitigation scheme.

7.2.1 Reduced Power Grid State-Space Model

Due to the complexity of power grids, the size of the state-space matrices is relatively large hindering the design of the controllers, i.e., the NE grid has 300 states. To preserve the correct system behavior while reducing its order, we use Hankel model reduction [152]. For this purpose, we calculate the Hankel Singular Values (HSVs) of the system states to optimize the system order reduction versus the preserved system accuracy. Table 7-1 shows the preserved system energy based on the reduced system order. Since 99.81% of the total system energy is contained within the first 30 HSVs, we reduced the system order to 30 states. Beyond 30, any order increase does not significantly improve accuracy while considerably adding to the controller synthesis complexity. This order reduction is only used for controller synthesis, while the presented simulations are performed on the actual grid, not the linearized nor the reduced model.

Table 7-1: Possibilities for Reducing System Order

Reduced System Order	Percentage of Preserved System Energy
10	83.93%
20	98.38%
30	99.81%
40	99.93%
50	99.97%

7.2.2 Case Study 1: Attacks in Absence of Mitigation without PSS

Based on the work presented in [16], [58], and [60] which discuss static attacks, switching attacks, and dynamic attacks respectively, we formulate our attack scenarios against the NE grid in the absence of the suggested mitigation strategy to demonstrate their impact as a base case. The mathematical formulations of these attacks are presented in [16], [58], and [60], and are based on these studies, and thus are not repeated herein. The first batch of attacks is simulated in the absence of a PSS and the impact is discussed in the following three cases.

- 1) Attack 1: is an 800 MW static attack initiated at $t=5$ seconds split on buses 3, 4, 24, and 29. This attack is a single spike in load equal to 13% of the system demand. Figure 7-4 demonstrates the frequency behavior of the generators in response to this attack. Attack 1 causes a frequency drop to 59 Hz followed by growing oscillations that are sustained due to the absence of a PSS.

- 2) Attack 2: is an 800 MW switching attack split equally on buses 3, 4, 24, and 29. Figure 7-5 demonstrates how this attack caused a huge frequency deviation that reached 71 Hz in 10 seconds. This attack would trip the generators resulting in a blackout.
- 3) Attack 3: is an 800 MW dynamic attack split on buses 3, 4, 24, and 29. Since the attack is formulated as a feedback loop so that the eigenvalues of the grid are shifted into an unstable region based on the attack methodology in [60], the loads do not always oscillate in phase. The result of this attack is demonstrated in Figure 7-6. The frequencies of all the generators experience wild oscillations that continue to grow to reach 74 Hz while oscillating against each other. This would trip all the generators to avoid damaging their shafts due to the violation of the safe frequency operation thresholds.

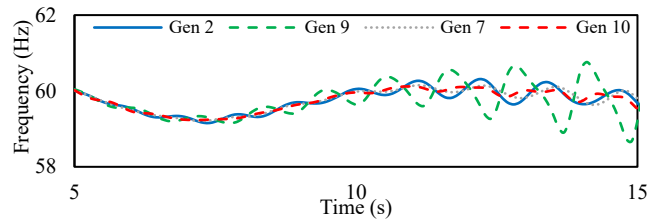


Figure 7-4: Generator frequency response under attack 1 with no PSS

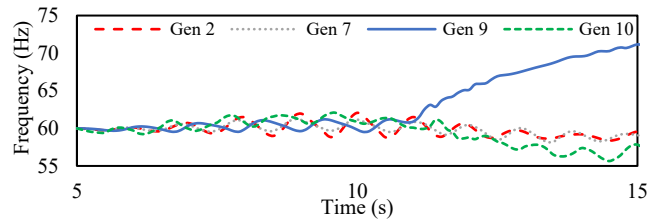


Figure 7-5: Generator frequency response under attack 2 with no PSS

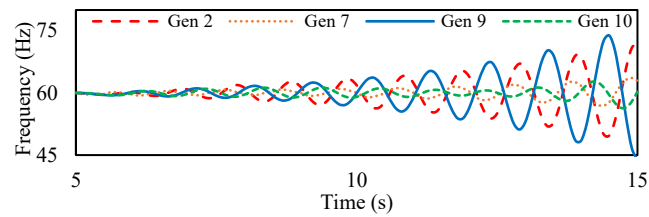


Figure 7-6: Generator frequency response under attack 3 with no PSS

7.2.3 Case Study 2: Attacks in Absence of Mitigation with PSS

In this case study, we repeat the three attack scenarios in the presence of the PSS at the generators. The PSS is meant to stabilize the grid by damping generator frequency swings but falls short of eliminating LA attack impacts.

- 1) Attack 1: is now repeated in the presence of the PSS. This static attack causes a 0.4 Hz frequency drop and minor oscillations that are eventually eliminated by the PSS as the grid regains stability.
- 2) Attack 2: is also repeated in the presence of the PSS which significantly limits the impact. However, the grid sustained frequency oscillations reaching a maximum deviation of 1.08 Hz. Figure 7-7 demonstrates this impact that causes the operator to shed 5% of the grid's load [55]. Figure 7-8 demonstrates a sample Attack 2 load. The average frequency deviation among the 10 generators was 0.74 Hz.

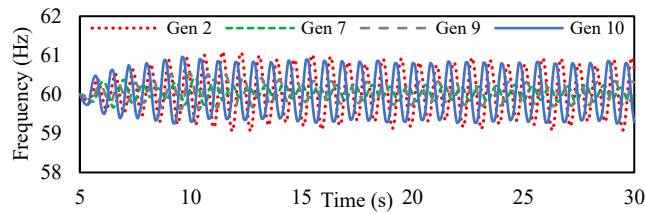


Figure 7-7: Generator frequency response under attack 2 with PSS

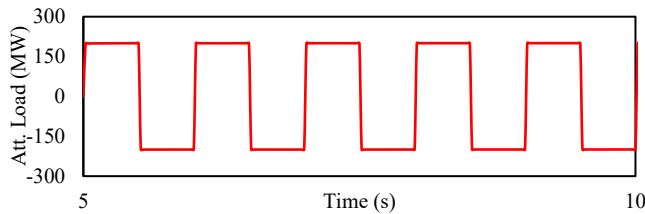


Figure 7-8: Attack 1 load on each of the buses

- 3) Attack 3: is also repeated in the presence of the PSS and again proved to be the strongest attack. The grid experienced the rapid frequency oscillation depicted in Figure 7-9. The maximum frequency reached 1.58 Hz. This causes the generators to trip instantaneously leading to a blackout. Figure 7-10 demonstrates a sample Attack 3 load and Figure 7-11 represents the aggregate of the 4 attack loads. The average frequency deviation among the 10 generators was 1.06 Hz.

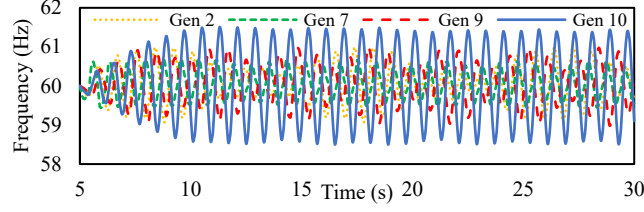


Figure 7-9: Generator frequency response under attack 3 with PSS

This case study demonstrates that even in the presence of the PSS the attack impact is not eliminated when it is crafted properly. To this end, adding a mitigation mechanism that can eliminate LA attack impacts becomes necessary.

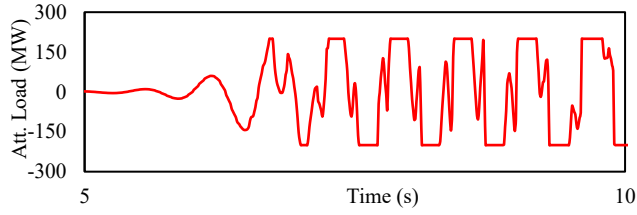


Figure 7-10: Attack 3 load on bus 4

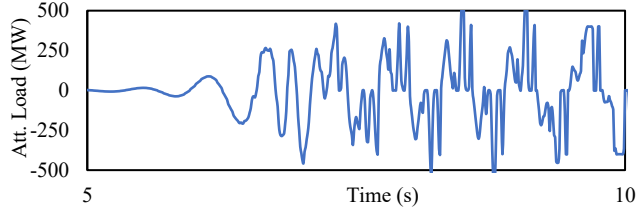


Figure 7-11: Attack 3 aggregate load

7.2.4 Case Study 3: H-2 and H- ∞ Control EV-Based Mitigation

Based on the methodology presented above, we design our EV-based mitigation scheme based on H-2 and H- ∞ robust control and evaluate the performance of both controller designs against the three types of LA attacks. The EV defender load is calculated as $\Delta PQ_{EV} = K_{def} \hat{x}$ and replicated on the NE grid that is under attack. It is important to mention that the H-2 and H- ∞ EV-based mitigation, immediately eliminates all traces of the static attack. The cases of switching and dynamic attacks are presented below.

7.2.4.1 H-2 EV mitigation

We repeat Attack 2 and Attack 3 on the NE grid after adding the EV feedback loop gain, K_{def} , calculated based on H-2 control and the results are as follows.

- 1) Attack 2: is repeated and the frequency responses of the generators are presented in Figure 7-12. The maximum frequency deviation was reduced to 0.065 Hz which represents a 93.9% decrease in the attack impact. The average frequency deviation was reduced to 0.04 Hz which is equal to a 99.6% reduction in attack impact.

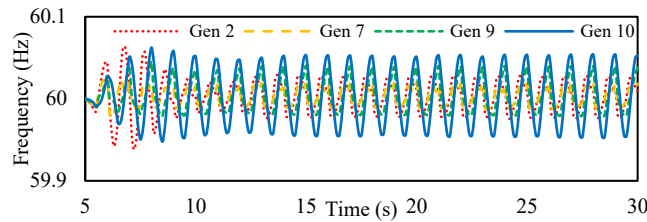


Figure 7-12: Generator frequency - attack 2 with H-2 controller

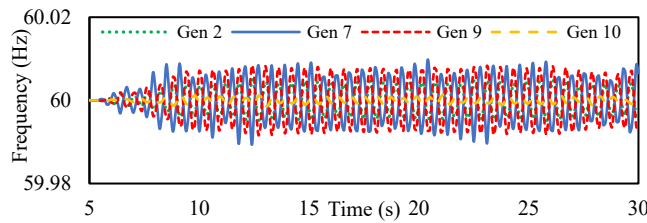


Figure 7-13: Generator frequency - attack 3 with H-2 controller

- 2) Attack 3: is repeated and the frequency response of the generators is tremendously improved. As presented in Figure 7-13, the maximum frequency deviation was reduced to 0.007 Hz which is roughly equivalent to a 99.6% reduction in the original attack impact, practically eliminating it. The average frequency deviation was reduced to 0.004 Hz which is equal to a 99.6% reduction in attack impact.

7.2.4.2 H-∞ EV mitigation

We repeat Attack 2 and Attack 3 on the NE grid after adding the EV feedback loop gain K_{def} calculated based on H-∞ control and the results are as follows.

- 1) Attack 2: is repeated and causes a frequency drop of 0.01 Hz which then recovers at t=30 seconds to 60 Hz, representing 100% recovery to the pre-attack state as seen by the frequency responses of the generators in Figure 7-14.

- 2) Attack 3: is repeated in the presence of the H_∞ EV mitigation scheme. Although this controller eliminates the impacts of the switching attacks, it falls short of achieving the same against the dynamic attack. The frequency responses of the generators are presented in Figure 7-15. The maximum frequency deviation was reduced to 0.1 Hz which is a 93.7% reduction of the LA attack impact. The average frequency deviation was reduced to 0.05 Hz which is equal to a 95.3% reduction in attack impact.

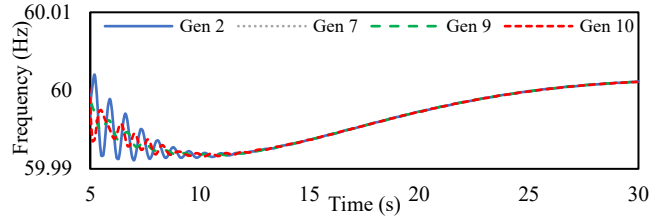


Figure 7-14: Generator frequency - attack 2 with H_∞ controller

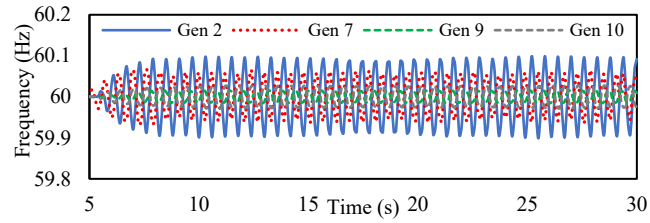


Figure 7-15: Generator frequency - attack 3 with H_∞ controller

This case study demonstrates that the H_∞ EV-based mitigation scheme performs better against switching attacks while the H_2 mitigation scheme performs better against dynamic attacks. In the case of the switching attack in the presence of the H_2 and the dynamic attack in the presence of the H_∞ controller, the governor of the generators would have to react since the frequency does return to the safe operation limit but not to the normal frequency range. Since this is a persisting attack, this means that the governors will have to constantly keep correcting the frequency. As a result, we recommend a mixed controller.

We now repeat the attacks to test the mitigation scheme's success when the defender does not control any EVs on one of the attacked buses. This is to demonstrate the success of our EV mitigation even if we eliminate one of its advantages which is the colocation with the attack load. The controller is successful in eliminating the attack impact but with slightly reduced performance. Attack 2 is repeated against the grid that has the H_∞ controller and results in a maximum 0.1 Hz frequency deviation which is equivalent to a 90.7% reduction in impact. The average frequency

deviation was reduced to 0.04 HZ which is equivalent to a 94.6% reduction. Attack 3 is also repeated against the grid that has the H-2 mitigation scheme which results in a maximum 0.06 Hz frequency deviation or 96.2% reduction in attack impact. The average frequency deviation was reduced to 0.03 Hz or a 97.2% reduction. This demonstrates the success of our attack mitigation even when the utility loses its resources on an attacked bus.

7.2.5 Case Study 4: Robust Mixed H-2/ ∞ EV-Based Mitigation

In this case study, we demonstrate the effectiveness of the mixed H-2/ ∞ robust control mitigation strategy and its advantage in our EV-based LA attack mitigation. Once again, the H-2/ ∞ controller eliminates any trace of the static attack.

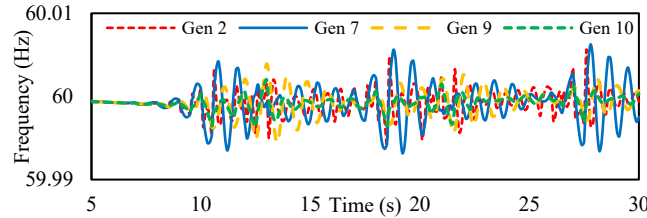


Figure 7-16: Generator frequency - attack 2 with mixed H-2/ ∞ controller

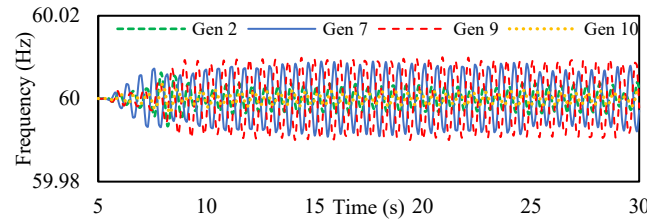


Figure 7-17: Generator frequency - attack 3 with mixed H-2/ ∞ controller

- 1) Attack 2: is repeated and Figure 7-16 demonstrates the success of the mixed control strategy in mitigating the impact of the switching attack. The frequency responses of the generators are presented in Figure 7-16, and it is evident that the performance is much better than the H-2 controller with a reduction of the switching attack impact by 99.5%. The average frequency drops slightly below 60 Hz but stabilizes towards $t=30$ seconds. Also, the sustained oscillations reach a maximum of 0.006 Hz. The average value of the sustained oscillations across all generators was also reduced to 0.003 Hz representing a 99.6% drop in average attack impact.

- 2) Attack 3: is repeated and the frequency responses of the generators are presented in Figure 7-17. Figure 7-17 demonstrates the success of the controller in counteracting the impact of the dynamic attack. The maximum impact of the attack was reduced from 1.5 Hz to 0.01 Hz representing a 99.4% impact reduction. This is also 10 times smaller than the impact of the same attack in the presence of the $H-\infty$ EV-based controller. The average value of the sustained oscillations was also reduced to 0.008 Hz representing a 99.3% drop in average attack impact.
- 3) We also study the case when the utility has no resources on the attacked buses. The switching attack and dynamic attack cause a maximum frequency deviation of 0.09 and 0.07 respectively. This is equivalent to a 91.7% and a 95.6% reduction in maximum attack impact respectively.

This case study proves that the mixed $H-2/\infty$ controller is superior to the individual controllers by addressing their gaps. By reducing the frequency oscillation and deviation caused by all types of LA attacks to lower than 0.01 Hz, the mixed controller returned the grid to a state where the frequency is well within the normal range in which the turbine governors are not engaged, and the system behaves as it would behave normally in the absence of any attack even when the attacks are sustained and persistent. Based on the above discussions and results, the best course of action would be the adoption of the EV-based robust mixed $H-2/\infty$ controller for the LA attack mitigation scheme. The complexity of designing the controller based on the presence of uncertainty is only during the planning phase. During deployment, the performance of the controller will not be impacted since it is based on matrix multiplication regardless of the method of its synthesis. Lastly, the presented case studies demonstrate the instantaneous reaction time of the presented mitigation scheme due to the advantage introduced by the power converters in the EVCSs that resulted in the immediate elimination of the attack impact.

Table 7-2: Max Frequency Deviation Vs Different Attack 2 and 3 Magnitudes

Attack Magnitude	Attack 2		Attack 3	
	No Mitigation	Mixed H-2/ ∞ Mitigation	No Mitigation	Mixed H-2/ ∞ Mitigation
800	1.08 Hz	0.006 Hz	1.58 Hz	0.01 Hz
700	0.97 Hz	0.006 Hz	1.42 Hz	0.01 Hz
600	0.87 Hz	0.005 Hz	1.21 Hz	0.009 Hz
500	0.79 Hz	0.004 Hz	1.03 Hz	0.008 Hz
400	0.65 Hz	0.003 Hz	0.91 Hz	0.006 Hz
300	0.54 Hz	0.003 Hz	0.76 Hz	0.004 Hz
200	0.32 Hz	0.001 Hz	0.46 Hz	0.002 Hz
100	0.17 Hz	0.001 Hz	0.26 Hz	0.001 Hz

7.2.6 Case Study 5: Smaller LA Attacks

The previous case studies aimed at demonstrating the EV-based robust mitigation scheme's success against large LA attacks (800 MW) to showcase the mitigation scheme's effectiveness. In this case study, however, we examine the impact of smaller attacks and the performance of our proposed EV-based mitigation scheme in such scenarios. As a starting point, we repeat Attack 2 and Attack 3 and cap their attack loads at different magnitudes between 100 MW and 800 MW. Table 7-2 demonstrates the impacts of such attacks before and after the addition of our EV-based robust mixed H-2/ ∞ mitigation scheme.

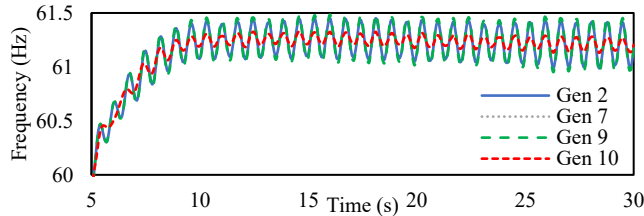


Figure 7-18: Generator frequency - attack 4 with mixed H-2/ ∞ controller

We now examine a new dynamic attack (Attack 4) based on the methodology in [60] while shifting the eigenvalues of the system further right (unstable region) than Attack 3. This results in a faster oscillation of the attack load. Attack 4 is initiated at $t=5$ seconds against buses 3, 4, 18, and 39 with a magnitude of 19% of the load on each bus for a total of 395.96 MW. Attack 4 causes the average frequency to reach 61.25 Hz while the forced oscillations reach 61.49 Hz as depicted in Figure 7-18. While this behavior does not cause instantaneous generator tripping since it does not exceed the 1.5 Hz limit, sustaining it for 30 seconds will cause the generator protection relays to trip. However, some utilities have stricter limits (61 Hz) meaning such an attack would

instantaneously trip the generators. Attack 4 is now repeated in the presence of the mixed H-2/ ∞ mitigation strategy. The frequency deviation/oscillation is reduced below 0.01 Hz meaning that the attack impact was successfully eliminated.

7.2.7 Impact on EV Range

We now evaluate the impact of our mitigation scheme on the EVs' range. This evaluation is based on the average charging rate of 24 kW. Mitigating Attacks 2 or 3 requires the EV to alternate between charging and V2G such that the net charge is approximately 0. Attacks 2 and 3 cause a loss of 0.001k Wh and 0.009 kWh respectively. The EVs also lose the opportunity to charge 0.2 kWh. The total loss is equivalent to a range of 1 mile for each EV. For an EV that was connected to an EVCS but not charging, the net impact is almost 0 kWh. Attack 1 on the other hand will result in a total loss of 0.4 kWh or 2 miles.

7.2.8 Mitigation Scheme Feasibility

An added advantage of using EV charging in our mitigation scheme is that the required communication and control infrastructure is already in place. The required central authority needed to communicate with the distributed resources (EVCSs) is the CMS that already exists in the EV ecosystem. This CMS communicates and controls all the public EVCSs in real-time. Using the OCPP protocol, the CMS can turn the individual EVCSs on and off, change their charging rate, and discharge using V2G [43] [44]. This means that adopting our mitigation scheme would not require the addition of any software, hardware, or communication to the ecosystem. The Hilo project gives the utility the same control capabilities over private EVCSs. This means that adopting our mitigation scheme would not require any software and communication capabilities to be added to the ecosystem. Furthermore, since our mitigation scheme only requires the frequencies at the generators which are already monitored by the utility, implementing our mitigation scheme does not require the addition of any measurement devices.

Mitigating these attacks using our suggested scheme requires an extremely minimal cost to be incurred by the utility. To demonstrate this, we consider 2 different EVCS charging levels in Quebec with a charging rate of 24 and 50 kW [190]. The hourly price of charging on these EVCSs

is 7.53 CAD and 12.77 CAD respectively and is billed per second [190]. This means that mitigating Attack 2 and Attack 3 costs the individual EV user 6.28 cents on the 24 kW EVCS and 5.1 cents on the 50 kW EVCS. This means that when the utility reimburses the EV users for this cost, the utility will have to pay a total of 1,683-2,072 CAD (1,242- 1,530 USD) plus whatever extra value the utility determines in its incentive program. Mitigating Attack 1 however, requires double the cost since the energy loss from the EV batteries will be double that of the other 2 attacks.

7.2.9 Mitigation Scheme Reaction to Non-Attack Scenarios

One issue that arises from the absence of a detection scheme is the EV controller's reaction to frequency fluctuations that are not caused by attacks. Our proposed scheme can react to sudden changes in power grid behavior such as the abrupt line or generator tripping studied in [191]. Such sudden events resemble static attacks. Figure 7-19 demonstrates the grid's behavior after the line connecting bus 4 to bus 5 tripped in the presence of the $H-2/\infty$ controller. It is evident that our EV-based mitigation successfully brings the grid back to stability after such a singular event and eliminates all traces of the impact.

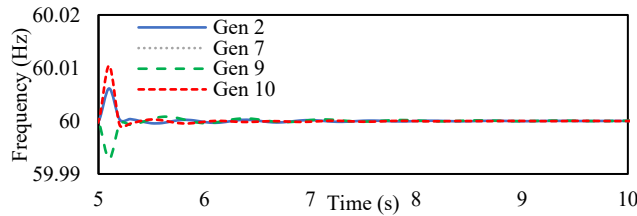


Figure 7-19: Grid frequency after line tripping line 4-5

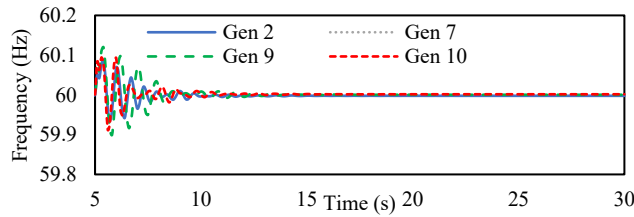


Figure 7-20: Grid frequency after Generator 1 tripping

Additionally, Figure 7-20 demonstrates the frequency behavior in the grid after tripping the generator connected at bus 39. This generator has an output of 1104 MW, which is the largest in our grid. In the absence of our proposed mitigation scheme, the frequency deviation surpasses 1 Hz and the generators start oscillating wildly leading to tripping. However, our proposed EV-based

H-2/ ∞ controller immediately limits the initial deviation to 0.1 Hz and then brings the frequency back to the nominal 60 Hz.

These 2 simulation results demonstrate the effectiveness of the proposed EV-based LA attack mitigation scheme against the singular events that are usually studied in the literature in the context of EV frequency support to the grid. However, such events are rare during the normal operation of a power grid. To avoid having the presented EV-based mixed H-2/ ∞ controller react to the normal frequency fluctuations corresponding to the random consumer behavior, we set a frequency deviation threshold of 0.03 Hz before the mitigation scheme is engaged. This threshold can be changed by the utility depending on their historic data which would indicate the maximum value of benign frequency fluctuations caused by the random user behavior.

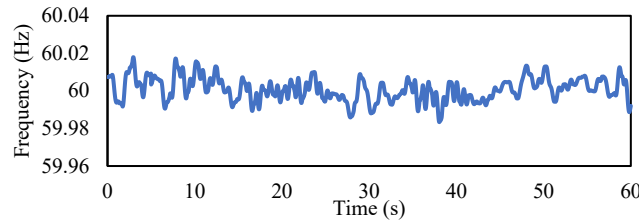


Figure 7-21: Grid frequency under normal random consumer behavior

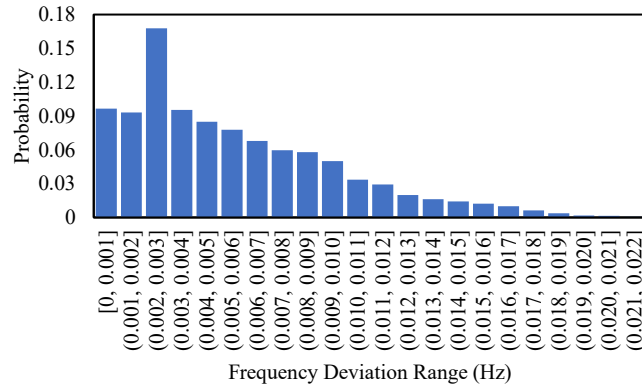


Figure 7-22: Frequency deviation probability during normal behavior

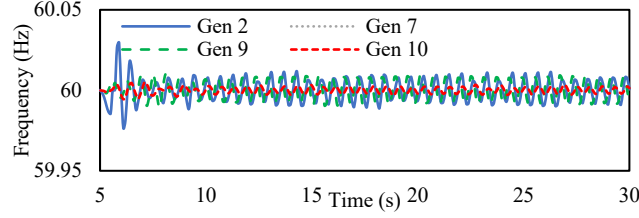


Figure 7-23: Grid frequency under attack 3 in the presence of a 0.03 Hz threshold

We simulated normal frequency fluctuations in our grid, using random load blocks that were added to all load buses. A sample of these simulated normal frequency fluctuations is presented in Figure 7-21. We simulated 3 weeks (21 days) of power grid behavior and collected the frequency readings. We then collected the value of the highest frequency deviation during each 1-minute window. A histogram representing the frequency deviation probability during normal behavior is presented in Figure 7-22. This histogram demonstrates that normal frequency fluctuation caused by consumer behavior does not exceed 0.022 Hz. Thus, our threshold for engaging the mitigation scheme was set at 0.03 Hz.

In the following, simulation, we repeat Attack 3, which was the most impactful attack, in the presence of the mixed H-2/ ∞ controller after setting its engagement threshold to 0.03 Hz. Figure 7-23 demonstrates the success of our mitigation strategy. The frequency rises to reach the 0.03 Hz threshold before the mitigation scheme is engaged and brings it back down to 0.01 Hz.

Additionally, our proposed scheme is superior to the EV-based frequency regulation schemes proposed in [81] - [83] since it is originally designed to deal with continuous persisting attacks especially the dynamic attack that adapts to the grid reaction. Such singular events resemble Attack 1, whose impact was eliminated completely. The work in [83] proposed a frequency regulation scheme for the small frequency fluctuations (<0.06 Hz) caused by the intermittency of renewable energy. Additionally, the presented scheme in [83] was optimized to handle sudden drops or spikes in renewable energy generation of 120 MW resembling the behavior of Attack 1. The presented methods in [81] [82] on the other hand are meant to address frequency fluctuations between 0.06 Hz and 0.07 Hz, caused by renewable energy intermittency, and reduce the frequency deviation to 0.05 Hz (29% reduction). In comparison, our EV-based LA attack mitigation scheme is designed to handle persistent static, switching, and dynamic attacks. Additionally, our proposed controller

is designed to mitigate the impact of attacks with much larger magnitudes than the events in [81] - [83] and reduce their impact by over 99% from the devastating range of 1.5 Hz to a normal 0.01 Hz range.

7.3 Stability and Performance Evaluation

In this section, we examine the performance of our EV-based mitigation when faced with real-life deployment obstacles.

7.3.1 Uncertainty and Controller Stability

In this subsection, we examine the stability of the proposed control strategy in the face of the uncertainty of the feedback EV defender load. By modeling this uncertainty into the design of the controller, the value of the matrix K_{def} changes to allow the mitigation scheme to perform well when facing these uncertainties. In case there is no uncertainty present, a carefully designed robust controller will achieve an extremely similar response to the original non-robust controller but will outperform it when uncertainty is added to the systems. Figure 7-24 presents the response of the worst-performing generator to Attack 3 in the presence of a random uncertainty of $\pm 5\%$ on each of the feedback EV inputs. Figure 7-24 demonstrates how the mixed robust controller performs better than a normal mixed controller when the feedback channel is not 100% certain.

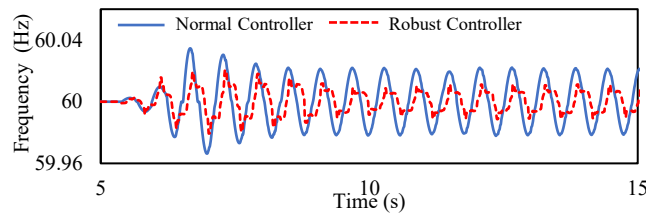


Figure 7-24: Generator frequency with normal and robust controllers

The three types of robust controllers were evaluated using MATLAB's "diskmargin" function to calculate their disk stability [152]. To this end, we consider the system states, x , as the object of our analysis for the sake of having a system with 30 inputs and 30 states.

Table 7-3 demonstrates the stability range of the system when all the inputs are varied independently with an uncertainty F_j presented (7.44). In (7.44) j is the index of the input/state and δ is a random complex number such that $|\delta| < 1$ represents the uncertainty in the channel gain and phase. Variable a is the multiplicative gain of the uncertainty and σ represents the skewness of F to shift the probability of the uncertainty in the positive or negative direction.

$$F_j = \frac{1 + a\{(1 - \sigma)/2\}\delta_j}{1 - a\{(1 + \sigma)/2\}\delta_j} \quad (7.44)$$

Table 7-3: Controller Stability Margin

Skew	$\sigma=-2$	$\sigma=-1$	$\sigma=0$	$\sigma=1$	$\sigma=2$
Controller	min/max	min/max	min/max	min/max	min/max
Robust H-2	0.01/1.50	0.01/2.00	0.18/5.56	0.53/8.34	0.67/9.08
Robust H- ∞	0.20/1.44	0.29/1.70	0.41/2.17	0.61/2.62	0.71/2.91
Robust Mixed H-2/ ∞	0.01/1.50	0.01/1.99	0.18/5.45	0.52/8.35	0.68/8.96

Table 7-3 demonstrates the range of uncertainty where our proposed mitigation robust controller remains stable in the presence of uncertainty. The uncertainty, δ , is a complex number to represent the uncertainty in both the magnitude and angle of the control signal. Uncertainty in magnitude represents the possibility of the control input being smaller or larger than the control signal due to the uncertainties discussed above. Uncertainty in phase represents the uncertainty added by a time delay in the feedback control channel due to communication channel delays. The skewness, σ , is used to study the stability of the controller when the uncertainty is biased in a given direction. This means that we consider the case in which the uncertainties can either increase or decrease the gain of the feedback control input, ΔPQ_{EV} . The actual value of the EVCS real and reactive power load/injections can be smaller than the calculated ΔPQ_{EV} in the case where attackers compromise some EVCSs or the case where the utility overestimates the number of EVCSs, the control signal is reaching. The actual value of the EVCS real and reactive power load/injections can be larger than the calculated ΔPQ_{EV} in case the utility underestimates the number of EVCSs the control signal is reaching especially if the clustering mechanism discussed above is used.

7.3.2 Smaller Defender Load

Another issue associated with the uncertainty of the feedback EV defender load is that the defender load might become smaller than the attack load. If the attacker successfully compromises enough EVs such that the total defender load is smaller than the total attack load, the defender would be able to partially mitigate the attack impact but not eliminate it. This assumption, however, would require an attacker with huge resources to compromise enough load and EVs as well as keep the EV compromise hidden from the utility. We repeat Attack 2 when the defender controls 25% less load than the attacker and the mitigation scheme successfully reduced the oscillations resulting from the attack to 0.25 Hz (75% reduction).

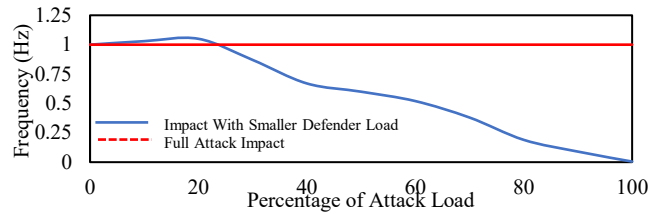


Figure 7-25: Maximum frequency deviation vs defender resources level

To demonstrate the impact of limiting the utility's resources below those of the attacker, Figure 7-25 presents the maximum frequency deviation achieved under Attack 2 when the utility EV load is capped at different levels. To this end, we use steps of 10% of the total attack load. We can conclude that even as we decrease the defender's resources, the attack impact is still reduced below its original value. It is only after the utility's EV load drops to 20% that the mitigation scheme stops having a positive impact.

Finally, we examine the possibility of an attacker gaining access to a large portion of EVCS (unsecured private EVCSs for instance [66]). However, the modeling of the uncertainty in the feedback load of the controller, $u = \Delta PQ_{EV}$, accounts for such scenario and the mitigation scheme remains successful as long as the attacker does not control a larger portion of the EVCSs than the utility. To put things into perspective, let us assume the attacker attempts to compromise several EVCS in tandem with the previous 800 MW attack. Based on the total (public and private) EVCS load curve in Figure 7-3 the average EVCS charging load is 2960 MW. Thus, the attacker is required to compromise 1080 MW of EVCS load in addition to the original 800 MW to start degrading the performance of the mitigation scheme. Under such a condition, the attacker has

compromised a total of 1880 MW while the defender still has access to 1880 MW of EV load. Even attackers knowledgeable of the presence of the mitigation scheme are required to compromise this much EVCS load to have an impact on the performance of our proposed EV-based mitigation. Beyond this point, the aggregate defender load starts becoming smaller than the aggregate attacker load following the behavior in Figure 7-25. However, we stress that this scenario is far-fetched and practically impossible. Such an assumption would require an attacker with enough resources to compromise 31% of the total load of the power grid, which is extremely implausible.

7.3.3 Effect of Communication Delay

In this subsection, we consider another aspect usually ignored in similar studies which is the communication and synchronization delay present during real deployment. To this end, we now simulate Attack 3 after adding a random Gaussian delay to each of the feedback signals between 0 and 10ms to examine the impact of the system incurring synchronization delay. The obtained generator frequency response is depicted in Figure 7-26. It is evident from this response that the mitigation scheme is still successful despite this delay in the communication channel. To quantify things in terms of controller success, the maximum and average frequency deviations were reduced to 0.026 Hz and 0.013 Hz respectively. This reduction is equivalent to eliminating 98.4% and 98.8% of the maximum and average frequency deviations caused by the LA attack respectively.

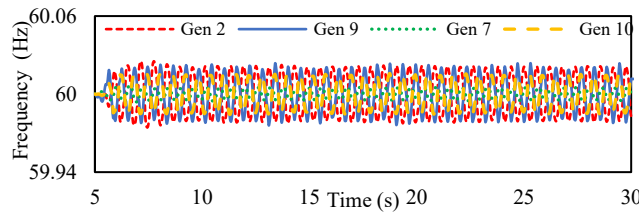


Figure 7-26: Generator frequency with controller feedback communication delay

Table 7-4 also serves to demonstrate the maximum frequency deviation caused by Attack 3 under the robust H-2, H- ∞ , and mixed sensitivity H-2/ ∞ control strategy. In this table, the delay is assumed equal in all the feedback channels. Table 7-4 demonstrates that the EV-based mitigation scheme is successful albeit with slightly reduced performance. This shows that the maximum possible 10ms synchronization delay has been effectively accounted for in the controller synthesis.

Table 7-4: Max Frequency Deviation vs Communication/Synchronization Delay

Delay (ms)	0	1	2	4	6	8	10
H-2	0.006	0.012	0.02	0.025	0.029	0.03	0.032
H- ∞	0.1	0.13	0.17	0.19	0.21	0.24	0.26
Mixed H-2/ ∞	0.01	0.04	0.07	0.1	0.11	0.12	0.13

7.3.4 Impact of Clustering

In this subsection, we briefly discuss the impact that the clustering suggested in Section 7.1 would have on the performance of the EV attack mitigation. To this end, we use the example that the utility clusters EVs into groups such that the expected participation is 10 EVs per cluster. To this end, we sample the feedback control signal and send a signal equal to a multiple of the power per cluster. Each cluster is assigned a load value equal to 10 EVs. With this clustering technique, Attack 2 is repeated and results in the frequency responses seen in Figure 7-27. It is evident that this technique reduces the effectiveness of the controller, but the achieved response is still within the acceptable range of normal frequency operation. The maximum and average frequency deviations were reduced by factors of 95.4% and 97.4% to reach 0.05 Hz and 0.019 Hz respectively.

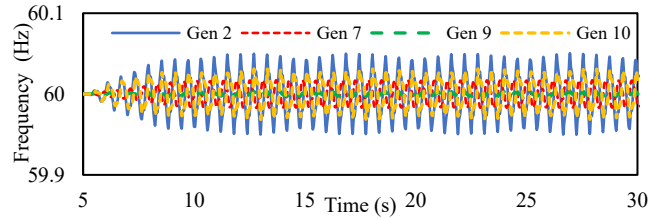


Figure 7-27: Generator frequency with controller EV load clustering

7.3.5 Impact of Grid Operating Point

Finally, we examine the impact of the grid's operating point on the success of the LA attack mitigation scheme. To this end, we scale the NE grid based on the NSW load profile [126]. The average load in the NSW grid is 6968 MW while the peak and lowest loads are 8214 and 5897 respectively. We repeated Case Study 4 on the scaled grids and observed that when using the

correct state-space matrices, the operating point has very little impact on the performance of our proposed mitigation scheme. This is to demonstrate that even when the dynamic behavior of the power grid changes, the mitigation scheme is still successful as long as the utility maintains updated and correct parameters of their grid in the calculation of the controller gain matrix.

Alternatively, the utility can model the grid's parameter uncertainty by modifying (7.19) and assigning a non-zero variable to ΔA in (7.20). Consequently, the uncertainty in matrix A of the state-space representation can be modeled using steps resembling (7.22) to (7.33) that were used to represent the uncertainty in the feedback loop and matrix B . However, as mentioned earlier, it is widely accepted to model the power grid as a state-space [140]- [142] and to use this state-space for controller design [91]- [144] while assuming the utility has complete and accurate knowledge of their own power grid parameters. Finally, in the farfetched case that a utility does not have an accurate state-space representation, they can follow the approach proposed in [191] to obtain an accurate state-space representation. This approach utilizes a system identification technique consisting of introducing a small probing signal and retrieving the grid's impulse response to create the state-space matrices using the Eigenvalue Realization Algorithm [192].

7.4 Chapter Concluding Remarks

In this chapter, we demonstrated how EVs can be modeled as a feedback loop controller used to stabilize the grid under LA attacks. Their power-electronics-based nature and their fast centralized communication infrastructure as well as their colocation with possible attack loads on all the grid's load busses, make them ideal for an attack mitigation scheme. The controller synthesis is based on the state-space model of the grid which is needed to design the feedback gain based on robust mixed H_2/H_∞ control. The mixed controller design incorporates the uncertainty in the feedback EV signal to achieve grid stability under static, switching, and dynamic attacks. The initial 1.5 Hz frequency deviation caused by an 800 MW attack was attenuated by our scheme below 0.01 Hz guaranteeing system stability. The controller was also successful under different operating conditions such as EV load uncertainty and communication delay. We also presented an EV clustering technique that can be used to preserve the privacy of home EVCSs. The performance of

the controller did vary slightly when clustering was implemented, but the result remained well within the normal frequency behavior of the grid.

Chapter Eight

Thesis Conclusion and Future Research Directions

The exponentially increasing number of EVs and the rapid adoption and deployment of the EV charging infrastructure have made it a significant element of the power grid. With governmental targets set to ban gasoline cars worldwide, EVs are expected to gain a more significant role in the power grid. As a result, securing this crucial ecosystem and understanding its possible impact on the power grid are of the utmost importance. To this end, this thesis is aimed at understanding the security posture of the EV ecosystem as well as understanding the impacts of EV-based LA attacks against power grid stability. Consequently, our first contribution was to examine the vulnerabilities of the different components of this new emerging ecosystem that allows attackers to gain control of the EVCS charging process to attack the grid. Additionally, we examine the special nature of the non-linear EV load that makes attacks through the EV charging process more impactful than similarly sized traditional loads. The second contribution contained in this thesis is the creation of a novel dynamic EV-based LA attack that accounts for the uncertainties in estimated grid parameters to guarantee the desired instability is achieved. To address the devastating impacts of such attacks, our third contribution is the creation of two distinct detection mechanisms. The first being a two-tiered detector tailored specifically to detect attacks by observing the charging behavior on the CMS and the individual EVCSs. The second detector was created from the perspective of the utility to detect all types of LA attacks. This novel detector relies on data preprocessing using the mathematical equations representing the physical grid followed by a FFNN that achieves near-perfect attack detection and is robust against data poisoning attacks. Finally, our last contribution is the design of a novel LA attack mitigation strategy that utilizes the EV charging load as its input and can completely eliminate the impact of all LA attacks.

Our future work in this direction includes the development of a sophisticated attack mitigation mechanism tailored specifically to address the attacks on the cyber layer of the EV ecosystem. Additionally, we acknowledge that the current number of EVs is not large enough to cause the impacts discussed in this chapter. However, EV numbers are growing at a rapid pace, and it is a matter of time before their numbers become sufficiently large to realize the discussion contained in this thesis. Another important direction we intend to pursue is performing penetration testing on EVCSs that are common to North America that do not provide a web-facing configuration/admin page.

The contributions contained within this thesis have all been published or submitted to top-tier venues summarized below:

- J1: “GridWatch: Robust Load-Altering Attack Detection and Localization Using a Physics-Assisted Feature Fusion Neural Network”. M. A. Sayed, K. Sareddine, Nathalie Wehbe, M. Arfaoui, R. Atallah, M. Debbabi, and C. Assi. Final writing stage. Submitted to IEEE Transactions on Smart Grid.
- J2: “Grid Chaos: An Uncertainty-Conscious Robust Dynamic EV Load-Altering Attack Strategy on Power Grid Stability”. M. A. Sayed, M. Ghafouri, R. Atallah, M. Debbabi, and C. Assi. Submitted to Applied Energy (Revised and awaiting second round of reviews).
- J3: “An Electric Vehicle Robust Mitigation Scheme Against Load Altering Attacks on Power Grids”. MA. Sayed, M. Ghafouri, R. Atallah, M. Debbabi, C. Assi. Applied Energy, 2023.
- J4: “Electric vehicle attack impact on power grid operation”, MA. Sayed, R. Atallah, C. Assi, M. Debbabi. International Journal of Electrical Power and Energy Systems, 2021.
- C1: “PEACE: Physics-Enabled Autoencoder Detection of Unknown Load-Altering Attacks in Smart Grids”. M. A. Sayed, Nathalie Wehbe, K. Sareddine, R. Atallah, C. Assi, and M. Debbabi. Final Writing Stage. (Submitted to IEEE Power and Energy Society General Meeting, 2024).
- C2: “A Hybrid Physics-Deep Learning Load-Altering Attack Detection and Localization Mechanism”. M. A. Sayed, Mohammad Amine Arfaoui, Ribal Atallah, Mourad Debbabi,

Chadi Assi. (IEEE) International Conference on Smart Grid and Renewable Energy (SGRE), 2024.

C3: “An Electric Vehicle Control Strategy to Mitigate Load Altering Attacks Against Power Grids”. MA. Sayed, M. Ghafouri, R. Atallah, M. Debbabi, C. Assi. IEEE International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), 2023.

C4: “Dynamic Load Altering EV Attacks Against Power Grid Frequency Control”, MA. Sayed, M. Ghafouri, M. Debbabi, C. Assi. IEEE Power and Energy Society General Meeting, 2022.

Throughout the Ph.D. the student has also collaborated on multiple projects and publications summarized below:

- 1) “Uncovering Covert Attacks on EV Charging Infrastructure: How OCPP Backend Vulnerabilities Could Compromise Your System,” K. Srieddine, M. A. Sayed, S. Torabi, R. Atallah, C. Assi, and M. Debbabi. ACM Asia Conference on Computer and Communications Security (Asia CCS), 2024.
- 2) “Edge-Based Detection and Localization of Adversarial Oscillatory Load Attacks Orchestrated by Compromised EV Charging Stations,” K. Srieddine, M. A. Sayed, S. Torabi, R. Atallah, C. Assi. International Journal of Electric Power and Energy Systems, 2023.
- 3) “A Data-Driven Framework for Improving Public EV Charging Infrastructure: Modeling and Forecasting,” N. Al-Dahabreh, M. A. Sayed, M. El-Hattab, K. Srieddine, R. Atallah, M. Khabbaz, C. Assi. IEEE Transactions on Intelligent Transportation Systems, 2023.
- 4) “EV Charging Infrastructure Discovery to Contextualize its Deployment Security,” K. Srieddine, M. A. Sayed R. Atallah, S. Torabi, C. Assi, J. Khoury, M. Safaei Pour, and E. Bou Harb. IEEE Transactions on Network and Service Management, 2023.
- 5) “Quality of Service Evaluation and Forecast for Infrastructure Resizing Based on Real-world Data,” R. Atallah, N. Al-Dahabreh, M. A. Sayed, M. El-Hattab, K. Srieddine, M. Khabbaz, C. Assi, (IEEE) International Conference on Wireless and Mobile Computing, Networking and Communications, 2023

- 6) “Investigating the Security of EV Charging Mobile Applications as an Attack Surface,” K. Sariaeddine, M. A. Sayed, S. Torabi, R. Atallah, and C. Assi, to Transactions on Cyber-Physical Systems, 2023.
- 7) “A Real-Time Co-simulation Testbed for EV Charging and Smart Grid Security,” K. Sariaeddine*, M. A. Sayed*, D. Jafarigiv, R. Atallah, M. Debbabi and C. Assi. IEEE Security & Privacy. (*equal authorship)
- 8) “Quality of Service Aware EV Charging Infrastructure Deployment Based on Real-world Data,” N. Al-Dahabreh, M. A. Sayed, M. Khabbaz, R. Atallah, C. Assi. Final implementation stage. (In progress)
- 9) “A Multi-Layered Real-time Monitoring Platform for Attack Detection in the Public EV Charging Ecosystem,” R. Reghunath, M. A. Sayed, K. Sariaeddine, R. Atallah, D. Jafarigiv, M. Kassouf, C. Assi. (In progress)

References

- [1] "Energy Production and Consumption," <https://ourworldindata.org/energy-production-consumption>.
- [2] "How The Smart Grid Promotes A Greener Future," <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Environmentalgroups.pdf>.
- [3] M.R. Rashed et al., "A survey on advanced metering infrastructure," *Int J Electr Power Energy Syst*, vol 63, pp. 473–484, 2014.
- [4] S. Che et al., "Cyber security of a power grid: state-of-the-art," *Int J Electr Power Energy Syst*, vol 99, pp 45–56, 2018.
- [5] "Gas shortages, price hikes reported amid Colonial Pipeline shutdown: CNBC After Hours," <https://www.cnbc.com/2021/05/11/gas-shortages-price-hikes-reported-amid-colonial-pipeline-shutdown.html>.
- [6] "The SolarWinds Body Count Now Includes NASA and the FAA," <https://www.wired.com/story/solarwinds-nasa-faa-robot-dog-fight-security-news/>.
- [7] "The inside story of the biggest hack in history," <https://money.cnn.com/2015/08/05/technology/aramco-hack/>.
- [8] "OPM hack's unprecedented haul: 1.1 million fingerprints," <https://money.cnn.com/2015/07/10/technology/opm-hack-fingerprints/?iid=EL>.
- [9] "The Real Story of Stuxnet," <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.
- [10] G. Liang et al., "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks.," *IEEE Trans Power Syst*, vol 32, no 4, pp 3317–8, 2017.
- [11] "Attacks on industrial control systems using ShadowPad," <https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/>.

- [12] "How 30 Lines of Code Blew Up a 27-Ton Generator," <https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/>.
- [13] "RedEcho, ShadowPad — how Chinese hackers may have accessed critical Indian computer systems," <https://theprint.in/theprint-essential/redecho-shadowpad-how-chinese-hackers-may-have-accessed-critical-indian-computer-systems/614523/>.
- [14] D. E. Sanger, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out," *The New York Times*, <https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html>.
- [15] "Chinese hackers targeted 7 Indian power hubs, govt says ops failed," *Hindustan Times*, <https://www.hindustantimes.com/india-news/chinese-hackers-targeted-7-indian-power-hubs-govt-says-ops-failed-101649356540330.html>.
- [16] S. Soltan et al., "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," *27th USENIX Security Symp*, pp. 15-32, 2018.
- [17] M. Antonakakis et al., "Understanding the Mirai botnet," *17th USENIX Security Symp*, pp 1093-1110, 2017.
- [18] A. Saber et al., "Plug-in Vehicles and Renewable Energy Sources for Cost and Emission Reductions," *IEEE Transactions on Industrial Electronics*, vol. 58, pp. 1229-1238, 2011.
- [19] IEA (2020), "Global EV Outlook 2020," *IEA, Paris*, <https://www.iea.org/reports/global-ev-outlook-2020>.
- [20] "The global electric vehicle market in 2020: statistics & forecasts," <https://www.virta.global/global-electric-vehicle-market>.
- [21] IEA (2022), "Global electric car sales have continued their strong growth in 2022 after breaking records last year," *IEA, Paris*, <https://www.iea.org/news/global-electric-car-sales-have-continued-their-strong-growth-in-2022-after-breaking-records-last-year>.
- [22] IEA (2023), "Global EV Outlook 2023, Electric car sales break new records with momentum expected to continue through 2023," *IEA Paris*.
- [23] "Global Plug-in Vehicle Sales Reached over 3,2 Million in 2020," <http://www.ev-volumes.com/>.
- [24] "Norway: Plug-In Car Electric Market Share Exceeded 79% In October 2020," <https://insideevs.com/news/452441/norway-plugin-car-sales-october-2020/>.

- [25] M. Holland, "EVs Take 90.6% Share In Norway — VW, Kia, Ford Debuts," <https://cleantechnica.com/2023/12/05/evs-take-90-6-share-in-norway/>, 2023.
- [26] "Electric car sales are on the rise – is coronavirus a turning point for the market?," <https://theconversation.com/electric-car-sales-are-on-the-rise-is-coronavirus-a-turning-point-for-the-market-144706>.
- [27] "Automotive Insights – Q2 2023 Canadian EV Information and Analysis," <https://www.spglobal.com/mobility/en/research-analysis/automotive-insights-q2-2023-canadian-ev-information-and-analys.html>, 2023.
- [28] "The shift to electric cars: Are we there yet?," <https://montrealgazette.com/news/local-news/the-shift-toelectric-cars-are-we-there-yet>.
- [29] "Quebec to ban sale of new gasoline-powered cars from 2035," <https://www.reuters.com/article/us-autos-canada-emissions-idUSKBN27W289>.
- [30] "Tesla, Uber join hands to create US lobbying group for electric vehicle industry," <https://auto.hindustantimes.com/auto/news/tesla-uber-join-hands-to-create-us-lobbying-group-for-electric-vehicle-industry-41605666844191.html>.
- [31] "The electric car industry now has its own lobbying group," <https://www.theverge.com/2020/11/17/21571747/zero-emissions-transportation-association-tesla-uber-rivian-lobby>.
- [32] "Russian EV Chargers Hacked, Screen Reads Glory To Ukraine," <https://www.dailymail.co.uk/news/article-10565697/Russian-electric-vehicle-chargers-hacked-display-message-supporting-Ukraine.html>.
- [33] "Isle of Wight: Council's electric vehicle chargers hacked to show porn site," <https://www.bbc.com/news/uk-england-hampshire-61006816>.
- [34] "A 19-year-old security researcher describes how he remotely hacked into over 25 Teslas," <https://www.businessinsider.com/teen-security-researcher-describes-how-he-hacked-into-25-teslas-2022-1>.
- [35] ScreenRant, "Hacked Electrify America Charger Exposes Major Cybersecurity Risk," <https://screenrant.com/electrify-america-hacked-charger-cybersecurity-risk/>.
- [36] K. Harnett et al., "DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging station Cybersecurity Report," Technical Report. John A. Volpe National Transportation Systems Center (US), 2018.

- [37] S. Acharya et al., "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," *IEEE Access*, vol 8, pp. 214434–214453, 2020.
- [38] G. Joos et al., "Design and simulation of a fast charging station for PHEV/EV batteries," *2010 IEEE Electric. Power and Energy Conf*, 2010.
- [39] Y. Kongjeen et al., "Estimation of the Quick Charging station for Electric Vehicles based on Location and Population Density Data," *Int J of Intell Engineering and Syst*, vol 11, pp 233–241, 2018.
- [40] Enel X, "Understanding the Different EV Charging Levels," <https://evcharging:enelx.com/news/blog/550-different-ev-charging-levels>, 2019.
- [41] OPEN CHARGE ALLIANCE, "Open Chargepoint Protocol".
- [42] "OCPP," The Mobility House.
- [43] "Open Charge Point Protocol 2.0," *Open Charge Alliance*, 2014.
- [44] OpenCharge Alliance, "OPEN CHARGE POINT PROTOCOL 2.0.1," <https://www.openchargealliance.org/protocols/ocpp-201/>.
- [45] "How Accurate Is Network Time Protocol (NTP)?," *TimeTools*, <https://timetoolsltd.com/ntp/ntp-timing-accuracy/>.
- [46] A. M. Foley et al., "State-of-the-art in electric vehicle charging infrastructure," *2010 IEEE Vehicle Power and Propulsion Conf, Lille*, pp 1-6, 2010.
- [47] S. Shafiq et al., "Reliability Evaluation of Composite Power Systems: Evaluating the Impact of Full and Plug-in Hybrid Electric Vehicles," *IEEE Access*, vol 8, pp 114305-114314, 2020.
- [48] J. Delgado et al., "Impacts of plug-in electric vehicles in the portuguese electrical grid," *Transportation Research Part D: Transport and Environment*, vol 62, pp 372–385, 2018.
- [49] H. Morais et al., "Evaluation of the electric vehicle impact in the power demand curve in a smart grid environment," *Energy Conversion and Management*, vol 82, pp 268–282, 2014.
- [50] L. P. Fernandez et al., "Assessment of the Impact of Plug-in Electric Vehicles on Distribution Networks," *IEEE Transactions on Power Systems*, vol 26, pp 206–213, 2011.
- [51] F. Sagstetter et al., "Security challenges in automotive hardware/software architecture design," *2013 Design, Automation & Test in Europe Conf & Exhibition*, pp 458-463, 2013.

- [52] M. Brandl et al., "Batteries and battery management systems for electric vehicles," *2012 Design, Automation & Test in Europe Conf & Exhibition*, pp. 971-976, 2012.
- [53] R. Baker et al., "Losing the Car Keys: Wireless PHYLayer Insecurity in EV Charging," *28th USENIX Security Symp*, pp. 407-424, 2019.
- [54] H. Margossian et al., "Partial grid false data injection attacks against state estimation," *Int J Electr Power Energy Syst*, vol. 110, pp 623-629, 2019.
- [55] B. Huang et al., "Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks," *28th USENIX Security Symp*, pp. 1115-1132, 2019.
- [56] K. Sariaeddine et al., "Investigating the Security of EV Charging Mobile Applications As an Attack Surface," *ACM Transactions on Cyber-Physical Systems*, 2023.
- [57] E. Hammad et al., "A Class of Switching Exploits Based on Inter-Area Oscillations," *IEEE Tran Smart Grid*, vol. 9, no. 5, pp. 4659-4668, 2018.
- [58] M.E. Kabir et al., "A Two-Stage Protection Method for Detection and Mitigation of "Coordinated EVSE Switching Attacks," *IEEE Trans Smart Grid*, vol 12 no 5, pp 4377–4388, 2021.
- [59] S. Liu et al., "A Framework for Modeling Cyber-Physical Switching Attacks in Smart Grid," *IEEE Transactions on Emerging Topics in Computing*, pp. 273-285, 2013.
- [60] M. A. Sayed et al., "Dynamic Load Altering EV Attacks Against Power Grid Frequency Control," *2022 IEEE PES General Meeting*, 2022.
- [61] S. Amini et al., "Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes," *IEEE Trans Smart Grid*, vol. 9, 2016.
- [62] S. Amini et al., "Dynamic load altering attacks in smart grid,," *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, pp. 1-5, 2015.
- [63] T. Shekari et al., "MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses," *1st USENIX Security Symposium (USENIX Security 22)*, pp. 3539-56, 2022.
- [64] A. H. Mohsenian-Rad et al., "Distributed Internet-Based Load Altering Attacks Against Smart Power Grids," *IEEE Transactions on Smart Grid*, vol. 2, pp. 667-674, 2011.
- [65] B. Li et al., "Cyber-Physical Attack Leveraging Subsynchronous Resonance," *11TH BULK POWER SYSTEMS DYNAMICS AND CONTROL SYMPOSIUM (IREP 2022)*, 2022.

- [66] M. A. Sayed et al., "Electric vehicle attack impact on power grid operation," *Int J Electr Power Energy Syst*, vol. 137, 2022.
- [67] S. Lakshminarayana et al., "Load-Altering Attacks Against Power Grids Under COVID-19 Low-Inertia Conditions," *IEEE Open Access Journal of Power and Energy*, vol. 9, pp. 226-240, 2022.
- [68] S. Acharya et al., "Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable," *IEEE Trans Smart Grid*, vol. 11, pp. 5099-5113, 2020.
- [69] M. Basnet et al., "Deep learning-based intrusion detection system for electric vehicle charging station," *2020 2nd Int Conf on Smart Power & Internet Energy Syst*, pp. 408-413, 2020.
- [70] R. M. Molina et al. , "On ransomware family attribution using pre-attack paranoia activities," *IEEE Transactions on Network and Service Management*, 2021.
- [71] M. Basnet et al., "Ransomware detection using deep learning in the scada system of electric vehicle charging station," *2021 IEEE PES ISGT - Latin America*, pp. 1-5, 2021.
- [72] D. Komanos et al., "A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles," *Array*, vol. 5, 2020.
- [73] A. e Sousa et al., "Load-altering attack detection on smart grid using functional observers," *International Journal of Critical Infrastructure Protection*, vol 37, 2022.
- [74] Q. Ma et al., "Dynamic load-altering attack detection based on adaptive fading Kalman filter in power systems," *Global Energy Interconnection*, vol 4, 2021.
- [75] Q. Su et al., "Observer-based detection and reconstruction of dynamic load altering attack in smart grid," *Journal of the Franklin Institute*, vol 358, 2021.
- [76] H. Jahangir, "A Deep-Learning-Based Solution for Securing the Power Grid Against Load Altering Threats by IoT-Enabled Devices," *IEEE INTERNET OF THINGS JOURNAL*, vol 10, 2023.
- [77] J. Wang et al., "Coordinated Electric Vehicle Charging With Reactive Power Support to Distribution Grids," *IEEE Trans Indust Informa*, vol 15, pp 54-63, 2019.
- [78] G. V. Krieking, "Peak shaving and cost minimization using model predictive control for uni- and bi-directional charging of electric vehicles," *Energy Reports*, vol 7, pp 8760-8771, 2021.

- [79] M. G. Vayá and G. Andersson, "Integrating renewable energy forecast uncertainty in smart-charging approaches for plug-in electric vehicles," *2013 IEEE Grenoble Conference, Grenoble*, pp 1-6, 2013.
- [80] S. Weckx and J. Driesen, "Load Balancing With EV Chargers and PV Inverters in Unbalanced Distribution Grids," *IEEE Trans Sust Energy*, vol 6, pp 635-643, 2015.
- [81] H. Liu et. al., "EV Dispatch Control for Supplementary Frequency Regulation Considering the Expectation of EV Owners," *IEEE Trans. on Smart Grids*, VOL. 9, pp. 3763-3772, 2018.
- [82] H. Liu et. al., "Vehicle-to-Grid Control for Supplementary Frequency Regulation Considering Charging Demands," *IEEE Trans. on Power Syst.*, vol. 30, pp. 3110-3119, 2015.
- [83] C. Mu et. al., "Hierarchically Adaptive Frequency Control for an EV-Integrated Smart Grid With Renewable Energy," *IEEE Trans. on Industrial Informatics*, Vol. 14, pp. 4254-4263, 2018.
- [84] K. Sun et al., "WAMS-Based HVDC Damping Control for Cyber Attack Defense," *IEEE TRANSACTIONS ON POWER SYSTEMS*, Vol. 38, 2023.
- [85] C. Wang et al., "Inference of compromised synchrophasor units within substation control networks," *IEEE Trans Smart Grid*, vol. 9, no. 6, pp. 5831-5842, 2017.
- [86] "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," *Mission Support Center Idaho National Laboratory*, 2016.
- [87] S. Park et al., "Exact Topology and Parameter Estimation in Distribution Grids with Minimal Observability," *2018 Power Syst Computation Conf (PSCC), Dublin, Ireland*, pp 1-6, 2018.
- [88] G. Cavraro et al., "Real-Time Identifiability of Power Distribution Network Topologies With Limited Monitoring," *IEEE Control Systems Letters*, vol 4, pp 325-330, 2020.
- [89] S. Taheri et al., "An MILP Approach for Distribution Grid Topology Identification using Inverter Probing," *2019 IEEE Milan PowerTech*, pp. 1-6, 2019.
- [90] G. Cavraro et al., "Inverter Probing for Power Distribution Network Topology Processing," *IEEE Transactions on Control of Network Syst*, vol 6, pp 980-992, 2019.
- [91] K. Moffat et al., "Unsupervised Impedance and Topology Estimation of Distribution Networks-Limitations and Tools," *IEEE Trans Smart Grid*, vol. 11, pp. 846-856, 2020.

- [92] A. Gandluru et al., "Joint Estimation of Operational Topology and Outages for Unbalanced Power Distribution Systems," *IEEE Transactions on Power Systems*, vol 35, pp 605-617, 2020.
- [93] D. Deka et al., "Topology Estimation Using Graphical Models in Multi-Phase Power Distribution Grids," *IEEE Trans on Power Syst*, vol 35, pp 1663-1673, 2020.
- [94] K. Moffat et al., "Real Time Effective Impedance Estimation for Power System State Estimation," *2020 IEEE PES Innovative Smart Grid Technologies Conf, Washington, DC, USA*, pp 1-5, 2020.
- [95] G. Cavraro et al., "Bus Clustering for Distribution Grid Topology Identification," *IEEE Trans on Smart Grid*, vol 11, pp 4080-4089, 2020.
- [96] "All Energy Infrastructure and Resources," <https://atlas.eia.gov/apps/all-energy-infrastructure-and-resources/explore>.
- [97] "ENTSO-E Transmission System Map," <https://www.entsoe.eu/data/map/>.
- [98] "New York Independent System Operator," <https://www.nyiso.com/real-time-dashboard>.
- [99] W. Wang et al., "Cybersecurity in the Smart Grid: Survey and challenges," *Computer Networks*, vol 57, pp 1344–1371, 2013.
- [100] Harold Booth, "Draft NISTIR 8138, Vulnerability Description Ontology (VDO)," 2016.
- [101] "Cyber assessment report of level 2 ac powered electric vehicle supply equipment," <https://avt.inl.gov/sites/default/files/pdf/reports/Level2EVSECyberReport.pdf>, 2018.
- [102] D. Skylar, "ChargePoint Home security research," *Technical Report. Kaspersky Lab Security Services*, 2018.
- [103] J. Schmutzler et al., "Evaluation of OCPP and IEC 61850 for smart charging electric vehicles," *13 World Electric Vehicle Symposium and Exhibition (EVS27), Barcelona*, pp 1-12, 2013.
- [104] J. Schmutzler et al., "Distributed energy resource management for electric vehicles using IEC 61850 and ISO/IEC 15118," *2012 IEEE Vehicle Power and Propulsion Conference, Seoul*, pp 1457-1462, 2012.
- [105] "ISO 15118-1:2013 road vehicles – vehicle to grid communication interface –part 1: general information and use-case definition," *ISO, Technical report*, 2013.

- [106] C. Alcaraz et al., "OCPP Protocol: Security Threats and Challenges," *IEEE Trans Smart Grid*, vol. 8, pp. 2452-2459, 2017.
- [107] "OWASP Top Ten," <https://owasp.org/www-project-top-ten/>.
- [108] P. Ferrara et al., "Static analysis for discovering IoT vulnerabilities," *Int J on Software Tools for Technology Transfer*, vol 23, pp 71-88, 2021.
- [109] T. Nasr et al., "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Computers and Security*, vol 112, 2022.
- [110] K. Srieddine et al., "Uncovering Covert Attacks on EV Charging Infrastructure: How," *19th ACM ASIA Conference on Computer and Communications Security (ACM Asia CCS)*, 2024.
- [111] K. Srieddine et al., "EV Charging Infrastructure Discovery to Contextualize its Deployment Security," *IEEE Trans on Network and Service Management*, Early Access, 2023.
- [112] V. Caliskan et al., "Analysis of three-phase rectifiers with constant-voltage loads," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol 50, pp. 1220-1225, 2003.
- [113] F. Chen et al., "Research on Harmonic Analysis and Harmonic Suppression Measures of Electric Vehicle Charging Station," *2019 IEEE 2nd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), Shenyang, China*, pp 71-75, 2019.
- [114] M. C. Kisacikoglu, "Reactive power operation analysis of a single-phase EV/PHEV bidirectional battery charger," *8th International Conference on Power Electronics - ECCE Asia, Jeju, Korea (South)*, pp 585-592, 2011.
- [115] T. A. Kneschke et al., "Distortion and power factor of nonlinear loads," *1999 IEEE PES Summer Meeting, Conf Proceedings, Edmonton, Alta. Canada*, vol 1 pp 457-462, 1999.
- [116] B. Singh et al., "A review of single-phase improved power quality AC-DC converters," *IEEE Transactions on Industrial Electronics*, vol 50, pp 962-981, 2003.
- [117] A. Cai et al., "Review on reactive power compensation of electric vehicle charging piles," *2019 22nd International Conference on Electrical Machines and Systems (ICEMS), Harbin, China*, pp 1-4, 2019.

- [118] N. Mohan et al, "Power Electronics Converters, Applications and Design," *John Wiley & Sons Inc.*, 3rd ed., 2003.
- [119] "Reactive Power Planning," *NERC System Analysis and Modeling Subcommittee (SAMS)*, 2017.
- [120] E. U. Soykan et al., "Disrupting the power grid via EV charging: The impact of the SMS Phishing attacks," *Sust Energy, Grids and Netw*, vol. 26, 2021.
- [121] J. Antoun et al, "A Detailed Security Assessment of the EV Charging Ecosystem," *IEEE Network*, vol 34, pp 200–207, 2020.
- [122] H. ElHussini et al., "A Tale of Two Entities Contextualizing Electric Vehicle Charging Stations Cyber-Fingerprint on the Power Grid," *ACM Trans on Internet of Things*, vol 2, pp 1-18, 2020.
- [123] "PlugShare," <https://www.plugshare.com/>.
- [124] Chargemap, "Chargemap - charging stations for electric cars," <https://chargemap.com/map>. [Online]. Available: <https://chargemap.com/map>.
- [125] "Alternative Fuels Data Center," https://afdc.energy.gov/data_download.
- [126] "Australian Energy Market Operator," <https://aemo.com.au/en>.
- [127] "Motor Vehicle Census, Australia," <https://www.abs.gov.au/statistics/industry/tourism-and-transport/motor-vehicle-census-australia>.
- [128] "Global EV Outlook 2022," *IEA 2022*, <https://www.iea.org/reports/global-ev-outlook-2022>.
- [129] T. Ma et al., "Multistep electric vehicle charging station occupancy prediction using hybrid LSTM neural networks," *Energy*, 2022.
- [130] O. G. M. Khan et al., "Impact of Electric Vehicles Botnets on the Power Grid," *2019 IEEE Electr Power and Energy Conf*, pp. 1-5, 2019.
- [131] J. D. Glover et al., "Power System Analysis and Design," *Stamford, CT: Cengage Learning*, 5th ed. 2012.
- [132] "PowerWorld," PowerWorld Simulator," <https://www.powerworld.com/>.
- [133] IEEE PES Task Force on Benchmark Systems for Stability Controls, "Benchmark Systems for Small-Signal Stability Analysis and Control".

- [134] X. Liu et al., "Masking Transmission Line Outages via False Data Injection Attacks," *IEEE Trans on Information Forensics and Security*, vol 11, pp 1592-1602, 2016.
- [135] PlugShare, "Tesla Supercharger Map," <https://www.plugshare.com/map/supercharger>.
- [136] ChargePoint, "World's Largest EV Charging Network Coming to Your Garage," <https://www.chargepoint.com/about/news/worlds-largest-ev-charging-network-coming-your-garage#:~:text=EV%20infrastructure%20needs.%E2%80%9D-,About%20ChargePoint,than%2020%2C000%20charging%20locations..>
- [137] Electrify America, "Find Charging Fast," <https://www.electrifyamerica.com/>.
- [138] Electrify Canada, "Find charging fast," <https://www.electrify-canada.ca/>.
- [139] S. Huang et al., "Vehicle-to-grid workplace discharging economics as a function of driving distance and type of electric vehicle," *Sustainable Energy, Grids and Networks*, vol. 31, 2022.
- [140] C. A. Cañizares et al., "Applications of optimization to voltage collapse analysis.," *IEEE-PES Summer Meeting*, San Diego, USA, vol. 26, 1998..
- [141] C. Rajagopalan et al., "Dynamic aspects of voltage/power characteristics," *EEE Transactions on Power Systems*, vol 7, 1992.
- [142] P Kundur, "Power System Stability and Control," *McGraw-Hill*, 1994.
- [143] X. Gao et al., "Stability Analysis of Grid-Following and Grid-Forming Converters Based on State-Space Model," *2022 International Power Electronics Conference*, Himeji, Japan, 2022, pp. 422-428.
- [144] L. S. Barros et. al, "Matrix Method to Linearization and State Space Representation of Power Systems Containing Doubly Fed Induction Machines Operating as Wind Generators," *2006 IEEE/PES Transmission & Distribution Conference and Exposition: Latin America*, Caracas, Venezuela, 2006, pp. 1-6.
- [145] M. A. Tabrizi et al., "Power system damping analysis on large power system networks: An energy case study," *2017 IEEE PES General Meeting*, pp. 1–5, 2017.
- [146] L. Fan et al., "Time-Domain Measurements-Based DQ-Frame Admittance Model Identification of Inverter-Based Resources," *IEEE Trans. on Power Systems*, vol. 36, no. 3, pp. 2211-2221, 2021.

- [147] J. N. Juang et al., "An Eigensystem realization algorithm for modal parameter identification and model reduction," *J. Guid., Control Dyn.*, vol. 8, no. 5, pp. 620–627, 1985.
- [148] F. Wilches-Bernal, "Damping of Inter-Area Oscillations via Modulation of Aggregated Loads," *IEEE Trans Power Syst*, vol 35, no 3, pp 2024-2036, 2020.
- [149] G. Duan and H. Yu, *LMIs in Control Systems: Analysis, Design and Applications*, CRC Press, 2013.
- [150] S. K. Pandey et al., "Full order observer based load frequency control of Single Area Power System," *2020 12th Int Conf on Comput Intell and Commun Netw*, pp. 239-242, 2020.
- [151] "New England IEEE 39-Bus System," <https://electricgrids.engr.tamu.edu/electric-grid-test-cases/new-england-ieee-39-bus-system>.
- [152] D. Gu et al., *Robust Control Design with MATLAB*, Advanced Textbooks in Control and Signal Processing, Springer London, 2014.
- [153] A. Perlman, "The Growing Role of Machine Learning in Cybersecurity," <https://www.securityroundtable.org/the-growing-role-of-machine-learning-in-cybersecurity/>.
- [154] A. Deshmukh et al., "Debunking the Myths. How Machine Learning (ML) Benefits Cyber Security," <https://www.securityhq.com/blog/debunking-the-myths-how-machine-learning-ml-benefits-cyber-security/>.
- [155] V. H. Nguyen et al., "Self-updating machine learning system for building load forecasting - method, implementation and case-study on COVID-19 impact," *Sustainable Energy, Grids and Networks*, vol 32, 2022.
- [156] E. Mocanu et al., "Energy disaggregation for real-time building flexibility detection," *2016 IEEE PES General Meeting*, 2016.
- [157] A. Et-taleby , "A combined convolutional neural network model and support vector machine technique for fault detection and classification based on electroluminescence images of photovoltaic modules," *Sustainable Energy, Grids and Networks*, vol 32, 2022.
- [158] Z. S. Warraich et al., "Early detection of cyber-physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids," *Accepted in Sustainable Energy, Grids and Networks*, 2023.

- [159] A. Zappone et al., "Wireless networks design in the era of deep learning: Model-based, AI-based, or both?," *IEEE Trans. on Commun.*, vol. 67, pp. 7331–7376, 2019.
- [160] K. Srieddine et al., " Edge-Based Detection and Localization of Adversarial Oscillatory Load Attacks Orchestrated By Compromised EV Charging Stations," *arXiv preprint arXiv:2302.12890*, 2023.
- [161] builtin, "An Introduction to the ReLU Activation Function," <https://builtin.com/machine-learning/relu-activation-function>.
- [162] baeldung, "How ReLU and Dropout Layers Work in CNNs," <https://www.baeldung.com/cs/ml-relu-dropout-layers>.
- [163] P. Solai, "Convolutions and Backpropagations," <https://pavisj.medium.com/convolutions-and-backpropagations-46026a8f5d2c>.
- [164] K. Srieddine et al., "A Real-Time Co-simulation Testbed for EV Charging and Smart Grid Security," *Accepted in: IEEE Security and Privacy*, 2023, <https://arxiv.org/abs/2302.12781>.
- [165] R. Mantovani et al., "Effectiveness of random search in svm hyper-parameter tuning," *2015 International Joint Conference on Neural Networks*, 2015, pp1-8.
- [166] C. Wang et al., "Inference of compromised synchrophasor units within substation control networks," *IEEE Trans Smart Grid*, vol. 9, no. 6, pp. 5831-5842, 2017.
- [167] Symantec, "Western energy sector targeted by sophisticated attack group," *Symantec Enterprise Blogs*, 2020.
- [168] F. Bellizio et al., "Verifying Machine Learning conclusions for securing Low Inertia systems," *Sustainable Energy, Grids and Networks*, vol. 30, 2022.
- [169] S. Jain , "An Overview of Regularization Techniques in Deep Learning (with Python code)," *Analytics Vidhya*, <https://www.analyticsvidhya.com/blog/2018/04/fundamentals-deep-learning-regularization-techniques/>.
- [170] S. Miller et al., "White Gaussian Noise Process," *Handbook of Statistics*, 2019.
- [171] C. Y. Chuang et al., "Study of Training Patterns for Employing Deep Neural Networks in Optical Communication Systems," *2018 European Conf on Optical Commun*, pp. 1-3, 2018.

- [172] N. Wehbe et al., "5GShield: HTTP/2 Anomaly Detection in 5G Service-Based Architecture," *2023 IFIP Networking Conference (IFIP Networking), Barcelona, Spain, 2023*.
- [173] J. Li et al., "Dynamic load altering attack detection for cyber physical power systems via sliding mode observer," *International Journal of Electrical Power and Energy Systems*, vol. 153, 2023.
- [174] J. Li et al., "Dynamic load altering attack detection in smart grid based on multiple fading factor adaptive Kalman Filter," *Electric Power Systems Research*, vol. 225, 2023.
- [175] F. A. Yerlikaya, "Data poisoning attacks against machine learning algorithms," *Expert Systems With Applications*, vol. 208, 2022.
- [176] K. Aryal, "Analysis of Label-Flip Poisoning Attack on Machine Learning Based Malware Detector," *2022 IEEE International Conference on Big Data (Big Data)*, 2022.
- [177] R. Tang et al., "An Embarrassingly Simple Approach for Trojan Attack in Deep Neural Networks," *KDD '20: Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2020.
- [178] S. Ghahremani et al., "A Novel Semi-Supervised Adversarially Learned Meta-Classifer for Detecting Neural Trojan Attacks," *IEEE Access*, vol. 11, 2023.
- [179] L. Verde et al., "Exploring the Impact of Data Poisoning Attacks on Machine Learning Model Reliability," *25th International Conference on Knowledge-Based and Intelligent Information & Engineering*, 2021.
- [180] C. Zhang et al., "Clean-label poisoning attack with perturbation causing dominant features," *Information Sciences*, vol. 644, 2023.
- [181] North American Electric Reliability Corporation (NERC), "Balancing and Frequency Control Reference Document," 2021.
- [182] M. Paolone et. al., "Fundamentals of Power Systems Modelling in the Presence of Converter-Interfaced Generation," *21st Power Systems Computation Conference*, 2020.
- [183] P. Lico et al., "Phase balancing by means of electric vehicles single-phase connection shifting in a low voltage Danish grid," *2015 50th International Universities Power Engineering Conference (UPEC)*, Stoke on Trent, UK, 2015, pp. 1-5.
- [184] X. Yang et al., "Robust H_∞ control for a class of uncertain mechanical systems," *Int J of Control*, vol 83, 2010.

- [185] P. Shukla et al., "A Study of H Infinity and H2 Synthesis for Active Vibration Control," *IFAC-PapersOnLine*, vol 49, 2016.
- [186] M. Chilali et al., "Robust pole placement in lmi regions," *IEEE Trans on Automat Contr*, vol 44, 1999.
- [187] R. Telang et al., "Electric vehicles and the charging infrastructure: a new mindset?," <https://www.pwc.com/us/en/industries/industrial-products/library/electric-vehicles-charging-infrastructure.html>.
- [188] "Hilo smart home," <https://www.hydroquebec.com/residential/energy-wise/saving-during-peak-periods/hilo-smart-home-service.html>.
- [189] US Department of Energy, Alternative Fuels Data Center, "Electric Vehicle Infrastructure Projection Tool (EVI-Pro) Lite," <https://afdc.energy.gov/evi-pro-lite/>.
- [190] Circuit Electrique, "Cost of Charging," <https://lecircuitelectrique.com/en/cost/>.
- [191] F. Wilches-Bernal, "Damping of Inter-Area Oscillations via Modulation of Aggregated Loads," *IEEE Trans Power Syst*, vol 35, pp 2024-2036, 2020.
- [192] J. N. Juang et. al., "Eigensystem realization algorithm for modal parameter identification and model reduction," *Guid., Control, Dyn.*, vol. 8, pp. 620–627, 1985.